aws

Benutzerhandbuch

Amazon Elastic Compute Cloud

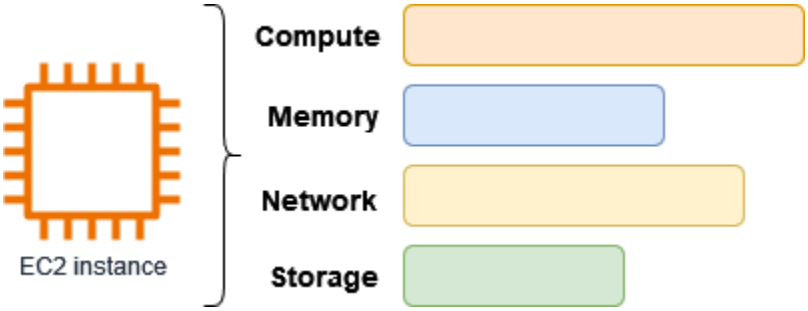
Amazon Elastic Compute Cloud: Benutzerhandbuch

Table of Contents

Was ist Amazon EC2?

Amazon Elastic Compute Cloud (Amazon EC2) bietet bedarfsbasiert skalierbare Rechenkapazität in der Amazon Web Services Cloud (AWS Cloud). Mit Amazon EC2 reduzieren Sie die Hardwarekosten, so dass Sie Anwendungen schneller entwickeln und bereitstellen können. 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. Sie können Kapazität hinzufügen (skalieren), um rechenintensive Aufgaben wie monatliche oder jährliche Prozesse oder Spitzen im Website-Datenverkehr zu bewältigen. Wenn die Nutzung abnimmt, können Sie die Kapazität wieder reduzieren (herunterskalieren).

Eine EC2-Instance ist ein virtueller Server in der AWS Cloud. Wenn Sie eine EC2-Instance starten, bestimmt der Instance-Typ, den Sie angeben, die Hardware, die für Ihre Instance verfügbar ist. Jeder Instance-Typ bietet ein anderes Gleichgewicht zwischen Rechen-, Arbeitsspeicher-, Netzwerk- und Speicherressourcen. Weitere Informationen finden Sie im Amazon EC2 Instance Types Guide.



Features von Amazon EC2

Amazon EC2 bietet die folgenden allgemeinen Features:

Instances

Virtuelle Server.

Amazon Machine Images (AMIs)

Vorkonfigurierte Vorlagen für Ihre Instances, die die Komponenten enthalten, die Sie für Ihren Server benötigen (einschließlich des Betriebssystems und zusätzlicher Software).

Instance-Typen

Verschiedene Konfigurationen von CPU, Arbeitsspeicher, Speicher, Netzwerkkapazität und Grafikhardware für Ihre Instances.

Amazon-EBS-Volumes

Persistente Speicher-Volumes für Ihre Daten mit Amazon Elastic Block Store (Amazon EBS).

Instance-Speicher-Volumes

Speicher-Volumes für temporäre Daten, die gelöscht werden, wenn Sie Ihre Instance anhalten, in den Ruhezustand versetzen oder beenden.

Schlüsselpaare

Sichere Anmeldeinformationen für Ihre Instances. AWS speichert den öffentlichen Schlüssel und Sie speichern den privaten Schlüssel an einem sicheren Ort.

Sicherheitsgruppen

Eine virtuelle Firewall, mit der Sie die Protokolle, Ports und Quell-IP-Bereiche festlegen können, die Ihre Instances erreichen können, sowie die Ziel-IP-Bereiche, mit denen sich Ihre Instances verbinden können.

Amazon EC2 unterstützt die Verarbeitung, Speicherung und Übertragung von Kreditkartendaten durch einen Händler oder Dienstanbieter. Außerdem wurde seine Konformität mit dem Payment Card Industry (PCI) Data Security Standard (DSS) bestätigt. Weitere Informationen zu PCI DSS, einschließlich der Möglichkeit, eine Kopie des AWS PCI Compliance Package anzufordern, finden Sie unter PCI DSS Level 1.

Zugehörige Services

Services zur Verwendung mit Amazon EC2

Sie können andere AWS-Services mit den Instances verwenden, die Sie mit Amazon EC2 bereitstellen.

Amazon EC2 Auto Scaling

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

AWS Backup

Automatisieren Sie die Sicherung Ihrer Amazon-EC2-Instances und der ihnen angefügten Amazon-EBS-Volumes.

Amazon CloudWatch

Überwachen Sie Ihre Instances und Amazon-EBS-Volumes.

Elastic Load Balancing

Verteilen Sie eingehenden Anwendungsdatenverkehr automatisch auf mehrere Instances.

Amazon GuardDuty

Erkennen Sie die potenziell unbefugte oder schädliche Nutzung Ihrer EC2-Instances.

EC2 Image Builder

Automatisieren Sie die Erstellung, Verwaltung und Bereitstellung von maßgeschneiderten, sicheren und up-to-date Server-Images.

AWS Launch Wizard

Größe, Konfiguration und Bereitstellung von AWS Ressourcen für Anwendungen von Drittanbietern, ohne einzelne AWS Ressourcen manuell identifizieren und bereitstellen zu müssen.

AWS Systems Manager

Mit dieser sicheren end-to-end Verwaltungslösung können Sie Operationen in großem Umfang auf EC2-Instances durchführen.

Zusätzliche Rechendienste

Sie können Instances mit einem anderen AWS Rechenservice starten, anstatt Amazon EC2 zu verwenden.

Amazon Lightsail

Erstellen Sie Websites oder Webanwendungen mit Amazon Lightsail, einer Cloud-Plattform, die die Ressourcen bereitstellt, die Sie für die schnelle Bereitstellung Ihres Projekts benötigen, und das zu einem niedrigen, vorhersehbaren monatlichen Preis. Einen Vergleich von Amazon EC2 und Lightsail finden Sie unter Amazon Lightsail oder Amazon EC2.

Amazon Elastic Container Service (Amazon ECS)

Nehmen Sie die Bereitstellung, Verwaltung und Skalierung von containerisierten Anwendungen in einem Cluster von EC2-Instances vor. Weitere Informationen finden Sie unter Einen Container-Service auswählen. AWS

Amazon Elastic Kubernetes Service (Amazon EKS)

Führen Sie Ihre Kubernetes-Anwendungen in AWS aus. Weitere Informationen finden Sie unter Einen AWS Container-Service auswählen.

Zugriff auf Amazon EC2

Sie können Ihre Amazon-EC2-Instances über die folgenden Schnittstellen erstellen und verwalten:

Amazon EC2-Konsole

Eine einfache Weboberfläche zum Erstellen und Verwalten von Amazon-EC2-Instances und -Ressourcen. Wenn Sie sich für ein AWS Konto angemeldet haben, können Sie auf die Amazon EC2 EC2-Konsole zugreifen, indem Sie sich bei der anmelden AWS Management Console und auf der Konsolen-Startseite EC2 auswählen.

AWS Command Line Interface

Ermöglicht Ihnen die Interaktion mit AWS Diensten mithilfe von Befehlen in Ihrer Befehlszeilen-Shell. Es wird auf Windows, Mac und Linux unterstützt. Weitere Informationen zur AWS CLI finden Sie im Benutzerhandbuch zu AWS Command Line Interface. Die Amazon-EC2-Befehle finden Sie in der AWS CLI -Befehlsreferenz.

AWS CloudFormation

Amazon EC2 unterstützt das Erstellen von Ressourcen mit AWS CloudFormation. Sie erstellen eine Vorlage im JSON- oder YAML-Format, die Ihre AWS Ressourcen beschreibt und diese Ressourcen für Sie AWS CloudFormation bereitstellt und konfiguriert. Sie können Ihre CloudFormation Vorlagen wiederverwenden, um dieselben Ressourcen mehrfach bereitzustellen, sei es in derselben Region und demselben Konto oder in mehreren Regionen und Konten. Weitere Informationen zu unterstützten Ressourcentypen und -eigenschaften für Amazon EC2 finden Sie in der EC2-Ressourcentypreferenz im AWS CloudFormation -Benutzerhandbuch.

AWS SDKs

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

AWS Tools for PowerShell

Eine Reihe von PowerShell Modulen, die auf den Funktionen basieren, die von der bereitgestellt werden. AWS SDK for .NET Mit den Tools für PowerShell können Sie über die PowerShell Befehlszeile Skripts für Operationen auf Ihren AWS Ressourcen erstellen. Informationen zu den ersten Schritten finden Sie im AWS Tools for Windows PowerShell -Benutzerhandbuch. Die Cmdlets für Amazon EC2 finden Sie in der AWS Tools for PowerShell -Cmdlet-Referenz.

Abfrage-API

Amazon EC2 stellt eine Abfrage-API zur Verfügung. Bei diesen Abfragen handelt es sich um HTTP- oder HTTPS-Abfragen, bei denen das HTTP-Verb GET oder POST sowie der Abfrageparameter verwendet wir `Action`. Weitere Informationen zu den API-Aktionen für Amazon EC2 finden Sie unter Aktionen im Amazon EC2 API Reference.

Preise für Amazon EC2

Amazon EC2 bietet die folgenden Preisoptionen:

Kostenloses Kontingent

Sie können kostenlos mit Amazon EC2 beginnen. Informationen zu den Optionen des kostenlosen Kontingents finden Sie unter Kostenloses AWS -Kontingent.

On-Demand Instances

Bezahlen Sie für die Instances, die Sie nutzen, nach der Sekunde, mit einem Minimum von 60 Sekunden, ohne langfristige Verpflichtungen oder Vorauszahlungen.

Savings Plans

Sie können die Amazon EC2-Kosten reduzieren, indem Sie sich auf eine konsistente Nutzung (in USD/h) für eine Laufzeit von ein oder drei Jahren festlegen.

Reserved Instances

Sie können die Amazon EC2-Kosten reduzieren, indem Sie sich auf eine konsistente Instance-Konfiguration (einschließlich Instance-Typ und Region) für eine Laufzeit von ein oder drei Jahren festlegen.

Spot Instances

Sie können ungenutzte EC2-Instances anfordern, wodurch sich die Amazon EC2-Kosten erheblich verringern lassen.

Dedicated Hosts

Senken Sie die Kosten, indem Sie einen physischen EC2-Server verwenden, der ausschließlich für Sie bestimmt ist, entweder bedarfsbasiert oder im Rahmen eines Savings Plans. Sie können Ihre vorhandenen servergebundenen Softwarelizenzen verwenden und erhalten Unterstützung bei der Erfüllung der Compliance-Anforderungen.

On-Demand Capacity Reservations

Reservieren Sie Rechenkapazität für Ihre EC2-Instances in einer bestimmten Availability Zone für einen beliebigen Zeitraum.

Sekundengenaue Abrechnung

Die Kosten für ungenutzte Minuten und Sekunden werden von Ihrer Rechnung gestrichen.

Eine vollständige Liste der Gebühren und Preise für Amazon EC2 und weitere Informationen zu den Kaufmodellen finden Sie unter Amazon EC2 – Preise.

Kostenvoranschläge, Abrechnung und Kostenoptimierung

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

Verwenden Sie den AWS Modernization Calculator for Microsoft Workloads, um die Kosten für die Umstellung von Microsoft-Workloads auf eine moderne Architektur abzuschätzen, die Open Source- und Cloud-native Dienste verwendet AWS, die auf bereitgestellt werden.

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

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

Informationen zur Berechnung der Kosten einer bereitgestellten Beispielumgebung finden Sie im Cloud Economics Center. Denken Sie bei der Berechnung der Kosten einer bereitgestellten Umgebung daran, Nebenkosten wie Snapshot-Speicher für EBS-Volumes einzubeziehen.

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

Sie können AWS Cost Explorer es verwenden, um die Kosten und die Nutzung Ihrer EC2-Instances zu analysieren. Sie können Daten der letzten 13 Monate einsehen und prognostizieren, wie viel Sie in den nächsten 12 Monaten voraussichtlich ausgeben werden. Weitere Informationen finden Sie unter Analysieren Ihrer Kosten mit AWS Cost Explorer im AWS Cost Management Benutzerhandbuch.

Ressourcen

- Funktionen von Amazon EC2
- AWS Re:POST
- AWS Skill Builder
- AWS Support
- Praktische Tutorials
- Webhosting
- Windows an AWS

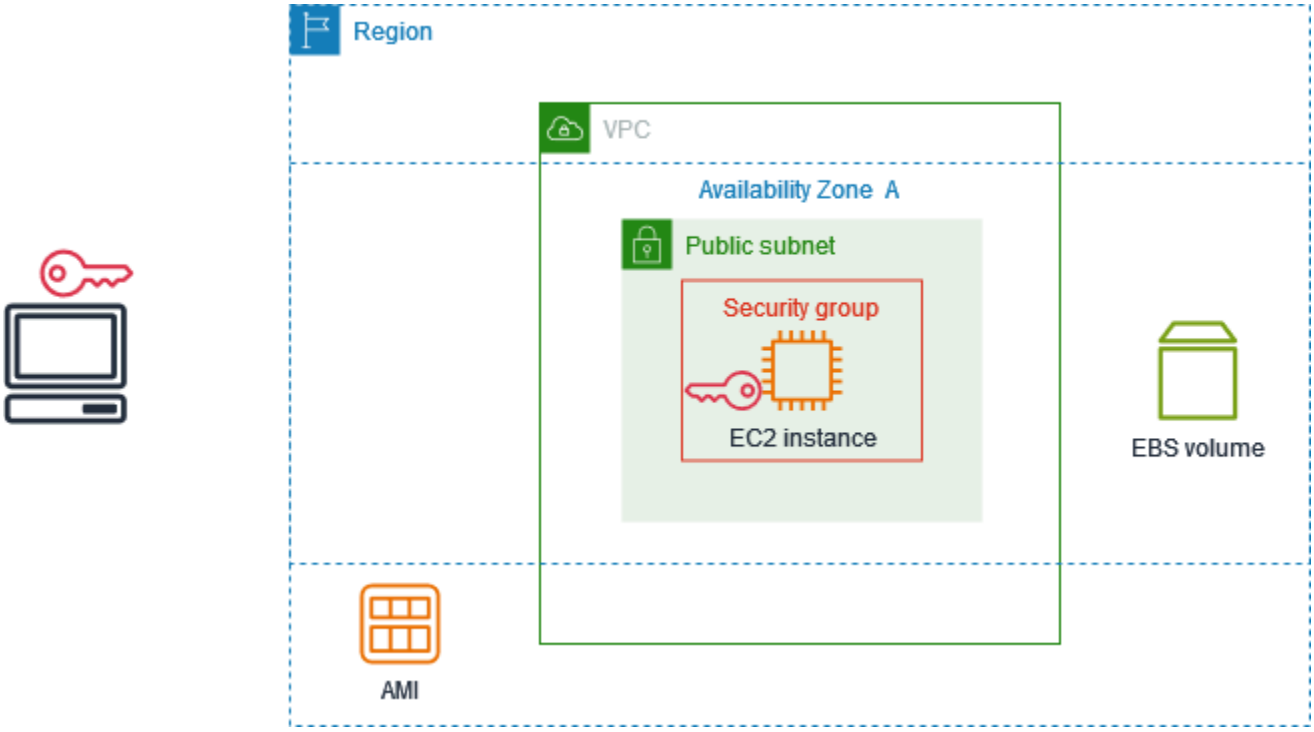
Erste Schritte mit Amazon EC2

Verwenden Sie dieses Tutorial, um mit Amazon Elastic Compute Cloud (Amazon EC2) zu beginnen. Sie erfahren, wie Sie eine EC2-Instance starten und eine Verbindung zu ihr herstellen. Eine Instanz ist ein virtueller Server in der AWS Cloud. Mit Amazon EC2 können Sie das Betriebssystem und die Anwendungen Ihrer Instance einrichten und konfigurieren.

Übersicht

Das folgende Diagramm zeigt die wichtigsten Komponenten, die Sie in diesem Tutorial verwenden werden:

- Ein Bild — Eine Vorlage, die die Software enthält, die auf Ihrer Instance ausgeführt werden soll, z. B. das Betriebssystem.
- Ein key pair — Eine Reihe von Sicherheitsanmeldedaten, mit denen Sie Ihre Identität nachweisen, wenn Sie eine Verbindung zu Ihrer Instance herstellen. Der öffentliche Schlüssel befindet sich auf Ihrer Instance und der private Schlüssel auf Ihrem Computer.
- Ein Netzwerk — Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk, das Ihrem AWS-Konto gewidmet ist. Um Ihnen den Einstieg zu erleichtern, verfügt Ihr Konto über eine Standard-VPC in jeder Availability Zone AWS-Region, und jede Standard-VPC hat ein Standardsubnetz in jeder Availability Zone.
- Eine Sicherheitsgruppe — Fungiert als virtuelle Firewall zur Steuerung des ein- und ausgehenden Datenverkehrs.
- Ein EBS-Volume — Wir benötigen ein Root-Volume für das Image. Sie können optional Datenvolumes hinzufügen.



Kosten für dieses Tutorial

Wenn Sie sich für registrieren AWS, können Sie mit Amazon EC2 beginnen, indem Sie den Kostenloses AWS-Kontingent. Wenn Sie Ihr Abonnement vor AWS-Konto weniger als 12 Monaten erstellt haben und die Vorteile des kostenlosen Kontingents für Amazon EC2 noch nicht überschritten haben, kostet es Sie nichts, dieses Tutorial abzuschließen, da wir Ihnen bei der Auswahl von Optionen helfen, die unter die Vorteile des kostenlosen Kontingents fallen. Andernfalls fallen ab dem Start der Instance so lange die standardmäßigen Amazon EC2-Nutzungsgebühren an, bis Sie die Instance beenden (die letzte Aufgabe dieses Tutorials). Dies gilt auch, wenn Sie sie nicht nutzen.

Anweisungen, mit denen Sie feststellen können, ob Sie für das kostenlose Kontingent in Frage kommen, finden Sie unterthe section called “Ihre Nutzung des kostenlosen Kontingents nachverfolgen”.

Aufgaben

- Schritt 1: Starten einer Instance
- Schritt 2: Verbindung mit der Instance herstellen
- Schritt 3: Bereinigen Ihrer Instance
- Nächste Schritte

Schritt 1: Starten einer Instance

Sie können eine EC2-Instance AWS Management Console wie im folgenden Verfahren beschrieben starten. Dieses Tutorial soll Ihnen helfen, Ihre erste Instance im Rahmen der Vorteile des kostenlosen Kontingents schnell zu starten. Daher werden nicht alle möglichen Optionen behandelt.

So starten Sie eine Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. In der Navigationsleiste oben auf dem Bildschirm zeigen wir die aktuelle Version an AWS-Region — zum Beispiel Ohio. Sie können die ausgewählte Region verwenden oder optional eine Region auswählen, die Ihnen näher liegt.
3. Wählen Sie im Dashboard der EC2-Konsole im Bereich Launch Instance aus.
4. Geben Sie unter Name and tags (Name und Tags) bei Name einen beschreibenden Namen für Ihre Instance ein.
5. Führen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) die folgenden Schritte aus:
   a. Wählen Sie Quick Start und dann das Betriebssystem (OS) für Ihre Instance aus. Für Ihre erste Linux-Instance empfehlen wir Ihnen, Amazon Linux zu wählen.
   b. Wählen Sie unter Amazon Machine Image (AMI) ein AMI aus, für das das kostenlose Kontingent gilt.
6. Wählen Sie unter Instance-Typ für Instance-Typ aus`t2.micro`, welches für das kostenlose Kontingent in Frage kommt. In Regionen, in denen `t2.micro` das Angebot nicht verfügbar `t3.micro` ist, gilt das kostenlose Kontingent.
7. Wählen Sie unter key pair (Anmeldung) für Schlüsselpaarname ein vorhandenes key pair aus, oder wählen Sie Neues key pair erstellen, um Ihr erstes Schlüsselpaar zu erstellen.

   > ⚠ Warning
   >
   > Wenn Sie Ohne key pair fortfahren wählen (nicht empfohlen), können Sie mit den in diesem Tutorial beschriebenen Methoden keine Verbindung zu Ihrer Instance herstellen.

8. Beachten Sie, dass wir unter Netzwerkeinstellungen Ihre Standard-VPC ausgewählt und die Option zur Verwendung des Standardsubnetzes in einer Availability Zone ausgewählt haben, die wir für Sie ausgewählt haben, und eine Sicherheitsgruppe mit einer Regel konfiguriert

haben, die Verbindungen zu Ihrer Instance von überall aus ermöglicht. Für Ihre erste Instance empfehlen wir Ihnen, die Standardeinstellungen zu verwenden. Andernfalls können Sie Ihre Netzwerkeinstellungen wie folgt aktualisieren:

- (Optional) Um ein bestimmtes Standardsubnetz zu verwenden, wählen Sie Bearbeiten und dann ein Subnetz aus.
- (Optional) Um eine andere VPC zu verwenden, wählen Sie Bearbeiten und dann eine vorhandene VPC aus. Wenn die VPC nicht für den öffentlichen Internetzugang konfiguriert ist, können Sie keine Verbindung zu Ihrer Instance herstellen.
- (Optional) Um den eingehenden Verbindungsverkehr auf ein bestimmtes Netzwerk zu beschränken, wählen Sie Benutzerdefiniert statt Anywhere und geben Sie den CIDR-Block für Ihr Netzwerk ein.
- (Optional) Um eine andere Sicherheitsgruppe zu verwenden, wählen Sie Bestehende Sicherheitsgruppe auswählen und anschließend eine vorhandene Sicherheitsgruppe aus. Wenn die Sicherheitsgruppe nicht über eine Regel verfügt, die Verbindungsverkehr aus Ihrem Netzwerk zulässt, können Sie keine Verbindung zu Ihrer Instance herstellen. Für eine Linux-Instance müssen Sie SSH-Verkehr zulassen. Für eine Windows-Instanz müssen Sie RDP-Verkehr zulassen.

9. Beachten Sie unter Speicher konfigurieren, dass wir ein Root-Volume, aber keine Datenvolumes konfiguriert haben. Dies ist für Testzwecke ausreichend.
10. Überprüfen Sie Ihre Instance-Konfiguration im Bereich Summary (Übersicht). Wenn alles in Ordnung ist, klicken Sie auf Launch instance (Instance starten).
11. Wenn der Start erfolgreich war, wählen Sie die ID der Instance aus der Erfolgsbenachrichtigung aus, um die Seite Instances zu öffnen und den Status des Starts zu überwachen.
12. Aktivieren Sie das Kontrollkästchen für die Instance. Der anfängliche Instanzstatus ist`pending`. Nach dem Start der Instance ändert sich ihr Zustand in `running`. Wählen Sie die Registerkarte Status und Alarme. Nachdem Ihre Instance die Statusprüfungen bestanden hat, ist sie bereit, Verbindungsanfragen zu empfangen.

Schritt 2: Verbindung mit der Instance herstellen

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instanz ab. Wenn Sie keine Verbindung mit Ihrer Instance herstellen können, helfen Ihnen die Informationen unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance weiter.

Linux-Instances

Sie können mit einem beliebigen SSH-Client eine Verbindung zu Ihrer Linux-Instance herstellen. Wenn Sie Windows auf Ihrem Computer ausführen, öffnen Sie ein Terminal und führen Sie den `ssh` Befehl aus, um zu überprüfen, ob ein SSH-Client installiert ist. Wenn der Befehl nicht gefunden wird, installieren Sie OpenSSH für Windows.

So stellen Sie per SSH eine Verbindung mit Ihrer Instance her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Wählen Sie auf der Seite Mit Instance Connect den Tab SSH-Client aus.
5. (Optional) Wenn Sie beim Starten der Instance und beim Herunterladen des privaten Schlüssels (.pem-Datei) auf einen Computer unter Linux oder macOS ein key pair erstellt haben, führen Sie den chmod Beispielbefehl aus, um die Berechtigungen für Ihren privaten Schlüssel festzulegen.
6. Kopieren Sie den SSH-Beispielbefehl. Im Folgenden finden Sie ein Beispiel, bei dem *`key-pair-name`* .pem der Name Ihrer privaten Schlüsseldatei, *`ec2-user`* der mit dem Bild verknüpfte Benutzername und die Zeichenfolge nach dem @-Symbol der öffentliche DNS-Name der Instanz ist.

   ```
   ssh -i key-pair-name.pem ec2-user@ec2-198-51-100-1.us-east-2.compute.amazonaws.com
   ```

7. Führen Sie in einem Terminalfenster auf Ihrem Computer den ssh Befehl aus, den Sie im vorherigen Schritt gespeichert haben. Wenn sich die private Schlüsseldatei nicht im aktuellen Verzeichnis befindet, müssen Sie in diesem Befehl den vollqualifizierten Pfad zur Schlüsseldatei angeben.

   Nachfolgend finden Sie eine Beispielantwort:

   ```
   The authenticity of host 'ec2-198-51-100-1.us-east-2.compute.amazonaws.com
    (198-51-100-1)' can't be established.
   ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
   Are you sure you want to continue connecting (yes/no)?
   ```

8. (Optional) Stellen Sie sicher, dass der Fingerabdruck in der Sicherheitswarnung mit dem Instanz-Fingerabdruck übereinstimmt, der in der Konsolenausgabe enthalten ist, wenn Sie eine Instance zum ersten Mal starten. Um die Konsolenausgabe abzurufen, wählen Sie Aktionen,

Überwachung und Fehlerbehebung, Systemprotokoll abrufen aus. Wenn die Fingerabdrücke nicht übereinstimmen, versucht möglicherweise jemand einen man-in-the-middle Angriff. Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren.

9. Geben Sie ei **`yes`**.

   Nachfolgend finden Sie eine Beispielantwort:

```
Warning: Permanently added 'ec2-198-51-100-1.us-
east-2.compute.amazonaws.com' (ECDSA) to the list of known hosts.
```

Windows-Instances

Um eine Verbindung zu einer Windows-Instanz herzustellen, müssen Sie das anfängliche Administratorkennwort abrufen und dieses Passwort verwenden, wenn Sie über Remote Desktop eine Verbindung zu Ihrer Instanz herstellen. (Nach dem Start der Instance dauert es einige Minuten, bis das Passwort verfügbar ist.)

Der Standardbenutzername für das Administratorkonto hängt von der Sprache des Betriebssystems (OS) ab, das im AMI enthalten ist. Um den richtigen Benutzernamen zu ermitteln, identifizieren Sie die Sprache des Betriebssystems Ihres AMI und wählen Sie dann den entsprechenden Benutzernamen. Für ein englisches Betriebssystem lautet der Benutzername beispielsweise`Administrator`, für ein französisches Betriebssystem ist es `Administrateur` und für ein portugiesisches Betriebssystem ist `Administrador` es. Wenn eine Sprachversion des Betriebssystems keinen Benutzernamen in derselben Sprache hat, wählen Sie den Benutzernamen`Administrator (Other)`. Weitere Informationen finden Sie unter Lokalisierte Namen für Administratorkonten in Windows im TechNet Microsoft-Wiki.

Wenn Sie Ihre Instance einer Domain zugewiesen haben, können Sie eine Verbindung mit Ihrer Instance mithilfe von Domain-Anmeldeinformationen herstellen, die Sie in AWS Directory Service definiert haben. Verwenden Sie auf dem Anmeldebildschirm für Remotedesktop anstelle des lokalen Computernamens und des generierten Kennworts den vollqualifizierten Benutzernamen für den Administrator (z. B. **`corp.example.com\Admin`**) und das Passwort für dieses Konto.

Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter the section called “Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen”.

Verwenden Sie einen RDP Client, um sich mit Ihrer Windows-Instance zu verbinden.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Wählen Sie auf der Seite Mit Instanz Connect die Registerkarte RDP-Client aus.
5. Wählen Sie unter Benutzername den Standardbenutzernamen für das Administratorkonto aus. Der von Ihnen gewählte Benutzername muss der Sprache des Betriebssystems (OS) entsprechen, das im AMI enthalten ist, mit dem Sie Ihre Instance gestartet haben. Wenn es keinen Benutzernamen in derselben Sprache wie Ihr Betriebssystem gibt, wählen Sie Administrator (Andere).
6. Wählen Sie Passwort abrufen.
7. Gehen Sie auf der Seite Windows-Passwort abrufen wie folgt vor:

   a. Wählen Sie Datei mit privatem Schlüssel hochladen und navigieren Sie zu der Datei mit dem privaten Schlüssel (`.pem`), die Sie beim Start der Instance angegeben haben. Wählen Sie die Datei aus und klicken Sie auf Open (Öffnen), um den gesamten Inhalt der Datei auf dieses Fenster zu kopieren.

   b. Wählen Sie Passwort entschlüsseln. Die Seite „Windows-Passwort abrufen“ wird geschlossen, und das Standard-Administratorkennwort für die Instanz wird unter Passwort angezeigt. Es ersetzt den zuvor angezeigten Link „Passwort abrufen“.

   c. Kopieren Sie das Passwort und speichern Sie es an einem sicheren Ort. Dieses Passwort wird benötigt, um eine Verbindung mit der Instance herzustellen.
8. Klicken Sie auf Download Remote Desktop File (Remotedesktop-Datei herunterladen). Klicken Sie nach dem Herunterladen der Datei auf Cancel (Abbrechen), um zur Seite Instances zurückzukehren. Navigieren Sie zu Ihrem Download-Verzeichnis und öffnen Sie die RDP-Datei.
9. Möglicherweise wird eine Warnmeldung angezeigt, dass der Herausgeber der Remote-Verbindung unbekannt ist. Wählen Sie Connect (Verbinden) aus, um eine Verbindung mit der Ihrer Instance herzustellen.
10. Standardmäßig wird das Administratorkonto ausgewählt. Fügen Sie das zuvor kopierte Passwort ein und wählen Sie dann OK.
11. Aufgrund der Art selbst signierter Zertifikate erhalten Sie möglicherweise eine Warnmeldung, dass das Sicherheitszertifikat nicht authentifiziert werden konnte. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie dem Zertifikat vertrauen, wählen Sie Ja, um eine Verbindung zu Ihrer Instance herzustellen.
- [Windows] Bevor Sie fortfahren, vergleichen Sie den Fingerabdruck des Zertifikats mit dem Wert im Systemprotokoll, um die Identität des Remotecomputers zu bestätigen. Wählen Sie Zertifikat anzeigen und dann auf der Registerkarte Details die Option Fingerabdruck aus. Vergleichen Sie diesen Wert mit dem Wert `RDPCERTIFICATE-THUMBPRINT` in Aktionen, Überwachung und Fehlerbehebung, Systemprotokoll abrufen.
- [Mac OS X] Bevor Sie fortfahren, vergleichen Sie den Fingerabdruck des Zertifikats mit dem Wert im Systemprotokoll, um die Identität des Remote-Computers zu bestätigen. Wählen Sie „Zertifikat anzeigen“, erweitern Sie „Details“ und wählen Sie „SHA1-Fingerabdrücke“. Vergleichen Sie diesen Wert mit dem Wert `RDPCERTIFICATE-THUMBPRINT` in Aktionen, Überwachung und Fehlerbehebung, Systemprotokoll abrufen.

Schritt 3: Bereinigen Ihrer Instance

Nachdem Sie alle Schritte für die Instance abgeschlossen haben, die Sie für dieses Tutorial erstellt haben, sollten Sie die Bereinigung durchführen, indem Sie die Instance beenden. Falls Sie vor dem Bereinigen für diese Instance noch weitere Schritte ausführen möchten, helfen Ihnen die Informationen unter weite Nächste Schritte.

> **Important**
>
> Die Beendigung einer Instance löscht diese. Nachdem Sie eine Instance beendet haben, können Sie keine erneute Verbindung mit ihr herstellen.

Wenn Sie eine Instance gestartet haben, die nicht unter das Kostenloses AWS-Kontingent fällt, fallen für diese Instance ab dem Zeitpunkt keine Gebühren mehr an, zu dem sich der Instance-Status in `shutting down` oder `terminated` ändert. Um Ihre Instance zur späteren Verwendung beizubehalten, ohne dass Gebühren anfallen, können Sie die Instance vorerst anhalten und später wieder starten. Weitere Informationen finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.

So beenden Sie Ihre Instance

1. Wählen Sie im Navigationsbereich Instances aus. Wählen Sie in der Liste mit den Instances die gewünschte Instance aus.

2. Wählen Sie Instance state (Instance-Status), Terminate instance (Instance beenden).
3. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.

   Amazon EC2 fährt Ihre Instance herunter und beendet sie. Nachdem Ihre Instance beendet wurde, bleibt sie auf der Konsole noch für kurze Zeit sichtbar, bevor der Eintrag automatisch gelöscht wird. Sie können die beendete Instance nicht selbst aus der Konsolenanzeige entfernen.

Nächste Schritte

Nachdem Sie Ihre Instance gestartet haben, sollten Sie sich mit den folgenden nächsten Schritten vertraut machen:

- Erfahren Sie, wie Sie Ihr kostenloses Kontingent nutzen, um Überraschungen bei der Rechnungsstellung zu vermeiden. Weitere Informationen finden Sie unter the section called “Ihre Nutzung des kostenlosen Kontingents nachverfolgen”.
- Konfigurieren Sie einen CloudWatch Alarm, der Sie benachrichtigt, wenn Ihre Nutzung das kostenlose Kontingent überschreitet. Weitere Informationen finden Sie im AWS Billing Benutzerhandbuch unter Nachverfolgung Ihrer Nutzung des AWS kostenlosen Kontingents.
- Fügen Sie ein EBS-Volume hinzu. Weitere Informationen finden Sie unter Erstellen eines Amazon EBS-Volumes im Amazon EBS-Benutzerhandbuch.
- Informieren Sie sich darüber, wie Sie die Remoteverwaltung für Ihre EC2-Instance mit dem Run-Befehl durchführen können. Weitere Informationen finden Sie unter AWS Systems Manager Run Command im Benutzerhandbuch für AWS Systems Manager .
- Erfahren Sie mehr über Kaufoptionen für Instances. Weitere Informationen finden Sie unter Instance-Kaufoptionen.
- Ratschläge zu Instance-Typen einholen. Weitere Informationen finden Sie unter Empfehlungen für Instance-Typen für einen neuen Workload erhalten:.

Bewährte Methoden für Amazon EC2

Um den größtmöglichen Nutzen von Amazon EC2 sicherzustellen, empfehlen wir Ihnen, den folgenden bewährten Methoden zu folgen.

Sicherheit

- Verwalten Sie den Zugriff auf AWS Ressourcen und APIs mithilfe eines Identitätsverbunds mit einem Identitätsanbieter und IAM-Rollen, wann immer dies möglich ist. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.
- Implementieren Sie Regeln mit den höchsten Einschränkungen für Ihre Sicherheitsgruppe. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln.
- Führen Sie regelmäßig Patches und Aktualisierungen durch; sichern Sie das Betriebssystem und die Anwendungen auf Ihrer Instance. Weitere Informationen finden Sie unter Update-Management. Spezifische Richtlinien für Windows-Betriebssysteme finden Sie unterBewährte Sicherheitsmethoden für Windows-Instanzen.
- Verwenden Sie Amazon Inspector, um Amazon-EC2-Instances automatisch auf Softwareschwachstellen und unbeabsichtigte Netzwerkrisiken zu untersuchen. Weitere Informationen finden Sie im Benutzerhandbuch für Amazon Inspector.
- Verwenden Sie AWS Security Hub Kontrollen, um Ihre Amazon EC2 EC2-Ressourcen anhand bewährter Sicherheitsmethoden und Sicherheitsstandards zu überwachen. Weitere Informationen zur Verwendung von Security Hub finden Sie unter Amazon Elastic Compute Cloud Kontrollen im AWS Security Hub -Benutzerhandbuch.

Speicher

- Erfahren Sie mehr über die Auswirkungen des Root-Gerätetyps auf Datenpersistenz, -sicherung und -wiederherstellung. Weitere Informationen finden Sie unter Speicher für das Root-Gerät.
- Verwenden Sie getrennte Amazon EBS-Volumes für das Betriebssystem und Ihre Daten. Stellen Sie sicher, dass das Volume mit Ihren Daten nach Beendigung der Instance erhalten bleibt. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.
- Nutzen Sie den für Ihre Instance verfügbaren Instance-Speicher zum Speichern von temporären Daten. Denken Sie daran, dass die im Instance-Speicher gespeicherten Daten gelöscht werden, wenn Sie Ihre Instance anhalten, in den Ruhezustand versetzen oder beenden. Wenn Sie

Instance-Speicher zur Datenbankspeicherung verwenden, stellen Sie sicher, dass Sie einen Cluster mit einem Replikationsfaktor haben, der Fehlertoleranz gewährleistet.

- Verschlüsseln Sie EBS-Volumes und Snapshots. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung im Amazon EBS-Benutzerhandbuch.

Ressourcenmanagement

- Nutzen Sie Instance-Metadaten und benutzerdefinierte Ressourcen-Tags zur Nachverfolgung und Identifizierung Ihrer AWS -Ressourcen. Weitere Informationen erhalten Sie unter Arbeiten mit Instance-Metadaten und Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).
- Zeigen Sie Ihre aktuellen Grenzwerte für Amazon EC2 an. Planen Sie Anfragen zur Erhöhung der Limits im Voraus vor dem Zeitpunkt, zu dem Sie sie benötigen. Weitere Informationen finden Sie unter Amazon-EC2-Service Quotas.
- Verwenden Sie es, AWS Trusted Advisor um Ihre AWS Umgebung zu untersuchen und dann Empfehlungen abzugeben, wenn Möglichkeiten bestehen, Geld zu sparen, die Systemverfügbarkeit und -leistung zu verbessern oder Sicherheitslücken zu schließen. Weitere Informationen finden Sie unter AWS Trusted Advisor im AWS Support -Benutzerhandbuch.

Sicherung und Wiederherstellung

- Sichern Sie Ihre EBS-Volumes regelmäßig mit Amazon EBS-Snapshots, und erstellen Sie ein Amazon Machine Image (AMI) aus Ihrer Instance, um die Konfiguration als Vorlage zum Starten zukünftiger Instances zu speichern. Weitere Informationen zu AWS Services, die zur Umsetzung dieses Anwendungsfalls beitragen, finden Sie unter AWS Backupund Amazon Data Lifecycle Manager.
- Stellen Sie kritische Komponenten Ihrer Anwendung in mehreren Availability Zones bereit, und replizieren Sie Ihre Daten entsprechend.
- Entwickeln Sie Ihre Anwendungen so, dass sie dynamische IP-Adressierung beim erneuten Starten Ihrer Instance verwalten können. Weitere Informationen finden Sie unter IP-Adressierung von Amazon EC2-Instances.
- Überwachen von und Reagieren auf Ereignisse. Weitere Informationen finden Sie unter Überwachen von Amazon EC2.
- Stellen Sie sicher, dass Sie auf die Bearbeitung von Failover vorbereitet sind. Als einfache Lösung können Sie einer Ersatz-Instance manuell eine Netzwerkschnittstelle oder Elastic IP-Adresse zuordnen. Weitere Informationen finden Sie unter Elastic-Network-Schnittstelle. Für eine

automatisierte Lösung können Sie Amazon EC2 Auto Scaling verwenden. Weitere Informationen hierzu finden Sie unter Amazon EC2 Auto Scaling-Benutzerhandbuch.

- Testen Sie regelmäßig den Prozess zur Wiederherstellung Ihrer Instances und Amazon-EBS-Volumes, um sicherzustellen, dass Daten und Services erfolgreich wiederhergestellt werden.

Netzwerk

- Setzen Sie den Wert time-to-live (TTL) für Ihre Anwendungen auf 255 für IPv4 und IPv6. Wenn Sie einen kleineren Wert verwenden, besteht das Risiko, dass die TTL abläuft, während der Anwendungsdatenverkehr unterwegs ist, was zu Erreichbarkeitsproblemen für Ihre Instances führt.

Amazon Machine Images (AMI)

Ein Amazon Machine Image (AMI) ist ein unterstütztes und verwaltetes Image, das von bereitgestellt wird und die Informationen bereitstellt AWS , die zum Starten einer Instance erforderlich sind. Beim Starten einer Instance müssen Sie ein AMI angeben. Sie können mehrere Instances aus einem einzigen AMI starten, wenn Sie mehrere Instances mit derselben Konfiguration benötigen. Sie können zum Starten von Instances unterschiedliche AMIs verwenden, wenn Sie Instances mit unterschiedlichen Konfigurationen benötigen.

Ein AMI umfasst Folgendes:

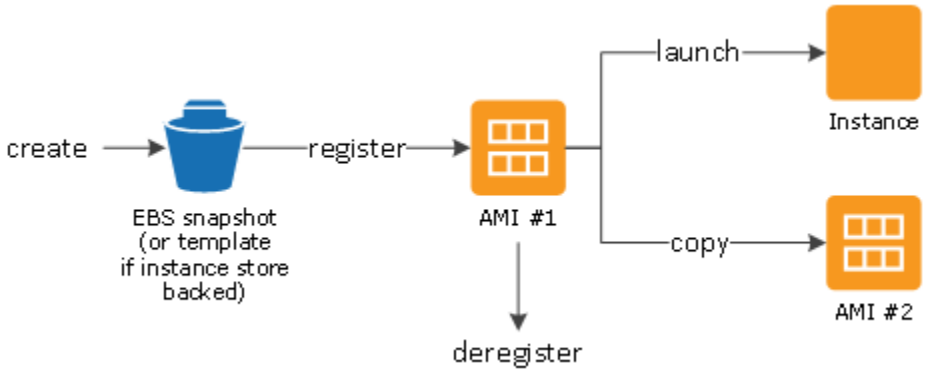
- Ein oder mehrere Amazon Elastic Block Store (Amazon EBS) -Snapshots oder, für instance-store-backed AMIs, eine Vorlage für das Root-Volume der Instance (z. B. ein Betriebssystem, ein Anwendungsserver und Anwendungen).
- Startberechtigungen, die steuern, welche AWS Konten das AMI zum Starten von Instances verwenden können.
- Eine Blockgerät-Zuweisung, die die Volumes angibt, die an die Instance beim Starten angefügt werden sollen

Themen zu Amazon Machine Image (AMI)

- AMI-Lebenszyklus
- Verwenden der Verschlüsselung mit EBS-gestützten AMIs
- Überwachen Sie AMI-Ereignisse mit Amazon EventBridge
- Verstehen von AMI-Fakturierungsdaten
- AMI-Kontingente

Verwenden eines AMI

Das folgende Diagramm fast den AMI-Lebenszyklus zusammen. Nachdem Sie ein AMI erstellt und angemeldet haben, können Sie es verwenden, um neue Instances zu starten. (Sie können Instances auch über ein AMI starten, wenn der AMI-Eigentümer Ihnen Startberechtigungen erteilt.) Sie können ein AMI innerhalb derselben AWS Region oder in verschiedene AWS Regionen kopieren. Wenn Sie ein AMI nicht mehr benötigen, können Sie es abmelden.



Sie können ein AMI suchen, das die Kriterien für Ihre Instance erfüllt. Sie können nach AMIs suchen, die von der Community bereitgestellt werden, AWS oder nach AMIs, die von der Community bereitgestellt werden. Weitere Informationen erhalten Sie unter AMI-Typen und Suchen eines AMI.

Nachdem Sie eine Instance über ein AMI gestartet haben, können Sie eine Verbindung zu ihr herstellen. Wenn Sie mit einer Instance verbunden sind, können Sie sie wie jeden anderen Server verwenden. Weitere Informationen zum Starten, Herstellen von Verbindungen und Verwenden von Instances finden Sie im Abschnitt Erste Schritte mit Amazon EC2.

Gestalten Ihres eigenen AMIs

Sie können eine Instance von einem vorhandenen AMI aus starten, die Instance anpassen (z. B. Software auf der Instance installieren) und diese aktualisierte Konfiguration dann als

benutzerdefiniertes AMI speichern. Instances, die über dieses neue benutzerdefinierte AMI gestartet werden, enthalten die Anpassungen, die Sie beim Erstellen des AMI vorgenommen haben.

Das Stamm-Speichergerät der Instance bestimmt das Verfahren, das Sie zum Erstellen eines AMI anwenden. Das Stamm-Volume einer Instance ist entweder ein Amazon Elastic Block Store (Amazon EBS)-Volume oder ein Instance-Speicher-Volume. Weitere Informationen zum Stammgeräte-Volume finden Sie unter Root-Volume der Amazon-EC2-Instance.

- Weitere Informationen zum Erstellen eines Amazon EBS-gestützten AMI finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.
- Weitere Informationen zum Erstellen eines Instance Store-Backed AMI finden Sie unter Erstellen einer Instance-Speicher-Backed Linux-AMI.

Zum Kategorisieren und Verwalten Ihrer AMIs können Sie ihnen benutzerdefinierte Tags (Markierungen) zuweisen. Weitere Informationen finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

Kaufen, teilen und verkaufen von AMIs

Nachdem Sie ein AMI erstellt haben, können Sie es privat halten, sodass nur Sie es verwenden können, oder Sie können es mit einer bestimmten Liste von AWS Konten teilen. Sie können Ihr benutzerdefiniertes AMI auch öffentlich machen, so dass die Community es verwenden kann. Der Aufbau eines sicheren, nutzbaren AMI zum öffentlichen Gebrauch ist ein relativ einfacher Prozess, wenn Sie ein paar simple Richtlinien befolgen. Weitere Informationen zum Erstellen und Verwenden gemeinsamer AMIs finden Sie unter Gemeinsame AMIs.

Sie können AMIs auch von Drittanbietern erwerben, einschließlich solcher AMIs, die mit Serviceverträgen von Organisationen wie Red Hat bereitgestellt werden. Sie können auch ein AMI erstellen und es an andere Amazon EC2-Benutzer verkaufen. Weitere Informationen zum Kaufen oder Verkaufen von AMIs finden Sie unter Gebührenpflichtige AMIs.

Abmelden Ihres AMI

Sie können ein AMI abmelden, wenn Sie es nicht mehr benötigen. Nachdem Sie ein AMI abgemeldet haben, können Sie es nicht mehr verwenden, um neue Instances zu starten. Vorhandene Instances, die über das AMI gestartet wurden, werden davon nicht beeinflusst. Weitere Informationen finden Sie unter Ein AMI abmelden (löschen).

Amazon Linux 2023 und Amazon Linux 2

Die neueste Version von Amazon Linux, AL2023, ist für Amazon EC2 optimiert und wird ohne zusätzliche Kosten für Amazon EC2-Benutzer bereitgestellt. Zu den Merkmalen von AL2023 gehören eine vorhersehbare Release-Kadenz, häufige Updates und langfristiger Support.

Weitere Informationen über die Funktionen von AL2023 und den Start eines AL2023 AMI finden Sie unter:

- AL2023-Merkmale
- Erste Schritte mit AL2023

Amazon Linux 2 (AL2) bietet eine stabile, sichere und leistungsstarke Ausführungsumgebung für Anwendungen, die auf Amazon EC2 ausgeführt werden. Weitere Informationen zu Amazon Linux 2 finden Sie unter Amazon Linux 2 auf Amazon EC2 im Amazon Linux 2-Benutzerhandbuch.

> **Note**
>
> Das Amazon Linux AMI hat seinen end-of-life Stand am 31. Dezember 2023 erreicht und wird ab dem 1. Januar 2024 keine Sicherheitsupdates oder Bugfixes erhalten. Weitere Informationen zum Amazon Linux AMI end-of-life und zum Wartungssupport finden Sie im Blogbeitrag Update on Amazon Linux AMI end-of-life. Wir empfehlen Ihnen, Ihre Anwendungen auf AL2023 zu aktualisieren, was langfristigen Support bis 2028 beinhaltet.

Windows-AMIs

AWS stellt eine Reihe öffentlich verfügbarer AMIs bereit, die für die Windows-Plattform spezifische Softwarekonfigurationen enthalten. Mit diesen AMIs können Sie schnell damit beginnen, Ihre Anwendungen mit Amazon EC2 zu erstellen und bereitzustellen. Wählen Sie zuerst das AMI aus, das Ihre spezifischen Anforderungen erfüllt, und starten Sie dann mithilfe eines AMI eine Instance. Rufen Sie das Passwort für das Administratorkonto ab, und melden Sie sich dann über die Remote Desktop Connection bei der Instance an, genau wie bei jedem anderen Windows-Server. Weitere Informationen zu AWS Windows-AMIs finden Sie in der AWS Windows AMI-Referenz.

Wenn Sie eine Instance aus einem Windows-AMI starten, ist das Stammgerät für die Windows-Instance ein Volume Amazon Elastic Block Store (Amazon EBS). Windows-AMIs unterstützen keinen Instance-Speicher für das Root-Gerät.

Windows-AMIs, die für einen schnelleren Start mit EC2 Fast Launch konfiguriert sind, sind vorab bereitgestellt und verwenden Snapshots, um Instances bis zu 65% schneller zu starten. Weitere Informationen zu EC2 Fast Launch finden Sie unter. Verwenden Sie EC2 Fast Launch für Ihre Windows-Instances

> **Note**
>
> Microsoft unterstützt Windows Server-Versionen vor Windows Server 2016 nicht mehr. Wir empfehlen, dass Sie neue EC2-Instances mit einer unterstützten Version von Windows Server starten. Wenn Sie EC2-Instances haben, die auf einer nicht unterstützten Version von Windows Server ausgeführt werden, sollten Sie ein Upgrade dieser Instances auf eine unterstützte Version von Windows Server vornehmen. Weitere Informationen finden Sie unter Aktualisieren einer Amazon EC2-Instance unter Windows Server auf eine neuere Version von Windows.

AMI-Typen

Sie können ein AMI aufgrund der folgenden Merkmale auswählen:

- Region (siehe Regionen und Zonen)
- Betriebssystem
- Architektur (32-Bit oder 64-Bit)
- Startberechtigungen
- Speicher für das Root-Gerät

Startberechtigungen

Der Eigentümer eines AMI legt dessen Verfügbarkeit durch Vergabe von Startberechtigungen fest. Startberechtigungen lassen sich in die folgenden Kategorien einteilen.

Startberechtigung	Beschreibung
öffentlich	Der Besitzer erteilt allen AWS Konten Startberechtigungen.

Startberechtigung	Beschreibung
explizit	Der Besitzer erteilt bestimmten AWS Konten, Organisationen oder Organisationseinheiten (OUs) Startberechtigungen.
implizit	Der Eigentümer hat implizite Startberechtigungen für ein AMI.

Amazon und die Amazon EC2-Community stellen eine große Auswahl von öffentlichen AMIs bereit. Weitere Informationen finden Sie unter Gemeinsame AMIs. Developer können für ihre AMIs Gebühren erheben. Weitere Informationen finden Sie unter Gebührenpflichtige AMIs.

Speicher für das Root-Gerät

Alle AMIs sind kategorisiert, entweder als gestützt durch Amazon EBS oder gestützt durch Instance-Speicher.

- Amazon-EBS-gestütztes AMI: Das Root-Gerät für eine Instance, die über das AMI gestartet wird, ist ein Amazon Elastic Block Store (Amazon EBS)-Volume, das über einen Amazon-EBS-Snapshot erstellt wird. Wird sowohl für Linux- als auch für Windows-AMIs unterstützt.
- Instance-Speicher-gestütztes AMI von Amazon: Das Root-Gerät für eine Instance, die über das AMI gestartet wird, ist ein Instance-Speicher-Volume, das aus einer in Amazon S3 gespeicherten Vorlage erstellt wird. Wird nur für Linux-AMIs unterstützt. Windows-AMIs unterstützen keinen Instance-Speicher für das Stammgerät.

Weitere Informationen finden Sie unter Root-Volume der Amazon-EC2-Instance.

Die folgende Tabelle fasst die wichtigsten Unterschiede bei der Verwendung der beiden Arten von AMIs zusammen.

Merkmal	Amazon EBS-Backed AMI	Amazon Instance Store-Backed AMI
Startzeit für eine Instance	Normalerweise unter 1 Minute	Normalerweise unter 5 Minuten

Merkmal	Amazon EBS-Backed AMI	Amazon Instance Store-Backed AMI
Größenbegrenzung für ein Root-Gerät	64 TiB**	10 GiB
Root-Gerät-Volume	EBS-Volume	Instance-Speicher-Volume
Datenpersistenz	Das Root-Volume wird standardmäßig gelöscht, wenn die Instance beendet wird.* Daten auf alle anderen EBS-Volumes nach Beendigung der Instance erhalten.	Daten auf Instance-Speicher-Volumes bleiben nur während der Lebensdauer der Instance erhalten.
Modifikationen	Instance-Typ, Kernel, RAM-Datenträger und Benutzerdaten können geändert werden, während die Instance gestoppt ist.	Instance-Attribute sind über die Lebensdauer einer Instance festgelegt.
Gebühren	Ihnen wird die Instance-Nutzung, EBS-Volume-Nutzung und das Speichern Ihres AMI als EBS-Snapshot berechnet.	Ihnen wird die Instance-Nutzung und das Speichern Ihres AMI in Amazon S3 berechnet.
AMI-Erstellung/-Bündelung	Verwendet einen einzelnen Befehl/Aufruf	Erfordert Installation und Verwendung von AMI-Tools
Angehaltener Zustand	Kann sich in einem angehaltenen Zustand befinden. Selbst wenn die Instance angehalten ist und nicht ausgeführt wird, wird das Stammvolumen in Amazon EBS dauerhaft gespeichert.	Darf nicht im angehaltenen Zustand sein; Instances werden ausgeführt oder wurden beendet

* Standardmäßig ist das Flag `DeleteOnTermination` für EBS-Root-Volumes auf `true` gesetzt. Weitere Informationen zum Ändern dieses Flags, so dass das Volume nach der Beendigung erhalten bleibt, finden Sie unter Ändern des beizubehaltenden Root-Volumes.

** Nur unterstützt mit `io2`-EBS Block Express. Weitere Informationen finden Sie unter Provisioned IOPS SSD Block Express-Volumes im Amazon EBS-Benutzerhandbuch.

Bestimmen des Root-Gerätetyps Ihres AMI

So ermitteln Sie den Root-Gerätetyp eines AMI mit der Konsole

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs und dann das AMI aus.
3. Prüfen Sie auf der Registerkarte Details den Wert unter Root-Gerätetyp wie folgt:
   - `ebs`: Dies ist ein EBS-gestütztes AMI.
   - `instance store`: Dies ist ein Instance-Speicher-gestütztes AMI.

So ermitteln Sie den Root-Gerätetyp eines AMI über die Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-images (AWS CLI)
- Get-EC2Image (AWS Tools for Windows PowerShell)

Angehaltener Zustand

Sie können eine Instance anhalten, die über ein EBS-Volume für ihr Root-Gerät verfügt, aber Sie können eine Instance nicht anhalten, die über ein Instance-Speicher-Volume für ihr Root-Gerät verfügt.

Beim Anhalten wird die Instance nicht mehr ausgeführt (der Zustand wechselt von `running` zu `stopping` und zu `stopped`). Eine angehaltene Instance bleibt in Amazon EBS gespeichert, deshalb kann sie erneut gestartet werden. Anhalten is nicht dasselbe wie Beenden; eine beendete Instance kann nicht erneut gestartet werden. Da Instances mit einem Instance-Speicher-Volume für das Root-Gerät nicht angehalten werden können, werden sie entweder ausgeführt oder beendet. Weitere

Informationen darüber, was passiert und was Sie tun können, während eine Instance angehalten ist, finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.

Standardmäßiger Datenspeicher und Persistenz

Instances, die ein Instance-Speicher-Volume für das Root-Gerät haben, verfügen automatisch über Instance-Speicher (das Root-Volume enthält die Root-Partition, und Sie können zusätzliche Daten speichern). Sie können persistenten Speicher zu Ihrer Instance hinzufügen, indem Sie weitere EBS-Volumes anfügen. Alle auf einem Instance-Speicher-Volume befindlichen Daten werden gelöscht, wenn die Instance ausfällt oder beendet wird. Weitere Informationen finden Sie unter Instance-Speicher-Volume und Lebensdauer der Daten.

An Instances, die Amazon EBS für das Root-Gerät haben, wird automatisch ein EBS-Volume angefügt. Das Volume wird wie jedes andere auch in Ihrer Volumes-Liste angezeigt. Bei den meisten Instance-Typen haben Instances, die ein EBS-Volume für das Root-Gerät haben, standardmäßig keine Instance-Speicher-Volumes. Sie können Instance-Speicher-Volumes oder zusätzliche EBS-Volumes mithilfe von Blockgerät-Zuweisung hinzufügen. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen.

Startzeiten

Von einem Amazon EBS-Backed AMI gestartete Instances werden schneller gestartet als von einem Instance Store-Backed AMI gestartete Instances. Wenn Sie eine Instance vom Instance Store-Backed AMI starten, müssen alle Teile aus Amazon S3 abgerufen werden, bevor die Instance verfügbar ist. Bei einem Amazon EBS-gestützten AMI müssen nur die Teile von dem Snapshot abgerufen werden, die zum Starten der Instance benötigt werden, bevor die Instance verfügbar ist. Allerdings ist die Leistung einer Instance, die ein EBS-Volume für das Root-Gerät verwendet, kurzfristig langsamer, während die restlichen Teile vom Snapshot abgerufen und in das Volume geladen werden. Wenn Sie die Instance anhalten und erneut starten, erfolgt der Start schnell, weil der Status in einem EBS-Volume gespeichert ist.

AMI-Erstellung

Um Linux-AMIs mit Unterstützung durch Instance-Speicher zu erstellen, müssen Sie mithilfe der Amazon EC2-AMI-Tools aus Ihrer Instance ein AMI auf der Instance selbst erstellen. Beachten Sie, dass Windows-AMIs den Instance-Speicher für das Root-Gerät nicht unterstützen.

Bei durch Amazon EBS gestützte AMIs ist die AMI-Erstellung viel einfacher. Mit der API-Aktion `CreateImage` wird Ihr Amazon EBS-gestütztes AMI erstellt und registriert. Es gibt auch eine

Schaltfläche AWS Management Console , mit der Sie ein AMI aus einer laufenden Instance erstellen können. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

Kostenberechnung

Bei AMIs mit Unterstützung durch Instance-Speicher werden Ihnen die Instance-Nutzung und das Speichern der AMI in Amazon S3 berechnet. Bei AMIs mit Unterstützung durch Amazon EBS wird Ihnen die Instance-Nutzung, EBS-Volume-Speicherung und die Speicherung Ihres AMI als EBS-Snapshot berechnet.

Bei Amazon EC2-Instance Store-Backed AMIs werden jedes Mal, wenn Sie ein AMI anpassen und ein neues erstellen, alle Teile für jedes AMI in Amazon S3 gespeichert. Daher entspricht der Speicherbedarf für jedes benutzerdefinierte AMI der vollen Größe des AMI. Bei Amazon EBS-gestützten AMIs werden jedes Mal, wenn Sie ein AMI anpassen und ein neues erstellen, nur die Änderungen gespeichert. Daher ist der Speicherbedarf für AMIs, die Sie nach dem ersten AMI anpassen, viel geringer, was niedrigere AMI-Speichergebühren zur Folge hat.

Wenn eine Instance mit einem EBS-Volume für ihr Root-Gerät angehalten wird, wird Ihnen die Instance-Nutzung nicht in Rechnung gestellt; der Volume-Speicher wird Ihnen jedoch weiterhin in Rechnung gestellt. Sobald Sie Ihre Instance starten, werden Sie mit der Mindestgebühr für eine Minute Nutzung belastet. Nach einer Minute berechnen wir nur die verwendeten Sekunden. Wenn Sie beispielsweise eine Instance 20 Sekunden lang ausführen und danach anhalten, berechnen wir eine volle Minute. Wenn Sie eine Instance 3 Minuten und 40 Sekunden lang ausführen, berechnen wir genau für 3 Minuten und 40 Sekunden der Nutzung. Wir berechnen jede Sekunde, bei einer Mindestgebühr von einer Minute, für die Sie die Instance ausführen, selbst wenn die Instance passiv bleibt und Sie keine Verbindung dazu herstellen.

AMI-Virtualisierungstypen

Amazon Machine Images verwenden einen von zwei Virtualisierungstypen: Paravirtual (PV) oder Hardware Virtual Machine (HVM). Die Hauptunterschiede zwischen PV- und HVM-AMIs sind die Art und Weise, wie sie gestartet werden und ob sie spezielle Hardwareerweiterungen (CPU, Netzwerk und Speicher) zur Verbesserung der Leistung nutzen können. Windows AMIs sind HVM-AMIs.

Um die bestmögliche Leistung zu erhalten, empfiehlt sich zum Starten der Instances die Verwendung von Instance-Typen und HVM-AMIs der aktuellen Generation. Weitere Informationen über Instance-Typen der aktuellen Generation finden Sie unter Amazon EC2-Instance-Typen. Wenn Sie Instance-Typen der vorherigen Generation verwenden und ein Upgrade durchführen möchten, helfen Ihnen die Informationen unter Upgrade-Pfade und Ändern des Instance-Typs weiter.

In der folgenden Tabelle werden HVM- und PV-AMIs verglichen.

	HVM (Hardwaregestützte virtuelle Maschine)	PV
Beschreibung	HVM-AMIs sind mit einem vollständig virtualisierten Hardwaresatz ausgestattet und werden durch Ausführen des Master Boot Records des Stamm-Blockgeräts Ihres Images gestartet. Dieser Virtualisierungstyp kann ein Betriebssystem direkt auf einer virtuellen Maschine ausführen, ohne dass diese modifiziert werden muss – ganz so, als würde es sich um Bare-Metal-Hardware handeln. Das Amazon EC2-Hosts ystem emuliert einige oder alle der zugrunde liegenden Hardware-Elemente, die dem Gast zur Verfügung gestellt werden.	PV-AMIs starten mit einem speziellen Boot-Loader mit der Bezeichnung PV-GRUB, der den Boot-Zyklus startet und dann das Chainloading des Kernels durchführt, der in der Datei `menu.lst` auf Ihrem Image angegeben ist. Paravirtual-Gäste können auf Host-Hardware ausgeführt werden, die keine explizite Unterstützung für Virtualis ierung hat. Früher verfügten PV-Gäste in vielen Fällen über eine bessere Leistung als HVM-Gäste, aber aufgrund von Verbesserungen der HVM-Virtualisierung und der Verfügbarkeit von PV-Treibe rn für HVM-AMIs ist dies nicht mehr der Fall. Weitere Informationen zu PV-GRUB und seiner Verwendung in Amazon EC2 finden Sie unter Von Benutzern bereitgestellte Kernel.
Unterstützung für Hardware-Erweiterungen	Ja. Anders als bei PV-Gästen können HVM-Gäste den Vorteil von Hardware-Erweiterungen nutzen, die einen schnellen Zugriff auf die	Nein, sie können keine speziellen Hardwaree rweiterungen wie erweiterte Netzwerk- oder GPU-Verar beitung nutzen.

	HVM (Hardwaregestützte virtuelle Maschine)	PV
	zugrunde liegende Hardware des Hostsystems ermöglichen. Weitere Informationen zu CPU-Virtualisierungserweiterungen, die in Amazon EC2 verfügbar sind, finden Sie unter Intel Virtualization Technology auf der Intel-Website. HVM-AMIs sind erforderlich, um eine verbesserte Netzwerkleistung und GPU-Verarbeitung nutzen zu können. Um Anweisungen an spezialisierte Netzwerk- und GPU-Geräte weiterleiten zu können, muss das Betriebssystem Zugriff auf die native Hardwareplattform haben. Hier stellt HVM-Virtualisierung den erforderlichen Zugriff bereit. Weitere Informationen finden Sie unter Verbessertes Networking auf Amazon EC2.	
Unterstützte Instance-Typen	Alle Instance-Typen der aktuellen Generation unterstützen HVM-AMIs.	Die folgenden Instance-Typen der vorherigen Generation unterstützen PV-AMIs: C1, C3, HS1, M1, M3, M2 und T1. Die Instance-Typen der aktuellen Generation unterstützen keine PV-AMIs.

	HVM (Hardwaregestützte virtuelle Maschine)	PV
Unterstützte Regionen	Alle Regionen unterstützen HVM-Instances.	Asien-Pazifik (Tokio), Asien-Pazifik (Singapur), Asien-Pazifik (Sydney), Europa (Frankfurt), Europa (Irland), Südamerika (São Paulo), US East (N. Virginia), USA West (Nordkalifornien), und USA West (Oregon)
So finden Sie sie	Stellen Sie sicher, dass der Virtualisierungstyp des AMI auf `hvm` festgelegt ist. Verwenden Sie hierzu die Konsole oder den Befehl describe-images. Weitere Informationen finden Sie unter Suchen eines AMI.	Stellen Sie sicher, dass der Virtualisierungstyp des AMI auf `paravirtual` festgelegt ist. Verwenden Sie hierzu die Konsole oder den Befehl describe-images. Weitere Informationen finden Sie unter Suchen eines AMI.

PV auf HVM

Paravirtuelle Gäste verfügten traditionell über eine bessere Performance bei Speicher- und Netzwerkoperationen als HVM-Gäste, da sie spezielle Treiber für die I/O nutzen konnten, mit denen der Mehraufwand für die Emulation von Netzwerk- und Datenträger-Hardware vermieden wurde. Im Gegensatz dazu mussten HVM-Gäste diese Anweisungen in emulierte Hardware übersetzen. PV-Treiber stehen jetzt HVM-Gästen zur Verfügung. Für Betriebssysteme, die nicht für die Ausführung in einer paravirtualisierten Umgebung (z. B. Windows) portiert werden können, können durch ihre Nutzung daher trotzdem Leistungsvorteile in Bezug auf Speicher- und Netzwerk-I/O erzielt werden. Mit diesen PV auf HVM-Treibern können HVM-Gäste die gleiche oder eine bessere Leistung als paravirtuelle Gäste erzielen.

Amazon EC2 EC2-Startmodi

Wenn ein Computer hochfährt, ist die erste Software, die er ausführt, für die Initialisierung der Plattform und die Bereitstellung einer Schnittstelle für das Betriebssystem zur Durchführung plattformspezifischer Vorgänge verantwortlich.

In Amazon EC2 werden zwei Varianten der Startmodus-Software unterstützt: Unified Extensible Firmware Interface (UEFI) und Legacy BIOS.

Mögliche Startmodus-Parameter für ein AMI

Ein AMI kann einen der folgenden Werte für den Startmodus-Parameter annehmen: `uefi`, `legacy-bios` oder `uefi-preferred`. Der AMI-Startmodus-Parameter ist optional. Für AMIs ohne Startmodus-Parameter verwenden die Instances, die von diesen AMIs gestartet werden, den Standardstartmodus-Wert des Instance-Typs.

Der Zweck des AMI-Startmodus-Parameters

Der AMI-Startmodus-Parameter signalisiert Amazon EC2, welcher Startmodus beim Starten einer Instance verwendet werden soll. Wenn der Startmodus-Parameter auf `uefi` festgelegt ist, versucht EC2, die Instance mit UEFI zu starten. Wenn das Betriebssystem nicht für die Verwendung von UEFI konfiguriert ist, wird die Instance nicht erfolgreich gestartet.

UEFI-Bevorzugt-Startmodus-Parameter

Sie können AMIs erstellen, die sowohl UEFI als auch Legacy-BIOS unterstützen, indem Sie den `uefi-preferred`-Startmodus-Parameter verwenden. Wenn der Startmodus-Parameter auf `uefi-preferred` festgelegt ist und der Instance-Typ UEFI unterstützt, wird die Instance auf UEFI gestartet. Wenn der Instance-Typ UEFI nicht unterstützt, wird die Instance auf Legacy-BIOS gestartet.

> **Warning**
>
> Einige Features, wie UEFI Secure Boot, sind nur auf Instances verfügbar, die auf UEFI gestartet werden. Wenn Sie den `uefi-preferred`-AMI-Startmodus-Parameter mit einem Instance-Typ verwenden, der UEFI nicht unterstützt, wird die Instance als Legacy-BIOS gestartet und das UEFI-abhängige Feature wird deaktiviert. Wenn Sie auf die Verfügbarkeit eines UEFI-abhängigen Features angewiesen sind, setzen Sie Ihren AMI-Startmodus-Parameter auf `uefi`.

Standard-Startmodi für Instance-Typen

- Instance-Typen für Graviton: UEFI
- Instance-Typen für Intel und AMD: Legacy-System BIOS

Intel- und AMD-Instance-Typen auf UEFI ausführen

Most Intel and AMD instance types kann sowohl auf UEFI als auch auf Legacy-BIOS ausgeführt werden. Um UEFI verwenden zu können, müssen Sie ein AMI auswählen, bei dem der Startmodus-Parameter auf `uefi` oder `uefi-preferred` festgelegt ist. Außerdem muss das im AMI enthaltene Betriebssystem für die Verwendung von UEFI konfiguriert sein.

Themen zu Startmodus

- Starten einer -Instance
- Den Startmodus-Parameter für ein AMI bestimmen
- Die unterstützten Startmodi eines Instance-Typs bestimmen
- Den Startmodus einer Instance bestimmen
- Bestimmen des Startmodus des Betriebssystems
- Den Startmodus eines AMI festlegen
- UEFI-Variablen
- UEFI Secure Boot

Starten einer -Instance

Sie können eine Instance in UEFI oder im Legacy-BIOS-Startmodus starten.

Themen

- Einschränkungen
- Überlegungen
- Anforderungen für den Start einer Instance auf UEFI

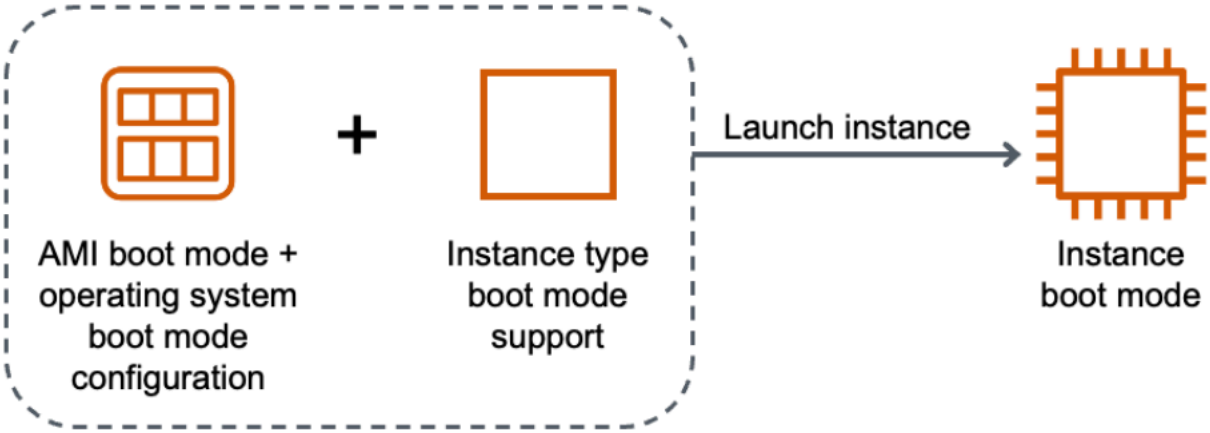
Einschränkungen

UEFI-Boot wird nicht in Local Zones, Wavelength Zones oder mit AWS Outposts unterstützt.

Überlegungen

Bitte beachten Sie beim Starten einer Instance Folgendes:

- Der Startmodus der Instance wird durch die Konfiguration des AMI, das darin enthaltene Betriebssystem und den Instance-Typ bestimmt, wie durch das folgende Bild veranschaulicht wird:



Die folgende Tabelle zeigt, dass der Startmodus einer Instance (angezeigt in der Spalte Resultierender Startmodus der Instance) durch eine Kombination aus dem Startmodus-Parameter des AMI (Spalte 1), der Startmodus-Konfiguration des im AMI enthaltenen Betriebssystems (Spalte 2) und der Startmodus-Unterstützung des Instance-Typs (Spalte 3) bestimmt wird.

AMI-Startmodus-Parameter	Startmodus-Konfiguration des Betriebssystems	Instance-Typ Startmodus-Unterstützung	Resultierender Startmodus der Instance
UEFI	UEFI	UEFI	UEFI
Legacy BIOS	Legacy BIOS	Legacy BIOS	Legacy BIOS
UEFI Preferred	UEFI	UEFI	UEFI
UEFI Preferred	UEFI	UEFI und Legacy BIOS	UEFI
UEFI Preferred	Legacy BIOS	Legacy BIOS	Legacy BIOS

AMI-Startmodus-Parameter	Startmodus-Konfiguration des Betriebssystems	Instance-Typ Startmodus-Unterstützung	Resultierender Startmodus der Instance
UEFI Preferred	Legacy BIOS	UEFI und Legacy BIOS	Legacy BIOS
Kein Startmodus angegeben – ARM	UEFI	UEFI	UEFI
Kein Startmodus angegeben – x86	Legacy BIOS	UEFI und Legacy BIOS	Legacy BIOS

- Standard-Startmodi:
  - Instance-Typen für Graviton: UEFI
  - Instance-Typen für Intel und AMD: Legacy-System BIOS
- Intel- und AMD-Instance-Typen, die zusätzlich zu Legacy-System BIOS auch UEFI unterstützen:
  - Alle Instances, die auf dem AWS Nitro-System basieren, außer: Bare-Metal-Instances, DL1, G4ad, P4, u-3tb1, u-6tb1, u-9tb1, u-12tb1, u-18tb1, u-24tb1 und VT1

Anzeigen der verfügbaren Instance-Typen, die UEFI in einer bestimmten Region unterstützen

Die verfügbaren Instance-Typen variieren je nach AWS-Region. Um die verfügbaren Instance-Typen anzuzeigen, die UEFI in einer Region unterstützen, verwenden Sie den Befehl describe-instance-types (Instance-Typen beschreiben) mit dem Parameter `--region`. Wenn Sie den `--region`-Parameter weglassen, wird Ihre Standardregion in der Anfrage verwendet. Schließen Sie den Parameter `--filters` ein, um die Ergebnisse auf die Instance-Typen zu beschränken, die UEFI unterstützen, und den Parameter `--query`, um die Ausgabe auf den Wert von `InstanceType` zu beschränken.

Verwenden Sie den Befehl für Ihr Betriebssystem.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi --
query "InstanceTypes[*].[InstanceType]" --output text | sort

a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge
c5.12xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {$_.SupportedBootModes -Contains "uefi"} | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration

CurrentGeneration: False

InstanceType
------------
a1.2xlarge
a1.4xlarge
a1.large
a1.medium
a1.metal
a1.xlarge

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
```

```
c5.9xlarge
...
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=processor-info.supported-architecture,Values=x86_64 --query "InstanceTypes[*].
[InstanceType]" --output text | sort

c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
c5.9xlarge
c5.large
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
 Where-Object {
     $_.SupportedBootModes -Contains "uefi" -and `
     $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
     } | `
 Sort-Object InstanceType | `
 Format-Table InstanceType -GroupBy CurrentGeneration

CurrentGeneration: True

InstanceType
------------
c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
c5.4xlarge
...
```

Anzeigen der verfügbaren Instance-Typen, die UEFI Secure Boot unterstützen und nichtflüchtige Variablen in einer bestimmten Region beibehalten

Derzeit unterstützen Bare-Metal-Instances UEFI Secure Boot und nichtflüchtige Variablen nicht. Verwenden Sie den Befehl describe-instance-types wie im vorhergehenden Beispiel beschrieben, aber filtern Sie die Bare-Metal-Instances heraus, indem Sie die Filter `Name=bare-metal,Values=false` einschließen. Informationen zu UEFI Secure Boot finden Sie unter UEFI Secure Boot.

Verwenden Sie den Befehl für Ihr Betriebssystem.

Linux

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-mode,Values=uefi
 Name=bare-metal,Values=false --query "InstanceTypes[*].[InstanceType]" --output
 text | sort

a1.2xlarge
a1.4xlarge
a1.large
a1.medium
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}

InstanceType     SupportedBootModes  BareMetal SupportedArchitectures
------------     ------------------  --------- ----------------------
a1.2xlarge       {uefi}                  False arm64
```

```
a1.4xlarge       {uefi}                 False arm64
a1.large         {uefi}                 False arm64
a1.medium        {uefi}                 False arm64
a1.xlarge        {uefi}                 False arm64
c5.12xlarge      {legacy-bios, uefi}    False x86_64
c5.18xlarge      {legacy-bios, uefi}    False x86_64
```

Windows

AWS CLI

```
$ aws ec2 describe-instance-types --filters Name=supported-boot-
mode,Values=uefi Name=bare-metal,Values=false Name=processor-info.supported-
architecture,Values=x86_64 --query "InstanceTypes[*].[InstanceType]" --output text |
 sort

c5.12xlarge
c5.18xlarge
c5.24xlarge
c5.2xlarge
...
```

PowerShell

```
PS C:\> Get-EC2InstanceType | `
    Where-Object { `
        $_.SupportedBootModes -Contains "uefi" -and `
        $_.BareMetal -eq $False -and `
        $_.ProcessorInfo.SupportedArchitectures -eq "x86_64"
        } | `
    Sort-Object InstanceType  | `
    Format-Table InstanceType, SupportedBootModes, BareMetal,
 @{Name="SupportedArchitectures";
 Expression={$_.ProcessorInfo.SupportedArchitectures}}

InstanceType    SupportedBootModes  BareMetal SupportedArchitectures
------------    ------------------  --------- ----------------------
c5.12xlarge     {legacy-bios, uefi}     False x86_64
c5.18xlarge     {legacy-bios, uefi}     False x86_64
c5.24xlarge     {legacy-bios, uefi}     False x86_64
c5.2xlarge      {legacy-bios, uefi}     False x86_64
c5.4xlarge      {legacy-bios, uefi}     False x86_64
```

```
c5.9xlarge      {legacy-bios, uefi}     False x86_64
```

Anforderungen für den Start einer Instance auf UEFI

Um eine Instance im UEFI-Startmodus zu starten, müssen Sie einen Instance-Typ auswählen, der UEFI unterstützt. Außerdem müssen Sie das AMI und Betriebssystem wie folgt für UEFI konfigurieren:

Instance-Typ

Beim Start einer Instance müssen Sie einen Instance-Typ auswählen, der UEFI unterstützt. Weitere Informationen finden Sie unter Die unterstützten Startmodi eines Instance-Typs bestimmen.

AMI

Beim Start einer Instance müssen Sie ein AMI auswählen, das für UEFI konfiguriert ist. Das AMI muss wie folgt konfiguriert sein:

- Betriebssystem – Das im AMI enthaltene Betriebssystem muss für die Verwendung von UEFI konfiguriert sein, andernfalls wird der Start der Instance fehlschlagen. Weitere Informationen finden Sie unter Bestimmen des Startmodus des Betriebssystems.
- AMI-Startmodus-Parameter – Der Startmodus-Parameter des AMI muss auf `uefi` oder `uefi-preferred` eingestellt sein. Weitere Informationen finden Sie unter Den Startmodus-Parameter für ein AMI bestimmen.

Linux — stellt AWS nur Linux-AMIs bereit, die so konfiguriert sind, dass sie UEFI für Graviton-basierte Instance-Typen unterstützen. Um Linux auf anderen UEFI-Instanztypen zu verwenden, müssen Sie das AMI konfigurieren, das AMI über VM Import/Export importieren oder das AMI über importieren. CloudEndure

Windows — Die folgenden Windows-AMIs unterstützen UEFI:

- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

- TPM-Windows_Server-2016-English-Core-Base

Den Startmodus-Parameter für ein AMI bestimmen

Der AMI-Startmodus-Parameter ist optional. Ein AMI kann einen der folgenden Werte für den Startmodus-Parameter annehmen: `uefi`, `legacy-bios` oder `uefi-preferred`.

Einige AMIs haben keinen Startmodus-Parameter. Wenn ein AMI keinen Startmodus-Parameter hat, verwenden die Instances, die von diesem AMI gestartet werden, den Standardwert des Instance-Typs, der `uefi` für Graviton und `legacy-bios` für alle Intel- und AMD-Instance-Typen ist.

Console

So ermitteln Sie den Startmodus-Parameter eines AMI (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs und wählen Sie dann das AMI aus.
3. Überprüfen Sie das Feld Startmodus.
   - Ein Wert von uefi gibt an, dass das AMI UEFI unterstützt.
   - Ein Wert von uefi-preferred gibt an, dass das AMI sowohl UEFI als auch Legacy BIOS unterstützt.
   - Wenn kein Wert vorhanden ist, verwenden die über das AMI gestarteten Instances den Standardwert des Instance-Typs.

So ermitteln Sie den Startmodus-Parameter eines AMI beim Start einer Instance (Konsole)

Wenn Sie eine Instance mit dem Launch Instance Wizard starten, überprüfen Sie bei der Auswahl eines AMI das Feld Startmodus. Weitere Informationen finden Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image).

AWS CLI

So ermitteln Sie den Startmodus-Parameter eines AMI (AWS CLI)

Verwenden Sie den Vorgang describe-images, um den Startmodus eines AMI zu bestimmen.

```
aws ec2 describe-images --region us-east-1 --image-id ami-0abcdef1234567890
```

```
{
    "Images": [
        {
         ...
            ],
            "EnaSupport": true,
            "Hypervisor": "xen",
            "ImageOwnerAlias": "amazon",
            "Name": "UEFI_Boot_Mode_Enabled-Windows_Server-2016-English-Full-
Base-2020.09.30",
            "RootDeviceName": "/dev/sda1",
            "RootDeviceType": "ebs",
            "SriovNetSupport": "simple",
            "VirtualizationType": "hvm",
            "BootMode":
 "uefi"
        }
    ]
}
```

In der Ausgabe gibt das `BootMode`-Feld den Startmodus des AMI an. Ein Wert von `uefi` gibt an, dass das AMI UEFI unterstützt. Ein Wert von `uefi-preferred` gibt an, dass das AMI sowohl UEFI als auch Legacy BIOS unterstützt. Wenn kein Wert vorhanden ist, verwenden die über das AMI gestarteten Instances den Standardwert des Instance-Typs.

PowerShell

Um den Startmodus-Parameter eines AMI zu ermitteln (Tools for PowerShell)

Verwenden Sie Cmdlet Get-EC2Image, um den Startmodus eines AMI zu bestimmen.

```
PS C:\> Get-EC2Image -Region us-east-1 -ImageId ami-0abcdef1234567890 | Format-List
 Name, BootMode, TpmSupport

Name       : TPM-Windows_Server-2016-English-Full-Base-2023.05.10
BootMode   : uefi
TpmSupport : v2.0
```

In der Ausgabe gibt das `BootMode`-Feld den Startmodus des AMI an. Ein Wert von `uefi` gibt an, dass das AMI UEFI unterstützt. Ein Wert von `uefi-preferred` gibt an, dass das AMI sowohl UEFI als auch Legacy BIOS unterstützt. Wenn kein Wert vorhanden ist, verwenden die über das AMI gestarteten Instances den Standardwert des Instance-Typs.

Die unterstützten Startmodi eines Instance-Typs bestimmen

Sie können die AWS CLI oder die Tools für verwenden PowerShell , um die unterstützten Startmodi eines Instance-Typs zu ermitteln.

So ermitteln Sie die unterstützten Startmodi eines Instance-Typs

Sie können die folgenden Methoden verwenden, um die unterstützten Startmodi eines Instance-Typs zu ermitteln.

AWS CLI

Sie können den Befehl describe-instance-types verwenden, um die unterstützten Startmodi eines Instance-Typs zu ermitteln. Indem Sie den `--query`-Parameter einbeziehen, können Sie die Ausgabe filtern. In diesem Beispiel wird die Ausgabe gefiltert, um nur die unterstützten Startmodi zurückzugeben.

Das folgende Beispiel zeigt, dass `m5.2xlarge` sowohl den Startmodus UEFI als auch den Startmodus Legacy-System BIOS unterstützt.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types m5.2xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Erwartete Ausgabe:

```
[
    [
        "legacy-bios",
        "uefi"
    ]
]
```

Das folgende Beispiel zeigt, dass `t2.xlarge` nur Legacy BIOS unterstützt.

```
aws ec2 describe-instance-types --region us-east-1 --instance-types t2.xlarge --
query "InstanceTypes[*].SupportedBootModes"
```

Erwartete Ausgabe:

```
[
    [
```

```
        "legacy-bios"
    ]
]
```

PowerShell

Sie können das Cmdlet Get-EC2InstanceType(Tools for PowerShell) verwenden, um die unterstützten Startmodi eines Instance-Typs zu ermitteln.

Das folgende Beispiel zeigt, dass `m5.2xlarge` sowohl den Startmodus UEFI als auch den Startmodus Legacy-System BIOS unterstützt.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType m5.2xlarge | Format-List
 InstanceType, SupportedBootModes
```

Erwartete Ausgabe:

```
InstanceType       : m5.2xlarge
SupportedBootModes : {legacy-bios, uefi}
```

Das folgende Beispiel zeigt, dass `t2.xlarge` nur Legacy BIOS unterstützt.

```
Get-EC2InstanceType -Region us-east-1 -InstanceType t2.xlarge | Format-List
 InstanceType, SupportedBootModes
```

Erwartete Ausgabe:

```
InstanceType       : t2.xlarge
SupportedBootModes : {legacy-bios}
```

Den Startmodus einer Instance bestimmen

Der Startmodus einer Instance wird in der Amazon-EC2-Konsole im Feld Startmodus und durch den `currentInstanceBootMode`-Parameter in der AWS CLI angezeigt.

Wenn eine Instance gestartet wird, wird der Wert für ihren Startmodus-Parameter wie folgt durch den Wert des Startmodus-Parameters des zum Start verwendeten AMI bestimmt:

- Ein AMI mit dem Startmodus-Parameter `uefi` erstellt eine Instance mit dem `currentInstanceBootMode`-Parameter `uefi`.

- Ein AMI mit dem Startmodus-Parameter `legacy-bios` erstellt eine Instance mit dem `currentInstanceBootMode`-Parameter `legacy-bios`.
- Ein AMI mit dem Startmodus-Parameter `uefi-preferred` erstellt eine Instance mit dem `currentInstanceBootMode`-Parameter `uefi`, wenn der Instance-Typ UEFI unterstützt; andernfalls erstellt es eine Instance mit einem `currentInstanceBootMode`-Parameter von `legacy-bios`.
- Ein AMI ohne Startmodus-Parameterwert erstellt eine Instance mit einem `currentInstanceBootMode`-Parameterwert, der davon abhängt, ob es sich bei der AMI-Architektur um ARM oder x86 handelt, und vom unterstützten Startmodus des Instance-Typs. Der Standard-Startmodus ist `uefi` für Graviton-Instance-Typen und `legacy-bios` für Intel- und AMD-Instance-Typen.

Console

So ermitteln Sie den Startmodus einer Instance (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Überprüfen Sie auf der Registerkarte Details das Feld Startmodus.

AWS CLI

So ermitteln Sie den Startmodus einer Instance (AWS CLI)

Verwenden Sie den Befehl describe-instances, um den Startmodus einer Instance zu bestimmen. Sie können auch den Startmodus des AMI bestimmen, das zum Erstellen der Instance verwendet wurde.

```
aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0

{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
```

```
                    "ImageId": "ami-0e2063e7f6dc3bee8",
                    "InstanceId": "i-1234567890abcdef0",
                    "InstanceType": "m5.2xlarge",
                    ...
                    },
                "BootMode": "uefi",
                "CurrentInstanceBootMode": "uefi"
            }
        ],
        "OwnerId": "1234567890",
        "ReservationId": "r-1234567890abcdef0"
    }
]
}
```

PowerShell

Um den Startmodus einer Instanz zu ermitteln (Tools for) PowerShell

Verwenden Sie den Cmdlet Get-EC2Image, um den Startmodus einer Instance zu bestimmen. Sie können auch den Startmodus des AMI bestimmen, das zum Erstellen der Instance verwendet wurde.

Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Instance -InstanceId i-1234567890abcdef0).Instances | Format-List BootMode,
 CurrentInstanceBootMode, InstanceType, ImageId

BootMode                : uefi
CurrentInstanceBootMode : uefi
InstanceType            : c5a.large
ImageId                 : ami-0265446f88eb4021b
```

In der Ausgabe beschreiben die folgenden Parameter den Startmodus:

- `BootMode` – Der Startmodus des AMI, das zum Erstellen der Instance verwendet wurde.
- `CurrentInstanceBootMode` – Der Startmodus, der beim Start der Instance verwendet wird.

Bestimmen des Startmodus des Betriebssystems

Der Startmodus des AMI leitet Amazon EC2 an, welcher Startmodus zum Starten einer Instance verwendet werden soll. Um zu sehen, ob das Betriebssystem Ihrer Instanz für UEFI konfiguriert ist, müssen Sie über SSH (Linux-Instanzen) oder RDP (Windows-Instanzen) eine Verbindung zu Ihrer Instance herstellen.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance.

Linux

Ermitteln des Startmodus des Betriebssystems der Instance

1. Stellen Sie eine Verbindung zu Ihrer Linux-Instance mit SSH her.
2. Um den Startmodus des Betriebssystems anzuzeigen, führen Sie einen der folgenden Schritte aus:

   - Führen Sie den folgenden Befehl aus.

     ```
     [ec2-user ~]$ sudo /usr/sbin/efibootmgr
     ```

     Erwartete Ausgabe einer im UEFI-Startmodus gestarteten Instance

     ```
     BootCurrent: 0001
     Timeout: 0 seconds
     BootOrder: 0000,0001
     Boot0000* UiApp
     Boot0001* UEFI Amazon Elastic Block Store vol-xyz
     ```

   - Führen Sie den folgenden Befehl aus, um zu überprüfen, ob das Verzeichnis `/sys/firmware/efi` vorhanden ist. Dieses Verzeichnis ist nur dann vorhanden, wenn die Instance mit UEFI gestartet wird. Wenn das Verzeichnis nicht vorhanden ist, gibt der Befehl `Legacy BIOS Boot Detected` zurück.

     ```
     [ec2-user ~]$ [ -d /sys/firmware/efi ] && echo "UEFI Boot Detected" || echo
      "Legacy BIOS Boot Detected"
     ```

     Erwartete Ausgabe einer im UEFI-Startmodus gestarteten Instance

```
UEFI Boot Detected
```

Erwartete Ausgabe einer im Legacy-System BIOS-Startmodus gestarteten Instance

```
Legacy BIOS Boot Detected
```

- Führen Sie den folgenden Befehl aus, um zu überprüfen, ob EFI in der Ausgabe `dmesg` enthalten ist.

```
[ec2-user ~]$ dmesg | grep -i "EFI"
```

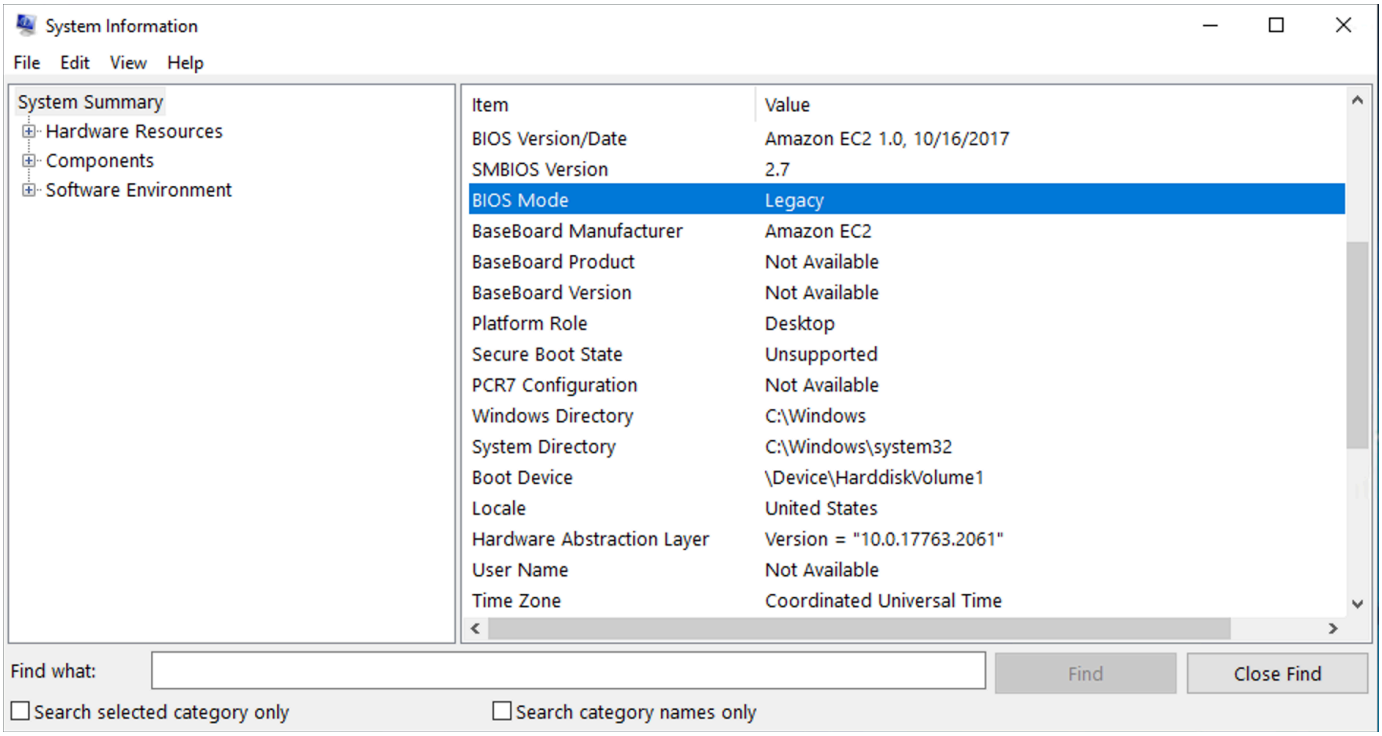
Erwartete Ausgabe einer im UEFI-Startmodus gestarteten Instance

```
[    0.000000] efi: Getting EFI parameters from FDT:
[    0.000000] efi: EFI v2.70 by EDK II
```

Windows

Ermitteln des Startmodus des Betriebssystems der Instance

1. Stellen Sie eine Verbindung mit Ihrer Windows-Instance mithilfe von RDP her.
2. Wechseln Sie zu Systeminformationen und überprüfen Sie die Zeile BIOS-Modus.



Den Startmodus eines AMI festlegen

Wenn Sie ein AMI mit dem Befehl register-image erstellen, können Sie den Startmodus des AMI entweder auf `uefi`, `legacy-bios` oder `uefi-preferred` festlegen.

Wenn der AMI-Startmodus auf `uefi-preferred` gesetzt ist, startet die Instance wie folgt:

- Bei Instance-Typen, die sowohl UEFI als auch Legacy BIOS unterstützen (z. B. `m5.large`), startet die Instance mit UEFI.
- Bei Instance-Typen, die nur Legacy BIOS unterstützen (z. B. `m4.large`), startet die Instance mit Legacy BIOS.

> **Note**
>
> Wenn Sie den AMI-Startmodus auf `uefi-preferred` einstellen, muss das Betriebssystem die Fähigkeit unterstützen, sowohl UEFI als auch Legacy BIOS zu starten.
> Derzeit können Sie den Befehl register-image nicht verwenden, um ein AMI zu erstellen, das sowohl NitroTPM als auch UEFI Preferred unterstützt.

> **Warning**
>
> Einige Features, wie UEFI Secure Boot, sind nur auf Instances verfügbar, die auf UEFI gestartet werden. Wenn Sie den `uefi-preferred`-AMI-Startmodus-Parameter mit einem Instance-Typ verwenden, der UEFI nicht unterstützt, wird die Instance als Legacy-BIOS gestartet und das UEFI-abhängige Feature wird deaktiviert. Wenn Sie auf die Verfügbarkeit eines UEFI-abhängigen Features angewiesen sind, setzen Sie Ihren AMI-Startmodus-Parameter auf `uefi`.

Um eine vorhandene Legacy-System BIOS-basierte Instance in UEFI oder eine vorhandene UEFI-basierte Instance in Legacy-System BIOS zu konvertieren, müssen Sie mehrere Schritte ausführen: Ändern Sie zunächst das Volume und das Betriebssystem der Instance, damit der ausgewählte Startmodus unterstützt wird. Erstellen Sie dann einen Snapshot des Volumes. Verwenden Sie schließlich register-image, um das AMI mithilfe des Snapshots zu erstellen.

Sie können den Startmodus eines AMI nicht mit dem Befehl create-image festlegen. Bei create-image übernimmt das AMI den Startmodus der EC2-Instance, die zum Erstellen des AMI verwendet wird. Wenn Sie beispielsweise ein AMI aus einer EC2-Instance erstellen, die mit Legacy-System BIOS ausgeführt wird, wird der AMI-Startmodus als konfigurier `legacy-bios`. Wenn Sie ein AMI aus einer EC2-Instance erstellen, die mit einem AMI mit einem Startmodus von `uefi-preferred` gestartet wurde, wird auch der Startmodus des erstellten AMI auf `uefi-preferred` gesetzt.

> **Warning**
>
> Durch das Festlegen des AMI-Startmodus-Parameters wird das Betriebssystem nicht automatisch für den angegebenen Startmodus konfiguriert. Bevor Sie mit diesen Schritten fortfahren, müssen Sie zunächst entsprechende Änderungen am Volume und am Betriebssystem der Instance vornehmen, um den Start unter Verwendung des ausgewählten Startmodus zu unterstützen. Andernfalls ist das resultierende AMI nicht verwendbar. Wenn Sie beispielsweise eine ältere BIOS-basierte Windows-Instanz in UEFI konvertieren, können Sie das MBR2GPT-Tool von Microsoft verwenden, um die Systemfestplatte von MBR in GPT zu konvertieren. Die erforderlichen Änderungen sind betriebssystemspezifisch. Weitere Informationen finden Sie im Handbuch zu Ihrem Betriebssystem.

So legen Sie den Startmodus für ein AMI fest (AWS CLI)

1. Nehmen Sie entsprechende Änderungen am Volume und am Betriebssystem der Instance vor, um den Start mit dem ausgewählten Startmodus zu unterstützen. Die erforderlichen Änderungen sind betriebssystemspezifisch. Weitere Informationen finden Sie im Handbuch zu Ihrem Betriebssystem.

   > **Note**
   >
   > Wenn Sie diesen Schritt nicht ausführen, ist das AMI nicht verwendbar.

2. Um die Volume-ID der Instance zu ermitteln, verwenden Sie den Befehl describe-instances. Im nächsten Schritt erstellen Sie einen Snapshot des Volumes.

   ```
   aws ec2 describe-instances --region us-east-1 --instance-ids i-1234567890abcdef0
   ```

   Erwartete Ausgabe

   ```
   ...
               "BlockDeviceMappings": [
                           {
                               "DeviceName": "/dev/sda1",
                               "Ebs": {
                                   "AttachTime": "",
                                   "DeleteOnTermination": true,
                                   "Status": "attached",
                                   "VolumeId": "vol-1234567890abcdef0"
                               }
                           }
                           ...
   ```

3. Um einen Snapshot des Volumes zu erstellen, verwenden Sie den Befehl create-snapshot. Verwenden Sie die Volume-ID aus dem vorherigen Schritt.

   ```
   aws ec2 create-snapshot --region us-east-1 --volume-id vol-1234567890abcdef0 --
   description "add text"
   ```

   Erwartete Ausgabe

   ```
   {
   ```

```
 "Description": "add text",
 "Encrypted": false,
 "OwnerId": "123",
 "Progress": "",
 "SnapshotId": "snap-01234567890abcdef",
 "StartTime": "",
 "State": "pending",
 "VolumeId": "vol-1234567890abcdef0",
 "VolumeSize": 30,
 "Tags": []
}
```

4. Notieren Sie sich die Snapshot-ID in der Ausgabe des vorherigen Schritts.
5. Warten Sie bis die Snapshot-Erstellung `completed` lautet, bevor Sie mit dem nächsten Schritt fortfahren. Um den Status des Snapshots abzufragen, verwenden Sie den Befehl describe-snapshots.

```
aws ec2 describe-snapshots --region us-east-1 --snapshot-ids snap-01234567890abcdef
```

Beispielausgabe

```
{
    "Snapshots": [
        {
            "Description": "This is my snapshot",
            "Encrypted": false,
            "VolumeId": "vol-049df61146c4d7901",
            "State": "completed",
            "VolumeSize": 8,
            "StartTime": "2019-02-28T21:28:32.000Z",
            "Progress": "100%",
            "OwnerId": "012345678910",
            "SnapshotId": "snap-01234567890abcdef",
...
```

6. Verwenden Sie den Befehl register-image, um ein neues AMI zu erstellen. Verwenden Sie die Snapshot-ID, die Sie im vorherigen Schritt notiert haben.

   - Um den Startmodus auf UEFI festzulegen, fügen Sie dem Befehl den Parameter `--boot-mode` hinzu und legen Sie `uefi` als Wert fest.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi
```

- Um den Startmodus auf `uefi-preferred` festzulegen, fügen Sie dem Befehl den Parameter `--boot-mode` hinzu und legen Sie `uefi-preferred` als Wert fest.

```
aws ec2 register-image \
   --region us-east-1 \
   --description "add description" \
   --name "add name" \
   --block-device-mappings "DeviceName=/dev/
sda1,Ebs={SnapshotId=snap-01234567890abcdef,DeleteOnTermination=true}" \
   --architecture x86_64 \
   --root-device-name /dev/sda1 \
   --virtualization-type hvm \
   --ena-support \
   --boot-mode uefi-preferred
```

Erwartete Ausgabe

```
{
"ImageId": "ami-new_ami_123"
}
```

7. Um zu überprüfen, ob das neu erstellte AMI den im vorherigen Schritt angegebenen Startmodus aufweist, verwenden Sie den Befehl describe-images.

```
aws ec2 describe-images --region us-east-1 --image-id ami-new_ami_123
```

Erwartete Ausgabe

```
{
  "Images": [
   {
   "Architecture": "x86_64",
   "CreationDate": "2021-01-06T14:31:04.000Z",
   "ImageId": "ami-new_ami_123",
   "ImageLocation": "",
   ...
   "BootMode": "uefi"
   }
   ]
}
```

8. Starten Sie eine neue Instance mit dem neu erstellten AMI.

   Wenn der AMI-Startmodus `uefi` oder ist `legacy-bios`, haben Instances, die aus diesem AMI erstellt wurden, denselben Startmodus wie das AMI. Wenn der AMI-Startmodus `uefi-preferred` ist, startet die Instance mit UEFI, sofern der Instance-Typ UEFI unterstützt. Andernfalls startet die Instance mit Legacy-BIOS. Weitere Informationen finden Sie unter Überlegungen.
9. Verwenden Sie den Befehl describe-instances, um zu überprüfen, ob die neue Instance den erwarteten Startmodus aufweist.

UEFI-Variablen

Wenn Sie eine Instance starten, für die der Startmodus auf UEFI eingestellt ist, wird eine Schlüssel-Werte-Datenbank für Variablen erstellt. Der Speicher kann von UEFI und dem Instance-Betriebssystem zum Speichern von UEFI-Variablen verwendet werden.

UEFI-Variablen werden vom Bootloader und dem Betriebssystem verwendet, um den frühen System-Startup zu konfigurieren. Sie ermöglichen es dem Betriebssystem, bestimmte Einstellungen des Startvorgangs zu verwalten, wie die Startreihenfolge oder die Verwaltung der Schlüssel für UEFI Secure Boot.

> **Warning**
>
> Jeder, der eine Verbindung zur Instanz herstellen kann (und möglicherweise zu jeder Software, die auf der Instanz ausgeführt wird), oder jeder, der über die Berechtigungen verfügt, die API auf der Instanz zu verwenden, kann die GetInstanceUefiDataVariablen lesen.

Speichern Sie sensible Daten wie Passwörter oder personenbezogene Daten niemals im UEFI-Variablenspeicher.

UEFI-Variablen-Persistenz

- Bei Instances, die an oder vor dem 10. Mai 2022 gestartet wurden, werden UEFI-Variablen beim Neustart oder Stopp gelöscht.
- Bei Instances, die am oder nach dem 11. Mai 2022 gestartet werden, werden UEFI-Variablen, die als nicht flüchtig gekennzeichnet sind, beim Neustart und Stopp/Start beibehalten.
- Bare-Metal-Instances behalten nicht flüchtige UEFI-Variablen über Instance-Stopp-/Start-Vorgänge hinweg nicht bei.

UEFI Secure Boot

UEFI Secure Boot baut auf dem langjährigen sicheren Startprozess von Amazon EC2 auf und bietet zusätzliche Funktionen, mit defense-in-depth denen Kunden Software vor Bedrohungen schützen können, die auch nach Neustarts bestehen. Es stellt sicher, dass die Instance nur Software startet, die mit kryptografischen Schlüsseln signiert ist. Die Schlüssel werden in der Schlüsseldatenbank des UEFI nicht flüchtige Variablenspeicher gespeichert. UEFI Secure Boot verhindert die unbefugte Änderung des Bootflows der Instance.

Themen

- So funktioniert UEFI Secure Boot
- Starten Sie eine Instance mit UEFI Secure Boot-Unterstützung
- Überprüfen Sie, ob eine Instance für UEFI Secure Boot aktiviert ist.
- Erstellen Sie ein Linux-AMI zur Unterstützung von UEFI Secure Boot
- Wie wird der binäre Blob erstellt AWS

So funktioniert UEFI Secure Boot

UEFI Secure Boot ist ein in UEFI spezifiziertes Feature, das eine Überprüfung des Status der Bootchain ermöglicht. Sie soll sicherstellen, dass nach der Selbstinitialisierung der Firmware nur kryptographisch verifizierte UEFI-Binärdateien ausgeführt werden. Zu diesen Binärdateien gehören UEFI-Treiber und der Haupt-Bootloader sowie kettengeladene Komponenten.

UEFI Secure Boot spezifiziert vier wichtige Datenbanken, die in einer Vertrauenskette verwendet werden. Die Datenbanken werden im UEFI-Variablenspeicher gespeichert.

Die Vertrauenskette lautet wie folgt:

Plattformschlüssel (PK)-Datenbank

Die PK-Datenbank ist der Vertrauensanker. Sie enthält einen einzigen öffentlichen PK-Schlüssel, der in der Vertrauenskette zum Aktualisieren der Schlüsselaustausch-Schlüssel (KEK)-Datenbank verwendet wird.

Um die PK-Datenbank zu ändern, benötigen Sie den privaten PK-Schlüssel, um eine Aktualisierungsanforderung zu signieren. Dies beinhaltet das Löschen der PK-Datenbank durch Schreiben eines leeren PK-Schlüssels.

Schlüsselaustausch-Schlüssel (KEK)-Datenbank

Die KEK-Datenbank ist eine Liste öffentlicher KEK-Schlüssel, die in der Vertrauenskette zum Aktualisieren der Signatur (db)- und Deny-Liste (dbx)-Datenbanken verwendet werden.

Um die um die öffentliche KEK-Datenbank zu ändern, benötigen Sie den privaten PK-Schlüssel, um eine Aktualisierungsanforderung zu signieren.

Signatur (db)-Datenbank

Die db-Datenbank ist eine Liste von öffentlichen Schlüsseln und Hashes, die in der Vertrauenskette verwendet werden, um alle UEFI-Boot-Binärdateien zu validieren.

Um die db-Datenbank zu ändern, benötigen Sie den privaten PK-Schlüssel einen der privaten KEK-Schlüssel, um eine Aktualisierungsanforderung zu signieren.

Signatur-Deny-Liste (dbx)-Datenbank

Die dbx-Datenbank ist eine Liste von öffentlichen Schlüsseln und binären Hashes, die nicht vertrauenswürdig sind und in der Vertrauenskette als Widerrufsdatei verwendet werden.

Die dbx-Datenbank hat immer Vorrang vor allen anderen wichtigen Datenbanken.

Um die dbx-Datenbank zu ändern, benötigen Sie den privaten PK-Schlüssel oder einen der privaten KEK-Schlüssel, um eine Aktualisierungsanforderung zu signieren.

Das UEFI-Forum unterhält eine öffentlich zugängliche dbx für viele bekanntermaßen fehlerhafte Binärdateien und Zertifikate unter https://uefi.org/revocationlistfile.

> **Important**
>
> UEFI Secure Boot erzwingt die Signaturvalidierung für alle UEFI-Binärdateien. Um die Ausführung einer UEFI-Binärdatei in UEFI Secure Boot zu erlauben, signieren Sie sie mit einem der oben beschriebenen privaten db-Schlüssel.

Standardmäßig ist UEFI Secure Boot deaktiviert und das System befindet sich im `SetupMode`. Wenn sich das System im `SetupMode` befindet, können alle Schlüsselvariablen ohne kryptografische Signatur aktualisiert werden. Wenn der PK gesetzt ist, ist UEFI Secure Boot aktiviert und der wird beendet. SetupMode

Starten Sie eine Instance mit UEFI Secure Boot-Unterstützung

Wenn Sie mit den folgenden Voraussetzungen eine Instance starten, validiert die Instance die UEFI-Boot-Binärdateien automatisch mit ihrer UEFI Secure Boot-Datenbank. Sie können UEFI Secure Boot auch nach dem Start für eine Instance konfigurieren.

> **Note**
>
> UEFI Secure Boot schützt Ihre Instance und ihr Betriebssystem vor Änderungen im Bootflow. In der Regel ist UEFI Secure Boot als Teil des AMI konfiguriert. Wenn Sie ein neues AMI mit unterschiedlichen Parametern vom Basis-AMI erstellen, z. B. ändern von `UefiData` innerhalb des AMI können Sie UEFI Secure Boot deaktivieren.

Voraussetzungen

Linux-AMIs

Um eine Linux-Instance zu starten, muss für das Linux-AMI UEFI Secure Boot aktiviert sein.

Amazon Linux unterstützt UEFI Secure Boot ab AL2023 Release 2023.1. UEFI Secure Boot ist jedoch in den Standard-AMIs nicht aktiviert. Weitere Informationen finden Sie unter UEFI Secure Boot im AL2023 Benutzerhandbuch. Ältere Versionen von Amazon-Linux-AMIs sind für UEFI Secure Boot nicht aktiviert. Um ein unterstütztes AMI zu verwenden, müssen Sie eine Reihe von Konfigurationsschritten für Ihr eigenes Linux-AMI ausführen. Weitere Informationen finden Sie unter Erstellen Sie ein Linux-AMI zur Unterstützung von UEFI Secure Boot.

Windows-AMIs

Um eine Windows-Instance zu starten, muss für das Windows-AMI UEFI Secure Boot aktiviert sein.

Die folgenden Windows-AMIs sind vorkonfiguriert, um UEFI Secure Boot mit Microsoft-Schlüsseln zu aktivieren:

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Derzeit wird das Importieren von Windows mit UEFI Secure Boot über den Befehl import-image nicht unterstützt.

Instance-Typ

- Unterstützt: Alle virtualisierten Instance-Typen, die UEFI unterstützen, unterstützen auch UEFI Secure Boot. Informationen zu den Instance-Typen, die UEFI Secure Boot unterstützen, finden Sie unter Überlegungen.
- Nicht unterstützt: Bare-Metal-Instance-Typen unterstützen UEFI Secure Boot nicht.

Überprüfen Sie, ob eine Instance für UEFI Secure Boot aktiviert ist.

Linux-Instances

Sie können das `mokutil`-Serviceprogramm verwenden, um zu überprüfen, ob eine Linux Instance für UEFI Secure Boot freigegeben ist. Wenn `mokutil` nicht auf Ihrer Instance installiert ist, müssen Sie es installieren. Die Installationsanweisungen für Amazon Linux 2 finden Sie unterhttps://docs.aws.amazon.com/linux/al2/ug/find-install-software.html. Informationen zu anderen Linux-Distributionen finden Sie in der jeweiligen Dokumentation.

So überprüfen Sie, ob eine Linux-Instance für UEFI Secure Boot aktiviert ist

Führen Sie den folgenden Befehl wie `root` auf Ihrer Instance aus.

```
mokutil --sb-state
```

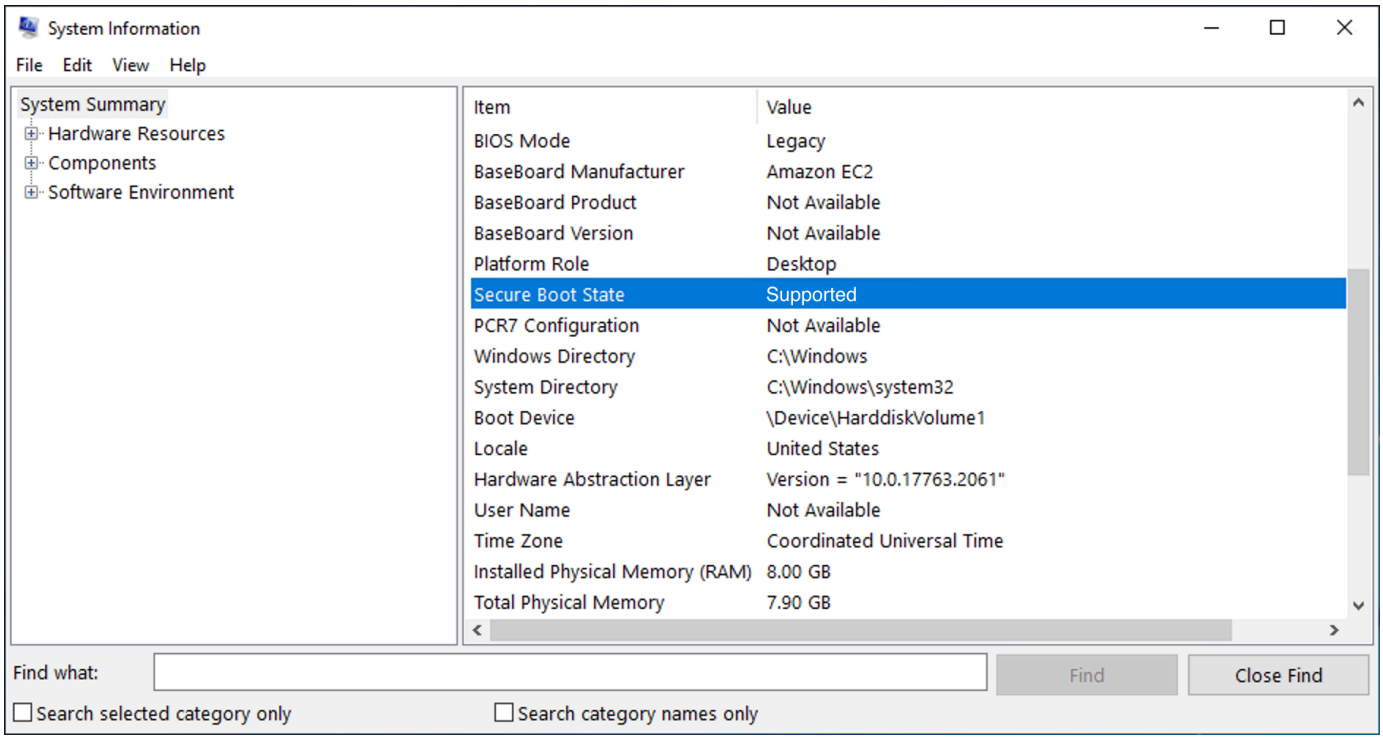
Erwartete Ausgabe:

- Wenn UEFI Secure Boot aktiviert ist, enthält die Ausgabe `SecureBoot enabled`.
- Wenn UEFI Secure Boot nicht aktiviert ist, enthält die Ausgabe `SecureBoot disabled` oder `Failed to read SecureBoot`.

Windows-Instances

So überprüfen Sie, ob eine Windows-Instance für UEFI Secure Boot aktiviert ist

1. Öffnen Sie das msinfo32-Tool.
2. Überprüfen Sie das Feld Secure Boot State (Sicherer Boot-Status). Unterstützt gibt an, dass UEFI Secure Boot aktiviert ist.



Sie können auch das PowerShell Windows-Cmdlet verwenden, `Confirm-SecureBootUEFI` um den Secure Boot-Status zu überprüfen. Weitere Informationen zum Cmdlet finden Sie unter Confirm-SecureBoot UEFI auf der Microsoft-Dokumentationswebsite.

Erstellen Sie ein Linux-AMI zur Unterstützung von UEFI Secure Boot

In den folgenden Verfahren wird beschrieben, wie Sie einen eigenen UEFI-Variablenspeicher für den sicheren Start mit maßgeschneiderten privaten Schlüsseln erstellen. Amazon Linux unterstützt UEFI Secure Boot ab AL2023 Release 2023.1. Weitere Informationen finden Sie unter UEFI Secure Boot im AL2023 Benutzerhandbuch.

> **Important**
>
> Die folgenden Verfahren zum Erstellen eines AMI zur Unterstützung von UEFI Secure Boot sind nur für fortgeschrittene Benutzer gedacht. Sie müssen über ausreichende Kenntnisse im Bootflow der SSL- und Linux-Distribution verfügen, um diese Verfahren verwenden zu können.

Voraussetzungen

- Die folgenden Tools werden verwendet:
  - OpenSSL – https://www.openssl.org/
  - efivar – https://github.com/rhboot/efivar
  - efitools – https://git.kernel.org/pub/scm/linux/kernel/git/jejb/efitools.git/
  - AWS CLI Befehl get-instance-uefi-data
- Ihre Linux-Instance muss mit einem Linux-AMI gestartet worden sein, das den UEFI-Startmodus unterstützt und es müssen nichtflüchtige Daten vorhanden sein.

Neu erstellte Instances ohne UEFI Secure Boot-Schlüssel werden in `SetupMode` erstellt, wodurch Sie Ihre eigenen Schlüssel registrieren können. Einige AMIs sind mit UEFI Secure Boot vorkonfiguriert und Sie können die vorhandenen Schlüssel nicht ändern. Wenn Sie die Schlüssel ändern möchten, müssen Sie ein neues AMI basierend auf dem ursprünglichen AMI erstellen.

Sie haben zwei Möglichkeiten, die Schlüssel im Variablenspeicher zu propagieren, die in den folgenden Optionen A und B beschrieben sind. Option A beschreibt, wie dies innerhalb der Instance geschieht und den Fluss echter Hardware nachahmt. Option B beschreibt, wie ein binäres Blob

erstellt wird, das dann als base64-kodierte Datei übergeben wird, wenn Sie das AMI erstellen. Für beide Optionen müssen Sie zuerst die drei Schlüsselpaare erstellen, die für die Vertrauenskette verwendet werden.

Um ein Linux-AMI zur Unterstützung von UEFI Secure Boot zu erstellen, erstellen Sie zuerst die drei Schlüsselpaare und führen Sie dann entweder Option A oder Option B aus:

- Erstellen von drei Schlüsselpaaren
- Option A: Fügen Sie Schlüssel aus der Instance zum Variablenspeicher hinzu
- Option B: Erstellen Sie ein binäres Blob mit einem vorgefüllten Variablenspeicher

> **Note**
>
> Diese Anweisungen können nur zum Erstellen eines Linux-AMI verwendet werden. Wenn Sie ein Windows-AMI benötigen, verwenden Sie eines der unterstützten Windows-AMIs. Weitere Informationen finden Sie unter Starten Sie eine Instance mit UEFI Secure Boot-Unterstützung.

Erstellen von drei Schlüsselpaaren

UEFI Secure Boot basiert auf den folgenden drei Schlüsseldatenbanken, die in einer Vertrauenskette verwendet werden: dem Plattformschlüssel (PK), dem Schlüsselaustauschschlüssel (KEK) und der Signaturdatenbank (db).[1]

Sie erstellen jeden Schlüssel auf der Instance. Um die öffentlichen Schlüssel in einem Format vorzubereiten, das für den UEFI Secure Boot-Standard gültig ist, erstellen Sie für jeden Schlüssel ein Zertifikat. `DER` definiert das SSL-Format (Binärkodierung eines Formats). Anschließend konvertieren Sie jedes Zertifikat in eine UEFI-Signaturliste, bei der es sich um das Binärformat handelt, das von UEFI Secure Boot verstanden wird. Und schließlich signieren Sie jedes Zertifikat mit dem entsprechenden Schlüssel.

Themen

- Bereiten Sie die Erstellung der Schlüsselpaare vor
- Schlüsselpaar 1: Erstellen Sie den Plattformschlüssel (PK)
- Schlüsselpaar 2: Erstellen Sie den Schlüsselaustauschschlüssel (KEK)
- Schlüsselpaar 3: Erstellen Sie die Signaturdatenbank (db)

- Signieren Sie das Boot-Image (Kernel) mit dem privaten Schlüssel.

Bereiten Sie die Erstellung der Schlüsselpaare vor

Erstellen Sie vor dem Erstellen der Schlüsselpaare einen global eindeutigen Bezeichner (GUID), der bei der Schlüsselgenerierung verwendet werden soll.

1. Stellen Sie eine Verbindung zur Instance her.
2. Führen Sie in der Eingabeaufforderung einen Shell-Befehl aus.

```
uuidgen --random > GUID.txt
```

Schlüsselpaar 1: Erstellen Sie den Plattformschlüssel (PK)

Der PK ist der Vertrauensanker für UEFI Secure Boot-Instances. Die private PK wird verwendet, um den KEK zu aktualisieren, der wiederum dazu verwendet werden kann, autorisierte Schlüssel zur Signaturdatenbank (db) hinzuzufügen.

Der X.509-Standard wird zum Erstellen des Schlüsselpaars verwendet. Informationen zum Standard finden Sie unter X.509 auf Wikipedia.

So erstellen Sie den PK

1. Erstellen Sie den Schlüssel. Sie müssen die Variable PK benennen.

```
openssl req -newkey rsa:4096 -nodes -keyout PK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Platform key/" -out PK.crt
```

   Die folgenden Parameter werden angegeben:

   - `-keyout PK.key` – Die private Schlüsseldatei.
   - `-days 3650` – Die Anzahl der Tage, an denen das Zertifikat gültig ist.
   - `-out PK.crt` – Das Zertifikat, das zum Erstellen der UEFI-Variablen verwendet wird.
   - `CN=Platform key` – Der gemeinsame Name (common name, CN) für den Schlüssel. Sie können den Namen Ihrer eigenen Organisation eingeben anstatt des *Plattformschlüssels*.
2. Erstellen Sie das Zertifikat.

```
openssl x509 -outform DER -in PK.crt -out PK.cer
```

3. Wandeln Sie das Zertifikat in eine UEFI-Signaturliste um.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" PK.crt PK.esl
```

4. Signieren Sie die UEFI-Signaturliste mit dem privaten PK (selbstsigniert).

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt PK PK.esl PK.auth
```

Schlüsselpaar 2: Erstellen Sie den Schlüsselaustauschschlüssel (KEK)

Der private KEK wird verwendet, um Schlüssel zur Datenbank hinzuzufügen, was die Liste der autorisierten Signaturen darstellt, die im System gestartet werden sollen.

So erstellen Sie den KEK

1. Erstellen Sie den Schlüssel.

```
openssl req -newkey rsa:4096 -nodes -keyout KEK.key -new -x509 -sha256 -days 3650 -
subj "/CN=Key Exchange Key/" -out KEK.crt
```

2. Erstellen Sie das Zertifikat.

```
openssl x509 -outform DER -in KEK.crt -out KEK.cer
```

3. Wandeln Sie das Zertifikat in eine UEFI-Signaturliste um.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" KEK.crt KEK.esl
```

4. Signieren Sie die Signaturliste mit dem privaten PK.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k PK.key -c PK.crt KEK KEK.esl KEK.auth
```

Schlüsselpaar 3: Erstellen Sie die Signaturdatenbank (db)

Die db-Liste enthält autorisierte Schlüssel, die zum Booten auf dem System autorisiert sind. Um die Liste zu ändern, ist der private KEK erforderlich. Boot-Images werden mit dem privaten Schlüssel signiert, der in diesem Schritt erstellt wird.

So erstellen Sie den db

1. Erstellen Sie den Schlüssel.

```
openssl req -newkey rsa:4096 -nodes -keyout db.key -new -x509 -sha256 -days 3650 -
subj "/CN=Signature Database key/" -out db.crt
```

2. Erstellen Sie das Zertifikat.

```
openssl x509 -outform DER -in db.crt -out db.cer
```

3. Wandeln Sie das Zertifikat in eine UEFI-Signaturliste um.

```
cert-to-efi-sig-list -g "$(< GUID.txt)" db.crt db.esl
```

4. Signieren Sie die Signaturliste mit dem privaten KEK.

```
sign-efi-sig-list -g "$(< GUID.txt)" -k KEK.key -c KEK.crt db db.esl db.auth
```

Signieren Sie das Boot-Image (Kernel) mit dem privaten Schlüssel.

Für Ubuntu 22.04 erfordern die folgenden Images Signaturen.

```
/boot/efi/EFI/ubuntu/shimx64.efi
/boot/efi/EFI/ubuntu/mmx64.efi
/boot/efi/EFI/ubuntu/grubx64.efi
/boot/vmlinuz
```

So signieren Sie ein Image

Verwenden Sie die folgende Syntax, um ein Image zu signieren.

```
sbsign --key db.key --cert db.crt --output /boot/vmlinuz /boot/vmlinuz
```

> **Note**
>
> Sie müssen alle neuen Kernel signieren. `/boot/vmlinuz` wird normalerweise einen Link zum zuletzt installierten Kernel führen.

In der Dokumentation Ihrer Distribution erfahren Sie mehr über Ihre Bootchain und die erforderlichen Images.

[1] Vielen Dank an die ArchWiki Community für all die Arbeit, die sie geleistet hat. Die Befehle zum Erstellen des PK, zum Erstellen des KEK, zum Erstellen der Datenbank und zum Signieren des Images stammen aus Creating keys und wurden vom ArchWiki Wartungsteam und/oder den ArchWiki Mitwirkenden verfasst.

Option A: Fügen Sie Schlüssel aus der Instance zum Variablenspeicher hinzu

Nachdem Sie die drei Schlüsselpaare erstellt haben, können Sie eine Verbindung zu Ihrer Instance herstellen und die Schlüssel innerhalb der Instance zum Variablenspeicher hinzufügen, indem Sie die folgenden Schritte ausführen.

Option A Schritte:

- Schritt 1: Starten Sie eine Instance mit UEFI Secure Boot-Unterstützung
- Schritt 2: Konfigurieren Sie eine Instance zur Unterstützung von UEFI Secure Boot
- Schritt 3: Erstellen eines AMI Ihrer Instance

Schritt 1: Starten Sie eine Instance mit UEFI Secure Boot-Unterstützung

Wenn Sie mit den folgenden Voraussetzungen eine Instance starten, kann die Instance dann für die Unterstützung von UEFI Secure Boot konfiguriert werden. Sie können die Unterstützung für UEFI Secure Boot nur für eine Instance beim Start aktivieren; Sie können sie später nicht aktivieren.

Voraussetzungen

- AMI – Das Linux-AMI muss den UEFI-Startmodus unterstützen. Um zu überprüfen, ob das AMI den UEFI-Startmodus unterstützt, muss der AMI-Startmodus-Parameter uefi sein. Weitere Informationen finden Sie unter Den Startmodus-Parameter für ein AMI bestimmen.

  Beachten Sie, dass AWS nur Linux-AMIs zur Verfügung stehen, die so konfiguriert sind, dass sie UEFI für Graviton-basierte Instance-Typen unterstützen. AWS stellt derzeit keine x86_64-

Linux-AMIs bereit, die den UEFI-Startmodus unterstützen. Sie können Ihr eigenes AMI so konfigurieren, dass es den UEFI-Boot-Modus für alle Architekturen unterstützt. Um ein Ihren eigenes AMI für die Unterstützung des UEFI-Startmodus zu konfigurieren, müssen Sie eine Reihe von Konfigurationsschritten auf Ihrem eigenen AMI durchführen. Weitere Informationen finden Sie unter Den Startmodus eines AMI festlegen.

- Instance-Typ – Alle virtualisierten Instance-Typen, die UEFI unterstützen, unterstützen auch UEFI Secure Boot. Bare-Metal-Instance-Typen unterstützen UEFI Secure Boot nicht. Informationen zu den Instance-Typen, die UEFI Secure Boot unterstützen, finden Sie unter Überlegungen.
- Starten Sie Ihre Instance nach dem Veröffentlichen von UEFI Secure Boot. Nur Instances, die nach dem 10. Mai 2022 (als UEFI Secure Boot veröffentlicht wurde) gestartet wurden, können UEFI Secure Boot unterstützen.

Nachdem Sie Ihre Instance gestartet haben, können Sie überprüfen, ob sie für die Unterstützung von UEFI Secure Boot konfiguriert werden kann (mit anderen Worten, Sie können mit Schritt 2 fortfahren), indem Sie prüfen, ob UEFI-Daten vorhanden sind. Das Vorhandensein von UEFI-Daten weist darauf hin, dass nichtflüchtige Daten beibehalten werden.

So überprüfen Sie, ob die Instance für Schritt 2 bereit ist

Verwenden Sie den Befehl get-instance-uefi-data und geben Sie die Instance-ID an.

```
aws ec2 get-instance-uefi-data --instance-id i-0123456789example
```

Die Instance ist bereit für Schritt 2, wenn UEFI-Daten in der Ausgabe vorhanden sind. Wenn die Ausgabe leer ist, kann die Instance nicht für die Unterstützung von UEFI Secure Boot konfiguriert werden. Dies kann passieren, wenn Ihre Instance gestartet wurde, bevor die UEFI Secure Boot-Unterstützung verfügbar wurde. Starten Sie eine neue Instance und versuchen Sie es erneut.

Schritt 2: Konfigurieren Sie eine Instance zur Unterstützung von UEFI Secure Boot

Registrieren Sie die Schlüsselpaare in Ihrem UEFI-Variablenspeicher in der Instance

> **Warning**
>
> Sie müssen Ihre Boot-Images signieren, nachdem Sie die Schlüssel registriert haben, sonst können Sie Ihre Instance nicht starten.

Nachdem Sie die signierten UEFI-Signaturlisten (`PK`, `KEK` und `db`) erstellt haben, müssen sie bei der UEFI-Firmware registriert sein.

Schreiben in der `PK`-Variablen ist nur möglich, wenn:

- Es ist noch keine PK angemeldet, was angegeben wird, wenn die `SetupMode`Variable `1` ist. Prüfen Sie dies mit dem folgenden Befehl: Die Ausgabe ist entweder `1` oder `0`.

  ```
  efivar -d -n 8be4df61-93ca-11d2-aa0d-00e098032b8c-SetupMode
  ```

- Die neue PK ist durch den privaten Schlüssel der bestehenden PK signiert.

So melden Sie die Schlüssel in Ihrem UEFI-Variablenspeicher an

Die folgenden Befehle müssen in der Instance ausgeführt werden.

Wenn aktiviert SetupMode ist (der Wert ist1), können die Schlüssel registriert werden, indem die folgenden Befehle auf der Instance ausgeführt werden:

```
[ec2-user ~]$ efi-updatevar -f db.auth db
```

```
[ec2-user ~]$ efi-updatevar -f KEK.auth KEK
```

```
[ec2-user ~]$ efi-updatevar -f PK.auth PK
```

So überprüfen Sie, ob UEFI Secure Boot aktiviert ist

Führen Sie die Schritte unter Überprüfen Sie, ob eine Instance für UEFI Secure Boot aktiviert ist. aus, um zu überprüfen, ob UEFI Secure Boot aktiviert ist.

Sie können Ihren UEFI-Variablenspeicher jetzt mit dem CLI-Befehl get-instance-uefi-data exportieren oder mit dem nächsten Schritt fortfahren und Ihre Boot-Images signieren, um sie in einer UEFI Secure Boot-fähigen Instance neu zu starten.

Schritt 3: Erstellen eines AMI Ihrer Instance

Um ein AMI von der Instance zu erstellen, können Sie die Konsole oder `CreateImage`-API, CLI oder SDKs verwenden. Informationen zur Verwendung der Konsole finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI. Die API-Anweisungen finden Sie unter CreateImage.

> **Note**
>
> Die `CreateImage`-API kopiert den UEFI-Variablenspeicher der Instance automatisch in das AMI. Die Konsole verwendet die `CreateImage`-API. Nachdem Sie Instances mit diesem AMI gestartet haben, haben die Instances denselben UEFI-Variablenspeicher.

Option B: Erstellen Sie ein binäres Blob mit einem vorgefüllten Variablenspeicher

Nachdem Sie die drei Schlüsselpaare erstellt haben, können Sie ein binäres Blob erstellen, das einen vorgefüllten Variablenspeicher enthält, der die UEFI Secure Boot-Schlüssel enthält.

> **Warning**
>
> Sie müssen Ihre Boot-Images signieren, bevor Sie die Schlüssel registrieren, sonst können Sie Ihre Instance nicht starten.

Option B Schritte:

- Schritt 1: Erstellen Sie einen neuen Variablenspeicher oder aktualisieren Sie einen vorhandenen
- Schritt 2: Hochladen des binären Blobs bei der AMI-Erstellung

Schritt 1: Erstellen Sie einen neuen Variablenspeicher oder aktualisieren Sie einen vorhandenen

Sie können den Variablenspeicher offline ohne eine laufende Instance erstellen, indem Sie das Python-Uefivars-Tool verwenden. Das Tool kann aus Ihren Schlüsseln einen neuen Variablenspeicher erstellen. Das Skript unterstützt derzeit das EDK2-Format, das AWS Format und eine JSON-Darstellung, die mit Tools auf höherer Ebene einfacher zu bearbeiten ist.

So erstellen Sie den Variablenspeicher offline ohne laufende Instance

1. Laden Sie das Tool unter folgendem Link herunter.

   ```
   https://github.com/awslabs/python-uefivars
   ```

2. Erstellen Sie einen neuen Variablenspeicher von Ihren Schlüsseln, indem Sie den folgenden Befehl ausführen. Dies wird ein base64-kodiertes binäres Blob in *`ihr_binäres_blob`*.bin erstellen. Das Tool unterstützt auch das Aktualisieren eines binären Blobs über die `-I`-Parameter.

```
./uefivars.py -i none -o aws -O your_binary_blob.bin -P PK.esl -K KEK.esl --db
 db.esl --dbx dbx.esl
```

Schritt 2: Hochladen des binären Blobs bei der AMI-Erstellung

Verwenden Sie register-image um Ihre UEFI-Variablenspeicherdaten zu übergeben. Geben Sie für den Parameter `--uefi-data` geben Sie Ihr binäres Blob an, und geben Sie für den Parameter `--boot-mode uefi` an.

```
aws ec2 register-image \
    --name uefi_sb_tpm_register_image_test \
    --uefi-data $(cat your_binary_blob.bin) \
    --block-device-mappings "DeviceName=/dev/sda1,Ebs=
 {SnapshotId=snap-0123456789example,DeleteOnTermination=true}" \
    --architecture x86_64 \
    --root-device-name /dev/sda1 \
    --virtualization-type hvm \
    --ena-support \
    --boot-mode uefi
```

Wie wird der binäre Blob erstellt AWS

Sie können die folgenden Schritte ausführen, um die UEFI Secure Boot-Variablen während der AMI-Erstellung anzupassen. Der KEK, der in diesen Schritten verwendet wird, ist auf dem Stand von September 2021. Wenn Microsoft den KEK aktualisiert, müssen Sie den neuesten KEK verwenden.

Um den AWS binären Blob zu erstellen

1. Erstellen Sie eine leere PK-Signaturliste.

   ```
   touch empty_key.crt
   cert-to-efi-sig-list empty_key.crt PK.esl
   ```

2. Laden Sie die KEK-Zertifikate herunter.

   ```
   https://go.microsoft.com/fwlink/?LinkId=321185
   ```

3. Verpacken Sie die KEK-Zertifikate in einer UEFI-Signaturliste (`siglist`).

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_KEK.esl MicCorKEKCA2011_2011-06-24.crt
```

4. Laden Sie Microsofts DB-Zertifikate herunter.

```
https://www.microsoft.com/pkiops/certs/MicWinProPCA2011_2011-10-19.crt
https://www.microsoft.com/pkiops/certs/MicCorUEFCA2011_2011-06-27.crt
```

5. Generieren Sie die DB-Signaturliste.

```
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_Win_db.esl MicWinProPCA2011_2011-10-19.crt
sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --output
 MS_UEFI_db.esl MicCorUEFCA2011_2011-06-27.crt
cat MS_Win_db.esl MS_UEFI_db.esl > MS_db.esl
```

6. Laden Sie eine aktualisierte dbx-Änderungsanforderung über den folgenden Link herunter.

```
https://uefi.org/revocationlistfile
```

7. Die dbx-Änderungsanforderung, die Sie im vorherigen Schritt heruntergeladen haben, ist bereits mit Microsoft-KEK signiert, daher müssen Sie sie entfernen oder entpacken. Sie können die folgenden Links verwenden.

```
https://gist.github.com/out0xb2/f8e0bae94214889a89ac67fceb37f8c0
```

```
https://support.microsoft.com/en-us/topic/microsoft-guidance-for-applying-secure-
boot-dbx-update-e3b9e4cb-a330-b3ba-a602-15083965d9ca
```

8. Erstellen Sie einen UEFI-Variablenspeicher mit dem `uefivars.py`-Skript.

```
./uefivars.py -i none -o aws -O uefiblob-microsoft-keys-empty-pk.bin -P ~/PK.esl -K
 ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx ~/dbx-2021-April.bin
```

9. Prüfen Sie das binäre Blob und den UEFI-Variablenspeicher.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o json | less
```

10. Sie können das Blob aktualisieren, indem Sie es erneut an dasselbe Tool übergeben.

```
./uefivars.py -i aws -I uefiblob-microsoft-keys-empty-pk.bin -o aws -O uefiblob-
microsoft-keys-empty-pk.bin -P ~/PK.esl -K ~/MS_Win_KEK.esl --db ~/MS_db.esl  --dbx
 ~/dbx-2021-April.bin
```

Erwartete Ausgabe

```
Replacing PK
Replacing KEK
Replacing db
Replacing dbx
```

Suchen eines AMI

Ein AMI umfasst die Komponenten und Anwendungen, wie das Betriebssystem und den Typ des Root-Volumes, die zum Starten einer Instance erforderlich sind. Um eine Instance zu starten, die Ihren Anforderungen entspricht, müssen Sie ein AMI finden, das Ihren Anforderungen entspricht.

Beachten Sie bei der Auswahl eines AMI die folgenden Anforderungen, die Sie möglicherweise für die Instances haben, die Sie starten möchten:

- Die Region — AMI-IDs sind für jede AWS Region einzigartig.
- Das Betriebssystem
- Die Architektur: 32-Bit- (`i386`), 64-Bit- (`x86_64`) oder 64-Bit-ARM (`arm64`)
- Der Root-Gerätetyp: Amazon EBS oder Instance-Speicher
- Der Provider (z. B. Amazon Web Services)
- Zusätzliche Software (z. B. SQL Server)

Es gibt verschiedene Möglichkeiten, ein AMI zu finden, das Ihren Anforderungen entspricht. In diesem Thema wird beschrieben, wie Sie mithilfe der Amazon EC2 EC2-Konsole, AWS CLI AWS Tools for Windows PowerShell, und AWS Systems Manager ein AMI finden.

Themen

- Finden Sie ein AMI mithilfe eines Systems Manager Manager-Parameters
- Finden Sie die neuesten AMIs mit Systems Manager
- Weitere Informationen zum Auffinden von AMIs

Finden Sie mithilfe der Amazon EC2 EC2-Konsole ein AMI

Sie können AMIs über die Amazon EC2 EC2-Konsole finden. Sie können in der Liste der AMIs auswählen, wenn Sie zum Instance-Start den Launch Instance Wizard verwenden oder alle verfügbaren AMIs auf der Seite Images durchsuchen.

So suchen Sie mit dem Launch-Instance-Assistenten nach einem AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen. AMI-IDs sind für jede AWS Region einzigartig.
3. Wählen Sie im Dashboard der Konsole die Option Launch Instance aus.
4. (Neue Konsole) Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) die OptionQuick Start (Schnellstart) aus. Wählen Sie das Betriebssystem für Ihre Instance aus und anschließend eines der gängigen AMIs aus der Liste unter Amazon Machine Image (AMI). Wenn das richtige AMI nicht angezeigt wird, können Sie Browser more AMIs (Weitere AMIs durchsuchen) auswählen, um den vollständigen AMI-Katalog zu durchsuchen. Weitere Informationen finden Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image).

   (Alte Konsole) Wählen Sie auf der Registerkarte Quick Start (Schnellstart) eines der am häufigsten genutzten AMIs in der Liste aus. Wenn das von Ihnen benötigte AMI nicht angezeigt wird, wählen Sie die Registerkarte My AMIs (Meine AMIs), AWS Marketplace oder Community AMIs (Community-AMIs) aus, um weitere AMIs zu finden. Weitere Informationen finden Sie unter Schritt 1: Auswählen eines Amazon Machine Images (AMI).

So suchen Sie auf der AMI-Seite nach einem AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen. AMI-IDs sind für jede AWS Region einzigartig.
3. Wählen Sie im Navigationsbereich die Option AMIs.
4. Mit den Optionen Filter und Search (Suche) können Sie die angezeigten AMIs so eingrenzen, dass nur die angezeigt werden, die Ihren Kriterien entsprechen.

   Um beispielsweise alle AMIs aufzulisten, die von bereitgestellt werden AWS, wählen Sie Öffentliche Images aus. Nutzen Sie dann die Optionen von Search (Suche), um die Liste der angezeigten AMIs weiter anzupassen. Wählen Sie die Suchleiste aus und anschließend im Menü Owner alias (Besitzeralias), dann den Operator = und den Wert amazon. Um nach AMIs zu suchen, die einer bestimmten Plattform entsprechen, z. B. Linux oder Windows, wählen Sie erneut in der Suchleiste Plattform, dann den Operator = und dann das Betriebssystem aus der bereitgestellten Liste.
5. (Optional) Wählen Sie das Symbol Einstellungen, um auszuwählen, welche Image-Attribute angezeigt werden sollen, z. B. der Root-Gerätetyp. Alternativ können Sie ein AMI in der Liste auswählen und seine Eigenschaften auf der Registerkarte Details anzeigen.
6. Bevor Sie ein AMI auswählen, müssen Sie Folgendes beachten: Sie müssen wissen, ob das AMI durch Instance-Speicher oder Amazon EBS gestützt ist, und die Auswirkungen dieses Unterschieds kennen. Weitere Informationen finden Sie unter Speicher für das Root-Gerät.
7. Um eine Instance von diesem AMI zu starten, wählen Sie sie aus und wählen Sie dann Instance von Image starten. Informationen zum Starten einer Instance über die Konsole finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard. Wenn Sie die Instance nicht sofort starten möchten, notieren Sie sich die AMI-ID für später.

Finden Sie ein AMI mit dem AWS CLI

Sie können den AWS CLI Befehl describe-images verwenden, um nur die AMIs aufzulisten, die Ihren Anforderungen entsprechen. Nachdem Sie ein AMI für Ihre Anforderungen gefunden haben, notieren Sie seine ID, um sie zum Starten von Instances verwenden können. Weitere Informationen zum Starten Ihrer Instance finden Sie im AWS Command Line Interface -Benutzerhandbuch.

Der Befehl describe-images unterstützt Filterparameter. Verwenden Sie beispielsweise den Parameter `--owners`, um öffentliche AMIs anzuzeigen, die Amazon gehören.

```
aws ec2 describe-images --owners amazon
```

Sie können dem vorherigen Befehl den folgenden Filter hinzufügen, um ausschließlich Windows-AMIs anzuzeigen.

```
--filters "Name=platform,Values=windows"
```

Sie können dem vorherigen Befehl den folgenden Filter hinzufügen, um ausschließlich AMIs anzuzeigen, die mit Amazon EBS gestützt sind:

```
--filters "Name=root-device-type,Values=ebs"
```

> **Important**
>
> Wenn Sie den `--owners` Parameter im `describe-images` Befehl weglassen, werden alle Images zurückgegeben, für die Sie Startberechtigungen haben, unabhängig von der Eigentümerschaft.

Finden Sie ein AMI mit dem AWS Tools for Windows PowerShell

Sie können PowerShell Cmdlets verwenden, um nur die Windows-AMIs aufzulisten, die Ihren Anforderungen entsprechen. Informationen und Beispiele finden Sie unter Find an Amazon Machine Image Using Windows PowerShell im AWS Tools for Windows PowerShell Benutzerhandbuch.

Nachdem Sie ein AMI für Ihre Anforderungen gefunden haben, notieren Sie seine ID, um sie zum Starten von Instances verwenden können. Weitere Informationen finden Sie im AWS Tools for Windows PowerShell Benutzerhandbuch unter Starten einer Amazon EC2 EC2-Instance mit Windows PowerShell.

Finden Sie ein AMI mithilfe eines Systems Manager Manager-Parameters

Wenn Sie eine Instance mit dem EC2-Instance-Startassistenten in der Amazon EC2 EC2-Konsole starten, können Sie entweder ein AMI aus der Liste auswählen (beschrieben unterFinden Sie mithilfe der Amazon EC2 EC2-Konsole ein AMI) oder Sie können einen AWS Systems Manager Parameter auswählen, der auf eine AMI-ID verweist (in diesem Abschnitt beschrieben). Wenn Sie Automatisierungscode zum Starten Ihrer Instances verwenden, können Sie den Systems Manager-Parameter anstelle der AMI-ID angeben.

Ein Systems Manager-Parameter ist ein vom Kunden definiertes Schlüssel-Wert-Paar, das Sie in Systems Manager Parameterspeicher erstellen können. Der Parameterspeicher bietet

einen zentralen Speicher zur Auslagerung Ihrer Anwendungskonfigurationswerte. Weitere Informationen finden Sie unter AWS Systems Manager Parameter Store im AWS Systems Manager Benutzerhandbuch zu .

Wenn Sie einen Parameter erstellen, der auf eine AMI-ID verweist, stellen Sie sicher, dass Sie den Datentyp als `aws:ec2:image` angeben. Die Angabe dieses Datentyps stellt sicher, dass beim Erstellen oder Ändern des Parameters der Parameterwert als AMI-ID validiert wird. Weitere Informationen finden Sie unter Unterstützung für native Parameter für Amazon Machine Image-IDs im Benutzerhandbuch zu AWS Systems Manager .

Themen

Anwendungsfälle

Wenn Sie Systems-Manager-Parameter verwenden, die auf AMI-IDs zu verweisen, können Ihre Benutzer beim Starten von Instances das richtige AMI einfacher auswählen. System-Manager-Parameter können auch die Verwaltung von Automatisierungscode vereinfachen.

Benutzerfreundlicher

Wenn Instances unter Verwendung eines bestimmten AMI gestartet werden müssen und dieses AMI regelmäßig aktualisiert wird, empfehlen wir, dass Ihre Benutzer einen Systems-Manager-Parameter auswählen müssen, um das AMI zu finden. Indem Sie erforderlich machen, dass Ihre Benutzer einen Systems-Manager-Parameter auswählen, wird sichergestellt, dass beim Starten von Instances das neueste AMI verwendet wird.

Beispielsweise könnten Sie in Ihrer Organisation jeden Monat eine neue Version Ihres AMIs erstellen, das die neuesten Betriebssystem- und Anwendungs-Patches enthält. Außerdem müssen Ihre Benutzer Instances mit der neuesten Version Ihres AMIs starten. Um sicherzustellen, dass Ihre Benutzer die neueste Version verwenden, können Sie einen Systems Manager-Parameter (z. B. `golden-ami`) erstellen, der auf die korrekte AMI-ID verweist. Jedes Mal, wenn eine neue Version des AMIs erstellt wird, aktualisieren Sie den AMI-ID-Wert im Parameter, sodass er immer auf das neueste AMI verweist. Ihre Benutzer brauchen nichts von den regelmäßigen Updates des AMI zu wissen, da sie weiterhin jedes Mal denselben Systems-Manager-Parameter auswählen. Die

Verwendung eines Systems-Manager-Parameters für Ihr AMI erleichtert ihnen die Auswahl des richtigen AMI für den Start einer Instance.

Vereinfachen Sie die automatisierte Codepflege

Wenn Sie Automatisierungscode zum Starten Ihrer Instances verwenden, können Sie den Systems Manager-Parameter anstelle der AMI-ID angeben. Wenn eine neue Version des AMI erstellt wird, können Sie den AMI-ID-Wert im Parameter so ändern, dass er auf das neueste AMI verweist. Der Automatisierungscode, der auf den Parameter verweist, muss nicht jedes Mal geändert werden, wenn eine neue Version des AMI erstellt wird. Das vereinfacht die Wartung der Automatisierung und trägt zur Senkung der Bereitstellungskosten bei.

> **Note**
>
> Laufende Instances sind nicht betroffen, wenn Sie die AMI-ID ändern, auf die der Systems-Manager-Parameter verweist.

Berechtigungen

Wenn Sie im Launch-Instance-Assistenten Systems Manager Manager-Parameter verwenden, die auf AMI-IDs verweisen, müssen Sie Ihrer IAM-Richtlinie die folgenden Berechtigungen hinzufügen:

- `ssm:DescribeParameters`— Erteilt die Berechtigung zum Anzeigen und Auswählen von Systems Manager Manager-Parametern.
- `ssm:GetParameters`— Erteilt die Berechtigung zum Abrufen der Werte der Systems Manager Manager-Parameter.

Sie können auch den Zugriff auf bestimmte Systems Manager-Parameter beschränken. Weitere Informationen und Beispiele für IAM-Richtlinien finden Sie unterBeispiel: Verwenden des EC2 Launch Instance Wizard.

Einschränkungen

AMIs und Systems Manager-Parameter sind regionsspezifisch. Um denselben Systems Manager-Parameternamen in allen Regionen zu verwenden, erstellen Sie in jeder Region einen Systems Manager-Parameter mit demselben Namen (z. B. `golden-ami`). Verweisen Sie in jeder Region mit dem Parameter Systems Manager auf ein AMI in dieser Region.

Starten einer Instance mit einem Systems Manager-Parameter

Sie können eine Instance über die Konsole oder die AWS CLI starten. Anstatt eine AMI-ID anzugeben, können Sie einen AWS Systems Manager Parameter angeben, der auf eine AMI-ID verweist.

New console

So suchen Sie ein AMI mithilfe eines Systems Manager Manager-Parameters (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen.
3. Wählen Sie im Dashboard der Konsole die Option Launch Instance aus.
4. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) die Option Browse more AMIs (Weitere AMIs durchsuchen) aus.
5. Wählen Sie die Pfeilschaltfläche rechts neben der Suchleiste und dann Search by Systems Manager parameter (Nach Systems-Manager-Parameter suchen) aus.
6. Wählen Sie für Systems Manager-Parameter einen Parameter aus. Die entsprechende AMI-ID wird unter Currently resolves to (Wird derzeit aufgelöst in) angezeigt.
7. Wählen Sie Search (Suchen) aus. Die AMIs, die der AMI-ID entsprechen, erscheinen in der Liste.
8. Wählen Sie die AMI aus der Liste und wählen Sie Select (Auswählen).

Weitere Informationen über das Starten einer Instance mithilfe des Launch Instance Wizard finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Old console

So suchen Sie ein AMI mithilfe eines Systems Manager Manager-Parameters (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen.
3. Wählen Sie im Dashboard der Konsole die Option Launch Instance aus.

4. Wählen Sie Search by Systems Manager parameter (Suchen nach Systems Manager-Parameter) (oben rechts).
5. Wählen Sie für Systems Manager-Parameter einen Parameter aus. Die entsprechende AMI-ID erscheint neben Currently resolves to (Gegenwärtig aufgelöst nach).
6. Wählen Sie Search (Suchen) aus. Die AMIs, die der AMI-ID entsprechen, erscheinen in der Liste.
7. Wählen Sie die AMI aus der Liste und wählen Sie Select (Auswählen).

Weitere Informationen über das Starten einer Instance über ein AMI mithilfe des Launch Instance Wizard finden Sie unter Schritt 1: Auswählen eines Amazon Machine Images (AMI).

Um eine Instance mit einem AWS Systems Manager Parameter anstelle einer AMI-ID zu starten (AWS CLI)

Das folgende Beispiel verwendet den Systems Manager-Parameter `golden-ami`, um eine `m5.xlarge`-Instance zu starten. Der Parameter verweist auf eine AMI-ID.

Um den Parameter im Befehl anzugeben, verwenden Sie die folgende Syntax: `resolve:ssm:/`*`parameter-name`*, wobei `resolve:ssm` das Standardpräfix und `parameter-name` der eindeutige Parametername ist. Beachten Sie die Groß-/Kleinschreibung des Parameternamens. Umgekehrte Schrägstriche für den Parameternamen sind nur erforderlich, wenn der Parameter Teil einer Hierarchie ist, z. B, `/amis/production/golden-ami`. Sie können den umgekehrten Schrägstrich weglassen, wenn der Parameter nicht Teil einer Hierarchie ist.

In diesem Beispiel sind die Parameter `--count` und `--security-group` nicht enthalten. Der Standardwert für `--count` lautet 1. Wenn Sie über eine Standard-VPC und eine Standardsicherheitsgruppe verfügen, werden diese verwendet.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami
    --instance-type m5.xlarge
    ...
```

Um eine Instance mit einer bestimmten Version eines AWS Systems Manager Parameters (AWS CLI) zu starten

Systems Manager-Parameter bieten Versionsunterstützung. Jeder Iteration eines Parameters wird eine eindeutige Versionsnummer zugewiesen. Sie können die Version des Parameters wie

folgt referenzieren: `resolve:ssm:`*`parameter-name`*`:`*`version`*, wobei `version` die eindeutige Versionsnummer ist. Standardmäßig wird die neueste Version des Parameters verwendet, wenn keine Version angegeben ist.

Das folgende Beispiel verwendet Version 2 des Parameters.

In diesem Beispiel sind die Parameter `--count` und `--security-group` nicht enthalten. Für `--count` ist der Standard 1. Wenn Sie über eine Standard-VPC und eine Standardsicherheitsgruppe verfügen, werden diese verwendet.

```
aws ec2 run-instances
    --image-id resolve:ssm:/golden-ami:2
    --instance-type m5.xlarge
    ...
```

Um eine Instance mit einem öffentlichen Parameter zu starten, der bereitgestellt wird von AWS

Systems Manager stellt öffentliche Parameter für öffentliche AMIs bereit, die von bereitgestellt werden AWS. Sie können die öffentlichen Parameter beim Starten von Instances verwenden, um sicherzustellen, dass Sie die neuesten AMIs verwenden.

Weitere Informationen finden Sie unter Finden Sie die neuesten AMIs mit Systems Manager.

Finden Sie die neuesten AMIs mit Systems Manager

AWS Systems Manager stellt öffentliche Parameter für öffentliche AMIs bereit, die von verwaltet werden AWS. Sie können die öffentlichen Parameter beim Starten von Instances verwenden, um sicherzustellen, dass Sie die neuesten AMIs verwenden. Beispielsweise `/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-arm64` ist der Parameter public in allen Regionen verfügbar und verweist immer auf die neueste Version des Amazon Linux 2023 AMI für die arm64-Architektur in einer bestimmten Region.

Die öffentlichen Parameter sind über die folgenden Pfade verfügbar:

- Linux – `/aws/service/ami-amazon-linux-latest`
- Windows – `/aws/service/ami-windows-latest`

Um eine Liste aller Linux- oder Windows-AMIs in der aktuellen AWS Region anzuzeigen

Verwenden Sie den folgenden AWS CLI Befehl get-parameters-by-path, um eine Liste aller Linux- oder Windows-AMIs in der aktuellen Region anzuzeigen. AWS Der Wert für den `--path` Parameter ist für Linux und Windows unterschiedlich.

Für Linux:

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-amazon-linux-latest \
    --query "Parameters[].Name"
```

Für Windows:

```
aws ssm get-parameters-by-path \
    --path /aws/service/ami-windows-latest \
    --query "Parameters[].Name"
```

So starten Sie eine Instance mit einem öffentlichen Parameter:

Das folgende Beispiel spezifiziert einen öffentlichen Systems Manager Manager-Parameter für die Image-ID, um eine Instance mit dem neuesten Amazon Linux 2023 AMI zu starten.

Um den Parameter im Befehl anzugeben, verwenden Sie die folgende Syntax: `resolve:ssm:`*`public-parameter`*, wobei `resolve:ssm` das Standardpräfix und *`public-parameter`* der Pfad und Name des öffentlichen Parameters ist.

In diesem Beispiel sind die Parameter `--count` und `--security-group` nicht enthalten. Der Standardwert für `--count` lautet 1. Wenn Sie über eine Standard-VPC und eine Standardsicherheitsgruppe verfügen, werden diese verwendet.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-amazon-linux-latest/al2023-ami-kernel-
default-x86_64 \
    --instance-type m5.xlarge \
    --key-name MyKeyPair
```

Weitere Informationen finden Sie unter Arbeiten mit öffentlichen Parametern im AWS Systems Manager -Benutzerhandbuch.

Beispiele für die Verwendung von Systems Manager Manager-Parametern finden Sie unter Abfragen der neuesten Amazon Linux-AMI-IDs mithilfe des AWS Systems Manager Parameterspeichers und Abfragen des neuesten Windows-AMIs mithilfe des AWS Systems Manager Parameterspeichers.

Weitere Informationen zum Auffinden von AMIs

Ein Amazon Linux 2023 AMI finden Sie unter AL2023 on Amazon EC2 im Amazon Linux 2023 User Guide.

Ein Ubuntu-AMI finden Sie unter Amazon EC2 AMI Locator auf der Canonical Ubuntu-Website.

Ein RHEL-AMI finden Sie unter Red Hat Enterprise Linux Images (AMI) Available on Amazon Web Services (AWS) auf der Red Hat Website.

Gemeinsame AMIs

Ein gemeinsames AMI ist ein AMI, das ein Entwickler nach der Erstellung für Andere verfügbar macht. Eine der einfachsten Möglichkeiten zum Einstieg in Amazon EC2 ist die Verwendung eines gemeinsamen AMI, dessen Komponenten Sie benötigen, und das Hinzufügen von benutzerdefinierten Inhalten. Sie können außerdem eigene AMIs erstellen und mit anderen teilen.

Die Verwendung gemeinsamer AMIs erfolgt auf eigenes Risiko. Amazon kann die Integrität oder Sicherheit von AMIs, die von anderen Amazon EC2-Benutzern geteilt werden, nicht gewährleisten. Behandeln Sie gemeinsame AMIs daher wie fremden Code bei der Bereitstellung in Ihrem eigenen Rechenzentrum und führen Sie die entsprechenden Due Diligence-Prüfungen durch. Wir empfehlen Ihnen, eine AMI von einer vertrauenswürdigen Quelle zu beziehen, beispielsweise von einem verifizierten Anbieter.

Verifizierter Anbieter

In der Amazon EC2-Konsole werden öffentliche AMIs, die Amazon oder einem verifizierten Amazon-Partner gehören, mit Verifizierter Anbieter gekennzeichnet.

Sie können auch den AWS CLI Befehl describe-images verwenden, um die öffentlichen AMIs zu identifizieren, die von einem verifizierten Anbieter stammen. Öffentliche Images, die im Besitz von Amazon oder einem verifizierten Partner sind, haben einen Aliasbesitzer, der entweder `amazon`oder `aws-marketplace` ist. In der CLI-Ausgabe erscheinen diese Werte für `ImageOwnerAlias`. Andere Benutzer können ihre AMIs nicht mit einem Alias versehen. So können Sie AMIs von Amazon oder verifizierten Partnern auf einfache Weise finden.

Um ein verifizierter Anbieter zu werden, müssen Sie sich als Verkäufer auf der AWS Marketplace registrieren. Nach der Registrierung können Sie Ihr AMI auf der AWS Marketplace auflisten. Weitere

Informationen finden Sie unter Erste Schritte als Verkäufer und AMI-basierte Produkte im AWS Marketplace -Verkäuferhandbuch.

Themen über gemeinsame AMIs

- Suchen gemeinsamer AMIs
- Veröffentlichen eines AMI
- Freigeben eines AMI für bestimmte Organisationen oder Organisationseinheiten
- Freigeben eines AMI für bestimmte AWS -Konten
- Kündigen Sie die gemeinsame Nutzung eines AMI mit Ihrem AWS-Konto
- Verwenden von Lesezeichen
- Richtlinien für gemeinsame Linux-AMIs

Wenn Sie nach Informationen zu anderen Themen suchen

- Hinweise zum Erstellen eines AMI finden Sie unter the section called “Erstellen einer Instance-Speicher-Backed Linux-AMI” oderthe section called “Erstellen Sie ein Amazon EBS-backed AMI”.
- Informationen zum Erstellen, Bereitstellen und Verwalten Ihrer Anwendungen auf der AWS Marketplace finden Sie in der AWS Marketplace -Dokumentation.

Suchen gemeinsamer AMIs

Verwenden Sie die Amazon EC2-Konsole oder die Befehlszeilenschnittstelle, um gemeinsame AMIs zu suchen.

AMIs sind eine regionale Ressource. Wenn Sie also nach einem gemeinsamen AMI (öffentlich oder privat) suchen, müssen Sie in derselben Region danach suchen, aus der es freigegeben wird. Um ein AMI in einer anderen Region verfügbar zu machen, kopieren Sie das AMI in die Region und geben Sie es dann frei. Weitere Informationen finden Sie unter Kopieren eines AMI.

Aufgaben

- Suchen eines freigegebenen AMI (Konsole)
- Suchen eines gemeinsamen AMI (AWS CLI)
- Suchen Sie ein geteiltes AMI (Tools für Windows PowerShell)
- Verwenden gemeinsamer AMIs

Suchen eines freigegebenen AMI (Konsole)

Suchen gemeinsamer privater AMIs mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie im ersten Filterfeld Private images aus. Alle mit Ihnen geteilten AMIs werden aufgeführt. Um die Suche zu verfeinern, wählen Sie die Search bar (Suchleiste) aus und verwenden Sie die im Menü bereitgestellten Filteroptionen.

Suchen gemeinsamer öffentlicher AMIs mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie im ersten Filterfeld Public images aus. Um die Suche zu verfeinern, wählen Sie das Feld Search (Suche) aus und verwenden Sie die im Menü bereitgestellten Filteroptionen.

Suchen von Amazons gemeinsamer öffentlicher AMIs mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie im ersten Filterfeld Public images aus.
4. Wählen Sie das Feld Suche und wählen Sie dann aus den angezeigten Menüoptionen Besitzer-Alias, dann = und dann Amazon, um nur die öffentlichen Images von Amazon anzuzeigen.

Suchen gemeinsamer öffentlicher AMIs von einem verifizierten Anbieter mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMI-Katalog aus.
3. Wählen Sie Community AMIs (Community-AMIs) aus.
4. Das Label Verifizierter Anbieter kennzeichnet die AMIs, die von Amazon oder einem verifizierten Partner stammen.

Suchen eines gemeinsamen AMI (AWS CLI)

Verwenden Sie den Befehl describe-images (AWS CLI) um AMIs anzuzeigen. Schränken Sie die Liste der für Sie interessanten AMIs bei Bedarf ein (siehe folgende Beispiele).

Beispiel: Aufführen aller öffentlichen AMIs

Mit dem folgenden Befehl werden alle öffentlichen AMIs sowie alle öffentlichen AMIs in Ihrem Besitz aufgeführt.

```
aws ec2 describe-images --executable-users all
```

Beispiel: Aufführen von AMIs mit explizite Startberechtigungen

Mit dem folgenden Befehl werden alle AMIs aufgeführt, für die Sie explizite Startberechtigungen haben. Die Liste enthält keine AMIs, die sich in Ihrem Besitz befinden.

```
aws ec2 describe-images --executable-users self
```

Beispiel: Aufführen von AMIs von verifizierten Anbietern

Mit dem folgenden Befehl werden AMIs von verifizierten Anbietern aufgeführt. Öffentliche AMIs im Besitz von verifizierten Anbietern (entweder Amazon oder verifizierte Partner) haben einen Aliasbesitzer, der als `amazon` oder `aws-marketplace` im Kontofeld erscheint. So können Sie AMIs von verifizierten Anbietern auf einfache Weise finden. Andere Benutzer können ihre AMIs nicht mit einem Alias versehen.

```
aws ec2 describe-images \
    --owners amazon aws-marketplace \
    --query 'Images[*].[ImageId]' \
    --output text
```

Beispiel: Aufführen von AMIs von einem Konto

Der folgende Befehl listet die AMIs auf, die dem angegebenen AWS-Konto gehören.

```
aws ec2 describe-images --owners 123456789012
```

Beispiel: Einschränken von AMIs mithilfe eines Filters

Um die Anzahl der angezeigten AMIs zu verringern, schränken Sie die angezeigten AMIs mithilfe eines Filters Ihren Interessen entsprechend ein. Beispiel: Verwenden Sie den folgenden Filter, um ausschließlich EBS-Backed AMIs anzuzeigen.

```
--filters "Name=root-device-type,Values=ebs"
```

Suchen Sie ein geteiltes AMI (Tools für Windows PowerShell)

Verwenden Sie den Get-EC2ImageBefehl (Tools für Windows PowerShell), um AMIs aufzulisten. Schränken Sie die Liste der für Sie interessanten AMIs bei Bedarf ein (siehe folgende Beispiele).

Beispiel: Aufführen aller öffentlichen AMIs

Mit dem folgenden Befehl werden alle öffentlichen AMIs sowie alle öffentlichen AMIs in Ihrem Besitz aufgeführt.

```
PS C:\> Get-EC2Image -ExecutableUser all
```

Beispiel: Aufführen von AMIs mit explizite Startberechtigungen

Mit dem folgenden Befehl werden alle AMIs aufgeführt, für die Sie explizite Startberechtigungen haben. Die Liste enthält keine AMIs, die sich in Ihrem Besitz befinden.

```
PS C:\> Get-EC2Image -ExecutableUser self
```

Beispiel: Aufführen von AMIs von verifizierten Anbietern

Mit dem folgenden Befehl werden AMIs von verifizierten Anbietern aufgeführt. Öffentliche AMIs im Besitz von verifizierten Anbietern (entweder Amazon oder verifizierte Partner) haben einen Aliasbesitzer, der als `amazon` oder `aws-marketplace` im Kontofeld erscheint. So können Sie AMIs von verifizierten Anbietern auf einfache Weise finden. Andere Benutzer können ihre AMIs nicht mit einem Alias versehen.

```
PS C:\> Get-EC2Image -Owner amazon aws-marketplace
```

Beispiel: Aufführen von AMIs von einem Konto

Der folgende Befehl listet die AMIs auf, die dem angegebenen AWS-Konto gehören.

```
PS C:\> Get-EC2Image -Owner 123456789012
```

Beispiel: Einschränken von AMIs mithilfe eines Filters

Um die Anzahl der angezeigten AMIs zu verringern, schränken Sie die angezeigten AMIs mithilfe eines Filters Ihren Interessen entsprechend ein. Beispiel: Verwenden Sie den folgenden Filter, um ausschließlich EBS-Backed AMIs anzuzeigen.

```
-Filter @{ Name="root-device-type"; Values="ebs" }
```

Verwenden gemeinsamer AMIs

Bevor Sie eine gemeinsame AMI verwenden, bestätigen Sie folgendermaßen, dass keine vorinstallierten Anmeldeinformationen, die unerwünschten Zugriff auf die Instance durch Dritte ermöglichen, und kein vorkonfigurierte Remoteprotokollierung vorhanden sind, die empfindliche Daten an Dritte übertragen könnte. Informationen zur Erhöhung der Systemsicherheit finden Sie in der Dokumentation für die von der AMI verwendete Linux-Distribution.

Damit Sie den Zugriff auf die Instance nicht unabsichtlich verlieren, empfehlen wir das Initiieren von zwei SSH-Sitzungen, wobei eine Sitzung offen bleibt, bis Sie alle unbekannten Anmeldeinformationen entfernt und bestätigt haben, dass Sie sich noch immer mit SSH in Ihrer Instance anmelden können.

1. Ermitteln Sie nicht autorisierte öffentliche SSH-Schlüssel und deaktivieren Sie sie. Der einzige Schlüssel in der Datei sollte der zum Starten des AMI verwendete sein. Mit dem folgenden Befehl suchen Sie `authorized_keys`-Dateien:

   ```
   [ec2-user ~]$ sudo find / -name "authorized_keys" -print -exec cat {} \;
   ```

2. Deaktivieren Sie Passwort-basierte Authentifizierung für den Root-Benutzer. Öffnen Sie die Datei `sshd_config` und bearbeiten Sie die `PermitRootLogin`-Zeile wie folgt:

   ```
   PermitRootLogin without-password
   ```

   Alternativ können Sie die Funktion zum Anmelden in der Instance als Root-Benutzer deaktivieren:

   ```
   PermitRootLogin No
   ```

   Starten Sie den sshd-Service neu.

3. Überprüfen Sie, ob es andere Benutzer gibt, die sich bei Ihrer Instance anmelden können. Benutzer mit Super-User-Privilegien sind besonders gefährlich. Entfernen oder sperren Sie die Passwörter unbekannter Konten.
4. Prüfen Sie, ob nicht verwendete offene Ports bestehen, die Netzwerkdienste ausführen und auf eingehende Verbindungen warten.
5. Um die vorkonfigurierte Fernprotokollierung zu verhindern, sollten Sie die vorhandene Konfigurationsdatei löschen und den `rsyslog`-Service neu starten. Beispielsweise:

```
[ec2-user ~]$ sudo rm /etc/rsyslog.conf
[ec2-user ~]$ sudo service rsyslog restart
```

6. Überprüfen Sie, ob alle cron-Aufträge rechtmäßig sind.

Wenn Sie ein öffentliches AMI entdecken, das ein Sicherheitsrisiko darstellt, wenden Sie sich an das AWS -Sicherheitsteam. Weitere Informationen erhalten Sie im AWS -Sicherheitszentrum.

Veröffentlichen eines AMI

Sie können Ihr AMI öffentlich zugänglich machen, indem Sie es mit allen teilen AWS-Konten.

Wenn Sie verhindern möchten, dass Ihre AMIs öffentlich geteilt werden, können Sie den öffentlichen Zugriff für AMIs sperren aktivieren. Dadurch werden alle Versuche, ein AMI zu veröffentlichen, blockiert, was dazu beiträgt, unbefugten Zugriff und potenziellen Missbrauch von AMI-Daten zu verhindern. Beachten Sie, dass die Aktivierung von Block Public Access keine Auswirkungen auf Ihre AMIs hat, die bereits öffentlich verfügbar sind; sie bleiben öffentlich verfügbar.

Wenn Sie nur bestimmten Konten erlauben möchten, Ihr AMI zum Starten von Instances zu verwenden, lesen Sie Freigeben eines AMI für bestimmte AWS -Konten.

Inhalt

Überlegungen

Beachten Sie Folgendes, bevor Sie ein AMI öffentlich machen.

- Eigentum — Um ein AMI zu veröffentlichen, AWS-Konto müssen Sie Eigentümer des AMI sein.
- Region: AMIs sind eine regionale Ressource. Wenn Sie ein AMI freigeben, ist es nur in der Region verfügbar, in der Sie es freigegeben haben. Um ein AMI in einer anderen Region verfügbar zu machen, kopieren Sie das AMI in die Region und geben Sie es dann frei. Weitere Informationen finden Sie unter Kopieren eines AMI.
- Öffentlichen Zugriff blockieren – Um ein AMI öffentlich zu teilen, muss das Sperren des öffentlichen Zugriffs für AMIs in jeder Region, in der das AMI öffentlich geteilt wird, deaktiviert sein. Nachdem Sie das AMI öffentlich freigegeben haben, können Sie Block Public Access for AMIs wieder aktivieren, um zu verhindern, dass Ihre AMIs weiterhin öffentlich geteilt werden.
- Einige AMIs können nicht veröffentlicht werden – Wenn Ihr AMI eines der folgenden Merkmale aufweist, können Sie es nicht veröffentlichen (Sie können es jedoch das AMI für bestimmte AWS-Konten freigeben):
  - Verschlüsselte Volumes
  - Snapshots von verschlüsselten Volumes
  - Produkt-Codes
- Offenlegung sensibler Daten vermeiden: Damit beim Freigeben eines AMI keine sensiblen Daten offengelegt werden, lesen Sie die Sicherheitserwägungen in Richtlinien für gemeinsame Linux-AMIs und folgen Sie den empfohlenen Verfahren.
- Nutzung: Wenn Sie ein AMI freigeben, können Benutzer Instances nur über das AMI starten. Sie können es nicht löschen, teilen oder ändern. Wenn die Benutzer jedoch eine Instance mit Ihrem AMI gestartet haben, können sie danach von der gestarteten Instance aus ein AMI erstellen.
- Automatische Veralterung – Standardmäßig ist das Veralterungsdatum aller öffentlichen AMIs auf zwei Jahre ab dem AMI-Erstellungsdatum festgelegt. Sie können das Veralterungsdatum auf weniger als zwei Jahre festlegen. Um das Verfallsdatum zu stornieren oder das Verfallsdatum auf ein späteres Datum zu verschieben, müssen Sie das AMI als privat kennzeichnen, indem Sie es nur mit bestimmten Personen teilen. AWS-Konten
- Veraltete AMIs entfernen — Wenn ein öffentliches AMI sein Verfallsdatum erreicht hat und sechs oder mehr Monate lang keine neuen Instances über das AMI gestartet wurden, wird AWS schließlich die Public Sharing-Eigenschaft entfernt, sodass veraltete AMIs nicht in den öffentlichen AMI-Listen erscheinen.
- Abrechnung — Ihnen wird nichts in Rechnung gestellt, wenn Ihr AMI von anderen AWS-Konten zum Starten von Instances verwendet wird. Die Konten, die Instances mit dem AMI starten, werden für die Instances abgerechnet, die sie starten.

Ein AMI mit allen AWS Konten teilen (öffentlich teilen)

Nachdem Sie ein AMI veröffentlicht haben, ist es in Community-AMIs in der Konsole verfügbar, auf die Sie über den AMI-Katalog im linken Navigator der EC2-Konsole oder beim Starten einer Instance über die Konsole zugreifen können. Hinweis: Nach der Veröffentlichung kann es etwas dauern, bis das AMI unter Community AMIs angezeigt wird.

Console

Veröffentlichen eines AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie das AMI in der Liste aus und wählen Sie Aktionen, AMI-Berechtigungen bearbeiten aus.
4. Unter AMI-Verfügbarkeit wählen Sie Öffentlich aus.
5. Wählen Sie Änderungen speichern aus.

AWS CLI

Jedes AMI hat eine `launchPermission` Eigenschaft, die steuert AWS-Konten, welche außer denen des Besitzers dieses AMI zum Starten von Instances verwenden dürfen. Indem Sie die `launchPermission` Eigenschaft eines AMI ändern, können Sie das AMI öffentlich machen (wodurch allen Startberechtigungen gewährt werden AWS-Konten) oder es nur mit den von Ihnen angegebenen AWS-Konten Benutzern teilen.

Sie können der Liste der Konten mit Startberechtigungen für ein AMI IDs hinzufügen oder IDs löschen. Um ein AMI zu veröffentlichen, geben Sie die `all`-Gruppe an. Sie können öffentliche und explizite Startberechtigungen angeben.

Veröffentlichen eines AMI

1. Verwenden Sie den Befehl modify-image-attribute wie folgt, um die `all`-Gruppe zur `launchPermission`-Liste für das angegebene AMI hinzuzufügen.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{Group=all}]"
```

2. Um die Startberechtigungen des AMI zu überprüfen, verwenden Sie den describe-image-attribute-Befehl.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

3. (Optional) Um das AMI erneut privat zu machen, entfernen Sie die `all`-Gruppe aus den Startberechtigungen. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{Group=all}]"
```

PowerShell

Jedes AMI hat eine `launchPermission` Eigenschaft, die steuert AWS-Konten, welche außer denen des Besitzers dieses AMI zum Starten von Instances verwenden dürfen. Indem Sie die `launchPermission` Eigenschaft eines AMI ändern, können Sie das AMI öffentlich machen (wodurch allen Startberechtigungen gewährt werden AWS-Konten) oder es nur mit den von Ihnen angegebenen AWS-Konten Benutzern teilen.

Sie können der Liste der Konten mit Startberechtigungen für ein AMI IDs hinzufügen oder IDs löschen. Um ein AMI zu veröffentlichen, geben Sie die `all`-Gruppe an. Sie können öffentliche und explizite Startberechtigungen angeben.

Veröffentlichen eines AMI

1. Verwenden Sie den Befehl Edit-EC2ImageAttribute wie folgt, um die `all`-Gruppe zur `launchPermission`-Liste für das angegebene AMI hinzuzufügen.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserGroup all
```

2. Um die Startberechtigungen des AMI zu überprüfen, verwenden Sie den folgenden Get-EC2ImageAttribute-Befehl.

```
PS C:\> Get-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

3. (Optional) Um das AMI erneut privat zu machen, entfernen Sie die `all`-Gruppe aus den Startberechtigungen. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserGroup all
```

Sperren Sie den öffentlichen Zugriff auf Ihre AMIs

Um zu verhindern, dass Ihre AMIs öffentlich geteilt werden, können Sie den öffentlichen Zugriff für AMIs sperren aktivieren. Diese Einstellung ist auf Kontoebene aktiviert, Sie müssen sie jedoch in allen Bereichen aktivieren, AWS-Region in denen Sie verhindern möchten, dass Ihre AMIs öffentlich geteilt werden.

Wenn Block Public Access aktiviert ist, wird jeder Versuch, ein AMI öffentlich zu machen, automatisch blockiert. Wenn Sie jedoch bereits über öffentliche AMIs verfügen, sind diese weiterhin öffentlich verfügbar.

Um AMIs öffentlich zu teilen, müssen Sie die Sperrung des öffentlichen Zugriffs deaktivieren. Wenn Sie mit dem Teilen fertig sind, empfiehlt es sich, Block Public Access wieder zu aktivieren, um ein unbeabsichtigtes öffentliches Teilen Ihrer AMIs zu verhindern.

Sie können die IAM-Berechtigungen auf Administratorbenutzer beschränken, sodass nur dieser den öffentlichen Zugriff für AMIs aktivieren oder deaktivieren kann.

Inhalt

Standardeinstellungen

Die Einstellung Öffentlichen Zugriff für AMIs blockieren ist standardmäßig entweder aktiviert oder deaktiviert, je nachdem, ob Ihr Konto neu oder bereits vorhanden ist und ob Sie öffentliche AMIs haben. In der folgenden Tabelle werden die Standardeinstellungen aufgeführt:

AWS Konto	Standardeinstellung „Öffentlichen Zugriff für AMIs blockieren“
Neue Konten	Aktiviert
Bestehende Konten ohne öffentliche AMIs[1]	Aktiviert
Bestehende Konten mit mindestens einem öffentlichen AMI	Disabled

[1] Wenn Ihr Konto am oder nach dem 15. Juli 2023 über mindestens einen öffentlichen AMI verfügte, ist die Option Öffentlichen Zugriff für AMIs blockieren standardmäßig für Ihr Konto deaktiviert, auch wenn Sie anschließend alle AMIs privat gemacht haben.

Erforderliche IAM-Berechtigungen

Um die Funktionen von Block Public Access zu nutzen, benötigen Sie die folgenden IAM-Berechtigungen:

- `EnableImageBlockPublicAccess`
- `DisableImageBlockPublicAccess`
- `GetImageBlockPublicAccessState`

Aktivieren Sie den blockierten öffentlichen Zugriff für AMIs

Um zu verhindern, dass Ihre AMIs öffentlich geteilt werden, aktivieren Sie die Option Öffentlichen Zugriff für AMIs sperren auf Kontoebene. Sie müssen die Option „Öffentlichen Zugriff sperren“ für AMIs in allen AWS-Region aktivieren, in denen Sie die öffentliche Nutzung Ihrer AMIs verhindern möchten. Wenn Sie bereits über öffentliche AMIs verfügen, bleiben diese öffentlich verfügbar.

Console

Um den öffentlichen Blockzugriff für AMIs in der angegebenen Region zu aktivieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste (oben auf dem Bildschirm) die Region aus, in der Sie den öffentlichen Zugriff für AMIs blockieren möchten.
3. Wenn das Dashboard nicht angezeigt wird, wählen Sie im Navigationsbereich EC2-Dashboardaus.
4. Wählen Sie unter Kontoattribute die Option Datenschutz und Sicherheit aus.
5. Wählen Sie unter Öffentlichen Zugriff für AMIs blockieren die Option Verwalten aus.
6. Wählen Sie das Kontrollkästchen Block public sharing (Öffentliche Freigabe blockieren) und wählen Sie Update (Aktualisieren).

> **Note**
>
> Die Konfiguration dieser Einstellung durch die API kann bis zu 10 Minuten dauern. Während dieser Zeit lautet der Wert Neues öffentliches Teilen erlaubt. Wenn die API die Konfiguration abgeschlossen hat, ändert sich der Wert automatisch auf Neues öffentliches Teilen blockiert.

AWS CLI

Um den öffentlichen Blockzugriff für AMIs in der angegebenen Region zu aktivieren

Verwenden Sie den Befehl enable-image-block-public-access und geben Sie die Region an, in der der öffentliche Blockzugriff für AMIs aktiviert werden soll. Geben Sie für den Parameter `--image-block-public-access-state` `block-new-sharing` an:

```
aws ec2 enable-image-block-public-access \
    --region us-east-1 \
    --image-block-public-access-state block-new-sharing
```

Erwartete Ausgabe

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
```

```
}
```

> **Note**
>
> Die Konfiguration dieser Einstellung durch die API kann bis zu 10 Minuten dauern. Wenn Sie während dieser Zeit den Befehl get-image-block-public-access-state ausführen, wird die Antwort angezeigt. `unblocked` Wenn die API die Konfiguration abgeschlossen hat, erfolgt die Antwort. `block-new-sharing`

Deaktivieren des blockierten öffentlichen Zugriffs für AMIs

Damit die Benutzer in Ihrem Konto Ihre AMIs öffentlich teilen können, deaktivieren Sie die Sperrung des öffentlichen Zugriffs auf Kontoebene. Sie müssen die Sperrung des öffentlichen Zugriffs für AMIs AWS-Region in allen Bereichen deaktivieren, in denen Sie das öffentliche Teilen Ihrer AMIs zulassen möchten.

Console

Um die Sperrung des öffentlichen Zugriffs für AMIs in der angegebenen Region zu deaktivieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste (oben auf dem Bildschirm) die Region aus, in der Sie den blockierten öffentlichen Zugriff für AMIs deaktivieren möchten.
3. Wenn das Dashboard nicht angezeigt wird, wählen Sie im Navigationsbereich EC2-Dashboardaus.
4. Wählen Sie unter Kontoattribute die Option Datenschutz und Sicherheit aus.
5. Wählen Sie unter Öffentlichen Zugriff für AMIs blockieren die Option Verwalten aus.
6. Wählen Sie das Kontrollkästchen Block public sharing (Öffentliche Freigabe blockieren) ab und wählen Sie Save (speichern).
7. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`confirm`** ein und wählen Sie dann Allow public sharing (Öffentliches Teilen zulassen) aus.

> **Note**
>
> Die Konfiguration dieser Einstellung durch die API kann bis zu 10 Minuten dauern. Während dieser Zeit lautet der Wert Neues öffentliches Teilen blockiert. Wenn die API

die Konfiguration abgeschlossen hat, ändert sich der Wert automatisch auf Neues öffentliches Teilen erlaubt.

AWS CLI

Um die Sperrung des öffentlichen Zugriffs für AMIs in der angegebenen Region zu deaktivieren

Verwenden Sie den Befehl disable-image-block-public-access und geben Sie die Region an, in der der öffentliche Blockzugriff für AMIs deaktiviert werden soll.

```
aws ec2 disable-image-block-public-access --region us-east-1
```

Erwartete Ausgabe

```
{
   "ImageBlockPublicAccessState": "unblocked"
}
```

> **Note**
>
> Die Konfiguration dieser Einstellung durch die API kann bis zu 10 Minuten dauern. Wenn Sie während dieser Zeit den Befehl get-image-block-public-access-state ausführen, wird die Antwort angezeigt. `block-new-sharing` Wenn die API die Konfiguration abgeschlossen hat, erfolgt die Antwort. `unblocked`

Zeigen Sie den Status „Öffentlichen Zugriff blockieren“ für AMIs an

Um zu sehen, ob das öffentliche Teilen Ihrer AMIs in Ihrem Konto gesperrt ist, können Sie den Status für die Sperrung des öffentlichen Zugriffs für AMIs einsehen. Sie müssen den Status in jedem AWS-Region einsehen, in dem Sie sehen möchten, ob das öffentliche Teilen Ihrer AMIs blockiert ist.

Console

Um den Status der Blockierung des öffentlichen Zugriffs für AMIs in der angegebenen Region anzuzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie auf der Navigationsleiste (oben auf dem Bildschirm) die Region aus, in der Sie den Status für den blockierten öffentlichen Zugriff für AMIs anzeigen möchten.
3. Wenn das Dashboard nicht angezeigt wird, wählen Sie im Navigationsbereich EC2-Dashboardaus.
4. Wählen Sie unter Kontoattribute die Option Datenschutz und Sicherheit aus.
5. Aktivieren Sie unter Öffentlichen Zugriff für AMIs blockieren das Feld Öffentlicher Zugriff. Der Wert lautet entweder Neues öffentliches Teilen blockiert oder Neues öffentliches Teilen erlaubt.

AWS CLI

Um den Status „Öffentlicher Zugriff blockieren“ für AMIs in der angegebenen Region abzurufen

Verwenden Sie den Befehl get-image-block-public-access-state und geben Sie die Region an, in der der Status des öffentlichen Blockzugriffs für AMIs abgerufen werden soll.

```
aws ec2 get-image-block-public-access-state --region us-east-1
```

Erwartete Ausgabe – Der Wert ist entweder oder. `block-new-sharing` `unblocked`

```
{
    "ImageBlockPublicAccessState": "block-new-sharing"
}
```

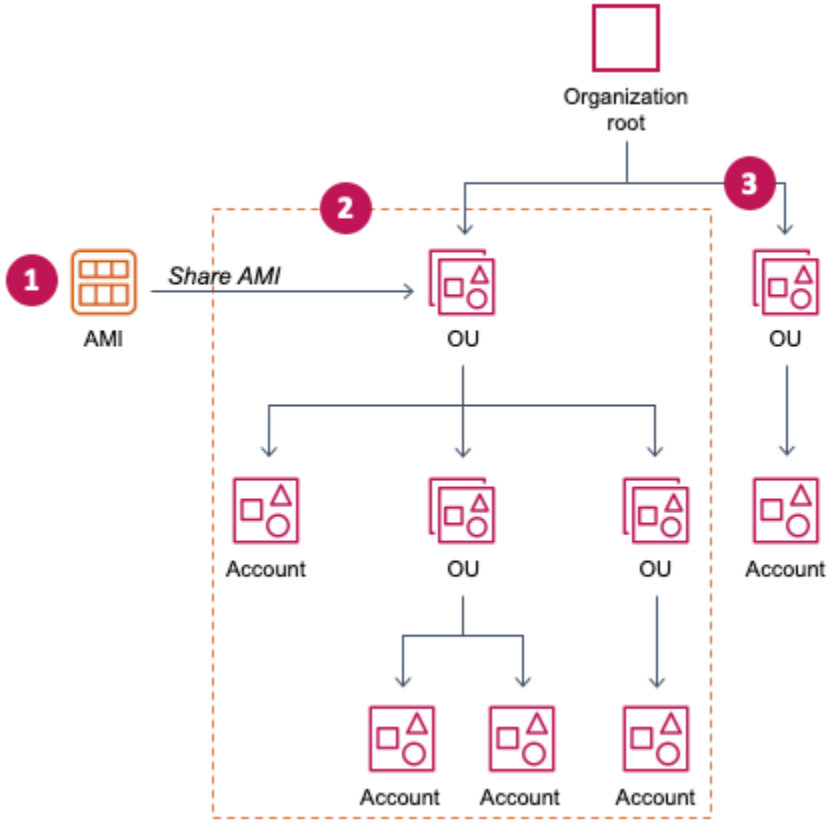
Freigeben eines AMI für bestimmte Organisationen oder Organisationseinheiten

AWS Organizationsist ein Kontoverwaltungsservice, mit dem Sie mehrere Konten zu einer Organisation AWS-Konten zusammenfassen können, die Sie selbst erstellen und zentral verwalten. Sie können ein AMI zusätzlich zur Freigabe für bestimmte Konten für eine von Ihnen erstellte Organisation oder Organisationseinheit (OE) freigeben.

Eine Organisation ist eine juristische Stelle, die Sie erstellen, um Ihre AWS-Konten zu konsolidieren und zentral zu verwalten. Sie können die Konten in einer hierarchischen, Baumstruktur organisieren, mit einem Stamm an der Spitze und Organisationseinheiten, die unterhalb des Organisationsstamms angeordnet sind. Jedes Konto kann direkt zum Root hinzugefügt oder in einer der OUs in der

Hierarchie platziert werden. Weitere Informationen finden Sie unter AWS -Organizations – Terminologie und Konzepte im AWS Organizations -Benutzerhandbuch.

Wenn Sie ein AMI für eine Organisation oder eine OE freigeben, erhalten alle untergeordneten Konten Zugriff auf das AMI. Im folgenden Diagramm wird das AMI beispielsweise mit einer Organisationseinheit der obersten Ebene geteilt (durch den Pfeil bei der Nummer 1 angezeigt). Alle OEs und Konten, die unter dieser OE der obersten Ebene verschachtelt sind (durch die gestrichelte Linie bei Nummer 2 gekennzeichnet), haben ebenfalls Zugriff auf das AMI. Die Konten in der Organisation und OE außerhalb der gestrichelten Linie (gekennzeichnet durch die Zahl 3) haben keinen Zugriff auf das AMI, da sie der OE nicht untergeordnet sind, für die das AMI freigegeben ist.



Überlegungen

Beachten Sie Folgendes, wenn Sie AMIs für bestimmte Organisationen oder Organisationseinheiten freigeben.

- Eigentümerschaft – Um ein AMI freizugeben, muss Ihr AWS-Konto Besitzer des AMI sein.
- Freigabelimits – Der AMI-Besitzer kann ein AMI für jede Organisation oder Organisationseinheit freigeben, einschließlich Organisationen und Organisationseinheiten, denen er nicht angehört.

Informationen zur maximalen Anzahl von Entitäten, für die ein AMI innerhalb einer Region freigegeben werden kann, finden Sie unter Amazon-EC2-Service-Quotas.

- Tags – Sie können keine benutzerdefinierten Tags (Tags, die Sie einem AMI anfügen) freigeben. Wenn Sie ein AMI teilen, sind Ihre benutzerdefinierten Tags für niemanden AWS-Konto in einer Organisation oder Organisationseinheit verfügbar, mit der das AMI geteilt wird.
- ARN-Format: Wenn Sie eine Organisation oder OE in einem Befehl angeben, achten Sie darauf, das richtige ARN-Format zu verwenden. Sie erhalten eine Fehlermeldung, wenn Sie nur die ID angeben, z. B. wenn Sie nur `o-123example` oder `ou-1234-5example` angeben.

  Richtige ARN-Formate:

  - ARN der Organisation: `arn:aws:organizations::`*`account-id`*`:organization/`*`organization-id`*
  - OE-ARN: `arn:aws:organizations::`*`account-id`*`:ou/`*`organization-id`*`/`*`ou-id`*

  Wobei gilt:

  - *`account-id`* ist beispielsweise die zwölfstellige Verwaltungskontonummer, `123456789012`. Wenn Sie die Verwaltungskontonummer nicht kennen, können Sie die Organisation oder die Organisationseinheit beschreiben, um den ARN zu erhalten, der die Verwaltungskontonummer enthält. Weitere Informationen finden Sie unter ARN abrufen.
  - *`organization-id`* ist die Organisations-ID, beispielsweise `o-123example`.
  - *`ou-id`* ist die ID der Organisationseinheit, beispielsweise `ou-1234-5example`.

  Weitere Informationen zum Format von ARNs finden Sie unter Amazon Resource Names (ARNs) im IAM-Benutzerhandbuch.
- Verschlüsselung und Schlüssel: Sie können AMIs freigeben, die durch unverschlüsselte und verschlüsselte Snapshots unterstützt werden.
  - Die verschlüsselten Snapshots müssen mit einem vom Kunden verwalteten Schlüssel verschlüsselt sein. Sie können keine AMIs teilen, die auf Snapshots basieren, die mit dem verwalteten Standardschlüssel verschlüsselt sind. AWS
  - Wenn Sie ein AMI gemeinsam nutzen, das auf verschlüsselten Snapshots basiert, müssen Sie den Organisationen oder Organisationseinheiten erlauben, die vom Kunden verwalteten Schlüssel zu verwenden, die zur Verschlüsselung der Snapshots verwendet wurden. Weitere Informationen finden Sie unter Organisationen und OEs erlauben, einen KMS-Schlüssel zu verwenden.

- Region: AMIs sind eine regionale Ressource. Wenn Sie ein AMI freigeben, ist es nur in der Region verfügbar, in der Sie es freigegeben haben. Um ein AMI in einer anderen Region verfügbar zu machen, kopieren Sie das AMI in die Region und geben Sie es dann frei. Weitere Informationen finden Sie unter Kopieren eines AMI.
- Nutzung: Wenn Sie ein AMI freigeben, können Benutzer Instances nur über das AMI starten. Sie können es nicht löschen, teilen oder ändern. Wenn die Benutzer jedoch eine Instance mit Ihrem AMI gestartet haben, können sie danach von der gestarteten Instance aus ein AMI erstellen.
- Abrechnung — Ihnen wird nichts in Rechnung gestellt, wenn Ihr AMI von anderen AWS-Konten zum Starten von Instances verwendet wird. Die Konten, die Instances mit dem AMI starten, werden für die Instances abgerechnet, die sie starten.

Organisationen und OEs erlauben, einen KMS-Schlüssel zu verwenden

Wenn Sie ein AMI gemeinsam nutzen, das durch verschlüsselte Snapshots unterstützt wird, müssen Sie auch den Organisationen oder Organisationseinheiten erlauben, die zur Verschlüsselung der Snapshots verwendet wurden AWS KMS keys , zu verwenden.

Verwenden Sie die `aws:PrincipalOrgPaths` Schlüssel `aws:PrincipalOrgID` und, um den AWS Organizations Pfad für den Principal, der die Anfrage stellt, mit dem Pfad in der Richtlinie zu vergleichen. Bei diesem Prinzipal kann es sich um einen Benutzer, eine IAM-Rolle, einen Verbundbenutzer oder einen AWS-Konto Root-Benutzer handeln. In einer Richtlinie stellt dieser Bedingungsschlüssel sicher, dass der Anforderer ein Kontomitglied innerhalb des angegebenen Organisationsstammes oder in OEs in AWS Organizations ist. Weitere Beispiele für Bedingungsanweisungen finden Sie unter aws:PrincipalOrgID und aws:PrincipalOrgPaths im IAM-Benutzerhandbuch.

Informationen zum Bearbeiten einer Schlüsselrichtlinie finden Sie unter Zulassen, dass Benutzer mit anderen Konten einen KMS-Schlüssel verwenden können im AWS Key Management Service Entwicklerhandbuch.

Wenn Sie einer Organisation oder OE die Berechtigung erteilen möchten, einen KMS-Schlüssel zu verwenden, fügen Sie der Schlüsselrichtlinie die folgende Anweisung hinzu.

```
{
    "Sid": "Allow access for organization root",
    "Effect": "Allow",
    "Principal": "*",
    "Action": [
```

```
        "kms:Describe*",
        "kms:List*",
        "kms:Get*",
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:PrincipalOrgID": "o-123example"
        }
    }
}
```

Um einen KMS-Schlüssel für mehrere OEs freizugeben, können Sie eine ähnliche Richtlinie wie im folgenden Beispiel verwenden.

```
{
        "Sid": "Allow access for specific OUs and their descendants",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "kms:Describe*",
            "kms:List*",
            "kms:Get*",
            "kms:Encrypt",
            "kms:Decrypt",
            "kms:ReEncrypt*",
            "kms:GenerateDataKey*"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": "o-123example"
            },
            "ForAnyValue:StringLike": {
                "aws:PrincipalOrgPaths": [
                    "o-123example/r-ab12/ou-ab12-33333333/*",
                    "o-123example/r-ab12/ou-ab12-22222222/*"
                ]
            }
```

```
        }
}
```

Freigeben eines AMI

Sie können die Amazon EC2 EC2-Konsole oder die verwenden AWS CLI , um ein AMI mit einer Organisation oder Organisationseinheit zu teilen.

Freigeben eines AMI (Konsole)

So geben Sie ein AMI für eine Organisation oder OE mithilfe der Konsole frei

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie das AMI in der Liste aus und wählen Sie dann Aktionen, AMI-Berechtigungen bearbeiten aus.
4. Unter AMI-Verfügbarkeit wählen Sie Privat aus.
5. Neben Shared organizations/OUs (gemeinsame Organisationen/OEs), wählen Sie Add organization/OU ARN (ARN der Organisation/OE hinzufügen) aus.
6. Geben Sie für Organization/OU ARN (ARN der Organisation/OE) den ARN der Organisation oder OE ein, für den Sie das AMI freigeben möchten, und wählen Sie dann Share AMI (AMI freigeben) aus. Beachten Sie, dass Sie den vollständigen ARN angeben müssen, nicht nur die ID.

   Um dieses AMI für mehrere Organisationen oder OEs freizugeben, wiederholen Sie diesen Schritt, bis alle erforderlichen Organisationen oder OEs hinzugefügt wurden.

   > **Note**
   >
   > Sie brauchen die Amazon-EBS-Snapshots, auf die ein AMI verweist, nicht zu teilen, um das AMI zu teilen. Nur das AMI selbst muss freigegeben werden. Das System stellt automatisch Instance-Zugriff auf die referenzierten Amazon-EBS-Snapshots für den Start bereit. Sie müssen jedoch die KMS-Schlüssel teilen, die zum Verschlüsseln von Snapshots verwendet werden, auf die das AMI verweist. Weitere Informationen finden Sie unter Organisationen und OEs erlauben, einen KMS-Schlüssel zu verwenden.
7. Wählen Sie abschließend Save changes (Änderungen speichern) aus.
8. (Optional) Um die Organisationen oder OEs anzuzeigen, für die Sie das AMI freigegeben haben, wählen Sie das AMI in der Liste und dann die Registerkarte Berechtigungen aus und scrollen

Sie nach untenShared organizations/OUs (Gemeinsame Organisationen/OEs)aus. Um AMIs zu finden, die für Sie freigegeben wurden, lesen Sie Suchen gemeinsamer AMIs.

Ein AMI teilen (Tools für Windows PowerShell)

Verwenden Sie den Edit-EC2ImageAttributeBefehl (Tools für Windows PowerShell), um ein AMI gemeinsam zu nutzen, wie in den folgenden Beispielen gezeigt.

So geben Sie ein AMI für eine Organisation oder einer OE frei

Der folgende Befehl erteilt der angegebenen Organisation Startberechtigungen für das angegebene AMI.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType add -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

> **Note**
>
> Sie brauchen die Amazon-EBS-Snapshots, auf die ein AMI verweist, nicht zu teilen, um das AMI zu teilen. Nur das AMI selbst muss freigegeben werden. Das System stellt automatisch Instance-Zugriff auf die referenzierten Amazon-EBS-Snapshots für den Start bereit. Sie müssen jedoch die KMS-Schlüssel freigeben, die zum Verschlüsseln von Snapshots verwendet werden, auf die das AMI verweist. Weitere Informationen finden Sie unter Organisationen und OEs erlauben, einen KMS-Schlüssel zu verwenden.

So beenden Sie die Freigabe eines AMI für eine Organisation oder OE

Der folgende Befehl entfernt Startberechtigungen für das angegebene AMI von der angegebenen Organisation:

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -
Attribute launchPermission -OperationType remove -OrganizationArn
 "arn:aws:organizations::123456789012:organization/o-123example"
```

Um die gemeinsame Nutzung eines AMI mit allen Organisationen, Organisationseinheiten und AWS-Konten

Der folgende Befehl entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Freigeben eines AMI (AWS CLI)

Verwenden Sie den Befehl modify-image-attribute (AWS CLI), um ein AMI freizugeben.

Um ein AMI mit einer Organisation zu teilen, die AWS CLI

Der modify-image-attribute -Befehl erteilt der angegebenen Organisation Startberechtigungen für das angegebene AMI. Beachten Sie, dass Sie den vollständigen ARN angeben müssen, nicht nur die ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Um ein AMI mit einer OU zu teilen, verwenden Sie den AWS CLI

Der Befehl modify-image-attribute erteilt der angegebenen OE Startberechtigungen für das angegebene AMI. Beachten Sie, dass Sie den vollständigen ARN angeben müssen, nicht nur die ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission
 "Add=[{OrganizationalUnitArn=arn:aws:organizations::123456789012:ou/o-123example/
ou-1234-5example}]"
```

> **Note**
>
> Sie brauchen die Amazon-EBS-Snapshots, auf die ein AMI verweist, nicht zu teilen, um das AMI zu teilen. Nur das AMI selbst muss freigegeben werden. Das System stellt automatisch Instance-Zugriff auf die referenzierten Amazon-EBS-Snapshots für den Start bereit. Sie müssen jedoch die KMS-Schlüssel freigeben, die zum Verschlüsseln von Snapshots

verwendet werden, auf die das AMI verweist. Weitere Informationen finden Sie unter Organisationen und OEs erlauben, einen KMS-Schlüssel zu verwenden.

Beenden der Freigabe eines AMI

Sie können die Amazon EC2 EC2-Konsole oder die verwenden AWS CLI , um die gemeinsame Nutzung eines AMI mit einer Organisation oder Organisationseinheit zu beenden.

Beenden der Freigabe eines AMI (Konsole)

So beenden Sie die Freigabe eines AMI für eine Organisation oder OE mithilfe der Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie das AMI in der Liste aus und wählen Sie dann Aktionen, AMI-Berechtigungen bearbeiten aus.
4. Wählen Sie unter Shared organizations/OUs (Gemeinsame Organisationen/OEs) die Organisationen oder OEs aus, für die Sie die Freigabe des AMI beenden möchten, und wählen Sie dann Remove selected (Auswahl entfernen) aus.
5. Wählen Sie abschließend Save changes (Änderungen speichern) aus.
6. (Optional) Um zu bestätigen, dass Sie das AMI nicht mehr für die Organisationen oder OEs freigeben, wählen Sie das AMI in der Liste und dann die Registerkarte Berechtigungen aus und scrollen Sie nach untenShared organizations/OUs (Gemeinsame Organisationen/OEs)aus.

Beenden der Freigabe eines AMI (AWS CLI)

Verwenden Sie die Befehle modify-image-attribute oder reset-image-attribute (AWS CLI), um die Freigabe eines AMI zu beenden.

Um die gemeinsame Nutzung eines AMI mit einer Organisation oder Organisationseinheit zu beenden, verwenden Sie den AWS CLI

Der Befehl modify-image-attribute entfernt Startberechtigungen für das angegebene AMI von der angegebenen Organisation. Beachten Sie, dass Sie den ARN angeben müssen.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
```

```
    --launch-permission
 "Remove=[{OrganizationArn=arn:aws:organizations::123456789012:organization/
o-123example}]"
```

Um die gemeinsame Nutzung eines AMI mit allen Organisationen und Organisationseinheiten zu beenden und die AWS-Konten Verwendung von AWS CLI

Der reset-image-attribute-Befehl entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

> **Note**
>
> Sie können die Freigabe eines AMI für ein bestimmtes Konto nicht beenden, wenn es sich in einer Organisation oder OE befindet, für die ein AMI freigegeben ist. Wenn Sie versuchen, die Freigabe des AMI zu beenden, indem Sie die Startberechtigungen für das Konto entfernen, gibt Amazon EC2 eine Erfolgsmeldung zurück. Das AMI ist jedoch weiterhin für das Konto freigegeben.

Anzeigen der Organisationen und OEs, für die ein AMI freigegeben ist

Sie können die Amazon EC2 EC2-Konsole oder die verwenden AWS CLI , um zu überprüfen, mit welchen Organisationen und Organisationseinheiten Sie Ihr AMI geteilt haben.

Anzeigen der Organisationen und OEs, für die ein AMI freigegeben ist (Konsole)

So prüfen Sie, für welche Organisationen und OEs Sie Ihr AMI über die Konsole freigegeben haben

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie das AMI in der Liste und dann die Registerkarte Berechtigungen aus und scrollen Sie nach unten zu Shared organizations/OUs (Gemeinsame Organisationen/OEs).

   Um AMIs zu finden, die für Sie freigegeben wurden, lesen Sie Suchen gemeinsamer AMIs.

Anzeigen der Organisationen und OEs, für die ein AMI freigegeben ist (AWS CLI)

Sie können überprüfen, für welche Organisationen und OEs Sie Ihr AMI freigegeben haben, indem Sie den Befehl describe-image-attribute (AWS CLI) und das `launchPermission`-Attribut verwenden.

Um zu überprüfen, mit welchen Organisationen und Organisationseinheiten Sie Ihr AMI geteilt haben, indem Sie den AWS CLI

Der Befehl describe-image-attribute beschreibt das `launchPermission`-Attribut für das angegebene AMI und gibt die Organisationen und OEs zurück, für die Sie das AMI freigegeben haben.

```
aws ec2 describe-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Beispielantwort

```
{
    "ImageId": "ami-0abcdef1234567890",
    "LaunchPermissions": [
        {
            "OrganizationalUnitArn": "arn:aws:organizations::111122223333:ou/
o-123example/ou-1234-5example"
        }
    ]
}
```

ARN abrufen

Die ARNs der Organisation und der Organisationseinheit enthalten die 12-stellige Verwaltungskontonummer. Wenn Sie die Verwaltungskontonummer nicht kennen, können Sie die Organisation und die Organisationseinheit beschreiben, um den jeweiligen ARN zu erhalten. In den folgenden Beispielen ist `123456789012` die Verwaltungskontonummer.

Bevor Sie die ARNs erhalten können, müssen Sie die Berechtigung haben, Organisationen und Organisationseinheiten zu beschreiben. Die folgende Richtlinie bietet die erforderliche Berechtigung.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:Describe*"
            ],
            "Resource": "*"
        }
    ]
}
```

So erhalten Sie den ARN einer Organisation

Verwenden Sie den Befehl describe-organization und den `--query`-Parameter der auf `'Organization.Arn'` gesetzt ist, um nur den Organisations-ARN zurückzugeben.

```
aws organizations describe-organization --query 'Organization.Arn'
```

Beispielantwort

```
"arn:aws:organizations::123456789012:organization/o-123example"
```

So erhalten Sie den ARN einer Organisationseinheit

Verwenden Sie den Befehl describe-organizational-unit, geben Sie die OE-ID an und setzen Sie den `--query`-Parameter auf `'OrganizationalUnit.Arn'`, um nur den ARN der Organisationseinheit zurückzugeben.

```
aws organizations describe-organizational-unit --organizational-unit-
id ou-1234-5example --query 'OrganizationalUnit.Arn'
```

Beispielantwort

```
"arn:aws:organizations::123456789012:ou/o-123example/ou-1234-5example"
```

Freigeben eines AMI für bestimmte AWS -Konten

Sie können ein AMI mit bestimmten Personen teilen, AWS-Konten ohne das AMI zu veröffentlichen. Sie benötigen lediglich die AWS-Konto IDs.

Eine AWS-Konto ID ist eine 12-stellige Zahl`012345678901`, die z. B. eine AWS-Konto eindeutig identifiziert. Weitere Informationen finden Sie in der SQL-Referenz zu AWS-Konto im AWS Account Management -Entwicklerhandbuch.

Überlegungen

Beachten Sie Folgendes, wenn Sie AMIs mit bestimmten AWS-Konten teilen.

- Eigentümerschaft – Um ein AMI freizugeben, muss Ihr AWS-Konto Besitzer des AMI sein.
- Freigabelimits – Informationen zur maximalen Anzahl von Entitäten, für die ein AMI innerhalb einer Region freigegeben werden kann, finden Sie unter Amazon-EC2-Service-Quotas.
- Tags – Sie können keine benutzerdefinierten Tags (Tags, die Sie einem AMI anfügen) freigeben. Wenn Sie ein AMI teilen, sind Ihre benutzerdefinierten Tags für niemanden verfügbar, mit dem AWS-Konto das AMI geteilt wird.
- Verschlüsselung und Schlüssel: Sie können AMIs freigeben, die durch unverschlüsselte und verschlüsselte Snapshots unterstützt werden.
  - Die verschlüsselten Snapshots müssen mit einem KMS-Schlüssel verschlüsselt werden. Sie können keine AMIs freigeben, die von Snapshots unterstützt werden, die mit dem verwalteten Standardschlüssel AWS verschlüsselt sind.
  - Wenn Sie ein AMI teilen, das von verschlüsselten Snapshots unterstützt wird, müssen Sie zulassen, dass die AWS-Konten KMS-Schlüssel verwendet werden, die zum Verschlüsseln der Snapshots verwendet wurden. Weitere Informationen finden Sie unter Organisationen und OEs erlauben, einen KMS-Schlüssel zu verwenden. Informationen zur Einrichtung der Schlüsselrichtlinie, die Sie zum Starten von Auto Scaling Scaling-Instances benötigen, wenn Sie einen vom Kunden verwalteten Schlüssel für die Verschlüsselung verwenden, finden Sie unter Erforderliche AWS KMS key Richtlinie für die Verwendung mit verschlüsselten Volumes im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Region: AMIs sind eine regionale Ressource. Wenn Sie ein AMI freigeben, ist es nur in der entsprechenden Region verfügbar. Um ein AMI in einer anderen Region verfügbar zu machen, kopieren Sie das AMI in die Region und geben Sie es dann frei. Weitere Informationen finden Sie unter Kopieren eines AMI.
- Nutzung: Wenn Sie ein AMI freigeben, können Benutzer Instances nur über das AMI starten. Sie können es nicht löschen, teilen oder ändern. Nachdem sie jedoch eine Instance mit Ihrem AMI gestartet haben, können sie dann ein AMI aus ihrer eigenen Instance erstellen.

- Kopieren gemeinsam verwendeter AMIs: Wenn Benutzer in einem anderen Konto ein freigegebenes AMI kopieren möchten, müssen Sie ihnen Leseberechtigungen für den Speicher erteilen, der das AMI sichert. Weitere Informationen finden Sie unter Kontoübergreifendes Kopieren.
- Abrechnung — Ihnen wird nichts in Rechnung gestellt, wenn Ihr AMI von anderen AWS-Konten zum Starten von Instances verwendet wird. Die Konten, die Instances mit dem AMI starten, werden für die Instances abgerechnet, die sie starten.

Freigeben eines AMI (Konsole)

Erteilen expliziter Startberechtigungen mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie das AMI in der Liste aus und wählen Sie dann Aktionen, AMI-Berechtigungen bearbeiten aus.
4. Wählen Sie Private (Privat) aus.
5. Wählen Sie unter Freigegebene Konten die Option Konto-ID hinzufügen aus.
6. Geben Sie unter AWS-Konto ID die AWS-Konto ID ein, mit der Sie das AMI teilen möchten, und wählen Sie dann Share AMI aus.

   Um dieses AMI für mehrere Konten freizugeben, wiederholen Sie die Schritte 5 und 6, bis Sie alle erforderlichen Konto-IDs hinzugefügt haben.

   > **Note**
   >
   > Sie brauchen die Amazon EBS-Snapshots, auf die ein AMI verweist, nicht zu teilen, um das AMI zu teilen. Nur das AMI selbst muss geteilt werden. Das System stellt automatisch Instancezugriff auf die referenzierten Amazon EBS-Snapshots für den Start bereit. Sie müssen jedoch sämtliche KMS-Schlüssel teilen, die zum Verschlüsseln von Snapshots verwendet werden, auf die das AMI verweist. Weitere Informationen finden Sie unter Einen Amazon EBS-Snapshot teilen im Amazon EBS-Benutzerhandbuch.

7. Wählen Sie abschließend Änderungen speichern aus.

8. (Optional) Um die AWS-Konto IDs anzuzeigen, mit denen Sie das AMI geteilt haben, wählen Sie das AMI in der Liste aus und klicken Sie dann auf die Registerkarte Berechtigungen. Um AMIs zu finden, die für Sie freigegeben wurden, lesen Sie Suchen gemeinsamer AMIs.

Ein AMI teilen (Tools für Windows PowerShell)

Verwenden Sie den Edit-EC2ImageAttributeBefehl (Tools für Windows PowerShell), um ein AMI gemeinsam zu nutzen, wie in den folgenden Beispielen gezeigt.

Erteilen expliziter Startberechtigungen

Der folgende Befehl erteilt Startberechtigungen für die angegebene AMI an das angegebene AWS-Konto. Ersetzen Sie im folgenden Beispiel die AMI-ID des Beispiels durch eine gültige AMI-ID und *account-id* ersetzen Sie sie durch die 12-stellige AWS-Konto ID.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType add -UserId "account-id"
```

> **Note**
>
> Sie brauchen die Amazon EBS-Snapshots, auf die ein AMI verweist, nicht zu teilen, um das AMI zu teilen. Nur das AMI selbst muss geteilt werden. Das System stellt automatisch Instancezugriff auf die referenzierten Amazon EBS-Snapshots für den Start bereit. Sie müssen jedoch sämtliche KMS-Schlüssel teilen, die zum Verschlüsseln von Snapshots verwendet werden, auf die das AMI verweist. Weitere Informationen finden Sie unter Einen Amazon EBS-Snapshot teilen im Amazon EBS-Benutzerhandbuch.

Entfernen von Startberechtigungen für ein Konto

Der folgende Befehl entfernt Startberechtigungen für die angegebene AMI vom angegebenen AWS-Konto. Ersetzen Sie im folgenden Beispiel die AMI-ID des Beispiels durch eine gültige AMI-ID und *account-id* ersetzen Sie sie durch die 12-stellige AWS-Konto ID.

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission -OperationType remove -UserId "account-id"
```

Entfernen aller Startberechtigungen

Der folgende Befehl entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt. Ersetzen Sie im folgenden Beispiel die Beispiel-AMI-ID durch eine gültige AMI-ID.

```
PS C:\> Reset-EC2ImageAttribute -ImageId ami-0abcdef1234567890 -Attribute
 launchPermission
```

Freigeben eines AMI (AWS CLI)

Verwenden Sie den Befehl modify-image-attribute (AWS CLI), um ein AMI wie in den folgenden Beispielen gezeigt freizugeben.

Erteilen expliziter Startberechtigungen

Der folgende Befehl erteilt Startberechtigungen für die angegebene AMI an das angegebene AWS-Konto. Ersetzen Sie im folgenden Beispiel die AMI-ID des Beispiels durch eine gültige AMI-ID und *account-id* ersetzen Sie sie durch die 12-stellige AWS-Konto ID.

```
aws ec2 modify-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Add=[{UserId=account-id}]"
```

> **Note**
>
> Sie brauchen die Amazon EBS-Snapshots, auf die ein AMI verweist, nicht zu teilen, um das AMI zu teilen. Nur das AMI selbst muss geteilt werden. Das System stellt automatisch Instancezugriff auf die referenzierten Amazon EBS-Snapshots für den Start bereit. Sie müssen jedoch sämtliche KMS-Schlüssel teilen, die zum Verschlüsseln von Snapshots verwendet werden, auf die das AMI verweist. Weitere Informationen finden Sie unter Einen Amazon EBS-Snapshot teilen im Amazon EBS-Benutzerhandbuch.

Entfernen von Startberechtigungen für ein Konto

Der folgende Befehl entfernt Startberechtigungen für die angegebene AMI vom angegebenen AWS-Konto. Ersetzen Sie im folgenden Beispiel die AMI-ID des Beispiels durch eine gültige AMI-ID und *account-id* ersetzen Sie sie durch die 12-stellige AWS-Konto ID.

```
aws ec2 modify-image-attribute \
```

```
    --image-id ami-0abcdef1234567890 \
    --launch-permission "Remove=[{UserId=account-id}]"
```

Entfernen aller Startberechtigungen

Der folgende Befehl entfernt alle öffentlichen und expliziten Startberechtigungen vom angegebenen AMI. Hinweis: Der Besitzer des AMI hat immer Startberechtigungen und bleibt daher von dem Befehl unberührt. Ersetzen Sie im folgenden Beispiel die Beispiel-AMI-ID durch eine gültige AMI-ID.

```
aws ec2 reset-image-attribute \
    --image-id ami-0abcdef1234567890 \
    --attribute launchPermission
```

Kündigen Sie die gemeinsame Nutzung eines AMI mit Ihrem AWS-Konto

Ein Amazon Machine Image (AMI) kann für bestimmte AWS-Konten freigegeben werden, indem die Konten zu den Startberechtigungen des AMI hinzugefügt werden. Wenn ein AMI mit Ihrem geteilt wurde AWS-Konto und Sie nicht mehr möchten, dass es mit Ihrem Konto geteilt wird, können Sie Ihr Konto aus den Startberechtigungen des AMI entfernen. Sie tun dies, indem Sie den `cancel-image-launch-permission` AWS CLI Befehl ausführen. Wenn Sie diesen Befehl ausführen, werden Ihnen AWS-Konto die Startberechtigungen für das angegebene AMI entzogen.

Sie können beispielsweise die Freigabe eines AMI für Ihr Konto aufheben, um die Wahrscheinlichkeit zu verringern, dass eine Instance mit einem ungenutzten oder veralteten AMI gestartet wird, das für Sie freigegeben wurde. Wenn Sie die Freigabe eines AMI für Ihr Konto aufheben, wird es nicht mehr in AMI-Listen in der EC2-Konsole oder in der Ausgabe für describe-images angezeigt.

Themen

- Einschränkungen
- Aufheben der Freigabe eines AMI für Ihr Konto
- AMIs finden, die für Ihr Konto freigegeben sind

Einschränkungen

- Sie können Ihr Konto aus den Startberechtigungen eines AMI entfernen, das AWS-Konto nur mit Ihnen geteilt wird. Sie können `cancel-image-launch-permission` nicht verwenden, um Ihr Konto aus den Startberechtigungen eines AMI zu entfernen, das für eine Organisation oder Organisationseinheit (OE) freigegeben ist, oder um den Zugriff auf öffentliche AMIs zu entfernen.

- Sie können Ihr Konto nicht dauerhaft aus den Startberechtigungen eines AMI entfernen. Ein AMI-Besitzer kann ein AMI wieder mit Ihrem -Konto teilen.
- AMIs sind eine regionale Ressource. Beim Ausführen von `cancel-image-launch-permission` müssen Sie die Region angeben, in der sich das AMI befindet. Geben Sie entweder die Region im Befehl an oder verwenden Sie die Umgebungsvariable AWS_DEFAULT_REGION.
- Nur die SDKs AWS CLI und unterstützen das Entfernen Ihres Kontos aus den Startberechtigungen eines AMI. Die EC2-Konsole unterstützt diese Aktion derzeit nicht.

Aufheben der Freigabe eines AMI für Ihr Konto

> **Note**
>
> Nachdem Sie die Freigabe eines AMI für Ihr Konto aufgehoben haben, können Sie dies nicht mehr rückgängig machen.. Um wieder Zugriff auf das AMI zu erhalten, muss der AMI-Besitzer es für Ihr Konto freigeben.

AWS CLI

Um zu kündigen, dass ein AMI mit Ihrem geteilt wird AWS-Konto

Verwenden Sie den Befehl cancel-image-launch-permission und geben Sie die AMI-ID an.

```
aws ec2 cancel-image-launch-permission \
    --image-id ami-0123456789example \
    --region us-east-1
```

Erwartete Ausgabe

```
{
    "Return": true
}
```

PowerShell

Um zu kündigen, dass ein AMI mit Ihnen geteilt wird, AWS-Konto indem Sie AWS Tools for PowerShell

Verwenden Sie den Befehl Stop-EC2ImageLaunchPermission und geben Sie die AMI-ID an.

```
Stop-EC2ImageLaunchPermission `
    -ImageId ami-0123456789example `
    -Region us-east-1
```

Erwartete Ausgabe

```
True
```

AMIs finden, die für Ihr Konto freigegeben sind

Informationen zu den AMIs, die mit Ihrem geteilt wurden AWS-Konto, finden Sie unterSuchen gemeinsamer AMIs.

Verwenden von Lesezeichen

Wenn Sie ein öffentliches AMI erstellt oder ein AMI mit einem anderen geteilt haben AWS-Konto, können Sie ein Lesezeichen erstellen, das es einem Benutzer ermöglicht, auf Ihr AMI zuzugreifen und sofort eine Instance in seinem eigenen Konto zu starten. Dies ist eine einfache Möglichkeit, um AMI-Referenzen zu teilen, damit Benutzer das AMI schneller finden und verwenden können.

Hinweis: Das AMI muss öffentlich sein oder Sie müssen es mit dem Benutzer geteilt haben, dem Sie das Lesezeichen senden möchten.

Erstellen von Lesezeichen für ein AMI

1. Geben Sie eine URL mit den folgenden Informationen ein. Geben Sie dabei für region die Region des AMI an:

   ```
   https://console.aws.amazon.com/ec2/v2/home?
   region=region#LaunchInstanceWizard:ami=ami_id
   ```

   Diese URL startet beispielsweise eine Instance aus dem AMI ami-0abcdef1234567890 in der `us-east-1`-Region USA Ost (Nord-Virginia):

   ```
   https://console.aws.amazon.com/ec2/v2/home?region=us-
   east-1#LaunchInstanceWizard:ami=ami-0abcdef1234567890
   ```

2. Teilen Sie den Link mit den Benutzern, die das AMI verwenden möchten.

3. Um ein Lesezeichen zu verwenden, wählen Sie den Link oder kopieren Sie ihn und fügen Sie ihn in den Browser ein. Der Launch Wizard wird geöffnet. Das AMI ist bereits ausgewählt.

Richtlinien für gemeinsame Linux-AMIs

Befolgen Sie folgende Richtlinien, um die Angriffsfläche zu verkleinern und die Zuverlässigkeit der erstellen AMIs zu erhöhen.

> **Important**
>
> Die Liste der Sicherheitsrichtlinien kann sehr umfassend sein. Seien Sie beim Erstellen gemeinsamer AMIs vorsichtig und überlegen Sie sorgfältig, an welcher Stelle empfindliche Daten offengelegt werden könnten.

Inhalt

Wenn Sie AMIs für erstellen AWS Marketplace, finden Sie im AWS Marketplace Verkäuferleitfaden unter Bewährte Methoden zum Erstellen von AMIs Richtlinien, Richtlinien und Best Practices.

Zusätzliche Informationen zum sicheren Teilen von AMIs finden Sie in den folgenden Artikeln:

- Sicheres Teilen und Verwenden öffentlicher AMIs
- Public AMI Publishing: Hardening and Clean-up Requirements

Aktualisieren der AMI-Tools vor der Verwendung

Für Instance Store-Backed AMIs empfehlen wir, die Amazon EC2 AMI-Erstellungstools während des Startups herunterzuladen und ein Upgrade durchzuführen, bevor Sie sie verwenden. Hierdurch

wird sichergestellt das neue AMIs, die auf gemeinsamen AMIs basieren, die aktuellsten AMI-Tools aufweisen.

Für Amazon Linux 2 installieren Sie das `aws-amitools-ec2`-Paket und fügen die AMI-Tools Ihrem Pfad mit dem folgenden Befehl hinzu. Für das Amazon Linux AMI ist das `aws-amitools-ec2`-Paket standardmäßig installiert.

```
[ec2-user ~]$ sudo yum install -y aws-amitools-ec2 && export PATH=$PATH:/opt/aws/bin
 > /etc/profile.d/aws-amitools-ec2.sh && . /etc/profile.d/aws-amitools-ec2.sh
```

Aktualisieren Sie die AMI-Tools mit dem folgenden Befehl:

```
[ec2-user ~]$ sudo yum upgrade -y aws-amitools-ec2
```

Stellen Sie für andere Verteilungen sicher, dass die aktuellen AMI-Tools installiert sind.

Deaktivieren von passwortbasierten Fernanmeldungen für den Stammbenutzer

Die Verwendung fester Root-Passwörter für öffentliche AMIs ist ein Sicherheitsrisiko, das schnell bekannt werden kann. Wenn die Benutzer bei der ersten Anmeldung zum Ändern des Passworts aufgefordert werden, bietet sich hierbei eine potenzielle Möglichkeit des Missbrauchs.

Um das Problem zu beheben, deaktivieren Sie die Passwort-basierte Remoteanmeldung für den Root-Benutzer.

Deaktivieren von passwortbasierten Fernanmeldungen für den Stammbenutzer

1. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Textbearbeitungsprogramm und suchen Sie nach folgender Zeile:

   ```
   #PermitRootLogin yes
   ```

2. Ändern Sie die Zeile folgendermaßen:

   ```
   PermitRootLogin without-password
   ```

   Der Speicherort dieser Konfigurationsdatei weicht von Ihrer Verteilung ggf. ab. Das ist auch der Fall, wenn Sie nicht OpenSSH verwenden. Ist dies der Fall, schlagen Sie in der entsprechenden Dokumentation nach.

Deaktivieren des lokalen Root-Zugriffs

Wenn Sie gemeinsame AMIs verwenden, hat sich das Deaktivieren direkter Root-Anmeldung als bewährte Methode etabliert. Melden Sie sich hierfür in der ausgeführten Instance an und geben Sie den folgenden Befehl aus:

```
[ec2-user ~]$ sudo passwd -l root
```

> **Note**
>
> Der Befehl beeinträchtigt nicht die Verwendung von `sudo`.

Entfernen von SSH-Host-Schlüsselpaaren

Wenn Sie ein von einem öffentlichen AMI abgeleitetes AMI teilen möchten, entfernen Sie die bestehenden SSH-Host-Schlüsselpaare in `/etc/ssh`. Hierdurch erstellt die SSH-Funktion neue eindeutige SSH-Schlüsselpaare, wenn eine Instance mit dem AMI gestartet wird. Dies verbessert die Sicherheit und verringert die Wahrscheinlichkeit von „Man-In-the-Middle (MITM)“-Angriffen.

Entfernen Sie die folgenden Schlüsseldateien aus Ihrem System.

- ssh_host_dsa_key
- ssh_host_dsa_key.pub
- ssh_host_key
- ssh_host_key.pub
- ssh_host_rsa_key
- ssh_host_rsa_key.pub
- ssh_host_ecdsa_key
- ssh_host_ecdsa_key.pub
- ssh_host_ed25519_key
- ssh_host_ed25519_key.pub

Sie können all diese Dateien mit folgendem Befehl sicher entfernen.

```
[ec2-user ~]$ sudo shred -u /etc/ssh/*_key /etc/ssh/*_key.pub
```

> **Warning**
>
> Dienstprogramme zum sicheren Entfernen wie **`shred`** entfernen möglicherweise nicht alle Kopien einer Datei vom Speichermedium. Journaling-Dateisysteme (u. a. Amazon Linux default ext4), Snapshots, Sicherungen, RAID und temporäres Caching erstellen möglicherweise versteckte Kopien von Dateien. Weitere Informationen finden Sie in der **`shred`** -Dokumentation.

> **Important**
>
> Wenn Sie die bestehenden SSH-Host-Schlüsselpaare nicht aus dem öffentlichen AMI entfernen, benachrichtigt unser routinemäßiger Prüfprozess Sie und alle Kunden, die Instances des AMI ausführen, über potenzielle Sicherheitsrisiken. Nach einer kurzen Übergangsfrist wird das AMI als privat markiert.

Installieren von Anmeldeinformationen für öffentliche Schlüssel

Wenn Sie das AMI so konfigurieren, dass keine Passwortanmeldung möglich ist, müssen Sie eine anderen Anmeldemethode für die Benutzer bereitstellen.

Amazon EC2 ermöglicht den Benutzern die Angabe eines öffentlich-privaten Schlüsselpaar-Namens beim Starten einer Instance. Wenn dem `RunInstances`-API-Aufruf (oder mittels Befehlszeilen-API-Tools) ein gültiger Schlüsselpaarname bereitgestellt wird, wird der öffentliche Schlüssel (der Teil des Schlüsselpaars, den Amazon EC2 nach einem `CreateKeyPair`- oder `ImportKeyPair`-Aufruf auf dem Server speichert) der Instance mittels HTTP-Abfrage gegen die Instance-Metadaten verfügbar gemacht.

Wenn Sie sich via SSH anmelden möchten, muss das AMI den Schlüsselwert beim Starten abrufen und `/root/.ssh/authorized_keys` (oder der entsprechenden Datei für das entsprechende Benutzerkonto im AMI) anhängen. Benutzer können Instances des AMI mit einem Schlüsselpaar starten und sich ohne Root-Passwort anmelden.

Viele Verteilungen, u. a. Amazon Linux und Ubuntu, verwenden das `cloud-init`-Paket zum Einfügen von Anmeldeinformationen für öffentliche Schlüssel für einen konfigurierten Benutzer. Wenn die Verteilung `cloud-init` nicht unterstützt, fügen Sie dem System-Startup-Skript (z. B. `/etc/`

`rc.local`) den folgenden Code hinzu, um den öffentlichen Schlüssel abzurufen, den Sie beim Start für den Root-Benutzer angegeben haben.

> **Note**
>
> Im folgenden Beispiel ist die IP-Adresse http://169.254.169.254/ eine lokale (link-local) Adresse und nur von der Instance aus gültig.

IMDSv2

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-
token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

IMDSv1

```
if [ ! -d /root/.ssh ] ; then
        mkdir -p /root/.ssh
        chmod 700 /root/.ssh
fi
# Fetch public key using HTTP
curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key > /tmp/my-key
if [ $? -eq 0 ] ; then
        cat /tmp/my-key >> /root/.ssh/authorized_keys
        chmod 700 /root/.ssh/authorized_keys
        rm /tmp/my-key
fi
```

Dies kann auf jeden Benutzer angewendet werden. Sie müssen es nicht auf den `root`-Benutzer beschränken.

> **Note**
>
> Beim erneuten Bündeln einer Instance basierend auf dem AMI wird der Schlüssel eingebunden, mit dem es gestartet wurde. Damit der Schlüssel nicht eingebunden wird, löschen (oder entfernen) Sie die `authorized_keys`-Datei oder schließen Sie diese Datei vom erneuten Bündeln aus.

Deaktivieren Sie SSHD-DNS-Prüfungen (optional)

Durch das Deaktivieren von sshd-DNS-Prüfungen wird die sshd-Sicherheit beeinträchtigt. Wenn bei der DNS-Auflösung allerdings ein Fehler auftritt, funktioniert die SSH-Anmeldung weiterhin. Wenn Sie die sshd-Prüfungen nicht deaktivieren, wird die Anmeldung durch Fehler bei der DNS-Auflösung verhindert.

Deaktivieren von sshd-DNS-Prüfungen

1. Öffnen Sie die Datei `/etc/ssh/sshd_config` in einem Textbearbeitungsprogramm und suchen Sie nach folgender Zeile:

   ```
   #UseDNS yes
   ```

2. Ändern Sie die Zeile folgendermaßen:

   ```
   UseDNS no
   ```

> **Note**
>
> Der Speicherort dieser Konfigurationsdatei kann von Ihrer Verteilung abweichen. Das ist auch der Fall, wenn Sie nicht OpenSSH verwenden. Ist dies der Fall, schlagen Sie in der entsprechenden Dokumentation nach.

Eigenschutz

Wir empfehlen, keine empfindlichen Daten oder empfindliche Software auf AMIs zu speichern, die Sie teilen. Benutzer, die ein gemeinsames AMI starten, könnten es erneut bündeln und als ihr eigenes registrieren. Gehen Sie folgendermaßen vor, um keine Sicherheitsrisiken zu übersehen:

- Wir empfehlen, die `--exclude` *`directory`*-Option für `ec2-bundle-vol` zu verwenden, um die Verzeichnisse und Unterverzeichnisse zu überspringen, die geheime Informationen enthalten. Schließen Sie beim Bündeln des Images vor allem alle öffentlichen/privaten SSH-Schlüsselpaare von Benutzern und SSH-`authorized_keys`-Dateien aus. Die öffentlichen Amazon-AMIs speichern diese für den Stamm-Benutzer in `/root/.ssh` und für normale Benutzer in /home/*`user_name`*`/.ssh/`. Weitere Informationen finden Sie unter ec2-bundle-vol.
- Löschen Sie vor dem Bündeln immer den Shell-Verlauf. Wenn Sie versuchen, mehr als einen Bundle-Upload im selben AMI durchzuführen, enthält der Shell-Verlauf Ihren Zugriffsschlüssel. Das folgende Beispiel muss der letzte ausgeführte Befehl vor dem Bündeln in einer Instance sein.

  ```
  [ec2-user ~]$ shred -u ~/.*history
  ```

  > **Warning**
  >
  > Die in der Warnung oben beschriebenen Einschränkungen von **`shred`** gelten auch hier. Hinweis: Bash schreibt den Verlauf der aktuellen Sitzung beim Beenden auf den Datenträger. Wenn Sie sich nach dem Löschen von `~/.bash_history` von der Instance ab- und anschließend wieder anmelden, werden Sie feststellen, dass die `~/.bash_history`-Datei neu erstellt wurde und alle Befehle enthält, die während der vorherigen Sitzung ausgeführt wurden.
  > Neben Bash schreiben auch andere Programme Verlaufsdaten auf den Datenträger. Seien Sie vorsichtig und entfernen Sie unnötige DOT-Dateien und -Verzeichnisse.

- Zum Bündeln einer ausgeführten Instance sind Ihr privater Schlüssel und das X.509-Zertifikat erforderlich. Legen Sie diese Daten und anderen Anmeldeinformationen an einem Speicherort ab, der nicht gebündelt wird (z. B. den Instance-Speicher).

Gebührenpflichtige AMIs

Ein kostenpflichtiges AMI ist ein AMI, das in der zum Verkauf angeboten wird AWS Marketplace. Das AWS Marketplace ist ein Online-Shop, in dem Sie Software kaufen können AWS, auf der Sie laufen

können, einschließlich AMIs, mit denen Sie Ihre EC2-Instance starten können. Die AWS Marketplace AMIs sind in Kategorien unterteilt, z. B. Entwicklertools, sodass Sie Produkte finden können, die Ihren Anforderungen entsprechen. Weitere Informationen zu AWS Marketplace finden Sie AWS Marketplaceauf der Website.

Sie können AMIs AWS Marketplace von Drittanbietern erwerben, einschließlich AMIs, die mit Serviceverträgen von Organisationen wie Red Hat geliefert werden. Sie können auch ein AMI erstellen und es AWS Marketplace an andere Amazon EC2 EC2-Benutzer verkaufen. Der Aufbau eines sicheren, nutzbaren AMI zum öffentlichen Gebrauch ist ein relativ einfacher Prozess, wenn Sie ein paar simple Richtlinien befolgen. Weitere Informationen zum Erstellen und Verwenden gemeinsamer AMIs finden Sie unter Gemeinsame AMIs.

Der Start einer Instance aus einem gebührenpflichtigen AMI erfolgt auf die gleiche Weise wie der Start aus jedem anderen AMI. Es sind keine zusätzlichen Parameter erforderlich. Die Instance wird gemäß den vom Eigentümer des AMI festgelegten Tarifen sowie den Standardnutzungsgebühren für die zugehörigen Webservices berechnet, z. B. dem Stundensatz für den Betrieb eines m5.small-Instance-Typs in Amazon EC2. Gegebenenfalls fallen zusätzliche Steuern an. Der Eigentümer eines gebührenpflichtigen AMI kann nachvollziehen, ob eine bestimmte Instance mithilfe dieses gebührenpflichtigen AMI gestartet wurde.

> **Important**
>
> Amazon DevPay akzeptiert keine neuen Verkäufer oder Produkte mehr. AWS Marketplace ist jetzt die einzige, einheitliche E-Commerce-Plattform für den Verkauf von Software und Dienstleistungen über AWS. Informationen zur Bereitstellung und zum Verkauf von Software finden Sie AWS Marketplace unter Verkaufen im AWS Marketplace. AWS Marketplace unterstützt AMIs, die von Amazon EBS unterstützt werden.

Inhalt

Verkaufen Ihres AMI

Sie können Ihr AMI verkaufen mit AWS Marketplace. AWS Marketplace bietet ein organisiertes Einkaufserlebnis. Unterstützt AWS Marketplace außerdem AWS Funktionen wie Amazon EBS-gestützte AMIs, Reserved Instances und Spot-Instances.

Informationen darüber, wie Sie Ihr AMI auf dem verkaufen können AWS Marketplace, finden Sie unter Verkaufen im AWS Marketplace.

Suchen eines gebührenpflichtigen AMI

Es gibt mehrere Möglichkeiten, verfügbare AMIs zu finden, die Sie kaufen können. Sie können z. B. AWS Marketplace, die Amazon EC2-Konsole oder die Befehlszeile verwenden. Oder ein Developer informiert Sie selbst über ein gebührenpflichtiges AMI.

Suchen eines gebührenpflichtigen AMI mit der Konsole

So suchen Sie ein gebührenpflichtiges AMI mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie im ersten Filterfeld Public images aus.
4. Wählen Sie in der Suchleiste Besitzer-Alias und dann = und aws-marketplace aus.
5. Wenn Sie den Produktcode kennen, wählen Sie Product Code, dann = und geben Sie dann den Produktcode ein.

Finden Sie ein kostenpflichtiges AMI mit AWS Marketplace

So finden Sie ein kostenpflichtiges AMI mit AWS Marketplace

1. Öffnen Sie AWS Marketplace.
2. Geben Sie den Namen des Betriebssystems in das Suchfeld ein und wählen Sie dann die Suchschaltfläche (Lupe) aus.
3. Sie können die Ergebnisse weiter eingrenzen, indem Sie die Kategorien oder Filter verwenden.
4. Alle Produkte sind mit dem Produkttyp gekennzeichnet: entweder `AMI` oder `Software as a Service`.

Finden Sie ein kostenpflichtiges AMI mit dem AWS CLI

Sie können ein gebührenpflichtiges AMI mit dem folgenden describe-images-Befehl (AWS CLI) suchen.

```
aws ec2 describe-images
    --owners aws-marketplace
```

Dieser Befehl gibt zahlreiche Details zu jedem AMI aus, u. a. auch den Produkt-Code für ein gebührenpflichtiges AMI. Der Eintrag zum Produkt-Code in der Ausgabe von `describe-images` sieht wie folgt aus:

```
"ProductCodes": [
    {
        "ProductCodeId": "product_code",
        "ProductCodeType": "marketplace"
    }
],
```

Wenn Sie den Produktcode kennen, können Sie die Ergebnisse nach Produktcode filtern. Dieses Beispiel gibt das neueste AMI mit dem angegebenen Produktcode zurück.

```
aws ec2 describe-images
    --owners aws-marketplace \
    --filters "Name=product-code,Values=product_code" \
    --query "sort_by(Images, &CreationDate)[-1].[ImageId]"
```

Finden Sie mit den Tools für Windows ein kostenpflichtiges AMI PowerShell

Mit dem folgenden Get-EC2ImageBefehl können Sie ein kostenpflichtiges AMI finden.

```
PS C:\> Get-EC2Image -Owner aws-marketplace
```

In der Ausgabe ist für jedes gebührenpflichtige AMI ein Produkt-Code enthalten.

```
ProductCodeId           ProductCodeType
-------------           ---------------
product_code            marketplace
```

Wenn Sie den Produktcode kennen, können Sie die Ergebnisse nach Produktcode filtern. Dieses Beispiel gibt das neueste AMI mit dem angegebenen Produktcode zurück.

```
PS C:\> (Get-EC2Image -Owner aws-marketplace -Filter @{"Name"="product-
code";"Value"="product_code"} | sort CreationDate -Descending | Select-Object -First
 1).ImageId
```

Kaufen eines gebührenpflichtigen AMI

Sie müssen sich für ein gebührenpflichtiges AMI (bzw. für den Kauf) registrieren, bevor Sie eine Instance mit dem AMI starten können.

In der Regel erhalten Sie vom Verkäufer des gebührenpflichtigen AMI alle erforderlichen Informationen, z. B. den Preis und den Link, unter dem Sie es kaufen können. Wenn Sie auf den Link klicken, werden Sie zunächst aufgefordert, sich anzumelden AWS, und dann können Sie das AMI kaufen.

Kaufen eines gebührenpflichtigen AMI mit der Konsole

Sie können ein gebührenpflichtiges AMI kaufen, indem Sie den Amazon EC2-Launch Wizard verwenden. Weitere Informationen finden Sie unter Starten Sie eine AWS Marketplace Instanz.

Abonnieren Sie ein Produkt mit AWS Marketplace

Um das nutzen zu können AWS Marketplace, benötigen Sie ein AWS Konto. Um Instances von AWS Marketplace Produkten aus zu starten, müssen Sie für die Nutzung des Amazon EC2-Service registriert sein und das Produkt abonniert haben, von dem aus die Instance gestartet werden soll. Es gibt zwei Möglichkeiten, Produkte im AWS Marketplace zu abonnieren:

- AWS Marketplace Website: Mit der 1-Click-Bereitstellungsfunktion können Sie vorkonfigurierte Software schnell starten.
- Der Amazon EC2-Startassistent: Sie können nach einer AMI suchen und eine Instance direkt aus dem Startassistenten starten. Weitere Informationen finden Sie unter Starten Sie eine AWS Marketplace Instanz.

Abrufen des Produkt-Codes für Ihre Instance

Sie können den AWS Marketplace Produktcode für Ihre Instance mithilfe der Instance-Metadaten abrufen. Wenn ein Produkt-Code für die Instance vorhanden ist, wird er von Amazon EC2

ausgegeben. Weitere Informationen zum Abrufen von Metadaten finden Sie unter Abrufen von Instance-Metadaten.

Verwenden Sie den Befehl für das Betriebssystem Ihrer Instanz, um einen Produktcode abzurufen.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/product-codes
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/product-codes
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/product-codes
```

Verwenden von gebührenpflichtigem Support

Mit Amazon EC2 können Developer auch Support für Software (oder abgeleitete AMIs) anbieten. Developer können Produkte für den Support erstellen, und Sie können sich für deren Verwendung registrieren. Bei der Registrierung für das Support-Produkt erhalten Sie von dem Developer einen Produkt-Code, den Sie anschließend mit Ihrem eigenen AMI verknüpfen müssen. Auf diese Weise kann der Developer sicherstellen, dass Ihre Instance berechtigt ist, den Support zu erhalten. Außerdem wird so sichergestellt, dass die Gebühren für das Produkt gemäß der Nutzungsbedingungen des Developers in Rechnung gestellt werden können, wenn Sie diesem Produkt zugeordnete Instances ausführen.

> **Important**
>
> Sie können ein Support-Produkt nicht mit Reserved Instances verwenden. Es wird immer der Preis berechnet, der vom Verkäufer des jeweiligen Support-Produkts angegeben wurde.

Sie verknüpfen einen Produkt-Code mit Ihrem AMI, indem Sie einen der folgenden Befehle verwenden; ami_id steht dabei für die ID des AMI und product_code für den Produkt-Code:

- modify-image-attribute (AWS CLI)

```
aws ec2 modify-image-attribute --image-id ami_id --product-codes "product_code"
```

- Edit-EC2ImageAttribute (AWS Tools for Windows PowerShell)

```
PS C:\> Edit-EC2ImageAttribute -ImageId ami_id -ProductCode product_code
```

Wenn Sie das Attribute für den Produkt-Code gesetzt haben, kann es nicht mehr geändert oder entfernt werden.

Rechnungen für gebührenpflichtige und unterstützte AMIs

Am Monatsende werden Sie per E-Mail benachrichtigt, mit welchem Betrag Ihre Kreditkarte für die Verwendung gebührenpflichtiger oder unterstützter AMIs in diesem Monat belastet wurde. Diese Rechnung wird separat von Ihrer regulären Amazon EC2-Rechnung erstellt. Weitere Informationen finden Sie unter Bezahlen für Produkte im AWS Marketplace -Käuferhandbuch.

Verwalte deine AWS Marketplace Abonnements

Auf der AWS Marketplace Website können Sie Ihre Abonnementdetails überprüfen, die Nutzungshinweise des Anbieters einsehen, Ihre Abonnements verwalten und vieles mehr.

So prüfen Sie Ihre Abonnementdaten

1. Melden Sie sich bei den AWS Marketplace an.
2. Wählen Sie Your Marketplace Account.
3. Wählen Sie Manage Your Software Subscriptions.
4. Alle aktuellen Abonnements werden aufgelistet. Wählen Sie Usage Instructions, um spezielle Informationen für die Nutzung des Products anzuzeigen, z. B. den Benutzernamen für die Verbindung mit Ihrer ausgeführten Instance.

Um ein AWS Marketplace Abonnement zu kündigen

1. Vergewissern Sie sich, dass Sie alle Instances beendet haben, die in dem Abonnement ausgeführt wurden.
   a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie im Navigationsbereich Instances aus.
   c. Wählen Sie die Instance und dann Instance-Status und Instance beenden aus.
   d. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.
2. Melden Sie sich bei AWS Marketplace an, klicken Sie auf Your Marketplace Account (Ihr Marketplace-Konto) und danach auf Manage Your Software Subscriptions (Software-Abonnements verwalten).
3. Wählen Sie Cancel subscription. Sie werden aufgefordert, die Kündigung zu bestätigen.

> **Note**
>
> Wenn Sie Ihr Abonnement gekündigt haben, ist es nicht mehr möglich, Instances aus diesem AMI zu starten. Um dieses AMI erneut verwenden zu können, müssen Sie es erneut abonnieren, entweder auf der AWS Marketplace Website oder über den Startassistenten in der Amazon EC2 EC2-Konsole.

AMI-Lebenszyklus

Sie können Ihre eigenen AMIs erstellen, kopieren, sichern und verwalten, bis Sie bereit sind, sie als veraltet zu kennzeichnen oder abzumelden.

Inhalt

- Ein AMI abmelden (löschen)
- Automatisieren des von EBS-unterstützten AMI-Lebenszyklus

Erstellen eines AMI

Sie können Linux- oder Windows-AMIs erstellen, die von Amazon EBS-Volumes unterstützt werden. Sie können auch Linux-AMIs erstellen, die von Instance-Speicher-Volumes unterstützt werden (Windows-AMIs unterstützen keinen Instance-Speicher für das Root-Gerät). Sie können Windows Sysprep auch verwenden, um Windows-AMIs zu erstellen.

Themen

- Erstellen Sie ein Amazon EBS-backed AMI
- Erstellen einer Instance-Speicher-Backed Linux-AMI
- Erstellen Sie ein AMI mit Windows Sysprep

Erstellen Sie ein Amazon EBS-backed AMI

Um ein Amazon EBS-backed AMI zu erstellen, beginnen Sie mit einer Instance, die Sie über ein vorhandenes Amazon EBS-backed AMI gestartet haben. Dies kann ein AMI sein, von dem Sie bezogen haben AWS Marketplace, ein AMI, das Sie mithilfe von AWS Server Migration Serviceoder VM Import/Export erstellt haben, oder jedes andere AMI, auf das Sie zugreifen können. Wenn Sie die Instance an Ihre Anforderungen angepasst haben, können Sie ein neues AMI erstellen und registrieren, das Sie zum Starten von neuen Instances mit diesen Anpassungen verwenden können.

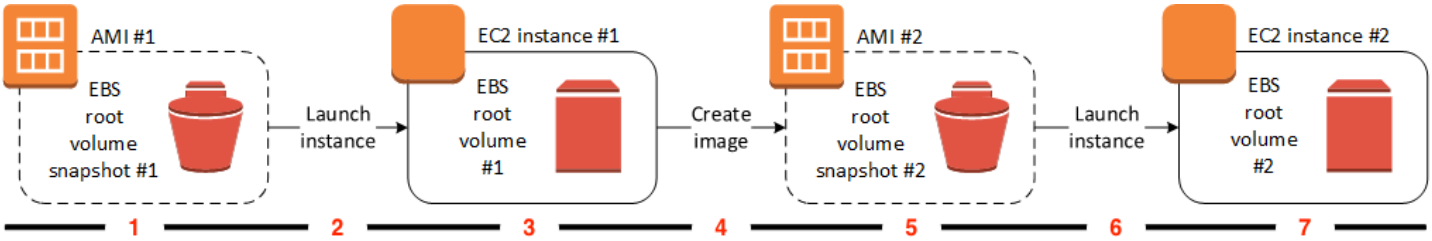
Die unten beschriebenen Verfahren funktionieren für Amazon EC2-Instances mit verschlüsselten Volumes Amazon Elastic Block Store (Amazon EBS) (einschließlich Stamm-Volume) und für unverschlüsselte Volumes.

Für Instance Store-Backed AMI gilt ein anderer AMIs-Erstellungsprozess. Informationen zu den Unterschieden zwischen Amazon EBS-gestützten und Instance-Speicher-gestützte Instances und zur Ermittlung des Root-Gerätetyps für Ihre Instance finden Sie unter Speicher für das Root-Gerät. Hinweise zur Erstellung eines durch einen instance store-backed AMI finden Sie unter. Erstellen einer Instance-Speicher-Backed Linux-AMI

Übersicht über die Erstellung von Amazon EBS-gestützten AMIs

Das folgende Diagramm fasst den Prozess zum Erstellen eines Amazon-EBS-gestützten AMI in einer laufenden EC2-Instance zusammen: Beginnen Sie mit einem vorhandenen AMI, starten Sie

eine Instance, passen Sie sie an, erstellen Sie daraus ein neues AMI und starten Sie schließlich eine Instance Ihres neuen AMI. Die Zahlen im Diagramm stimmen mit den Zahlen in der folgenden Beschreibung überein.



1: AMI Nr. 1: Beginnen Sie mit einem vorhandenen AMI.

Finden Sie ein vorhandenes AMI, das dem zu erstellenden AMI ähnelt. Dies kann ein AMI sein, von dem Sie bezogen haben AWS Marketplace, ein AMI, das Sie mithilfe von AWS Server Migration Serviceoder VM Import/Export erstellt haben, oder jedes andere AMI, auf das Sie zugreifen können. Sie passen dieses AMI an Ihre Bedürfnisse an.

Im Diagramm gibt EBS root volume snapshot #1 (EBS-Root-Volume-Snapshot Nr. 1) an, dass das AMI ein Amazon-EBS-gestütztes AMI ist und dass Informationen über das Root-Volume in diesem Snapshot gespeichert sind.

2: Starten Sie eine Instance über ein vorhandenes AMI.

Um ein AMI zu konfigurieren, starten Sie eine Instance über das AMI, auf dem Ihr neues AMI basieren soll, und passen Sie die Instance an (im Diagramm mit 3 gekennzeichnet). Dann erstellen Sie ein neues AMI, das die Anpassungen enthält (4 im Diagramm).

3: EC2-Instance Nr. 1: Passen Sie die Instance an.

Stellen Sie eine Verbindung mit Ihrer Instance her und passen Sie sie an Ihre Bedürfnisse an. Ihr neues AMI wird diese Anpassungen enthalten.

Sie können die folgenden Aktionen für Ihre Instance durchführen, um sie anzupassen:

- Installieren von Software und Anwendungen
- Kopieren von Daten
- Reduzieren der Startzeit durch Löschen von temporären Dateien und Defragmentieren Ihrer Festplatte
- Anfügen zusätzlicher EBS-Volumes

4: Erstellen Sie ein Image.

Wenn Sie ein AMI aus einer Instance erstellen, fährt Amazon EC2 die Instance vor dem Erstellen des AMI herunter, um sicherzustellen, dass alle Vorgänge auf der Instance angehalten werden und sich während des Erstellungsprozesses in einem einheitlichen Zustand befinden. Wenn Sie sicher sind, dass sich die Instance in einem einheitlichen und für die AMI-Erstellung geeigneten Zustand befindet, können Sie Amazon EC2 anweisen, die Instance nicht herunterzufahren und neu zu starten. Bei einigen Dateisystemen, z. B. XFS, können Aktivitäten vorübergehend eingefroren werden, damit das Image ohne Neustart der Instance auf sichere Weise erstellt werden kann.

Während der AMI-Erstellung erstellt Amazon EC2 Snapshots des Stamm-Volumes Ihrer Instance und von allen anderen EBS-Volumes, die an Ihre Instance angefügt sind. Ihnen werden Gebühren für die Snapshots in Rechnung gestellt, bis Sie die Registrierung des AMI aufheben und die Snapshots löschen. Wenn an die Instance angefügte Volumes verschlüsselt sind, wird das neue AMI nur auf den Instances erfolgreich gestartet, die Amazon-EBS-Verschlüsselung unterstützen.

Je nach der Größe des Volumes kann die Erstellung des AMI mehrere Minuten in Anspruch nehmen (manchmal sogar bis zu 24 Stunden). Es kann deutlich effizienter sein, vor der Erstellung eines AMI Snapshots der Volumes zu erstellen. Auf diese Weise müssen bei der AMI-Erstellung nur kleine, inkrementelle Snapshots erstellt werden und der Prozess ist schneller abgeschlossen (die Gesamtzeit der Snapshoterstellung bleibt gleich).

5: AMI Nr. 2: Neues AMI

Nach Abschluss des Prozesses verfügen Sie über ein neues AMI und einen Snapshot Snapshot Nr. 2, der für das Root-Volume der Instance erstellt wurde. Wenn Sie der Instance zusätzlich zum Root-Gerät-Volume Instance-Speicher-Volumes oder EBS-Volumes hinzugefügt haben, enthält die Blockgerät-Zuweisung für das neue AMI Informationen zu diesen Volumes.

Amazon EC2 registriert das AMI automatisch für Sie.

6: Starten Sie eine Instance über das neue AMI.

Sie können das neue AMI verwenden, um eine Instance zu starten.

7: EC2-Instance Nr. 2: Neue Instance

Wenn Sie eine Instance mit dem neuen AMI starten, erstellt Amazon EC2 wir mithilfe des Snapshots ein neues EBS-Volume für das Root-Volume der Instance. Wenn Sie beim Anpassen der Instance Instance-Speicher-Volumes oder EBS-Volumes hinzugefügt haben, enthält die

Blockgerät-Zuweisung für das neue AMI Informationen zu diesen Volumes. Außerdem enthalten die Blockgerät-Zuweisungen für Instances, die Sie über das neue AMI starten, automatisch Informationen zu diesen Volumes. Die Instance-Speicher-Volumes, die in der Blockgerät-Zuweisung für die neue Instance angegeben sind, sind neu und enthalten keine Daten von den Instance-Speicher-Volumes der Instance, die Sie zum Erstellen des AMI verwendet haben. Die Daten auf den EBS-Volumes werden beibehalten. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen.

Wenn Sie eine neue Instance aus einem EBS-gestützten AMI erstellen, sollten Sie sowohl das Root-Volume als auch den zusätzlichen EBS-Speicher initialisieren, bevor Sie die Instance in Betrieb nehmen. Weitere Informationen finden Sie unter Amazon EBS-Volumes initialisieren im Amazon EBS-Benutzerhandbuch.

Erstellen Sie ein AMI aus einer Instance

Sie können ein AMI mit der AWS Management Console oder der Befehlszeile erstellen.

Console

Um ein AMI zu erstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance, von der aus Sie das AMI erstellen möchten, und wählen Sie Actions (Aktionen), dann Image and templates (Image und Vorlagen) und dann Create image (Image erstellen).

   > **Tip**
   >
   > Wenn diese Option deaktiviert ist, handelt es sich bei Ihrer Instance nicht um eine Amazon EBS-gestützte Instance.

4. Geben Sie auf der Seite Create image (Image erstellen) die folgenden Informationen an:

   a. Geben Sie für Image name (Image-Name) einen eindeutigen Namen für das Image ein, der bis zu 127 Zeichen lang sein kann.

   b. Für Image description (Image-Beschreibung), geben Sie eine optionale Beschreibung des Images mit einer Länge von maximal 255 Zeichen ein.

c. Lassen Sie bei No reboot (Kein Neustart) entweder das Kontrollkästchen Enable (Aktivieren) frei (Standardeinstellung), oder wählen Sie es aus.

- Wenn das Kontrollkästchen Aktivieren für Kein Neustart deaktiviert ist, startet Amazon EC2 bei der Erstellung des neuen AMI die Instance neu. Dadurch können Snapshots der angefügten Volumes erstellt werden, während sich die Daten im Ruhezustand befinden, um so einen konsistenten Status zu gewährleisten.
- Wenn das Kontrollkästchen Aktivieren für Kein Neustart ausgewählt ist, wird die Instance beim Erstellen des neuen AMI durch Amazon EC2 nicht heruntergefahren und neu gestartet.

> **Warning**
>
> Wenn Sie No reboot (Kein Neustart) wählen, können wir die Dateisystemintegrität des erstellten Images nicht garantieren.

d. Instance volumes (Instance-Volumes) – Sie können wie folgt das Stamm-Volume ändern sowie weitere Amazon-EBS- und Instance-Speicher-Volumes hinzufügen:

i. Das Stamm-Volume wird in der ersten Zeile definiert.

- Um die Größe des Stamm-Volumes zu ändern, geben Sie für Size (Größe) den erforderlichen Wert ein.
- Wenn Sie Delete on termination (Bei Beenden löschen) auswählen, wird das EBS-Volume gelöscht, sobald Sie die Instance beenden, die aus diesem AMI erstellt wurde. Wenn Sie Delete on termination (Bei Beenden löschen) nicht auswählen, wird das EBS-Volume nicht gelöscht, sobald Sie die Instance beenden. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.

ii. Wählen Sie zum Hinzufügen eines EBS-Volumes die Option Add volume (Volume hinzufügen) (dadurch wird eine neue Zeile hinzugefügt). Wählen Sie als Speichertyp die Option EBS und füllen Sie die Felder in der Zeile aus. Wenn Sie eine Instance aus Ihrem neuen AMI starten, werden diese zusätzlichen Volumes automatisch der Instance zugeordnet. Leere Volumes müssen formatiert und „gemountet“ werden. Volumes, die auf einem Snapshot basieren, müssen „gemountet“ werden.

iii. Informationen zum Hinzufügen eines Instance-Speicher-Volumes finden Sie unter Hinzufügen von Instance-Speicher-Volumes zu einem AMI. Wenn Sie eine Instance

aus Ihrem neuen AMI starten, werden zusätzliche Volumes automatisch initialisiert und gemountet. Diese Volumes enthalten keine Daten aus den Instance-Speicher-Volumes der ausgeführten Instance, auf der Ihr AMI basiert.

e. Tags (Markierungen) – Sie können das AMI und die Snapshots mit denselben Tags (Markierungen) oder mit unterschiedlichen Tags (Markierungen) markieren.

- Um das AMI und die Snapshots mit den gleichen Tags (Markierungen) zu markieren, wählen Sie Tag image and snapshots together (Image und Snapshots zusammen markieren). Die gleichen Tags (Markierungen) werden auf das AMI und jeden erstellten Snapshot angewendet.
- Um das AMI und die Snapshots mit verschiedenen Tags (Markierungen) zu markieren, wählen Sie Tag image and snapshots separately (Image und Snapshots separat markieren). Verschiedene Tags (Markierungen) werden auf das AMI und die erstellten Snapshots angewendet. Alle Snapshots erhalten jedoch die gleichen Tags (Markierungen). Sie können nicht jeden Snapshot mit einem anderen Tags (Markierungen) versehen.

Sie fügen ein Tag (Markierung) hinzu, indem Sie Add Tags (Tag (Markierung) hinzufügen) auswählen und den Schlüssel und den Wert für das Tags (Markierungen) eingeben. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

f. Wenn Sie bereit sind, Ihr AMI zu erstellen, wählen Sie Create image (Image erstellen).

5. Sehen Sie den Status Ihres AMI während der Erstellung ein wie folgt:

a. Wählen Sie im Navigationsbereich die Option AMIs.

b. Legen Sie den Filter auf Owned by me (Eigentum von mir) fest, um Ihr AMI in der entsprechenden Liste zu finden.

Am Anfang wird als Status `pending` angezeigt; nach einigen Minuten sollte sich der Status jedoch in `available` ändern.

6. (Optional) Wie Sie den Snapshot anzeigen, der für das neue AMI erstellt wurde:

a. Notieren Sie die ID des AMIs, das Sie im vorherigen Schritt ausfindig gemacht haben.

b. Wählen Sie im Navigationsbereich die Option Snapshots.

c. Stellen Sie den Filter auf Owned by me (Eigentum von mir) ein, und suchen Sie dann den Snapshot mit der neuen AMI-ID in der Spalte Description (Beschreibung).

Wenn Sie eine Instance über dieses AMI starten, verwendet Amazon EC2 diesen Snapshot, um das dazugehörige Stamm-Gerät-Volume zu erstellen.

AWS CLI

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- create-image (AWS CLI)
- New-EC2Image (AWS Tools for Windows PowerShell)

Erstellen eines Linux-AMI aus einem Snapshot

Wenn Sie über einen Snapshot des Root-Geräte-Volumes einer Instance verfügen, können Sie mit der AWS Management Console oder der Befehlszeile aus diesem Snapshot ein Linux-AMI erstellen. Diese Funktion ist derzeit nicht für Windows-Instances verfügbar.

Console

So erstellen Sie ein AMI aus einem Snapshot

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie den Snapshot aus, aus dem das AMI erstellt werden soll, und wählen Sie dann Actions (Aktionen), Create image from snapshot (Image aus Snapshot erstellen) aus.
4. Geben Sie auf der Seite Image aus Snapshot erstellen die folgenden Informationen an:
   a. Geben Sie unter Image-Name einen beschreibenden Namen für das Image ein.
   b. Geben Sie unter Beschreibung eine kurze Beschreibung für das Image ein.
   c. Wählen Sie unter Architektur die Image-Architektur aus. Wählen Sie i386 für 32-Bit, x86_64 für 64-Bit, arm64 für 64-Bit-ARM oder x86_64 für 64-Bit-MacOS.
   d. Geben Sie für Root-Gerätename den Gerätenamen ein, der für die Root-Gerät-Volume verwendet werden soll. Weitere Informationen finden Sie unter Gerätenamen auf Amazon EC2 EC2-Instances.

e. Wählen Sie für Virtualisierungstyp den Virtualisierungstyp aus, der von Instances verwendet werden soll, die von diesem AMI gestartet werden. Weitere Informationen finden Sie unter AMI-Virtualisierungstypen.

f. (Nur zur paravirtuellen Virtualisierung) Für Kernel-ID, wählen Sie den Betriebssystem-Kernel für das Image aus. Wenn Sie einen Snapshot des Root-Gerät-Volumes einer Instance verwenden, wählen Sie dieselbe Kernel-ID wie die ursprüngliche Instance aus. Wenn Sie sich nicht sicher sind, verwenden Sie den Standardkernel.

g. (Nur für Paravirtualisierung) Wählen Sie für RAM-Festplatten-ID die RAM-Festplatte für das Image aus. Wenn Sie einen bestimmten Kernel ausgewählt haben, müssen Sie möglicherweise einen bestimmten RAM-Datenträger mit den Treibern auswählen, die ihn unterstützen.

h. Wählen Sie für den Startmodus den Startmodus für das Image aus, oder wählen Sie Standard verwenden, sodass eine Instance, wenn sie mit diesem AMI gestartet wird, mit dem vom Instance-Typ unterstützten Startmodus gestartet wird. Weitere Informationen finden Sie unter Den Startmodus eines AMI festlegen.

i. (Optional) Passen Sie unter Gerätezuordnungen blockieren das Root-Volume an und fügen Sie zusätzliche Datenvolumes hinzu.

   Für jedes Volume können Sie Größe, Typ, Leistungsmerkmale, das Verhalten des Löschens beim Beenden und den Verschlüsselungsstatus angeben. Für das Stamm-Volume darf die Größe nicht kleiner sein als die Größe des Snapshots. Für den Volume-Typ ist standardmäßig die Allzweck-SSD `gp3` ausgewählt.

j. (Optional) Unter Tags können Sie dem neuen AMI ein oder mehrere Tags hinzufügen. Sie fügen ein Tag (Markierung) hinzu, indem Sie Add Tags (Tag (Markierung) hinzufügen) auswählen und den Schlüssel und den Wert für das Tags (Markierungen) eingeben. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

k. Wenn Sie bereit sind, Ihr AMI zu erstellen, wählen Sie Create image (Image erstellen).

AWS CLI

So erstellen Sie über die Befehlszeile aus einem Snapshot ein AMI

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- Registerbild (CLI)AWS

- Register-EC2Image (AWS Tools for Windows PowerShell)

Starten Sie eine Instance von einem AMI aus, das Sie erstellt haben

Sie können eine Instance von einem AMI aus starten, das Sie von einer Instance oder einem Snapshot erstellt haben.

So starten Sie eine Instance über Ihr AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Images die Option AMIs aus.
3. Legen Sie den Filter auf Eigentum von mir fest und wählen Sie Ihr AMI aus.
4. Wählen Sie Instance über Vorlage starten aus.
5. Übernehmen Sie die Standardwerte oder geben Sie benutzerdefinierte Werte im Launch Instance Wizard an. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Erstellen einer Instance-Speicher-Backed Linux-AMI

Anhand des AMI, das Sie beim Starten Ihrer Instance angeben, wird der Typ des Root-Gerät-Volumes ermittelt.

Beginnen Sie auf einer Instance, die Sie über ein vorhandenes Instance Store-Backupes Linux-AMI gestartet haben, um ein Instance Store-Backupes Linux-AMI zu erstellen. Nachdem Sie die Instance an Ihre Anforderungen angepasst haben, können Sie das Volume als Paket bündeln (Bundle) und ein neues AMI erstellen und registrieren, um es zum Starten von neuen Instances mit diesen Anpassungen zu verwenden.

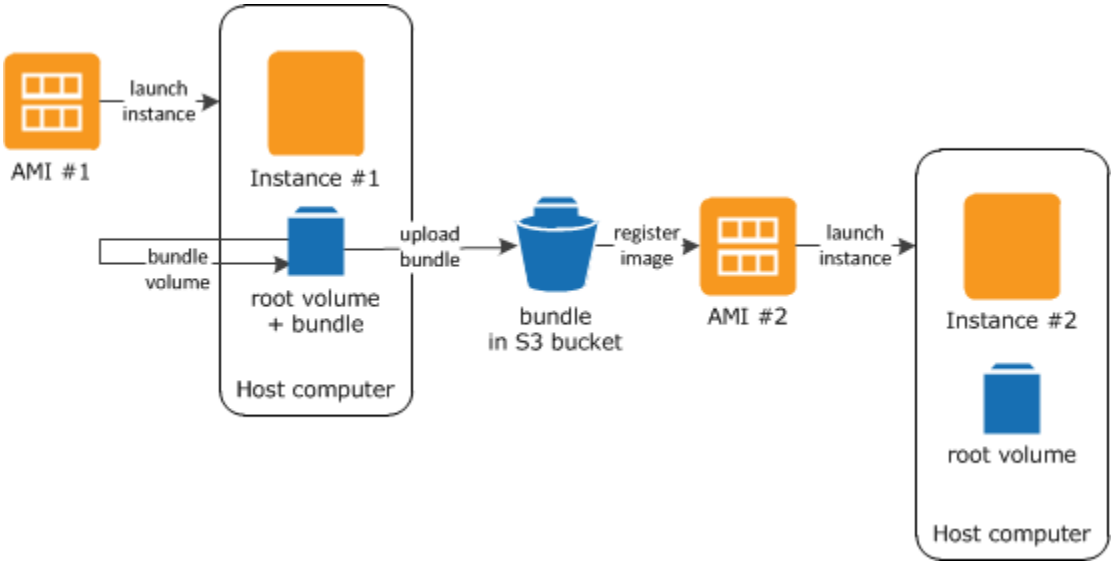
Sie können kein Windows-AMI erstellen, das vom Instanzspeicher unterstützt wird, da Windows-AMIs den Instance-Speicher für das Root-Gerät nicht unterstützen.

> **Important**
>
> Nur die folgenden Instance-Typen unterstützen ein Instance-Speicher-Volume als Root-Gerät: C1, C3, D2, I2, M1, M2, M3, R3 und X1.

Für das Erstellen von Amazon EBS-backed AMIs wird ein anderer Prozess verwendet. Weitere Informationen zu den Unterschieden zwischen Amazon EBS-gestützten und Instance Store-Backed-Instances und zur Ermittlung des Root-Gerätetyps für Ihre Instance erhalten Sie unter Speicher für das Root-Gerät. Informationen zum Erstellen eines Amazon EBS-backed AMI finden Sie unter. Erstellen Sie ein Amazon EBS-backed AMI

Übersicht über den Erstellungsprozess für Instance Store-Backed AMIs

Im folgenden Diagramm ist der Prozess zum Erstellen eines AMI über eine Instance Store-Backupe Instance dargestellt.



Starten Sie zuerst eine Instance über ein AMI, das dem zu erstellenden AMI ähnelt. Sie können eine Verbindung mit Ihrer Instance herstellen und sie anpassen. Wenn die Instance nach Ihren Vorstellungen konfiguriert ist, können Sie dafür ein Paket (Bundle) erstellen. Es dauert mehrere Minuten, bis die Paketerstellung abgeschlossen ist. Nach Abschluss des Prozesses verfügen Sie über ein Paket, das aus einem Image-Manifest (`image.manifest.xml`) und Dateien (`image.part.xx`) besteht, die eine Vorlage für das Stamm-Volume enthalten. Als Nächstes laden Sie das Paket in Ihren Amazon S3-Bucket hoch und registrieren anschließend Ihr AMI.

> **Note**
>
> Um Objekte für Ihr Instance-Speicher-gestütztes Linux-AMI in einen S3-Bucket hochzuladen, müssen ACLs für den Bucket aktiviert sein. Andernfalls kann Amazon EC2 keine ACLs für die hochzuladenden Objekte festlegen. Wenn Ihr Ziel-Bucket die erzwungene Einstellung für den Bucket-Eigentümer für S3 Object Ownership verwendet, funktioniert dies nicht, da ACLs

deaktiviert sind. Weitere Informationen finden Sie unter Steuern der Eigentümerschaft an hochgeladenen Objekten mit S3 Object Ownership.

Beim Starten einer Instance mit dem neuen AMI erstellen wir das Stamm-Volume für die Instance mithilfe des Pakets, das Sie in Amazon S3 hochgeladen haben. Für den Speicherplatz, der von dem Paket in Amazon S3 verwendet wird, werden Ihrem Konto Kosten berechnet, bis Sie es löschen. Weitere Informationen finden Sie unter Ein AMI abmelden (löschen).

Wenn Sie Ihrer Instance zusätzlich zum Root-Gerät-Volume Instance-Speicher-Volumes hinzufügen, enthält die Blockgerät-Zuweisung für das neue AMI Informationen zu diesen Volumes. Außerdem enthalten die Blockgerät-Zuweisungen für Instances, die Sie über das neue AMI starten, automatisch Informationen zu diesen Volumes. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen.

Voraussetzungen

Bevor Sie ein AMI erstellen können, müssen Sie die folgenden Aufgaben durchführen:

- Installieren Sie die AMI-Tools. Weitere Informationen finden Sie unter Einrichten der AMI-Tools.
- Installieren Sie das. AWS CLI Weitere Informationen erhalten Sie unter Einrichtung der AWS Command Line Interface.
- Stellen Sie sicher, dass Sie über einen S3-Bucket für das Bundle verfügen und dass für Ihren Bucket ACLs aktiviert sind. Weitere Informationen zur Konfiguration von ACLs finden Sie unter Konfigurieren von ACLs.
  - Um einen S3-Bucket mit dem zu erstellen AWS Management Console, öffnen Sie die Amazon S3 S3-Konsole unter https://console.aws.amazon.com/s3/ und wählen Sie Create Bucket.
  - Um einen S3-Bucket mit dem zu erstellen AWS CLI, können Sie den Befehl mb verwenden. Wenn Ihre installierte Version der AMI-Tools 1.5.18 oder höher ist, können Sie auch den `ec2-upload-bundle`-Befehl verwenden, um den S3-Bucket zu erstellen. Weitere Informationen finden Sie unter ec2-upload-bundle.
- Stellen Sie sicher, dass Sie Ihre AWS Konto-ID haben. Weitere Informationen finden Sie im Referenzhandbuch zur AWS Kontoverwaltung unter AWS-Konto Identifikatoren anzeigen.
- Stellen Sie sicher, dass Sie über Anmeldeinformationen zur Verwendung von AWS CLI verfügen. Weitere Informationen finden Sie im AWS Account Management Referenzhandbuch unter Bewährte Methoden für AWS Konten.
- Stellen Sie sicher, dass Sie über ein X.509-Zertifikat und den entsprechenden privaten Schlüssel verfügen.

  - Informationen zur Erstellung eines X.509-Zertifikats erhalten Sie unter Verwalten von Signaturzertifikaten. Das X.509-Zertifikat und der private Schlüssel werden verwendet, um Ihr AMI zu verschlüsseln und zu entschlüsseln.
  - [China (Peking)] Verwenden Sie das Zertifikat `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-cn-north-1.pem`.
  - [AWS GovCloud (US-West)] Verwenden Sie das `$EC2_AMITOOL_HOME/etc/ec2/amitools/cert-ec2-gov.pem` Zertifikat.
- Stellen Sie eine Verbindung mit Ihrer Instance her und passen Sie sie an. Sie können beispielsweise Software und Anwendungen installieren, Daten kopieren, temporäre Dateien löschen und die Linux-Konfiguration ändern.

Aufgaben

- Einrichten der AMI-Tools
- Erstellen eines AMI aus einer Instance-Speicher-Backed Amazon-Linux-Instance
- Erstellen eines AMI aus einer Instance-Speicher-Backed Ubuntu-Instance
- Konvertieren Ihres Instance-Speicher-Backed AMI in ein Amazon EBS-gestütztes AMI

Einrichten der AMI-Tools

Mit den AMI-Tools erstellen und verwalten Sie Instance Store-Backed AMIs für Linux. Um die Tools verwenden zu können, müssen Sie sie auf Ihrer Linux-Instance installieren. Die AMI-Tools sind als RPM-Paket und für Linux-Distributionen, die RPM nicht unterstützen, auch als ZIP-Datei verfügbar.

So richten Sie die AMI-Tools per RPM ein

1. Installieren Sie Ruby mithilfe des Paket-Managers für Ihre Linux-Veteilung, z. B. yum. Beispiel:

   ```
   [ec2-user ~]$ sudo yum install -y ruby
   ```

2. Laden Sie die RPM-Datei mit einem Tool wie wget oder curl herunter. Beispiel:

   ```
   [ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.noarch.rpm
   ```

3. Überprüfen Sie die Signatur der RPM-Datei, indem Sie den folgenden Befehl eingeben:

   ```
   [ec2-user ~]$ rpm -K ec2-ami-tools.noarch.rpm
   ```

Der obige Befehl sollte ergeben, dass die SHA1- und MD5-Hashes der Datei `OK.` sind. Wenn der Befehl ergibt, dass die Hashes `NOT OK` sind, verwenden Sie den folgenden Befehl, um die Header SHA1- und MD5-Hashes der Datei anzuzeigen:

```
[ec2-user ~]$ rpm -Kv ec2-ami-tools.noarch.rpm
```

Vergleichen Sie dann die Header SHA1- und MD5-Hashes Ihrer Datei mit den folgenden verifizierten AMI-Tools-Hashes, um die Authentizität der Datei zu bestätigen:

- Header SHA1: a1f662d6f25f69871104e6a62187fa4df508f880
- MD5: 9faff05258064e2f7909b66142de6782

Wenn die Header SHA1- und MD5-Hashes Ihrer Datei mit den verifizierten AMI-Tools-Hashes übereinstimmen, fahren Sie mit dem nächsten Schritt fort.

4. Installieren Sie RPM mit dem folgenden Befehl:

```
[ec2-user ~]$ sudo yum install ec2-ami-tools.noarch.rpm
```

5. Überprüfen Sie die Installation der AMI-Tools mit dem Befehl ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

> **Note**
>
> Wenn Sie einen Ladefehler wie „Diese Datei kann nicht geladen werden -- ec2/amitools/version (LoadError)“ erhalten, führen Sie den nächsten Schritt aus, um den Speicherort Ihrer AMI-Tools-Installation zu Ihrem Pfad hinzuzufügen. `RUBYLIB`

6. (Optional) Wenn Sie im vorherigen Schritt einen Fehler erhalten haben, ist es ratsam, dem `RUBYLIB`-Pfad den Installationsspeicherort Ihrer AMI-Tools hinzuzufügen.

   a. Führen Sie den folgenden Befehl aus, um die hinzuzufügenden Pfade zu ermitteln.

```
[ec2-user ~]$ rpm -qil ec2-ami-tools | grep ec2/amitools/version
/usr/lib/ruby/site_ruby/ec2/amitools/version.rb
/usr/lib64/ruby/site_ruby/ec2/amitools/version.rb
```

Im obigen Beispiel befindet sich die fehlende Datei aus dem vorherigen Ladefehler unter `/usr/lib/ruby/site_ruby` und `/usr/lib64/ruby/site_ruby`.

b. Fügen Sie die Speicherorte aus dem vorherigen Schritt Ihrem `RUBYLIB`-Pfad hinzu.

```
[ec2-user ~]$ export RUBYLIB=$RUBYLIB:/usr/lib/ruby/site_ruby:/usr/lib64/ruby/site_ruby
```

c. Überprüfen Sie die Installation der AMI-Tools mit dem Befehl ec2-ami-tools-version.

```
[ec2-user ~]$ ec2-ami-tools-version
```

So richten Sie die AMI-Tools per ZIP-Datei ein

1. Führen Sie die Ruby-Installation und das Entzippen mithilfe des Paket-Managers für Ihre Linux-Distribution durch, z. B. apt-get. Beispiel:

```
[ec2-user ~]$ sudo apt-get update -y && sudo apt-get install -y ruby unzip
```

2. Laden Sie die ZIP-Datei mit einem Tool wie wget oder curl herunter. Beispiel:

```
[ec2-user ~]$ wget https://s3.amazonaws.com/ec2-downloads/ec2-ami-tools.zip
```

3. Entzippen Sie die Dateien in ein geeignetes Installationsverzeichnis, z. B. `/usr/local/ec2`.

```
[ec2-user ~]$ sudo mkdir -p /usr/local/ec2
$ sudo unzip ec2-ami-tools.zip -d /usr/local/ec2
```

Beachten Sie, dass die ZIP-Datei den Ordner "ec2-ami-tools-*x.x.x*", wobei *x.x.x* die Versionsnummer der Tools ist (z. B. `ec2-ami-tools-1.5.7`).

4. Legen Sie die Umgebungsvariable `EC2_AMITOOL_HOME` auf das Installationsverzeichnis für die Tools fest. Beispiel:

```
[ec2-user ~]$ export EC2_AMITOOL_HOME=/usr/local/ec2/ec2-ami-tools-x.x.x
```

5. Fügen Sie die Tools Ihrer Umgebungsvariablen `PATH` hinzu. Beispiel:

```
[ec2-user ~]$ export PATH=$EC2_AMITOOL_HOME/bin:$PATH
```

6. Sie können die Installation der AMI-Tools mit dem Befehl ec2-ami-tools-version überprüfen.

```
[ec2-user ~]$ ec2-ami-tools-version
```

Verwalten von Signaturzertifikaten

Für bestimmte Befehle in den AMI-Tools ist ein Signaturzertifikat erforderlich (auch als X.509-Zertifikat bezeichnet). Sie müssen das Zertifikat erstellen und es dann in hochladen. AWS Beispielsweise können Sie zum Erstellen des Zertifikats ein Drittanbieter-Tool wie OpenSSL verwenden.

So erstellen Sie ein Signaturzertifikat

1. Installieren und konfigurieren Sie OpenSSL.
2. Erstellen Sie mit dem Befehl `openssl genrsa` einen privaten Schlüssel und speichern Sie die Ausgabe in einer `.pem`-Datei. Wir empfehlen Ihnen, einen RSA-Schlüssel mit 2 048 oder 4 096 Bit zu erstellen.

```
openssl genrsa 2048 > private-key.pem
```

3. Generieren Sie mit dem Befehl `openssl req` ein Zertifikat.

```
openssl req -new -x509 -nodes -sha256 -days 365 -key private-key.pem -outform PEM -
out certificate.pem
```

Verwenden Sie den Befehl AWSupload-signing-certificate, um das Zertifikat hochzuladen.

```
aws iam upload-signing-certificate --user-name user-name --certificate-body
 file://path/to/certificate.pem
```

Verwenden Sie den Befehl list-signing-certificates, um die Zertifikate für einen Benutzer aufzulisten:

```
aws iam list-signing-certificates --user-name user-name
```

Verwenden Sie den Befehl update-signing-certificate, um ein Signaturzertifikat für einen Benutzer zu deaktivieren oder wieder zu aktivieren. Mit dem folgenden Befehl wird das Zertifikat deaktiviert:

```
aws iam update-signing-certificate --certificate-id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE --
status Inactive --user-name user-name
```

Verwenden Sie den Befehl delete-signing-certificate, um ein Zertifikat zu löschen:

```
aws iam delete-signing-certificate --user-name user-name --certificate-
id OFHPLP4ZULTHYPMSYEX7O4BEXAMPLE
```

Erstellen eines AMI aus einer Instance-Speicher-Backed Instance

Die folgenden Verfahren dienen zum Erstellen eines Instance Store-Backed AMI aus einer Instance Store-Backupen Instance. Stellen Sie sicher, dass Sie die Voraussetzungen gelesen haben, bevor Sie beginnen.

Themen

- Erstellen eines AMI aus einer Instance-Speicher-Backed Amazon-Linux-Instance
- Erstellen eines AMI aus einer Instance-Speicher-Backed Ubuntu-Instance

Erstellen eines AMI aus einer Instance-Speicher-Backed Amazon-Linux-Instance

In diesem Abschnitt wird die Erstellung eines AMI aus einer Amazon Linux-Instance beschrieben. Die folgenden Verfahren funktionieren unter Umständen nicht für Instances, auf denen andere Linux-Distributionen ausgeführt werden. Informationen zu den Verfahren, die für Ubuntu gelten, erhalten Sie unter Erstellen eines AMI aus einer Instance-Speicher-Backed Ubuntu-Instance.

So bereiten Sie die Verwendung der AMI-Tools vor (nur HVM-Instances)

1. Für die AMI-Tools ist das richtige Starten von GRUB Legacy-System erforderlich. Verwenden Sie den folgenden Befehl, um GRUB zu installieren:

   ```
   [ec2-user ~]$ sudo yum install -y grub
   ```

2. Installieren Sie die Pakete für die Partitionsverwaltung mit dem folgenden Befehl:

   ```
   [ec2-user ~]$ sudo yum install -y gdisk kpartx parted
   ```

So erstellen Sie ein AMI aus einer Instance Store-Backupen Amazon Linux-Instance

Hierbei wird vorausgesetzt, dass Sie die Voraussetzungen unter Voraussetzungen erfüllt haben.

Ersetzen Sie in den folgenden Befehlen jeden *Platzhalter für Benutzereingaben* durch Ihre eigenen Informationen.

1. Laden Sie Ihre Anmeldeinformationen auf Ihre Instance hoch. Wir verwenden diese Anmeldeinformationen, um sicherzustellen, dass nur Sie und Amazon EC2 Zugriff auf Ihr AMI haben.

   a. Erstellen Sie auf Ihrer Instance wie folgt ein temporäres Verzeichnis für Ihre Anmeldeinformationen:

   ```
   [ec2-user ~]$ mkdir /tmp/cert
   ```

   Auf diese Weise können Sie Ihre Anmeldeinformationen aus der Image-Erstellung ausschließen.

   b. Kopieren Sie Ihr X.509-Zertifikat und den dazugehörigen privaten Schlüssel von Ihrem Computer in das Verzeichnis `/tmp/cert` auf Ihrer Instance, indem Sie ein Secure Copy-Tool nutzen, z. B. scp. Die Option `-i my-private-key.pem` im folgenden scp-Befehl ist der private Schlüssel, den Sie zum Herstellen der Verbindung für Ihre Instance mit SSH verwenden, und nicht der private X.509-Schlüssel. Beispiel:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
   path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
   ```

   Da dies reine Textdateien sind, können Sie das Zertifikat und den Schlüssel in einem Text-Editor öffnen und den Inhalt jeweils in neue Dateien unter kopiere `/tmp/cert`.

2. Bereiten Sie das Paket für den Upload in Amazon S3 vor, indem Sie den Befehl ec2-bundle-vol über Ihre Instance ausführen. Achten Sie darauf, die Option `-e` anzugeben, um das Verzeichnis auszuschließen, in dem Ihre Anmeldeinformationen gespeichert sind. Während des Paketprozesses werden standardmäßig Dateien ausgeschlossen, die ggf. vertrauliche Informationen enthalten. Dies sind beispielsweise die Dateien `*.sw`, `*.swo`, `*.swp`,

`*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` und `*/.bash_history`. Verwenden Sie die Option `--no-filter`, wenn Sie alle diese Dateien einbinden möchten. Mit der Option `--include` können Sie einzelne Dateien einbinden.

> **Important**
>
> Standardmäßig wird beim Prozess zur Erstellung des AMI-Pakets eine komprimierte, verschlüsselte Sammlung von Dateien im Verzeichnis `/tmp` erstellt, das als Ihr Stamm-Volume dient. Falls unter `/tmp` nicht genügend freier Speicherplatz zum Speichern des Pakets vorhanden ist, müssen Sie mit der Option `-d` *`/path/to/bundle/storage`* einen anderen Speicherort für das Paket angeben. Bei einigen Instances ist flüchtiger Speicher eingehängt `/mnt` oder Sie können `/media/ephemeral0` ihn verwenden, oder Sie können auch ein neues Amazon (EBS) -Volume erstellen, anhängen und mounten, um das Paket zu speichern. Weitere Informationen finden Sie unter Erstellen eines Amazon EBS-Volumes im Amazon EBS-Benutzerhandbuch.

a. Sie müssen den ec2-bundle-vol-Befehl als Root-Benutzer ausführen. Für die meisten Befehle können Sie sudo verwenden, um erhöhte Berechtigungen zu erhalten. In diesem Fall sollten Sie aber sudo -E su ausführen, um Ihre Umgebungsvariablen beizubehalten.

```
[ec2-user ~]$ sudo -E su
```

Beachten Sie, dass Sie in der bash-Eingabeaufforderung nun als root-Benutzer identifiziert werden und dass das Dollarzeichen durch einen Hashtag ersetzt wurde. Hiermit wird angegeben, dass Sie sich in einer root-Shell befinden:

```
[root ec2-user]#
```

b. Führen Sie den Befehl ec2-bundle-vol wie folgt aus, um das AMI-Paket zu erstellen:

```
[root ec2-user]# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 123456789012 -r x86_64 -e /tmp/cert --
partition gpt
```

> **Note**
>
> Verwenden Sie für die Regionen China (Peking) und AWS GovCloud (USA West) den `--ec2cert` Parameter und geben Sie die Zertifikate gemäß den Voraussetzungen an.

Die Image-Erstellung kann einige Minuten dauern. Nach Abschluss dieses Befehls enthält Ihr Verzeichnis `/tmp` (bzw. das nicht standardmäßige Verzeichnis) das Paket (`image.manifest.xml` sowie mehrere `image.part.`*xx*-Dateien).

c. Beenden Sie die root-Shell.

```
[root ec2-user]# exit
```

3. (Optional) Bearbeiten Sie die Blockgerät-Zuweisungen in der Datei `image.manifest.xml` für Ihr AMI, um mehr Instance-Speicher-Volumes hinzuzufügen. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen.

   a. Erstellen Sie ein Backup der Datei `image.manifest.xml`.

   ```
   [ec2-user ~]$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
   ```

   b. Formatieren Sie die Datei `image.manifest.xml` neu, damit sie leichter gelesen und bearbeitet werden kann.

   ```
   [ec2-user ~]$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
   image.manifest.xml
   ```

   c. Bearbeiten Sie die Blockgerät-Zuweisungen in `image.manifest.xml` mit einem Text-Editor. Das Beispiel unten enthält einen neuen Eintrag für das Instance-Speicher-Volume `ephemeral1`.

   > **Note**
   >
   > Eine Liste der ausgeschlossenen Dateien finden Sie unter ec2-bundle-vol.

   ```
       <block_device_mapping>
   ```

```
      <mapping>
        <virtual>ami</virtual>
        <device>sda</device>
      </mapping>
      <mapping>
        <virtual>ephemeral0</virtual>
        <device>sdb</device>
      </mapping>
      <mapping>
        <virtual>ephemeral1</virtual>
        <device>sdc</device>
      </mapping>
      <mapping>
        <virtual>root</virtual>
        <device>/dev/sda1</device>
      </mapping>
    </block_device_mapping>
```

d. Speichern Sie die Datei `image.manifest.xml` und beenden Sie den Text-Editor.

4. Führen Sie den Befehl ec2-upload-bundle wie folgt aus, um Ihr Paket in Amazon S3 hochzuladen:

```
[ec2-user ~]$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Wenn Sie Ihr AMI in einer anderen Region als US East (N. Virginia) registrieren möchten, müssen Sie sowohl die Zielregion mit der Option `--region` als auch einen Bucket-Pfad angeben, der in der Zielregion bereits vorhanden ist (bzw. einen eindeutigen Bucket-Pfad, der in der Zielregion erstellt werden kann).

5. (Optional) Nach dem Upload des Pakets in Amazon S3 können Sie das Paket mit dem folgenden `/tmp`-Befehl aus dem Verzeichnis rm auf der Instance entfernen:

```
[ec2-user ~]$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Wenn Sie mit der Option `-d` */path/to/bundle/storage* einen Pfad in Step 2 angegeben haben, sollten Sie diesen Pfad anstelle von `/tmp` verwenden.

6. Führen Sie den Befehl register-image wie folgt aus, um Ihr AMI zu registrieren:

```
[ec2-user ~]$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Wenn Sie zuvor für den Befehl ec2-upload-bundle eine Region angegeben haben, müssen Sie die entsprechende Region für diesen Befehl noch einmal angeben.

Erstellen eines AMI aus einer Instance-Speicher-Backed Ubuntu-Instance

In diesem Abschnitt wird die Erstellung eines AMI aus einer Ubuntu-Linux-Instance mit einem Instance-Speichervolume als Root-Volume beschrieben. Die folgenden Verfahren funktionieren unter Umständen nicht für Instances, auf denen andere Linux-Distributionen ausgeführt werden. Für Amazon Linux spezifische Vorgehensweisen finden Sie unter Erstellen eines AMI aus einer Instance-Speicher-Backed Amazon-Linux-Instance.

So bereiten Sie die Verwendung der AMI-Tools vor (nur HVM-Instances)

Für die AMI-Tools ist das richtige Starten von GRUB Legacy-System erforderlich. Ubuntu ist jedoch für die Nutzung von GRUB 2 konfiguriert. Sie müssen überprüfen, ob Ihre Instance GRUB Legacy-System nutzt. Falls nicht, sollten Sie die Installation und Konfiguration durchführen.

Außerdem müssen für HVM-Instances Partitionierungstools installiert werden, damit die AMI-Tools richtig funktionieren.

1. GRUB Legacy-System (Version 0.9*x* oder niedriger) muss auf Ihrer Instance installiert sein. Prüfen Sie, ob GRUB Legacy-System vorhanden ist, und führen Sie bei Bedarf die Installation durch.

   a. Überprüfen Sie die Version Ihrer GRUB-Installation.

```
ubuntu:~$ grub-install --version
grub-install (GRUB) 1.99-21ubuntu3.10
```

In diesem Beispiel ist die GRUB-Version höher als 0.9*x*, so dass GRUB Legacy-System installiert werden muss. Fahren Sie mit Step 1.b fort. Falls GRUB Legacy-System bereits vorhanden ist, können Sie mit Step 2 fortfahren.

b. Installieren Sie das `grub`-Paket mit dem folgenden Befehl:

```
ubuntu:~$ sudo apt-get install -y grub
```

2. Installieren Sie die folgenden Pakete für die Partitionsverwaltung, indem Sie den Paket-Manager für Ihre Verteilung verwenden.

   - `gdisk` (In einigen Verteilungen hat dieses Paket ggf. den Namen `gptfdisk`.)
   - `kpartx`
   - `parted`

   Verwenden Sie den folgenden Befehl.

```
ubuntu:~$ sudo apt-get install -y gdisk kpartx parted
```

3. Überprüfen Sie die Kernel-Parameter für Ihre Instance.

```
ubuntu:~$ cat /proc/cmdline
BOOT_IMAGE=/boot/vmlinuz-3.2.0-54-virtual root=UUID=4f392932-ed93-4f8f-
aee7-72bc5bb6ca9d ro console=ttyS0 xen_emul_unplug=unnecessary
```

Beachten Sie die Optionen, die auf die Parameter für den Kernel und das Root-Gerät folgen: `ro`, `console=ttyS0` und `xen_emul_unplug=unnecessary`. Ihre Optionen können ggf. hiervon abweichen.

4. Überprüfen Sie die Kernel-Einträge in `/boot/grub/menu.lst`.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=hvc0
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
kernel  /boot/memtest86+.bin
```

Beachten Sie, dass der Parameter `console` nicht auf `hvc0` verweist, sondern auf `ttyS0`, und dass der Parameter `xen_emul_unplug=unnecessary` fehlt. Auch hier können Ihre Optionen ggf. abweichen.

5. Bearbeiten Sie die Datei `/boot/grub/menu.lst` mit Ihrem bevorzugten Text-Editor (z. B. vim oder nano), um die Konsole zu ändern und die zuvor ermittelten Parameter den Boot-Einträgen hinzuzufügen.

```
title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs
 ro console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, kernel 3.2.0-54-virtual (recovery mode)
root            (hd0)
kernel          /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro
 single console=ttyS0 xen_emul_unplug=unnecessary
initrd          /boot/initrd.img-3.2.0-54-virtual

title           Ubuntu 12.04.3 LTS, memtest86+
root            (hd0)
kernel          /boot/memtest86+.bin
```

6. Vergewissern Sie sich, dass Ihre Kernel-Einträge jetzt die richtigen Parameter enthalten.

```
ubuntu:~$ grep ^kernel /boot/grub/menu.lst
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro console=ttyS0
 xen_emul_unplug=unnecessary
kernel  /boot/vmlinuz-3.2.0-54-virtual root=LABEL=cloudimg-rootfs ro single
 console=ttyS0 xen_emul_unplug=unnecessary
kernel  /boot/memtest86+.bin
```

7. [Nur für Ubuntu 14.04 und höher] Ab Ubuntu 14.04 werden für Instance Store-Backed Ubuntu-AMIs eine GPT-Partitionstabelle und eine separat gemountete EFI-Partition unter verwende `/boot/efi`. Mit dem Befehl ec2-bundle-vol wird diese Boot-Partition nicht als Paket gebündelt. Daher müssen Sie den Eintrag `/etc/fstab` für die EFI-Partition wie im folgenden Beispiel auskommentieren.

```
LABEL=cloudimg-rootfs   /        ext4   defaults        0 0
#LABEL=UEFI     /boot/efi       vfat    defaults        0 0
```

```
/dev/xvdb       /mnt    auto    defaults,nobootwait,comment=cloudconfig 0       2
```

So erstellen Sie ein AMI aus einer Instance Store-Backupen Ubuntu-Instance

Hierbei wird vorausgesetzt, dass Sie die Voraussetzungen unter Voraussetzungen erfüllt haben.

Ersetzen Sie in den folgenden Befehlen jeden *Platzhalter für Benutzereingaben* durch Ihre eigenen Informationen.

1. Laden Sie Ihre Anmeldeinformationen auf Ihre Instance hoch. Wir verwenden diese Anmeldeinformationen, um sicherzustellen, dass nur Sie und Amazon EC2 Zugriff auf Ihr AMI haben.

   a. Erstellen Sie auf Ihrer Instance wie folgt ein temporäres Verzeichnis für Ihre Anmeldeinformationen:

   ```
   ubuntu:~$ mkdir /tmp/cert
   ```

   Auf diese Weise können Sie Ihre Anmeldeinformationen aus der Image-Erstellung ausschließen.

   b. Kopieren Sie Ihr X.509-Zertifikat und den privaten Schlüssel von Ihrem Computer in das Verzeichnis `/tmp/cert` auf Ihrer Instance, indem Sie ein Secure Copy-Tool nutzen, z. B. scp. Die Option `-i my-private-key.pem` im folgenden scp-Befehl ist der private Schlüssel, den Sie zum Herstellen der Verbindung für Ihre Instance mit SSH verwenden, und nicht der private X.509-Schlüssel. Beispiel:

   ```
   you@your_computer:~ $ scp -i my-private-key.pem /
   path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem /
   path/to/cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
   user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
   pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
   cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  685     0.7KB/s   00:00
   ```

   Da dies reine Textdateien sind, können Sie das Zertifikat und den Schlüssel in einem Text-Editor öffnen und den Inhalt jeweils in neue Dateien unter kopiere `/tmp/cert`.

2. Bereiten Sie das Paket für den Upload in Amazon S3 vor, indem Sie den Befehl ec2-bundle-vol über Ihre Instance ausführen. Achten Sie darauf, die Option `-e` anzugeben, um das

Verzeichnis auszuschließen, in dem Ihre Anmeldeinformationen gespeichert sind. Während des Paketprozesses werden standardmäßig Dateien ausgeschlossen, die ggf. vertrauliche Informationen enthalten. Dies sind beispielsweise die Dateien `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` und `*/.bash_history`. Verwenden Sie die Option `--no-filter`, wenn Sie alle diese Dateien einbinden möchten. Mit der Option `--include` können Sie einzelne Dateien einbinden.

> **Important**
>
> Standardmäßig wird beim Prozess zur Erstellung des AMI-Pakets eine komprimierte, verschlüsselte Sammlung von Dateien im Verzeichnis `/tmp` erstellt, das als Ihr Stamm-Volume dient. Falls unter `/tmp` nicht genügend freier Speicherplatz zum Speichern des Pakets vorhanden ist, müssen Sie mit der Option `-d` *`/path/to/bundle/storage`* einen anderen Speicherort für das Paket angeben. Bei einigen Instances ist flüchtiger Speicher eingehängt `/mnt` oder Sie können `/media/ephemeral0` ihn verwenden, oder Sie können auch ein neues Amazon (EBS) -Volume erstellen, anhängen und mounten, um das Paket zu speichern. Weitere Informationen finden Sie unter Erstellen eines Amazon EBS-Volumes im Amazon EBS-Benutzerhandbuch.

a. Sie müssen den ec2-bundle-vol-Befehl als Root-Benutzer ausführen. Für die meisten Befehle können Sie sudo verwenden, um erhöhte Berechtigungen zu erhalten. In diesem Fall sollten Sie aber sudo -E su ausführen, um Ihre Umgebungsvariablen beizubehalten.

```
ubuntu:~$ sudo -E su
```

Beachten Sie, dass Sie in der bash-Eingabeaufforderung nun als root-Benutzer identifiziert werden und dass das Dollarzeichen durch einen Hashtag ersetzt wurde. Hiermit wird angegeben, dass Sie sich in einer root-Shell befinden:

```
root@ubuntu:#
```

b. Führen Sie den Befehl ec2-bundle-vol wie folgt aus, um das AMI-Paket zu erstellen:

```
root@ubuntu:# ec2-bundle-vol -k /tmp/cert/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c /tmp/cert/cert-
```

```
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u your_aws_account_id -r x86_64 -e /tmp/
cert --partition gpt
```

> **Important**
>
> Fügen Sie für Ubuntu 14.04 und höhere HVM-Instances das Flag `--partition mbr` hinzu, um die Boot-Anweisungen richtig in einem Paket zu bündeln. Andernfalls wird das neu erstellte AMI nicht gestartet.

Die Image-Erstellung kann einige Minuten dauern. Nach Abschluss dieses Befehls enthält Ihr Verzeichnis `tmp` das Paket (`image.manifest.xml` sowie mehrere `image.part.`*xx*-Dateien).

c. Beenden Sie die root-Shell.

```
root@ubuntu:# exit
```

3. (Optional) Bearbeiten Sie die Blockgerät-Zuweisungen in der Datei `image.manifest.xml` für Ihr AMI, um mehr Instance-Speicher-Volumes hinzuzufügen. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen.

   a. Erstellen Sie ein Backup der Datei `image.manifest.xml`.

   ```
   ubuntu:~$ sudo cp /tmp/image.manifest.xml /tmp/image.manifest.xml.bak
   ```

   b. Formatieren Sie die Datei `image.manifest.xml` neu, damit sie leichter gelesen und bearbeitet werden kann.

   ```
   ubuntu:~$ sudo xmllint --format /tmp/image.manifest.xml.bak > /tmp/
   image.manifest.xml
   ```

   c. Bearbeiten Sie die Blockgerät-Zuweisungen in `image.manifest.xml` mit einem Text-Editor. Das Beispiel unten enthält einen neuen Eintrag für das Instance-Speicher-Volume *ephemeral1*.

   ```
       <block_device_mapping>
         <mapping>
           <virtual>ami</virtual>
           <device>sda</device>
   ```

```
    </mapping>
    <mapping>
      <virtual>ephemeral0</virtual>
      <device>sdb</device>
    </mapping>
    <mapping>
      <virtual>ephemeral1</virtual>
      <device>sdc</device>
    </mapping>
    <mapping>
      <virtual>root</virtual>
      <device>/dev/sda1</device>
    </mapping>
  </block_device_mapping>
```

d. Speichern Sie die Datei `image.manifest.xml` und beenden Sie den Text-Editor.

4. Führen Sie den Befehl ec2-upload-bundle wie folgt aus, um Ihr Paket in Amazon S3 hochzuladen:

```
ubuntu:~$ ec2-upload-bundle -b my-s3-bucket/bundle_folder/bundle_name -m /tmp/
image.manifest.xml -a your_access_key_id -s your_secret_access_key
```

> **Important**
>
> Wenn Sie Ihr AMI in einer anderen Region als US East (N. Virginia) registrieren möchten, müssen Sie sowohl die Zielregion mit der Option `--region`, als auch einen Bucket-Pfad angeben, der in der Zielregion bereits vorhanden ist (bzw. einen eindeutigen Bucket-Pfad, der in der Zielregion erstellt werden kann).

5. (Optional) Nach dem Upload des Pakets in Amazon S3 können Sie das Paket mit dem folgenden `/tmp`-Befehl aus dem Verzeichnis rm auf der Instance entfernen:

```
ubuntu:~$ sudo rm /tmp/image.manifest.xml /tmp/image.part.* /tmp/image
```

> **Important**
>
> Wenn Sie mit der Option `-d` */path/to/bundle/storage* einen Pfad in Step 2 angegeben haben, sollten Sie diesen Pfad unten anstelle von `/tmp` verwenden.

6. Führen Sie den Befehl register-image AWS CLI wie folgt aus, um Ihr AMI zu registrieren:

```
ubuntu:~$ aws ec2 register-image --image-location my-s3-
bucket/bundle_folder/bundle_name/image.manifest.xml --name AMI_name --
virtualization-type hvm
```

> **Important**
>
> Wenn Sie zuvor für den Befehl ec2-upload-bundle eine Region angegeben haben, müssen Sie die entsprechende Region für diesen Befehl noch einmal angeben.

7. [Ubuntu 14.04 und höher] Heben Sie die Auskommentierung des EFI-Eintrags in `/etc/fstab` auf. Andernfalls kann Ihre ausgeführte Instance nicht neu gestartet werden.

Konvertieren Ihres Instance-Speicher-Backed AMI in ein Amazon EBS-gestütztes AMI

Sie können ein Instance Store-Backed Linux-AMI, dessen Eigentümer Sie sind, in ein Amazon EBS-gestütztes Linux-AMI konvertieren.

> **Important**
>
> Sie können ein AMI, das Sie nicht besitzen, nicht konvertieren.

So konvertieren Sie ein Instance Store-Backed AMI in ein Amazon EBS-gestütztes AMI

1. Starten Sie eine Amazon Linux-Instance über ein Amazon EBS-gestütztes AMI. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard. Auf Amazon Linux-Instances sind die Tools AWS CLI und AMI vorinstalliert.
2. Laden Sie den privaten X.509-Schlüssel, den Sie zum Bündeln Ihres Instance Store-Backed AMI als Paket (Bundle) verwendet haben, auf Ihre Instance hoch. Wir verwenden diesen Schlüssel, um sicherzustellen, dass nur Sie und Amazon EC2 Zugriff auf Ihr AMI haben.
   a. Erstellen Sie auf Ihrer Instance wie folgt ein temporäres Verzeichnis für Ihren privaten X.509-Schlüssel:

```
[ec2-user ~]$ mkdir /tmp/cert
```

b. Kopieren Sie Ihren privaten X.509-Schlüssel von Ihrem Computer in das Verzeichnis `/tmp/cert` auf Ihrer Instance, indem Sie ein Secure Copy-Tool nutzen, z. B. scp. Der Parameter *my-private-key* im folgenden Befehl ist der private Schlüssel, den Sie zum Herstellen der Verbindung für Ihre Instance mit SSH verwenden. Beispielsweise:

```
you@your_computer:~ $ scp -i my-private-key.pem /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem ec2-
user@ec2-203-0-113-25.compute-1.amazonaws.com:/tmp/cert/
pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem  100%  717     0.7KB/s   00:00
```

3. Konfigurieren Sie Ihre Umgebungsvariablen für die Verwendung der AWS CLI. Weitere Informationen finden Sie unter Schlüsselpaar erstellen.

   a. (Empfohlen) Legen Sie Umgebungsvariablen für Ihren AWS Zugriffsschlüssel, Ihren geheimen Schlüssel und Ihr Sitzungstoken fest.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   [ec2-user ~]$ export AWS_SESSION_TOKEN=your_session_token
   ```

   b. Legen Sie Umgebungsvariablen für Ihren AWS Zugriffsschlüssel und Ihren geheimen Schlüssel fest.

   ```
   [ec2-user ~]$ export AWS_ACCESS_KEY_ID=your_access_key_id
   [ec2-user ~]$ export AWS_SECRET_ACCESS_KEY=your_secret_access_key
   ```

4. Bereiten Sie ein Volume Amazon Elastic Block Store (Amazon EBS) für Ihr neues AMI vor.

   a. Erstellen Sie ein leeres EBS-Volume in derselben Availability Zone wie für Ihre Instance, indem Sie den Befehl create-volume verwenden. Notieren Sie sich die Volume-ID in der Befehlsausgabe.

   > **Important**
   >
   > Dieses EBS-Volume muss mindestens die gleiche Größe wie das ursprüngliche Stamm-Volume des Instance-Speichers haben.

```
[ec2-user ~]$ aws ec2 create-volume --size 10 --region us-west-2 --
availability-zone us-west-2b
```

b. Fügen Sie das Volume mit dem Befehl attach-volume an Ihre Amazon EBS-gestützte Instance an.

```
[ec2-user ~]$ aws ec2 attach-volume --volume-id volume_id --instance-
id instance_id --device /dev/sdb --region us-west-2
```

5. Erstellen Sie einen Ordner für Ihr Paket.

```
[ec2-user ~]$ mkdir /tmp/bundle
```

6. Laden Sie das Paket für Ihr Instance Store-Backed AMI in das Verzeichnis `/tmp/bundle` herunter, indem Sie den Befehl ec2-download-bundle verwenden.

```
[ec2-user ~]$ ec2-download-bundle -b my-s3-bucket/bundle_folder/bundle_name -m
 image.manifest.xml -a $AWS_ACCESS_KEY_ID -s $AWS_SECRET_ACCESS_KEY --privatekey /
path/to/pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d /tmp/bundle
```

7. Stellen Sie die Image-Datei mit dem Befehl ec2-unbundle aus dem Paket wieder her.

a. Wechseln Sie in den Paketordner (bundle).

```
[ec2-user ~]$ cd /tmp/bundle/
```

b. Führen Sie den Befehl ec2-unbundle aus.

```
[ec2-user bundle]$ ec2-unbundle -m image.manifest.xml --privatekey /path/to/pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem
```

8. Kopieren Sie die Dateien aus dem entpackten Image auf das neue EBS-Volume.

```
[ec2-user bundle]$ sudo dd if=/tmp/bundle/image of=/dev/sdb bs=1M
```

9. Überprüfen Sie das Volume auf neue Partitionen, die aus dem Paket entpackt wurden.

```
[ec2-user bundle]$ sudo partprobe /dev/sdb1
```

10. Listen Sie die Blockgeräte auf, um den Gerätenamen für das Mounten ermitteln zu können.

```
[ec2-user bundle]$ lsblk
NAME         MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/sda    202:0    0   8G  0 disk
##/dev/sda1 202:1    0   8G  0 part /
/dev/sdb    202:80   0  10G  0 disk
##/dev/sdb1 202:81   0  10G  0 part
```

In diesem Beispiel lautet die Partition für das Mounten `/dev/sdb1`, aber Ihr Gerätename lautet wahrscheinlich anders. Falls Ihr Volume nicht partitioniert ist, lautet das Gerät für das Mounten etwa `/dev/sdb` (ohne nachgestellte Ziffer für die Gerätepartition).

11. Erstellen Sie einen Mounting-Punkt für das neue EBS-Volume und mounten Sie das Volume.

```
[ec2-user bundle]$ sudo mkdir /mnt/ebs
[ec2-user bundle]$ sudo mount /dev/sdb1 /mnt/ebs
```

12. Öffnen Sie die Datei `/etc/fstab` auf dem EBS-Volume mit Ihrem bevorzugten Text-Editor (z. B. vim oder nano) und entfernen Sie alle Einträge für Instance-Speicher-Volumes (flüchtiger Speicher). Da das EBS-Volume unter `/mnt/ebs` gemountet wurde, befindet sich die Datei `fstab` unter `/mnt/ebs/etc/fstab`.

```
[ec2-user bundle]$ sudo nano /mnt/ebs/etc/fstab
#
LABEL=/     /           ext4    defaults,noatime  1   1
tmpfs       /dev/shm    tmpfs   defaults        0   0
devpts      /dev/pts    devpts  gid=5,mode=620  0   0
sysfs       /sys        sysfs   defaults        0   0
proc        /proc       proc    defaults        0   0
/dev/sdb        /media/ephemeral0       auto    defaults,comment=cloudconfig    0
     2
```

In diesem Beispiel sollte die letzte Zeile entfernt werden.

13. Heben Sie das Mounting des Volumes auf und trennen Sie es von der Instance.

```
[ec2-user bundle]$ sudo umount /mnt/ebs
[ec2-user bundle]$ aws ec2 detach-volume --volume-id volume_id --region us-west-2
```

14. Erstellen Sie aus dem neuen EBS-Volume wie folgt ein AMI.

    a. Erstellen Sie einen Snapshot des neuen EBS-Volumes.

```
[ec2-user bundle]$ aws ec2 create-snapshot --region us-west-2 --description
 "your_snapshot_description" --volume-id volume_id
```

b. Überprüfen Sie, ob Ihr Snapshot vollständig ist.

```
[ec2-user bundle]$ aws ec2 describe-snapshots --region us-west-2 --snapshot-
id snapshot_id
```

c. Ermitteln Sie die auf dem ursprünglichen AMI verwendete Prozessorarchitektur, den Virtualisierungstyp und das Kernel-Image (`aki`) mit dem Befehl describe-images. Für diesen Schritt benötigen Sie die AMI-ID des ursprünglichen Instance Store-Backed AMI.

```
[ec2-user bundle]$ aws ec2 describe-images --region us-west-2 --image-id ami-id
 --output text
IMAGES x86_64 amazon/amzn-ami-pv-2013.09.2.x86_64-s3 ami-8ef297be amazon
 available public machine aki-fc8f11cc instance-store paravirtual xen
```

In diesem Beispiel werden als Architektur `x86_64` und als Kernel-Image-ID `aki-fc8f11cc` verwendet. Nutzen Sie diese Werte im folgenden Schritt. Falls in der Ausgabe des obigen Befehls auch eine `ari`-ID aufgeführt ist, sollten Sie sich diese ebenfalls notieren.

d. Registrieren Sie Ihr neues AMI mit der Snapshot-ID Ihres neuen EBS-Volumes und den Werten aus dem vorherigen Schritt. Wenn in der Ausgabe des vorherigen Befehls eine `ari`-ID aufgeführt ist, sollten Sie diese im folgenden Befehl als `--ramdisk-id` *`ari_id`* einfügen.

```
[ec2-user bundle]$ aws ec2 register-image --region us-west-2 --
name your_new_ami_name --block-device-mappings DeviceName=device-
name,Ebs={SnapshotId=snapshot_id} --virtualization-type paravirtual --
architecture x86_64 --kernel-id aki-fc8f11cc --root-device-name device-name
```

15. (Optional) Nachdem Sie per Test sichergestellt haben, dass Sie über Ihr neues AMI eine Instance starten können, können Sie das für dieses Verfahren erstellte EBS-Volume löschen.

```
aws ec2 delete-volume --volume-id volume_id
```

AMI-Tools – Referenz

Mit den AMI Tools-Befehlen erstellen und verwalten Sie Instance Store-Backed AMIs für Linux. Weitere Informationen über das Einrichten der Tools finden Sie unter Einrichten der AMI-Tools.

Informationen zu Ihren Zugriffsschlüsseln finden Sie unter Bewährte Methoden für AWS -Konten im AWS Account Management -Referenzhandbuch.

Befehle

- ec2-ami-tools-version
- ec2-bundle-image
- ec2-bundle-vol
- ec2-delete-bundle
- ec2-download-bundle
- ec2-migrate-manifest
- ec2-unbundle
- ec2-upload-bundle
- Allgemeine Optionen für AMI-Tools

ec2-ami-tools-version

Beschreibung

Beschreibt die Version der AMI-Tools.

Syntax

`ec2-ami-tools-version`

Output

Die Versionsinformationen

Beispiel

Dieser Beispielbefehl zeigt die Versionsinformationen für die AMI-Tools an, die Sie verwenden.

```
[ec2-user ~]$ ec2-ami-tools-version
```

```
1.5.2 20071010
```

ec2-bundle-image

Beschreibung

Erstellt ein Instance Store-Backed AMI für Linux aus einem Betriebssystem-Image, das in einer Loopback-Datei erstellt wurde.

Syntax

ec2-bundle-image -c *path* -k *path* -u *account* -i *path* [-d *path*] [--ec2cert *path*] [-r *architecture*] [--productcodes *code1*,*code2*,...] [-B *mapping*] [-p *prefix*]

Optionen

`-c, --cert` path

Die PEM-kodierte öffentliche RSA-Schlüsselzertifikatsdatei des Benutzers

Erforderlich: Ja

`-k, --privatekey` path

Der Pfad zu einer PEM-kodierten RSA-Schlüsseldatei. Sie müssen diesen Schlüssel zum Entpacken dieses Pakets angeben, bewahren Sie ihn daher gut auf. Beachten Sie, dass der Schlüssel nicht in Ihrem AWS Konto registriert sein muss.

Erforderlich: Ja

`-u, --user` account

Die AWS Konto-ID des Benutzers ohne Bindestriche.

Erforderlich: Ja

`-i, --image` path

Der Pfad zum Image, das gebündelt werden soll

Erforderlich: Ja

`-d, --destination` path

Das Verzeichnis, in dem das Paket erstellt wird

Standard: `/tmp`

Erforderlich: Nein

`--ec2cert` path

Der Pfad zum öffentlichen Amazon EC2 X.509-Schlüsselzertifikat, das zum Verschlüsseln des Image-Manifests verwendet wird.

Die Regionen `us-gov-west-1` und `cn-north-1` verwenden ein nicht standardmäßiges öffentliches Schlüsselzertifikat, und der Pfad zu diesem Zertifikat muss mit dieser Option angegeben werden. Der Pfad zum Zertifikat variiert ausgehend von der Installationsmethode der AMI-Tools. Für Amazon Linux befinden sich die Zertifikate unter `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Wenn Sie die AMI-Tools aus der RPM- oder ZIP-Datei in Einrichten der AMI-Tools installiert haben, befinden sich die Zertifikate unter `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Erforderlich: Nur für die Regionen `us-gov-west-1` und `cn-north-1`.

`-r, --arch` architecture

Image-Architektur. Wenn Sie die Architektur nicht in der Befehlszeile angeben, werden Sie dazu aufgefordert, sobald das Bündeln beginnt.

Zulässige Werte: `i386` | `x86_64`

Erforderlich: Nein

`--productcodes` code1,code2,...

Produkt-Codes, die dem Image zum Zeitpunkt der Registrierung angefügt werden, durch Kommas getrennt

Erforderlich: Nein

`-B, --block-device-mapping` mapping

Definiert, wie Blockgeräte für eine Instance dieses AMI bereitgestellt werden, wenn der Instance-Typ das angegebene Gerät unterstützt.

Geben Sie eine durch Komma getrennte Liste von Schlüssel-Wert-Paaren an, wobei jeder Schlüssel ein virtueller Name und jeder Wert der entsprechende Gerätename ist. Virtuelle Namen umfassen Folgendes:

- `ami` — Das Stammdateisystemgerät, wie es von der Instance erfasst wird
- `root` — Das Stammdateisystemgerät, wie es vom Kernel erfasst wird
- `swap` — Das Swap-Gerät, wie es von der Instance erfasst wird
- `ephemeralN` — Das n-te Instance-Speicher-Volume

Erforderlich: Nein

`-p, --prefix` prefix

Das Dateinamenpräfix für gebündelte AMI-Dateien

Standard: Der Name der Imagedatei. Wenn der Pfad des Images beispielsweise `/var/spool/my-image/version-2/debian.img` ist, dann ist das Standardpräfix `debian.img`.

Erforderlich: Nein

`--kernel` kernel_id

Veraltet. Verwenden Sie zum Festlegen des Kernels register-image.

Erforderlich: Nein

`--ramdisk` ramdisk_id

Veraltet. Verwenden Sie zum Festlegen des RAM-Datenträgers (sofern erforderlich) register-image.

Erforderlich: Nein

Output

Statusmeldung, die die Phasen und Status des Bündelungsprozesses beschreibt

Beispiel

Dieses Beispiel erstellt ein gebündeltes AMI aus einem Betriebssystem-Image, das in einer Loopback-Datei erstellt wurde.

```
[ec2-user ~]$ ec2-bundle-image -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c cert-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -i image.img -d bundled/ -r x86_64
Please specify a value for arch [i386]:
Bundling image file...
Splitting bundled/image.gz.crypt...
```

```
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
Created image.part.04
Created image.part.05
Created image.part.06
Created image.part.07
Created image.part.08
Created image.part.09
Created image.part.10
Created image.part.11
Created image.part.12
Created image.part.13
Created image.part.14
Generating digests for each part...
Digests generated.
Creating bundle manifest...
ec2-bundle-image complete.
```

ec2-bundle-vol

Beschreibung

Erstellt ein Instance Store-Backed AMI für Linux durch Komprimieren, Verschlüsseln und Signieren einer Kopie des Root-Gerät-Volumes für die Instance.

Amazon EC2 versucht, Produkt-Codes, Kernel-Einstellungen, RAM-Datenträgereinstellungen und Blockgerät-Zuweisungen von der Instance zu erben.

Während des Paketprozesses werden standardmäßig Dateien ausgeschlossen, die ggf. vertrauliche Informationen enthalten. Dies sind beispielsweise die Dateien `*.sw`, `*.swo`, `*.swp`, `*.pem`, `*.priv`, `*id_rsa*`, `*id_dsa*` `*.gpg`, `*.jks`, `*/.ssh/authorized_keys` und `*/.bash_history`. Verwenden Sie die Option `--no-filter`, wenn Sie alle diese Dateien einbinden möchten. Mit der Option `--include` können Sie einzelne Dateien einbinden.

Weitere Informationen finden Sie unter Erstellen einer Instance-Speicher-Backed Linux-AMI.

Syntax

```
ec2-bundle-vol -c path -k path -u account [-d path] [--ec2cert path] [-
r architecture] [--productcodes code1,code2,...] [-B mapping] [--all] [-e
```

directory1,_directory2_,...] [-i _file1_,_file2_,...] [--no-filter] [-p _prefix_] [-s _size_] [--[no-]inherit] [-v _volume_] [-P _type_] [-S _script_] [--fstab _path_] [--generate-fstab] [--grub-config _path_]

Optionen

`-c, --cert` path

Die PEM-kodierte öffentliche RSA-Schlüsselzertifikatsdatei des Benutzers

Erforderlich: Ja

`-k, --privatekey` path

Der Pfad zur PEM-kodierten RSA-Schlüsseldatei des Benutzers

Erforderlich: Ja

`-u, --user` account

Die AWS Konto-ID des Benutzers ohne Bindestriche.

Erforderlich: Ja

`-d, --destination` destination

Das Verzeichnis, in dem das Paket erstellt wird

Standard: `/tmp`

Erforderlich: Nein

`--ec2cert` path

Der Pfad zum öffentlichen Amazon EC2 X.509-Schlüsselzertifikat, das zum Verschlüsseln des Image-Manifests verwendet wird.

Die Regionen `us-gov-west-1` und `cn-north-1` verwenden ein nicht standardmäßiges öffentliches Schlüsselzertifikat, und der Pfad zu diesem Zertifikat muss mit dieser Option angegeben werden. Der Pfad zum Zertifikat variiert ausgehend von der Installationsmethode der AMI-Tools. Für Amazon Linux befinden sich die Zertifikate unter `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Wenn Sie die AMI-Tools aus der RPM- oder ZIP-Datei in Einrichten der AMI-Tools installiert haben, befinden sich die Zertifikate unter `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Erforderlich: Nur für die Regionen `us-gov-west-1` und `cn-north-1`.

`-r, --arch` architecture

Die Architektur des Images. Wenn Sie sie nicht in der Befehlszeile angeben, werden Sie dazu aufgefordert, sobald das Bündeln beginnt.

Zulässige Werte: `i386` | `x86_64`

Erforderlich: Nein

`--productcodes` code1,code2,...

Produkt-Codes, die dem Image zum Zeitpunkt der Registrierung angefügt werden, durch Kommas getrennt

Erforderlich: Nein

`-B, --block-device-mapping` mapping

Definiert, wie Blockgeräte für eine Instance dieses AMI bereitgestellt werden, wenn der Instance-Typ das angegebene Gerät unterstützt.

Geben Sie eine durch Komma getrennte Liste von Schlüssel-Wert-Paaren an, wobei jeder Schlüssel ein virtueller Name und jeder Wert der entsprechende Gerätename ist. Virtuelle Namen umfassen Folgendes:

- `ami` — Das Stammdateisystemgerät, wie es von der Instance erfasst wird
- `root` — Das Stammdateisystemgerät, wie es vom Kernel erfasst wird
- `swap` — Das Swap-Gerät, wie es von der Instance erfasst wird
- `ephemeralN` — Das n-te Instance-Speicher-Volume

Erforderlich: Nein

`-a, --all`

Bündeln Sie alle Verzeichnisse, einschließlich derer, die sich auf remote bereitgestellten Dateisystemen befinden.

Erforderlich: Nein

`-e, --exclude` directory1,directory2,...

Eine Liste absoluter Verzeichnispfade und Dateien, die aus dem Bündelungsvorgang ausgeschlossen werden sollen. Dieser Parameter überschreibt die Option `--all`. Wenn ein

Ausschließen festgelegt ist, werden die mit dem Parameter aufgeführten Verzeichnisse und Unterverzeichnisse nicht mit dem Volume gebündelt.

Erforderlich: Nein

`-i, --include` file1,file2,...

Eine Liste von Dateien, die in den Bündelungsvorgang einbezogen werden sollen. Die angegeben Dateien werden ansonsten aus dem AMI ausgeschlossen, da sie möglicherweise vertrauliche Informationen enthalten.

Erforderlich: Nein

`--no-filter`

Wenn dies angegeben ist werden wir die Dateien nicht aus dem AMI ausschließen, da sie möglicherweise vertrauliche Informationen enthalten.

Erforderlich: Nein

`-p, --prefix` prefix

Das Dateinamenpräfix für gebündelte AMI-Dateien

Standard: `image`

Erforderlich: Nein

`-s, --size` size

Die Größe der zu erstellenden Image-Datei in MB (1024 * 1024 Bytes). Die maximale Größe ist 10240 MB.

Standard: 10240

Erforderlich: Nein

`--[no-]inherit`

Gibt an, ob das Image die Metadaten der Instance erben soll (standardmäßig werden sie geerbt). Das Bündeln schlägt fehl, wenn Sie `--inherit` aktivieren, auf die Instance-Metadaten aber nicht zugegriffen werden kann.

Erforderlich: Nein

`-v, --volume` volume

Der absolute Pfad zum bereitgestellten Volume, aus dem das Bündel erstellt werden soll

Standard: Das Stammverzeichnis (/)

Erforderlich: Nein

`-P, --partition` type

Gibt an, ob das DatenträgerImage eine Partitionstabelle verwenden soll. Wenn Sie keinen Partitionstabellentyp angeben, wird standardmäßig der Typ festgelegt, der im übergeordneten Blockgerät des Volumes verwendet wird (sofern zutreffend), andernfalls ist der Standard `gpt`.

Zulässige Werte: `mbr` | `gpt` | `none`

Erforderlich: Nein

`-S, --script` script

Ein vor dem Bündeln auszuführendes Anpassungsskript. Das Skript muss ein einzelnes Argument, den Mountingpoint des Volumes, erwarten.

Erforderlich: Nein

`--fstab` path

Der Pfad zum fstab, das im Image gebündelt werden soll. Wenn das nicht festgelegt ist, bündelt Amazon EC2 /etc/fstab.

Erforderlich: Nein

`--generate-fstab`

Bündelt das Volume mit einem von Amazon EC2 bereitgestellten fstab.

Erforderlich: Nein

`--grub-config`

Der Pfad zu einer alternativen Grub-Konfigurationsdatei, die im Image gebündelt werden soll. Standardmäßig erwartet `ec2-bundle-vol`, dass entweder `/boot/grub/menu.lst` oder `/boot/grub/grub.conf` auf dem geklonten Image vorhanden ist. Mit dieser Option können Sie einen Pfad zu einer alternativen Grub-Konfigurationsdatei festlegen, der dann in die Standardeinstellungen (wenn vorhanden) kopiert wird.

Erforderlich: Nein

`--kernel` kernel_id

Veraltet. Verwenden Sie zum Festlegen des Kernels register-image.

Erforderlich: Nein

`--ramdisk`ramdisk_id

Veraltet. Verwenden Sie zum Festlegen des RAM-Datenträgers (sofern erforderlich) register-image.

Erforderlich: Nein

Output

Statusmeldung, die die Phasen und Status der Bündelung beschreibt

Beispiel

Dieses Beispiel erstellt eine gebündeltes AMI durch Komprimieren, Verschlüsseln und Signieren eines Snapshots des Stammdateisystems des lokalen Computers.

```
[ec2-user ~]$ ec2-bundle-vol -d /mnt -k pk-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -c
 cert-HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -u 111122223333 -r x86_64
  Copying / into the image file /mnt/image...
  Excluding:
       sys
       dev/shm
       proc
       dev/pts
       proc/sys/fs/binfmt_misc
       dev
       media
       mnt
       proc
       sys
       tmp/image
       mnt/img-mnt
  1+0 records in
  1+0 records out
  mke2fs 1.38 (30-Jun-2005)
  warning: 256 blocks unused.
```

```
Splitting /mnt/image.gz.crypt...
Created image.part.00
Created image.part.01
Created image.part.02
Created image.part.03
...
Created image.part.22
Created image.part.23
Generating digests for each part...
Digests generated.
Creating bundle manifest...
Bundle Volume complete.
```

ec2-delete-bundle

Beschreibung

Löscht das festgelegte Paket aus dem Amazon S3-Speicher. Wenn Sie ein Paket löschen, können Sie aus dem entsprechenden AMI keine Instances starten.

Syntax

ec2-delete-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* [-t *token*] [--url *url*] [--region *region*] [--sigv *version*] [-m *path*] [-p *prefix*] [--clear] [--retry] [-y]

Optionen

`-b, --bucket` bucket

Der Name des Amazon S3-Buckets, der das gebündelte AMI enthält, gefolgt von einem optionalen, durch "/" getrennten Pfadpräfix

Erforderlich: Ja

`-a, --access-key` access_key_id

Die AWS Zugriffsschlüssel-ID.

Erforderlich: Ja

`-s, --secret-key` secret_access_key

Der AWS geheime Zugriffsschlüssel.

Erforderlich: Ja

`-t, --delegation-token` token

Das Delegierungstoken, das an die AWS Anfrage weitergegeben werden soll. Weitere Informationen finden Sie unter Using Temporary Security Credentials.

Erforderlich: Nur wenn Sie temporäre Sicherheitsanmeldeinformationen verwenden.

Standard: Der Wert der `AWS_DELEGATION_TOKEN`-Umgebungsvariablen (wenn festgelegt)

`--region`region

Die in der Anforderungssignatur zu verwendende Region.

Standard: `us-east-1`

Erforderlich: Ist erforderlich, wenn Signaturversion 4 verwendet wird

`--sigv`Version

Die beim Signieren der Anforderung zu verwendende Signaturversion

Zulässige Werte: `2` | `4`

Standard: `4`

Erforderlich: Nein

`-m, --manifest`path

Der Pfad zur Manifestdatei

Erforderlich: Sie müssen `--prefix` oder `--manifest` angeben.

`-p, --prefix` prefix

Das gebündelte AMI-Dateinamenpräfix. Geben Sie das gesamte Präfix an. Verwenden Sie beim Präfix "image.img" beispielsweise `-p image.img` und nicht `-p image`.

Erforderlich: Sie müssen `--prefix` oder `--manifest` angeben.

`--clear`

Löscht nach dem Löschen des angegebenen Pakets den Amazon S3-Bucket, wenn er leer ist.

Erforderlich: Nein

`--retry`

Versucht bei allen Amazon S3-Fehlern den Vorgang automatisch erneut, bis zu fünfmal pro Vorgang.

Erforderlich: Nein

`-y, --yes`

Es wird automatisch davon ausgegangen, dass die Antwort auf alle Eingabeaufforderungen "ja" ist.

Erforderlich: Nein

Output

Amazon EC2 zeigt Statusmeldungen an, die die Phasen und Status des Löschvorgangs angeben.

Beispiel

Dieses Beispiel löscht ein Paket aus Amazon S3.

```
[ec2-user ~]$ ec2-delete-bundle -b DOC-EXAMPLE-BUCKET1 -a your_access_key_id -
s your_secret_access_key
Deleting files:
DOC-EXAMPLE-BUCKET1/image.manifest.xml
DOC-EXAMPLE-BUCKET1/image.part.00
DOC-EXAMPLE-BUCKET1/image.part.01
DOC-EXAMPLE-BUCKET1/image.part.02
DOC-EXAMPLE-BUCKET1/image.part.03
DOC-EXAMPLE-BUCKET1/image.part.04
DOC-EXAMPLE-BUCKET1/image.part.05
DOC-EXAMPLE-BUCKET1/image.part.06
Continue? [y/n]
y
Deleted DOC-EXAMPLE-BUCKET1/image.manifest.xml
Deleted DOC-EXAMPLE-BUCKET1/image.part.00
Deleted DOC-EXAMPLE-BUCKET1/image.part.01
Deleted DOC-EXAMPLE-BUCKET1/image.part.02
Deleted DOC-EXAMPLE-BUCKET1/image.part.03
Deleted DOC-EXAMPLE-BUCKET1/image.part.04
Deleted DOC-EXAMPLE-BUCKET1/image.part.05
Deleted DOC-EXAMPLE-BUCKET1/image.part.06
```

```
ec2-delete-bundle complete.
```

ec2-download-bundle

Beschreibung

Lädt die angegebenen Instance Store-Backed AMIs für Linux vom Amazon S3-Speicher herunter.

Syntax

ec2-download-bundle -b *bucket* -a *access_key_id* -s *secret_access_key* -k *path* [--url *url*] [--region *region*] [--sigv *version*] [-m *file*] [-p *prefix*] [-d *directory*] [--retry]

Optionen

`-b, --bucket` bucket

Der Name des Amazon S3-Buckets, in dem sich das Paket befindet, gefolgt von einem optionalen, durch "/" getrennten Pfadpräfix

Erforderlich: Ja

`-a, --access-key` access_key_id

Die AWS Zugriffsschlüssel-ID.

Erforderlich: Ja

`-s, --secret-key` secret_access_key

Der AWS geheime Zugriffsschlüssel.

Erforderlich: Ja

`-k, --privatekey` path

Der private Schlüssel, der zum Entschlüsseln des Manifests verwendet wird

Erforderlich: Ja

`--url` url

Die Amazon S3-Service-URL

Standard: `https://s3.amazonaws.com/`

Erforderlich: Nein

`--region` region

Die in der Anforderungssignatur zu verwendende Region.

Standard: `us-east-1`

Erforderlich: Ist erforderlich, wenn Signaturversion 4 verwendet wird

`--sigv` version

Die beim Signieren der Anforderung zu verwendende Signaturversion

Zulässige Werte: `2` | `4`

Standard: `4`

Erforderlich: Nein

`-m, --manifest` file

Der Name der Manifestdatei (ohne den Pfad). Wir empfehlen Ihnen, dass Sie entweder das Manifest (`-m`) oder ein Präfix (`-p`) angeben.

Erforderlich: Nein

`-p, --prefix` prefix

Das Dateinamenpräfix für gebündelte AMI-Dateien

Standard: `image`

Erforderlich: Nein

`-d, --directory` directory

Das Verzeichnis, in dem das heruntergeladene Paket gespeichert wird. Das Verzeichnis muss vorhanden sein.

Standard: Das aktuelle Arbeitsverzeichnis

Erforderlich: Nein

`--retry`

Versucht bei allen Amazon S3-Fehlern den Vorgang automatisch erneut, bis zu fünfmal pro Vorgang.

Erforderlich: Nein

Output

Statusmeldungen werden angezeigt, die die unterschiedlichen Phasen und Status des Download-Vorgangs angeben.

Beispiel

Dieses Beispiel erstellt das `bundled`-Verzeichnis (mithilfe des Linux-Befehls mkdir) und lädt das Paket vom Amazon S3-Bucket `DOC-EXAMPLE-BUCKET1` herunter.

```
[ec2-user ~]$ mkdir bundled
[ec2-user ~]$ ec2-download-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name
 -m image.manifest.xml -a your_access_key_id -s your_secret_access_key -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -d mybundle
Downloading manifest image.manifest.xml from DOC-EXAMPLE-BUCKET1 to mybundle/
image.manifest.xml ...
Downloading part image.part.00 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.00 ...
Downloaded image.part.00 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.01 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.01 ...
Downloaded image.part.01 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.02 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.02 ...
Downloaded image.part.02 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.03 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.03 ...
Downloaded image.part.03 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.04 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.04 ...
Downloaded image.part.04 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.05 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.05 ...
Downloaded image.part.05 from DOC-EXAMPLE-BUCKET1
Downloading part image.part.06 from DOC-EXAMPLE-BUCKET1/bundles/bundle_name to
 mybundle/image.part.06 ...
```

```
Downloaded image.part.06 from DOC-EXAMPLE-BUCKET1
```

ec2-migrate-manifest

Beschreibung

Verändert ein Instance Store-Backed Linux AMI (z. B. das Zertifikat, den Kernel und den RAM-Datenträger) so, dass es eine andere Region unterstützt.

Syntax

ec2-migrate-manifest -c *path* -k *path* -m *path* {(-a *access_key_id* -s *secret_access_key* --region *region*) | (--no-mapping)} [--ec2cert *ec2_cert_path*] [--kernel *kernel-id*] [--ramdisk *ramdisk_id*]

Optionen

`-c, --cert` path

Die PEM-kodierte öffentliche RSA-Schlüsselzertifikatsdatei des Benutzers

Erforderlich: Ja

`-k, --privatekey` path

Der Pfad zur PEM-kodierten RSA-Schlüsseldatei des Benutzers

Erforderlich: Ja

`--manifest` path

Der Pfad zur Manifestdatei

Erforderlich: Ja

`-a, --access-key` access_key_id

Die AWS Zugriffsschlüssel-ID.

Erforderlich: Ist erforderlich, wenn das automatische Mapping verwendet wird.

`-s, --secret-key` secret_access_key

Der AWS geheime Zugriffsschlüssel.

Erforderlich: Ist erforderlich, wenn das automatische Mapping verwendet wird.

`--region` region

Die in der Mapping-Datei zu suchende Region

Erforderlich: Ist erforderlich, wenn das automatische Mapping verwendet wird.

`--no-mapping`

Deaktiviert das automatische Mapping von Kernels und RAM-Datenträgern.

Während der Migration ersetzt Amazon EC2 den Kernel und den RAM-Datenträger in der Manifestdatei durch einen Kernel und einen RAM-Datenträger, die für die Zielregion erstellt wurden. Sofern der Parameter `--no-mapping` nicht angeben wurde, verwendet `ec2-migrate-bundle` unter Umständen die Vorgänge `DescribeRegions` und `DescribeImages` für automatisierte Zuweisungen.

Erforderlich: Ist erforderlich, wenn Sie die Optionen `-a`, `-s` und `--region` nicht angeben, die für das automatische Mapping verwendet werden.

`--ec2cert` path

Der Pfad zum öffentlichen Amazon EC2 X.509-Schlüsselzertifikat, das zum Verschlüsseln des Image-Manifests verwendet wird.

Die Regionen `us-gov-west-1` und `cn-north-1` verwenden ein nicht standardmäßiges öffentliches Schlüsselzertifikat, und der Pfad zu diesem Zertifikat muss mit dieser Option angegeben werden. Der Pfad zum Zertifikat variiert ausgehend von der Installationsmethode der AMI-Tools. Für Amazon Linux befinden sich die Zertifikate unter `/opt/aws/amitools/ec2/etc/ec2/amitools/`. Wenn Sie die AMI-Tools aus der ZIP-Datei in Einrichten der AMI-Tools installiert haben, befinden sich die Zertifikate unter `$EC2_AMITOOL_HOME/etc/ec2/amitools/`.

Erforderlich: Nur für die Regionen `us-gov-west-1` und `cn-north-1`.

`--kernel` kernel_id

Die ID des Kernels, der ausgewählt werden soll

> **Important**
>
> Wir empfehlen Ihnen die Verwendung von PV-GRUB anstelle von Kernels und RAM-Datenträgern. Weitere Informationen finden Sie unter Vom Benutzer bereitgestellte Kernel im Amazon Linux 2-Benutzerhandbuch.

Erforderlich: Nein

`--ramdisk` ramdisk_id

Die ID des RAM-Datenträgers, der ausgewählt werden soll

> **Important**
>
> Wir empfehlen Ihnen die Verwendung von PV-GRUB anstelle von Kernels und RAM-Datenträgern. Weitere Informationen finden Sie unter Vom Benutzer bereitgestellte Kernel im Amazon Linux 2-Benutzerhandbuch.

Erforderlich: Nein

Output

Statusmeldung, die die Phasen und Status des Bündelungsprozesses beschreibt

Beispiel

Dieses Beispiel kopiert das im `my-ami.manifest.xml`-Manifest angegebene AMI aus den USA in die EU.

```
[ec2-user ~]$ ec2-migrate-manifest --manifest my-ami.manifest.xml
 --cert cert-HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --privatekey pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBZQ55CLO.pem --region eu-west-1

Backing up manifest...
Successfully migrated my-ami.manifest.xml It is now suitable for use in eu-west-1.
```

ec2-unbundle

Beschreibung

Erstellt das Paket neu aus einem Instance Store-Backed AMI für Linux.

Syntax

ec2-unbundle -k *path* -m *path* [-s *source_directory*] [-d *destination_directory*]

Optionen

`-k, --privatekey` path

Der Pfad zu Ihrer PEM-kodierten RSA-Schlüsseldatei

Erforderlich: Ja

`-m, --manifest` path

Der Pfad zur Manifestdatei

Erforderlich: Ja

`-s, --source` source_directory

Das Verzeichnis, das das Paket enthält

Standard: Das aktuelle Verzeichnis

Erforderlich: Nein

`-d, --destination` destination_directory

Das Verzeichnis, in dem das AMI entpackt wird. Das Zielverzeichnis muss vorhanden sein.

Standard: Das aktuelle Verzeichnis

Erforderlich: Nein

Beispiel

Dieses Linux- und UNIX-Beispiel entpackt das AMI, das in der `image.manifest.xml`-Datei angegeben ist.

```
[ec2-user ~]$ mkdir unbundled
$ ec2-unbundle -m mybundle/image.manifest.xml -k pk-
HKZYKTAIG2ECMXYIBH3HXV4ZBEXAMPLE.pem -s mybundle -d unbundled
$ ls -l unbundled
total 1025008
-rw-r--r-- 1 root root 1048578048 Aug 25 23:46 image.img
```

Output

Statusmeldungen werden angezeigt, die die unterschiedlichen Phasen und Status des Entpackvorgangs angeben.

ec2-upload-bundle

Beschreibung

Lädt das Bundle für ein Instance-Speicher-unterstütztes Linux AMI in Amazon S3 hoch und legt die entsprechenden Zugriffskontrolllisten (ACLs) für die hochgeladenen Objekte fest. Weitere Informationen finden Sie unter Erstellen einer Instance-Speicher-Backed Linux-AMI.

> **Note**
>
> Um Objekte für Ihr Instance-Speicher-gestütztes Linux-AMI in einen S3-Bucket hochzuladen, müssen ACLs für den Bucket aktiviert sein. Andernfalls kann Amazon EC2 keine ACLs für die hochzuladenden Objekte festlegen. Wenn Ihr Ziel-Bucket die erzwungene Einstellung für den Bucket-Eigentümer für S3 Object Ownership verwendet, funktioniert dies nicht, da ACLs deaktiviert sind. Weitere Informationen finden Sie unter Steuern der Eigentümerschaft an hochgeladenen Objekten mit S3 Object Ownership.

Syntax

```
ec2-upload-bundle -b bucket -a access_key_id -s secret_access_key [-t
token] -m path [--url url] [--region region] [--sigv version] [--acl acl]
[-d directory] [--part part] [--retry] [--skipmanifest]
```

Optionen

`-b, --bucket` bucket

Der Name des Amazon S3-Buckets, in dem das Paket gespeichert werden soll, gefolgt von einem optionalen durch "/" getrennten Pfadpräfix. Wenn der Bucket nicht vorhanden ist, wird er erstellt, sofern der Bucket-Name verfügbar ist. Wenn der Bucket nicht vorhanden ist und die Version der AMI-Tools 1.5.18 oder höher ist, legt dieser Befehl außerdem die ACLs für den Bucket fest.

Erforderlich: Ja

`-a, --access-key` access_key_id

Ihre AWS Zugangsschlüssel-ID.

Erforderlich: Ja

`-s, --secret-key` secret_access_key

Ihr AWS geheimer Zugangsschlüssel.

Erforderlich: Ja

`-t, --delegation-token` token

Das Delegierungstoken, das an die AWS Anfrage weitergegeben werden soll. Weitere Informationen finden Sie unter Using Temporary Security Credentials.

Erforderlich: Nur wenn Sie temporäre Sicherheitsanmeldeinformationen verwenden.

Standard: Der Wert der `AWS_DELEGATION_TOKEN`-Umgebungsvariablen (wenn festgelegt)

`-m, --manifest` path

Der Pfad zur Manifestdatei Die Manifestdatei wird während des Bündelungsvorgangs erstellt. Sie finden sie in dem Verzeichnis, das das Paket enthält.

Erforderlich: Ja

`--url` url

Veraltet. Verwenden Sie die Option `--region`, wenn Ihr Bucket nicht auf den Standort `EU` (nicht `eu-west-1`) beschränkt ist. Das Flag `--location` ist die einzige Möglichkeit, um auf diese spezifische Standortbeschränkung einzugehen.

Die Amazon S3-Endpunkt-Service-URL

Standard: `https://s3.amazonaws.com/`

Erforderlich: Nein

`--region` region

Die Region, die in der Anforderungssignatur für den S3-Ziel-Bucket verwendet werden soll

- Wenn der Bucket nicht vorhanden ist und Sie keine Region angeben, erstellt das Tool den Bucket ohne eine Standortbeschränkung (in `us-east-1`).
- Wenn der Bucket nicht vorhanden ist und Sie eine Region angeben, erstellt das Tool den Bucket in der angegebenen Region.
- Wenn der Bucket vorhanden ist und Sie keine Region angeben, verwendet das Tool den Standort des Buckets.

- Wenn der Bucket vorhanden ist und Sie `us-east-1` als Region angeben, verwendet das Tool den tatsächlichen Standort des Buckets, ohne eine Fehlermeldung auszugeben, und vorhandene übereinstimmende Dateien werden überschrieben.
- Wenn der Bucket vorhanden ist und Sie eine Region angeben, die nicht `us-east-1` ist und nicht mit dem tatsächlichen Standort des Buckets übereinstimmt, wird das Tool mit einem Fehler beendet.

Wenn Ihr Bucket auf den Standort `EU` (nicht `eu-west-1`) beschränkt ist, verwenden Sie das Flag `--location`. Das Flag `--location` ist die einzige Möglichkeit, um auf diese spezifische Standortbeschränkung einzugehen.

Standard: `us-east-1`

Erforderlich: Ist erforderlich, wenn Signaturversion 4 verwendet wird

`--sigv` version

Die beim Signieren der Anforderung zu verwendende Signaturversion

Zulässige Werte: `2` | `4`

Standard: `4`

Erforderlich: Nein

`--acl` acl

Die Richtlinie für die Access Control List des gebündelten Images

Zulässige Werte: `public-read` | `aws-exec-read`

Standard: `aws-exec-read`

Erforderlich: Nein

`-d, --directory` directory

Das Verzeichnis, das die gebündelten AMI-Teile enthält

Standard: Das Verzeichnis, das die Manifestdatei enthält (siehe die Option `-m`)

Erforderlich: Nein

`--part` part

Beginnt mit dem Hochladen des angegebenen Teils und aller folgenden Teile. z. B. `--part 04`.

Erforderlich: Nein

`--retry`

Versucht bei allen Amazon S3-Fehlern den Vorgang automatisch erneut, bis zu fünfmal pro Vorgang.

Erforderlich: Nein

`--skipmanifest`

Lädt das Manifest nicht hoch.

Erforderlich: Nein

`--location` location

Veraltet. Verwenden Sie die Option `--region`, wenn Ihr Bucket nicht auf den Standort EU (nicht `eu-west-1`) beschränkt ist. Das Flag `--location` ist die einzige Möglichkeit, um auf diese spezifische Standortbeschränkung einzugehen.

Die Standortbeschränkung des Amazon S3-Ziel-Buckets. Wenn der Bucket vorhanden ist und Sie einen Standort angegeben haben, der nicht mit dem tatsächlichen Standort des Buckets übereinstimmt, wird das Tool mit einem Fehler beendet. Wenn der Bucket vorhanden ist und Sie keinen Standort angeben, verwendet das Tool den Standort des Buckets. Wenn der Bucket nicht vorhanden ist und Sie einen Standort angeben, erstellt das Tool den Bucket am angegebenen Standort. Wenn der Bucket nicht vorhanden ist und Sie keinen Standort angeben, erstellt das Tool den Bucket ohne eine Standortbeschränkung (in `us-east-1`).

Standard: Wenn `--region` angegeben ist, wird der Standort auf die angegebene Region festgelegt. Wenn `--region` nicht angegeben ist, ist der Standort standardmäßig `us-east-1`.

Erforderlich: Nein

Output

Amazon EC2 zeigt Statusmeldungen an, die die Phasen und Status des Upload-Vorgangs angeben.

Beispiel

Dieses Beispiel lädt das Paket hoch, das vom `image.manifest.xml`-Manifest festgelegt wurde.

```
[ec2-user ~]$ ec2-upload-bundle -b DOC-EXAMPLE-BUCKET1/bundles/bundle_name -m
 image.manifest.xml -a your_access_key_id -s your_secret_access_key
Creating bucket...
Uploading bundled image parts to the S3 bucket DOC-EXAMPLE-BUCKET1 ...
Uploaded image.part.00
Uploaded image.part.01
Uploaded image.part.02
Uploaded image.part.03
Uploaded image.part.04
Uploaded image.part.05
Uploaded image.part.06
Uploaded image.part.07
Uploaded image.part.08
Uploaded image.part.09
Uploaded image.part.10
Uploaded image.part.11
Uploaded image.part.12
Uploaded image.part.13
Uploaded image.part.14
Uploading manifest ...
Uploaded manifest.
Bundle upload completed.
```

Allgemeine Optionen für AMI-Tools

Die meisten AMI-Tools akzeptieren die folgenden optionalen Parameter.

`--help, -h`

Zeigt die Hilfenachricht an.

`--version`

Zeigt die Version und das Copyright an.

`--manual`

Zeigt die manuelle Eingabe an.

`--batch`

Wird im Stapelmodus ausgeführt und unterdrückt interaktive Eingabeaufforderungen.

`--debug`

Zeigt Informationen an, die bei der Problembehebung hilfreich sind.

Erstellen Sie ein AMI mit Windows Sysprep

Das Microsoft System Preparation (Sysprep)-Tool vereinfacht das Duplizieren einer benutzerdefinierten Installation von Windows. Sie können Sysprep verwenden, um ein Standard-Amazon-Machine-Image (AMI) zu erstellen. Anschließend können Sie aus diesem standardisierten Image neue Amazon EC2 Instances für Windows erstellen.

Wir empfehlen, EC2 Image Builder zu verwenden, um die Erstellung, Verwaltung und Bereitstellung von benutzerdefinierten, sicheren und up-to-date „goldenen“ Server-Images zu automatisieren, die vorinstalliert und mit Software und Einstellungen vorkonfiguriert sind.

Wenn Sie Windows Sysprep verwenden, um ein standardisiertes AMI zu erstellen, empfehlen wir, dass Sie Sysprep mit ausführen. EC2Launch v2 Wenn Sie weiterhin die Agents EC2Config (Windows Server 2012 R2 und früher) oder EC2Launch (Windows Server 2016 und 2019) verwenden, finden Sie in der Dokumentation zur Verwendung von Sysprep mit EC2Config und EC2Launch unten weitere Informationen.

> **Important**
>
> Verwenden Sie Sysprep nicht zum Erstellen von Instance-Backups Sysprep entfernt systemspezifische Informationen, was ungewünschte Auswirkungen auf Instance-Backups nach sich ziehen kann.

Informationen zur Problembehandlung bei Sysprep finden Sie unter Beheben Sie Sysprep-Probleme mit Windows-Instanzen.

Inhalt

Bevor Sie beginnen

- Sie sollten vor Ausführung von Sysprep alle lokalen Benutzerkonten und alle Kontoprofile entfernen, abgesehen von einem einzigen Administratorkonto, mit dem Sysprep ausgeführt wird.

Wenn Sie Sysprep mit zusätzlichen Konten und Profilen ausführen, könnte dies zu nicht erwarteten Verhaltensweisen einschließlich des Verlusts von Profildaten oder des nicht erfolgreichen Abschlusses von Sysprep führen.

- Erfahren Sie mehr über Sysprep auf Microsoft. TechNet
- Erfahren Sie, welche Serverrollen für Sysprep unterstützt werden.

Verwenden von Sysprep mit EC2Launch v2

Dieser Abschnitt enthält Details zu den verschiedenen Sysprep-Ausführungsphasen und den Aufgaben, die der EC2Launch v2-Service während der Vorbereitung des Image ausführt. Er enthält auch die Schritte zum Erstellen eines standardisierten AMI mit Sysprep mit dem EC2Launch v2-Service.

Sysprep mit EC2Launch v2-Themen

- Sysprep-Phasen
- Sysprep-Aktionen
- Nach Sysprep
- Sysprep mit EC2Launch v2 ausführen

Sysprep-Phasen

Folgende Phasen werden beim Ausführen von Sysprep durchlaufen:

- Generalisieren: Das Tool entfernt Image-spezifische Informationen und Konfigurationen. Zum Beispiel entfernt Sysprep u. a. die Sicherheits-ID (SID), den Computer-Namen, die Ereignisprotokolle und bestimmte Treiber. Anschließend kann vom Betriebssystem (OS) ein AMI erstellt werden.

  > **Note**
  >
  > Wenn Sie Sysprep mit dem EC2Launch v2-Service ausführen, verhindert das System, dass Treiber entfernt werden, da die `PersistAllDeviceInstalls`-Einstellung standardmäßig auf true festgelegt ist.

- Spezialisieren: Plug & Play durchsucht den Computer und installiert Treiber für alle erkannten Geräte. Das Tool erstellt OS-Anforderungen, z. B. Computer-Name und SID. Optional können Sie Befehle in dieser Phase ausführen.

- Out-of-Box Experience (OOBE): Das System führt ein verkürztes Windows Setup aus und fordert Sie zur Eingabe von Informationen wie Systemsprache, Zeitzone und einer registrierten Organisation auf. Wenn Sie Sysprep mit EC2Launch v2 ausführen, automatisiert die Antwortdatei diese Phase.

Sysprep-Aktionen

Sysprep und EC2Launch v2 führen beim Vorbereiten eines Image die folgenden Aktionen aus.

1. Wenn Sie im Dialogfeld EC2Launch-Einstellungen die Option Shutdown with Sysprep wählen, führt das System den Befehl `ec2launch sysprep` aus.
2. EC2Launch v2 bearbeitet den Inhalt der `unattend.xml`-Datei, indem der Registrierungswert unter `HKEY_USERS\.DEFAULT\Control Panel\International\LocaleName` gelesen wird. Die Datei befindet sich im folgenden Verzeichnis: `C:\ProgramData\Amazon\EC2Launch\sysprep`.
3. Das System führt das au `BeforeSysprep.cmd`. Dieser Befehl erstellt den folgenden Registrierungsschlüssel:

   reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f

   Der Registrierungsschlüssel deaktiviert RDP-Verbindungen bis sie erneut aktiviert werden. Die Deaktivierung von RDP-Verbindungen ist eine notwendige Sicherheitsmaßnahme, da während der ersten Boot-Session nach der Ausführung von Sysprep kurzzeitig Verbindungen von RDP zugelassen werden und noch kein Administratorkennwort vergeben ist.
4. Der EC2Launch v2-Service ruft Sysprep mit dem folgenden Befehl auf:

   sysprep.exe /oobe /generalize /shutdown /unattend: "C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml"

Generalisierungsphase

- EC2Launch v2 entfernt Image-spezifische Informationen und Konfigurationen, z. B. Computer-Name und SID. Wenn die Instance Mitglied einer Domain ist, wird sie von der Domain entfernt. Die `unattend.xml`-Antwortdatei enthält folgende Einstellungen, die sich auf diese Phase auswirken:
  - PersistAllDeviceInstalls: Diese Einstellung verhindert, dass Windows Setup Geräte entfernt und neu konfiguriert, wodurch der Image-Vorbereitungsprozess beschleunigt wird, da Amazon-AMIs

bestimmte Treiber zur Ausführung benötigen und die erneute Erkennung dieser Treiber einige Zeit in Anspruch nehmen würde.

- DoNotCleanUpNonPresentGeräte: Bei dieser Einstellung werden Plug & Play-Informationen für Geräte beibehalten, die derzeit nicht vorhanden sind.

- Sysprep beendet das Betriebssystem beim Erstellen des AMI. Das System startet entweder eine neue Instance oder die ursprüngliche Instance.

Spezialisierungsphase

Das System erstellt OS-spezifische Anforderungen, z. B. Computer-Name und eine SID. Das System führt zudem die folgenden Aktionen basierend auf Konfigurationen durch, die Sie in der `unattend.xml`-Antwortdatei angeben.

- CopyProfile: Sysprep kann so konfiguriert werden, dass alle Benutzerprofile gelöscht werden, einschließlich des integrierten Administratorprofils. Die Einstellung behält das integrierte Administratorkonto bei, sodass alle an diesem Konto vorgenommenen Anpassungen auf das neue Image übertragen werden. Der Standardwert ist `True`.

  CopyProfileersetzt das Standardprofil durch das vorhandene lokale Administratorprofil. Alle Konten, mit denen Sie sich nach der Ausführung von Sysprep anmelden, erhalten bei der ersten Anmeldung eine Kopie dieses Profils und seiner Inhalte.

  Wenn es keine spezifischen Benutzerprofilanpassungen gibt, die Sie auf das neue Image übertragen möchten, legen Sie diese Einstellung auf fes `False`. Sysprep entfernt alle Benutzerprofile. Dies spart Zeit und Festplattenspeicher.
- TimeZone: Die Zeitzone ist standardmäßig auf Coordinate Universal Time (UTC) eingestellt.
- Synchronous command with order 1: Das System führt den folgenden Befehl zur Aktivierung des Administratorkontos und Angabe der Passwortanforderungen aus.

  ```
  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER /
  PASSWORDREQ:YES
  ```
- Synchronous command with order 2: Das System verschlüsselt das Administratorpasswort. Diese Sicherheitsmaßnahme soll verhindern, dass nach Abschluss von Sysprep auf die Instanz zugegriffen werden kann, wenn Sie die `setAdminAccount` Aufgabe nicht konfiguriert haben.

  Das System führt den folgenden Befehl von Ihrem lokalen Launch-Agent-Verzeichnis aus () `C:\Program Files\Amazon\EC2Launch\` aus.

```
EC2Launch.exe internal randomize-password --username Administrator
```

- Um Remote-Desktop-Verbindungen zu aktivieren, setzt das System den `fDenyTSConnections` Terminalserver-Registrierungsschlüssel auf False.

OOBE-Phase

1. Das System gibt die folgenden Konfigurationen mithilfe der EC2Launch v2-Antwortdatei an:
   - `<InputLocale>en-US</InputLocale>`
   - `<SystemLocale>en-US</SystemLocale>`
   - `<UILanguage>en-US</UILanguage>`
   - `<UserLocale>en-US</UserLocale>`
   - `<HideEULAPage>true</HideEULAPage>`
   - `<HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>`
   - `<ProtectYourPC>3</ProtectYourPC>`
   - `<BluetoothTaskbarIconEnabled>false</BluetoothTaskbarIconEnabled>`
   - `<TimeZone>UTC</TimeZone>`
   - `<RegisteredOrganization>Amazon.com</RegisteredOrganization>`
   - `<RegisteredOwner>EC2</RegisteredOwner>`

   > **Note**
   >
   > Während der Verallgemeinerungs- und Spezialisierungsphasen überwacht EC2Launch v2 den Status des Betriebssystems. Wenn EC2Launch v2 erkennt, dass sich das OS in einer Sysprep-Phase befindet, schreibt es die folgende Mitteilung in das Systemprotokoll: Windows wird konfiguriert. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Das System führt EC2Launch v2 aus.

Nach Sysprep

Nach Abschluss von Sysprep sendet EC2Launch v2 die folgende Meldung an die Konsolenausgabe:

```
Windows sysprep configuration complete.
```

EC2Launch v2 führt anschließend die folgenden Aktionen aus:

1. Liest den Inhalt der `agent-config.yml`-Datei und führt konfigurierte Aufgaben aus.
2. Führt alle Aufgaben in der `preReady`-Phase aus.
3. Danach sendet es die Nachricht `Windows is ready` an die Systemprotokolle der Instance.
4. Führt alle Aufgaben in der `PostReady`-Phase aus.

Weitere Informationen zu EC2Launch v2 finden Sie unter Konfigurieren einer Windows-Instance mithilfe von EC2Launch v2.

Sysprep mit EC2Launch v2 ausführen

Gehen Sie wie folgt vor, um ein standardisiertes AMI mit Sysprep mit EC2Launch v2 zu erstellen.

1. Suchen Sie in der Amazon EC2 EC2-Konsole ein AMI, das Sie duplizieren möchten.
2. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
3. Passen Sie sie an.
4. Suchen Sie im Start-Menü von Windows nach Amazon EC2Launch Settings (Amazon EC2Launch-Einstellungen) und wählen Sie diese aus. Weitere Informationen zu den Optionen und Einstellungen im Dialogfeld Amazon EC2Launch Settings (Amazon EC2Launch-Einstellungen) finden Sie unter Einstellungen für EC2Launch v2.
5. Wählen Sie Shutdown with Sysprep (Herunterfahren mit Sysprep) oder Shutdown without Sysprep (Herunterfahren ohne Sysprep) aus.

Wenn Sie zum Bestätigen der Ausführung von Sysprep und zum Beenden der Instance aufgefordert werden, klicken Sie auf Yes (Ja). EC2Launch v2 führt Sysprep aus. Sie werden dann von der Instance abgemeldet und die Instance wird beendet. Auf der Seite Instances in der Amazon EC2-Konsole wechselt der Instance-Status von `Running` zu `Stopping` und zu `Stopped`. Jetzt kann ein AMI aus dieser Instance erstellt werden.

Sie können das Sysprep-Tool manuell mittels Befehlszeile und dem folgenden Befehl aufrufen:

```
"%programfiles%\amazon\ec2launch\ec2launch.exe" sysprep --shutdown=true
```

Verwenden von Sysprep mit EC2Launch

EC2Launch bietet eine standardmäßige Antwortdatei und Batch-Dateien für Sysprep, mit denen die Image-Vorbereitung auf Ihrem AMI automatisiert und gesichert wird. Das Ändern dieser Dateien ist optional. Sie befinden sich standardmäßig in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.

> **Important**
>
> Verwenden Sie Sysprep nicht zum Erstellen von Instance-Backups. Sysprep entfernt systemspezifische Informationen. Wenn Sie diese Informationen entfernen, könnte dies bei einer Instance-Sicherung unbeabsichtigte Folgen haben.

Sysprep mit EC2Launch-Themen

- EC2Launch-Antwort- und -Batchdateien für Sysprep
- Ausführen von Sysprep mit EC2Launch
- Aktualisieren von Metadaten/KMS-Routen für Server 2016 und höher beim Starten eines benutzerdefinierten AMI

EC2Launch-Antwort- und -Batchdateien für Sysprep

Die EC2Launch-Antwortdatei und die Batch-Dateien für Sysprep enthalten Folgendes:

`Unattend.xml`

Dies ist die standardmäßige Antwortdatei. Wenn Sie ShutdownWithSysprep in der Benutzeroberfläche ausführen `SysprepInstance.ps1` oder auswählen, liest das System die Einstellung aus dieser Datei.

`BeforeSysprep.cmd`

Passen Sie diese Batch-Datei so an, dass Befehle ausgeführt werden, bevor EC2Launch Sysprep ausführt.

`SysprepSpecialize.cmd`

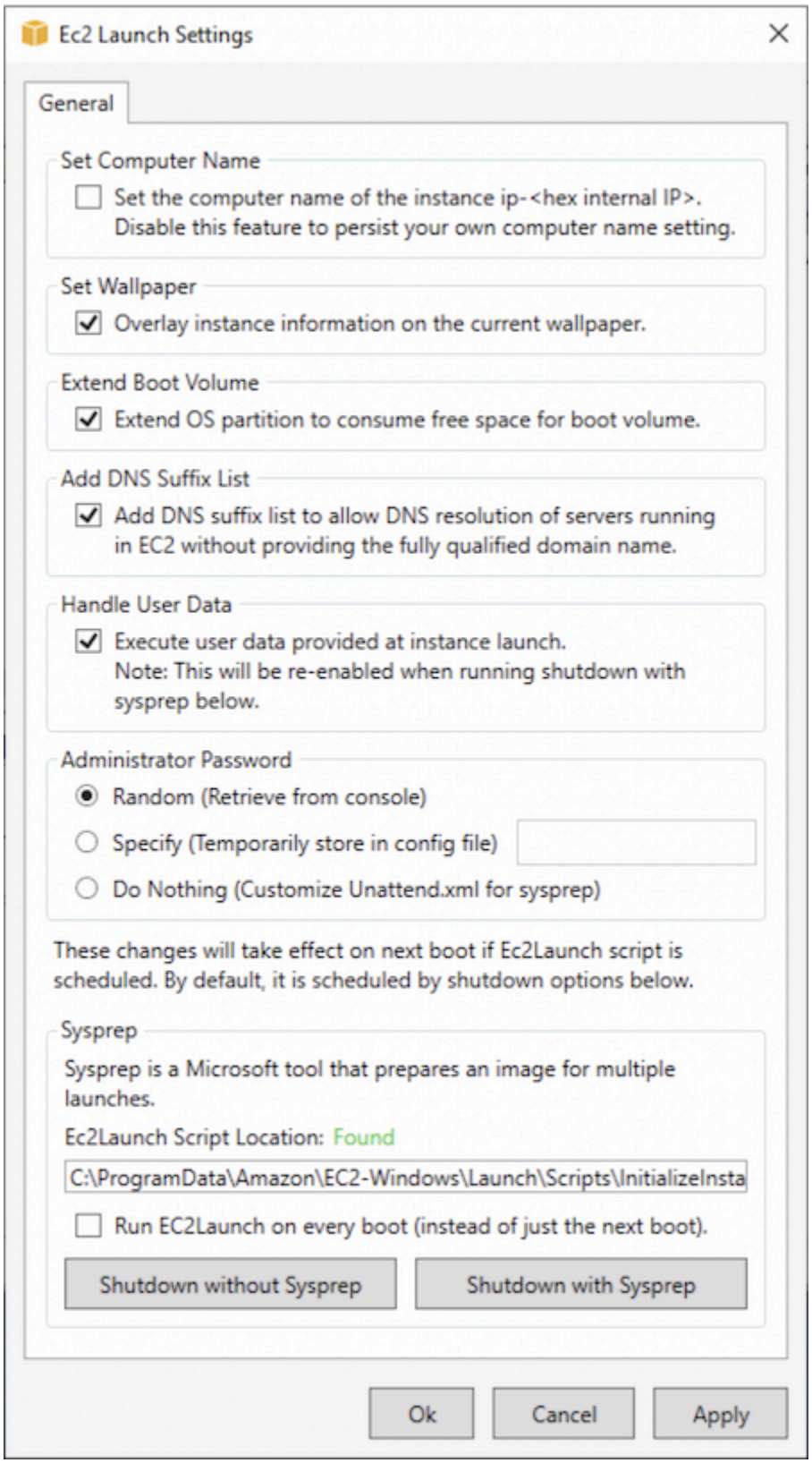
Passen Sie diese Batch-Datei so an, dass Befehle während der Sysprep-Spezialisierungsphase ausführt werden.

Ausführen von Sysprep mit EC2Launch

Bei der vollständigen Installation von Windows Server 2016 und höher (mit Desktoperfahrung) können Sie Sysprep manuell mit EC2Launch oder mit der Anwendung der EC2 Launch Settings (EC2-Starteinstellungen) ausführen.

So führen Sie Sysprep mit der Anwendung für EC2Launch-Einstellungen aus

1. Suchen oder erstellen Sie in der Amazon EC2-Konsole ein AMI mit Windows Server 2016 oder höher.
2. Starten Sie über das AMI eine Windows-Instance.
3. Stellen Sie eine Verbindung mit Ihrer Windows-Instance her, und passen Sie sie an.
4. Suchen Sie nach der LaunchSettingsEC2-Anwendung und führen Sie sie aus. Standardmäßig befindet sie sich in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Settings`.



5. Wählen oder löschen Sie die Optionen nach Bedarf. Diese Einstellungen werden in der Datei `LaunchConfig.json` gespeichert.

6. Gehen Sie für Administrator Password wie folgt vor:

   - Wählen Sie Random. EC2Launch generiert ein Passwort und verschlüsselt es mit dem Schlüssel des Benutzers: Die Einstellung wird vom System nach dem Start der Instance deaktiviert, so dass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.
   - Wählen Sie Specify, und geben Sie ein Passwort ein, das den Systemanforderungen entspricht. Das Passwort wird in `LaunchConfig.json` im Klartext gespeichert und gelöscht, wenn Sysprep das Administratorpasswort einstellt. Wenn Sie den Service gleich beenden, wird das Passwort sofort festgelegt. EC2Launch verschlüsselt das Passwort mit dem Schlüssel des Benutzers.
   - Wählen Sie ein Passwort DoNothingund geben Sie es in der `unattend.xml` Datei an. Wenn Sie in der Datei `unattend.xml` kein Passwort angeben, ist das Administratorkonto deaktiviert.

7. Wählen Sie Shutdown with Sysprep (Herunterfahren mit Sysprep).

So führen Sie Sysprep manuell mit EC2Launch aus

1. Finden oder erstellen Sie in der Amazon EC2-Konsole ein AMI der Datacenter-Edition von Windows Server 2016 oder höher, das Sie duplizieren wollen.
2. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
3. Passen Sie die Instance an.
4. Geben Sie Einstellungen in der Datei `LaunchConfig.json` an. Diese Datei befindet sich standardmäßig im Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

   Geben Sie für `adminPasswordType` einen der folgenden Werte an:

   `Random`

   EC2Launch generiert ein Passwort und verschlüsselt es mit dem Schlüssel des Benutzers: Die Einstellung wird vom System nach dem Start der Instance deaktiviert, so dass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.

   `Specify`

   EC2Launch verwendet das Passwort, das Sie unter angebe `adminPassword`. Wenn das Passwort nicht den Systemanforderungen entspricht, erstellt EC2Launch stattdessen ein zufälliges Passwort. Das Passwort wird in `LaunchConfig.json` im Klartext gespeichert und

gelöscht, wenn Sysprep das Administratorpasswort einstellt. EC2Launch verschlüsselt das Passwort mit dem Schlüssel des Benutzers.

`DoNothing`

EC2Launch verwendet das Passwort, das Sie in der Datei `unattend.xml`-Datei angeben. Wenn Sie in der Datei `unattend.xml` kein Passwort angeben, ist das Administratorkonto deaktiviert.

5. (Optional) Geben Sie Einstellungen in `unattend.xml` und anderen Konfigurationsdateien an. Wenn Sie eine beaufsichtigte Installation planen, brauchen Sie keine Änderung in diesen Dateien vorzunehmen. Die Dateien befinden sich standardmäßig in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep`.
6. Führen Sie in Windows PowerShell aus `./InitializeInstance.ps1 -Schedule`. Das Script befindet sich standardmäßig in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`. Dieses Script plant die Initialisierung der Instance beim nächsten Starten. Sie müssen diese Script ausführen, bevor Sie im nächsten Schritt das Script `SysprepInstance.ps1` ausführen.
7. Führen Sie in Windows PowerShell aus `./SysprepInstance.ps1`. Das Script befindet sich standardmäßig in folgendem Verzeichnis: `C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts`.

Sie werden von der Instance abgemeldet und die Instance wird beendet. Auf der Seite Instances in der Amazon EC2-Konsole wechselt der Instance-Zustand von `Running` zu `Stopping` und zu `Stopped`. Jetzt kann ein AMI aus dieser Instance erstellt werden.

Aktualisieren von Metadaten/KMS-Routen für Server 2016 und höher beim Starten eines benutzerdefinierten AMI

So aktualisieren Sie Metadaten/KMS-Routen für Server 2016 und höher beim Starten eines benutzerdefinierten AMI:

- Führen Sie die LaunchSettings EC2-GUI aus (C:\\ AmazonProgramData\ EC2-Windows\ Launch \ Settings\ Ec2 LaunchSettings .exe) und wählen Sie die Option zum Herunterfahren mit Sysprep aus.
- Führen Sie EC2 aus LaunchSettings und fahren Sie es ohne Sysprep herunter, bevor Sie das AMI erstellen. Dadurch wird veranlasst, dass die Initialisierungsaufgaben des EC2-Starts beim nächsten Systemstart ausgeführt werden. Die Routen werden dann basierend auf dem Subnetz für die Instance festgelegt.

- Planen Sie die Initialisierungsaufgaben von EC2 Launch manuell neu, bevor Sie ein AMI von erstellen. PowerShell

> **Important**
>
> Beachten Sie das Standardverhalten beim Zurücksetzen des Passworts, bevor Sie Aufgaben neu planen.

- Informationen zum Aktualisieren der Routen auf einer ausgeführten Instance, bei der eine Windows-Aktivierung oder Kommunikation mit Instance-Metadatenfehlern auftritt, finden Sie unter „Windows kann nicht aktiviert werden“.

Verwenden von Sysprep mit EC2config

Dieser Abschnitt enthält Details über die unterschiedlichen Sysprep-Ausführungsphasen und die Aufgaben des EC2Config-Service beim Vorbereiten des Image kennen. Er enthält auch die Schritte zum Erstellen eines standardisierten AMI mit Sysprep mit dem EC2Config-Service.

Sysprep mit EC2Config-Themen

- Sysprep-Phasen
- Sysprep-Aktionen
- Nach Sysprep
- Ausführen von Sysprep mit dem EC2Config-Service

Sysprep-Phasen

Folgende Phasen werden beim Ausführen von Sysprep durchlaufen:

- Generalisieren: Das Tool entfernt Image-spezifische Informationen und Konfigurationen. Zum Beispiel entfernt Sysprep u. a. die Sicherheits-ID (SID), den Computer-Namen, die Ereignisprotokolle und bestimmte Treiber. Anschließend kann vom Betriebssystem (OS) ein AMI erstellt werden.

> **Note**
>
> Wenn Sie Sysprep mit dem Dienst EC2Config ausführen, verhindert das System, dass Treiber entfernt werden, da die PersistAllDeviceInstalls Einstellung standardmäßig auf true gesetzt ist.

- Spezialisieren: Plug & Play durchsucht den Computer und installiert Treiber für alle erkannten Geräte. Das Tool erstellt OS-Anforderungen, z. B. Computer-Name und SID. Optional können Sie Befehle in dieser Phase ausführen.
- Out-of-Box Experience (OOBE): Das System führt ein verkürztes Windows Setup aus und fordert den Benutzer zur Eingabe von Informationen wie Systemsprache, Zeitzone und einer registrierten Organisation auf. Wenn Sie Sysprep mit EC2Config ausführen, automatisiert die Antwortdatei diese Phase.

Sysprep-Aktionen

Sysprep und der EC2Config-Service führen folgende Aktionen beim Vorbereiten eines Images aus.

1. Wenn Sie im Dialogfeld EC2-Serviceeigenschaften die Option Mit Sysprep herunterfahren auswählen, führt das System den Befehl ec2config.exe -sysprep aus.
2. Der EC2Config-Service liest den Inhalt der Datei `BundleConfig.xml` ein. Diese Datei befindet sich standardmäßig im folgenden Verzeichnis: `C:\Program Files\Amazon\Ec2ConfigService\Settings`.

   Die `BundleConfig.xml`-Datei umfasst die folgenden Einstellungen. Sie können diese Einstellungen ändern:

   - AutoSysprep: Gibt an, ob Sysprep automatisch verwendet werden soll. Sie brauchen diesen Wert nicht zu ändern, wenn Sie Sysprep vom Dialogfeld „EC2 Service Properties“ aus ausführen. Der Standardwert ist `No`.
   - SetRDPCertificate: Legt ein selbstsigniertes Zertifikat für den Remote-Desktop-Server fest. Auf diese Weise können Sie das Remote Desktop Protocol (RDP) sicher verwenden, um eine Verbindung zur Instance herzustellen. Ändern Sie den Wert in `Yes`, wenn neue Instances ein Zertifikat verwenden sollen. Diese Einstellung wird bei Windows Server 2012-Instanzen nicht verwendet, da diese Betriebssysteme ihre eigenen Zertifikate generieren können. Der Standardwert ist `No`.

- SetPasswordAfterSysprep: Legt ein zufälliges Passwort für eine neu gestartete Instanz fest, verschlüsselt es mit dem Benutzerstartschlüssel und gibt das verschlüsselte Passwort an die Konsole aus. Ändern Sie den Wert in `No`, wenn die neuen Instances nicht als zufällig verschlüsseltes Passwort festgelegt werden sollen. Der Standardwert ist `Yes`.
- PreSysprepRunCmd: Der Speicherort des auszuführenden Befehls. Der Befehl befindet sich standardmäßig in folgendem Verzeichnis: `C:\Program Files\Amazon\Ec2ConfigService\Scripts\BeforeSysprep.cmd`

3. Das System führt au `BeforeSysprep.cmd`. Dieser Befehl erstellt den folgenden Registrierungsschlüssel:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v
 fDenyTSConnections /t REG_DWORD /d 1 /f
```

   Der Registrierungsschlüssel deaktiviert RDP-Verbindungen bis sie erneut aktiviert werden. Die Deaktivierung von RDP-Verbindungen ist eine notwendige Sicherheitsmaßnahme, da während der ersten Boot-Session nach der Ausführung von Sysprep kurzzeitig Verbindungen von RDP zugelassen werden und noch kein Administratorkennwort vergeben ist.

4. Der EC2Config-Service ruft Sysprep mit dem folgenden Befehl auf:

```
sysprep.exe /unattend: "C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml" /
oobe /generalize /shutdown
```

Generalisierungsphase

- Das Tool entfernt Image-spezifische Informationen und Konfigurationen, z. B. Computer-Name und SID. Wenn die Instance Mitglied einer Domain ist, wird sie von der Domain entfernt. Die `sysprep2008.xml`-Antwortdatei enthält folgende Einstellungen, die sich auf diese Phase auswirken:
  - PersistAllDeviceInstalls: Diese Einstellung verhindert, dass Windows Setup Geräte entfernt und neu konfiguriert, wodurch der Image-Vorbereitungsprozess beschleunigt wird, da Amazon-AMIs bestimmte Treiber zur Ausführung benötigen und die erneute Erkennung dieser Treiber einige Zeit in Anspruch nehmen würde.
  - DoNotCleanUpNonPresentGeräte: Bei dieser Einstellung werden Plug & Play-Informationen für Geräte beibehalten, die derzeit nicht vorhanden sind.

- Sysprep beendet das Betriebssystem beim Erstellen des AMI. Das System startet entweder eine neue Instance oder die ursprüngliche Instance.

Spezialisierungsphase

Das System erstellt OS-spezifische Anforderungen, z. B. Computer-Name und eine SID. Das System führt zudem die folgenden Aktionen basierend auf Konfigurationen durch, die Sie in der sysprep2008.xml-Antwortdatei angeben.

- CopyProfile: Sysprep kann so konfiguriert werden, dass alle Benutzerprofile gelöscht werden, einschließlich des integrierten Administratorprofils. Die Einstellung behält das integrierte Administratorkonto bei, sodass alle an diesem Konto vorgenommenen Anpassungen auf das neue Image übertragen werden. Der Standardwert ist „True“.

  CopyProfileersetzt das Standardprofil durch das vorhandene lokale Administratorprofil. Alle Konten, die sich nach der Ausführung von Sysprep anmelden, erhalten bei der ersten Anmeldung eine Kopie dieses Profils und seiner Inhalte.

  Wenn es keine spezifischen Benutzerprofilanpassungen gibt, die Sie auf das neue Image übertragen möchten, legen Sie diese Einstellung auf „False“ fest. Sysprep entfernt alle Benutzerprofile. Dies spart Zeit und Festplattenspeicher.
- TimeZone: Die Zeitzone ist standardmäßig auf Coordinate Universal Time (UTC) eingestellt.
- Synchronous command with order 1: Das System führt den folgenden Befehl zur Aktivierung des Administratorkontos und Angabe der Passwortanforderungen aus.

  net user Administrator /ACTIVE:YES /LOGONPASSWORDCHG:NO /EXPIRES:NEVER / PASSWORDREQ:YES
- Synchronous command with order 2: Das System verschlüsselt das Administratorpasswort. Die Sicherheitsmaßnahme dient dazu, den Zugriff auf die Instance nach Abschluss von Sysprep zu verhindern, wenn die ec2setpassword-Einstellung nicht aktiviert wurde.

  C:\Program Dateien\ Amazon\ Ec2ConfigService\ ScramblePassword .exe“ -u Administrator
- Synchronous command with order 3: Das System führt den folgenden Befehl aus:

  C:\Program Dateien\ Amazon\ Ec2\ ScriptsConfigService\ SysprepSpecialize Phase.cmd

  Der Befehl fügt den folgenden Registrierungsschlüssel hinzu, der RDP erneut aktiviert:

reg füge „HKEY_LOCAL_MACHINE\ SYSTEM\ CurrentControl Set\ Control\ Terminal Server“ hinzu /v fDenytsConnections /t REG_DWORD /d 0 /f

OOBE-Phase

1. Das System gibt mit der EC2Config-Service-Antwortdatei die folgenden Konfigurationen an:
   - < >de-US</ > InputLocale InputLocale
   - < SystemLocale >de-US</ SystemLocale >
   - <UILanguage>en-US</UILanguage>
   - < UserLocale >de-US</ UserLocale >
   - <HideEULAPage>true</HideEULAPage>
   - < HideWireless SetupIn OOBE>Wahr</ HideWireless SetupIn OOBE>
   - < NetworkLocation >Andere</ NetworkLocation >
   - < PC>3</ PC> ProtectYour ProtectYour
   - < BluetoothTaskbar IconEnabled >falsch</ BluetoothTaskbar IconEnabled >
   - < TimeZone >UTC</ TimeZone >
   - < RegisteredOrganization >Amazon.com</ RegisteredOrganization >
   - < RegisteredOwner RegisteredOwner >Amazon</ >

   > **Note**
   >
   > Während der Generalisierungs- und Spezialisierungsphasen überwacht der EC2Config-Service den Status des Betriebssystems. Wenn EC2Config erkennt, dass sich das OS in einer Sysprep-Phase befindet, schreibt es die folgende Mitteilung in das Systemprotokoll: ConfigMonitorEC2-Status: 0 Windows wird konfiguriert. SysprepState=IMAGE_STATE_UNDEPLOYABLE

2. Nach Abschluss der OOBE-Phase führt das System `SetupComplete.cmd` von folgendem Standort aus: `C:\Windows\Setup\Scripts\SetupComplete.cmd`. In öffentlichen AMIs von Amazon vor April 2015 war die Datei leer und es wurden keine Befehle für das Image ausgeführt. In öffentlichen AMIs, die nach April 2015 datiert wurden, enthält die Datei den folgenden Wert: call "C:\Program Files\Amazon\Ec2ConfigService\Scripts\PostSysprep.cmd".
3. Das System führt `PostSysprep.cmd` aus, das die folgenden Vorgänge ausführt:

- Legt das Administratorpasswort so fest, dass es nicht ablaufen kann. Wenn das Passwort abläuft, können sich Administratoren anschließend möglicherweise nicht mehr anmelden.
- Legt den MSSQLServer-Computer-Namen (sofern installiert) fest, sodass der Name mit dem AMI synchronisiert wird.

Nach Sysprep

Nach dem Abschluss von Sysprep sendet der EC2Config-Service die folgende Mitteilung an die Konsolenausgabe:

```
Windows sysprep configuration complete.
   Message: Sysprep Start
   Message: Sysprep End
```

EC2Config führt anschließend die folgenden Aktionen aus:

1. Liest den Inhalt der config.xml-Datei aus und führt alle aktivierten Plugins aus.
2. Führt alle Plugins vom Typ „Before Windows is ready“ gleichzeitig aus.
   - Ec2 SetPassword
   - Ec2-Name SetComputer
   - Ec2 InitializeDrives
   - Ec2 EventLog
   - Ec2ConfigureRDP
   - Ec2OutputRDPCert
   - Ec2-Brief SetDrive
   - Ec2 WindowsActivate
   - Ec2 DynamicBoot VolumeSize
3. Sendet nach Abschluss die Meldung „Windows is ready“ an die Instance-Systemprotokolle.
4. Führt alle Plugins vom Typ „After Windows is ready“ gleichzeitig aus.
   - CloudWatch Amazon-Protokolle
   - UserData
   - AWS Systems Manager (Systems Manager)

Weitere Informationen über Windows-Plug-ins finden Sie unter Konfigurieren Sie eine Windows-Instanz mithilfe des EC2Config-Dienstes (Legacy).

Ausführen von Sysprep mit dem EC2Config-Service

Mit dem folgenden Verfahren erstellen Sie ein standardisiertes AMI mit Sysprep und dem EC2Config-Service.

1. Suchen Sie in der Amazon EC2-Konsole das zu duplizierende AMI oder erstellen Sie eines.
2. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
3. Passen Sie sie an.
4. Geben Sie Konfigurationseinstellungen in der EC2Config-Service-Antwortdatei an:

   ```
   C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml
   ```
5. Wählen Sie im Windows-Startmenü Alle Programme und anschließend ConfigServiceEC2-Einstellungen aus.
6. Wählen Sie die Registerkarte Image (Image) im Dialogfeld Ec2 Service Properties (Ec2-Service-Eigenschaften) aus. Weitere Informationen zu den Optionen und Einstellungen im Ec2 Service Properties-Dialogfeld finden Sie unter Ec2-Service-Eigenschaften.
7. Wählen Sie eine Option für das Administratorpasswort aus und wählen Sie anschließend Shutdown with Sysprep (Herunterfahren mit Sysrep) oder Shutdown without Sysprep (Herunterfahren ohne Sysprep). EC2Config bearbeitet die Einstellungsdateien basierend auf der ausgewählten Passwortoption.
   - Random (Zufällig): EC2Config erstellt ein Passwort, verschlüsselt es mit dem Benutzerschlüssel und gibt das verschlüsselte Passwort an die Konsole aus. Die Einstellung wird nach dem ersten Start deaktiviert, sodass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.
   - Specify (Angeben): Das Passwort wird unverschlüsselt (Klartext) in der Sysprep-Antwortdatei gespeichert. Bei der nächsten Ausführung von Sysprep wird das Administratorpasswort festgelegt. Wenn Sie den Service gleich beenden, wird das Passwort sofort festgelegt. Sobald der Service erneut startet, wird das Administratorpasswort entfernt. Bewahren Sie das Passwort unbedingt gut auf, da Sie es später nicht erneut abrufen können.
   - Keep Existing (Vorhandenes beibehalten): Das bestehende Passwort für das Administratorkonto ändert sich nicht, wenn Sysprep ausgeführt oder EC2Config neu gestartet wird. Bewahren Sie das Passwort unbedingt gut auf, da Sie es später nicht erneut abrufen können.
8. Klicken Sie auf OK.

Wenn Sie zum Bestätigen der Ausführung von Sysprep und zum Beenden der Instance aufgefordert werden, klicken Sie auf Yes (Ja). EC2Config führt Sysprep aus. Anschließend werden Sie von der Instance abgemeldet und die Instance wird beendet. Auf der Seite Instances in der Amazon EC2-Konsole wechselt der Instance-Zustand von `Running` zu `Stopping` und abschließend zu `Stopped`. Jetzt kann ein AMI aus dieser Instance erstellt werden.

Sie können das Sysprep-Tool manuell mittels Befehlszeile und dem folgenden Befehl aufrufen:

```
"%programfiles%\amazon\ec2configservice\"ec2config.exe -sysprep""
```

> **Note**
>
> Die doppelten Anführungszeichen im Befehl sind nicht erforderlich, wenn sich Ihre CMD-Shell bereits im Verzeichnis C:\Program Files\ Amazon\ EC2ConfigService\ befindet.

Achten Sie aber sorgfältig auf die Angabe der richtigen XML-Dateioptionen im Ordner `Ec2ConfigService\Settings`, andernfalls kann möglicherweise keine Verbindung zur Instance hergestellt werden. Weitere Informationen zu diesen Einstellungsdateien finden Sie unter EC2Config-Einstellungsdateien. Ein Beispiel für die Konfiguration und das anschließende Ausführen von Sysprep über die Befehlszeile finden Sie unter `Ec2ConfigService\Scripts\InstallUpdates.ps1`.

Ändern eines -AMIs

Sie können eine begrenzte Anzahl von Amazon Machine Image (AMI) Attributen ändern, z. B. die Beschreibung und die Sharing-Eigenschaften des AMI. Der AMI-Inhalt (Volumen-Binärdaten) kann jedoch nicht geändert werden. Um den AMI-Inhalt zu ändern, müssen Sie ein neues AMI erstellen.

> **Important**
>
> Sie können den Inhalt (Volumen-Binärdaten) eines EBS-gestützten AMI nicht ändern, da die Snapshots, auf denen sie basieren, unveränderlich sind. Sie können auch den Inhalt (Volume-Binärdaten) eines Linux-AMIs mit Instance-Speicher (S3-unterstützt) nicht ändern, da der Inhalt signiert ist und Instance-Starts fehlschlagen, wenn die Signaturen nicht übereinstimmen.

Informationen zu den AMI-Attributen, die geändert werden können, finden Sie unter ModifyImageAttribute in der Amazon EC2 API-Referenz.

Die folgenden Themen enthalten Anweisungen zur Verwendung der Amazon EC2 EC2-Konsole und AWS CLI zum Ändern der Attribute eines AMI:

- Veröffentlichen eines AMI
- Freigeben eines AMI für bestimmte Organisationen oder Organisationseinheiten
- Freigeben eines AMI für bestimmte AWS -Konten
- Verwenden von gebührenpflichtigem Support
- Konfigurieren des AMI

Kopieren eines AMI

Sie können ein Amazon Machine Image (AMI) innerhalb oder zwischen AWS Regionen kopieren. Sie können sowohl Amazon EBS-gestützte AMIs als auch Instance-Store-gestützte AMIs kopieren. Sie können EBS-gestützte AMIs mit verschlüsselten Snapshots kopieren und auch den Verschlüsselungsstatus während des Kopiervorgangs ändern. Sie können AMIs kopieren, die für Sie freigegeben wurden.

Das Kopieren eines Quell-AMI führt zu einem identischen, aber unterschiedlichen neuen AMI, das wir auch als Ziel-AMI bezeichnen. Das Ziel-AMI hat seine eigene eindeutige AMI-ID. Sie können das Quell-AMI ändern oder die Registrierung aufheben. Dies hat keine Auswirkungen auf das Ziel-AMI. Umgekehrt gilt dies auch.

Bei einem EBS-gestützten AMI wird jeder seiner Backing-Snapshots in einen identischen, aber unterschiedlichen Ziel-Snapshot kopiert. Wenn Sie eine AMI in eine neue Region kopieren, sind die Snapshots vollständige (nicht inkrementelle) Kopien. Wenn Sie unverschlüsselte Backing-Snapshots verschlüsseln oder in einen neuen KMS-Schlüssel verschlüsseln, sind die Snapshots vollständige (nicht inkrementelle) Kopien. Nachfolgende Kopiervorgänge eines AMI-Ergebnisses in inkrementellen Kopien der Backing-Snapshots.

Inhalt

- Kontoübergreifendes Kopieren
- Verschlüsselung und Kopieren

Überlegungen

- Berechtigung zum Kopieren von AMIs — Mithilfe von IAM-Richtlinien können Sie Benutzern die Berechtigung zum Kopieren von AMIs gewähren oder verweigern. Die für die `CopyImage`-Aktion angegebenen Berechtigungen auf Ressourcenebene gelten nur für das neue AMI. Sie können keine Berechtigungen auf Ressourcenebene für das Quell-AMI angeben.
- Startberechtigungen und Amazon S3 S3-Bucket-Berechtigungen — kopiert AWS keine Startberechtigungen oder Amazon S3 S3-Bucket-Berechtigungen vom Quell-AMI in das neue AMI. Nachdem der Kopiervorgang abgeschlossen ist, können Sie Startberechtigungen und Amazon-S3-Bucketberechtigungen auf das neue AMI anwenden.
- Tags — Sie können nur benutzerdefinierte AMI-Tags kopieren, die Sie an das Quell-AMI angehängt haben. System-Tags (Präfix mit `aws:`) und benutzerdefinierte Tags, die von anderen AWS-Konten angehängt wurden, werden nicht kopiert. Beim Kopieren eines AMI können Sie neue Tags an das Ziel-AMI und die zugehörigen Snapshots anhängen.

Kosten

Für das Kopieren eines AMI fallen keine zusätzlichen Gebühren an. Es fallen allerdings die Standardgebühren für Datenspeicherung und -übertragung an. Wenn Sie ein EBS-gestütztes AMI kopieren, fallen Gebühren für die Speicherung zusätzlicher EBS-Snapshots an.

IAM-Berechtigungen

Um ein EBS-gestütztes oder instance store-backed AMI zu kopieren, benötigen Sie die folgenden IAM-Berechtigungen:

- `ec2:CopyImage`— Um das AMI zu kopieren. Für EBS-gestützte AMIs wird damit auch die Erlaubnis erteilt, die Backing-Snapshots des AMI zu kopieren.
- `ec2:CreateTags`— Um das Ziel-AMI zu taggen. Für EBS-gestützte AMIs gewährt es auch die Erlaubnis, die Backing-Snapshots des Ziel-AMIs zu taggen.

Wenn Sie ein auf einer Instanz gespeichertes AMI kopieren, benötigen Sie die folgenden zusätzlichen IAM-Berechtigungen:

- `s3:CreateBucket`— Um den S3-Bucket in der Zielregion für das neue AMI zu erstellen
- `s3:GetBucketAcl`— Um die ACL-Berechtigungen für den Quell-Bucket zu lesen
- `s3:ListAllMyBuckets`— Um einen vorhandenen S3-Bucket für AMIs in der Zielregion zu finden
- `s3:GetObject`— Um die Objekte im Quell-Bucket zu lesen
- `s3:PutObject`— Um die Objekte in den Ziel-Bucket zu schreiben
- `s3:PutObjectAcl`— Um die Berechtigungen für die neuen Objekte in den Ziel-Bucket zu schreiben

Beispiel für eine IAM-Richtlinie zum Kopieren eines EBS-gestützten AMI und zum Markieren des Ziel-AMI und der Snapshots

Die folgende Beispielrichtlinie gewährt Ihnen die Erlaubnis, jedes EBS-gestützte AMI zu kopieren und das Ziel-AMI und seine Backing-Snapshots zu taggen.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "PermissionToCopyAllImages",
        "Effect": "Allow",
        "Action": [
            "ec2:CopyImage",
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:*::image/*"
    }]
}
```

Beispiel für eine IAM-Richtlinie zum Kopieren eines EBS-gestützten AMI, ohne dass die neuen Snapshots markiert werden

Die `ec2:CopySnapshot` Genehmigung wird automatisch erteilt, wenn Sie die Genehmigung erhalten. `ec2:CopyImage` Dazu gehört die Erlaubnis, die neuen Backing-Snapshots des Ziel-AMI mit Tags zu versehen. Die Erlaubnis, die neuen Backing-Snapshots zu taggen, kann ausdrücklich verweigert werden.

Die folgende Beispielrichtlinie gewährt Ihnen die Erlaubnis, jedes EBS-gestützte AMI zu kopieren, verweigert Ihnen jedoch, die neuen Backing-Snapshots des Ziel-AMI zu taggen.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:::snapshot/*"
        }
    ]
}
```

Beispiel für eine IAM-Richtlinie zum Kopieren eines durch einen instance store-backed AMI und zum Taggen des Ziel-AMI

Die folgende Beispielrichtlinie gewährt Ihnen die Berechtigung, jedes durch einen instance store-backed AMI im angegebenen Quell-Bucket in die angegebene Region zu kopieren und das Ziel-AMI zu taggen.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "PermissionToCopyAllImages",
            "Effect": "Allow",
            "Action": [
                "ec2:CopyImage",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*::image/*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListAllMyBuckets",
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
```

```
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::ami-source-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:GetBucketAcl",
                "s3:PutObjectAcl",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amis-for-account-in-region-hash"
            ]
        }
    ]
}
```

Um den Amazon-Ressourcennamen (ARN) des AMI-Quell-Buckets zu finden, öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/, wählen im Navigationsbereich AMIs aus und suchen den Namen des Buckets in der Spalte Source (Quelle).

> **Note**
>
> Die `s3:CreateBucket` Genehmigung ist nur erforderlich, wenn Sie ein durch einen Instance-Speicher gestütztes AMI zum ersten Mal in eine einzelne Region kopieren. Danach wird der Amazon S3-Bucket, der bereits in der Region erstellt wurde, zum Speichern aller von Ihnen zukünftig in diese Region kopierten AMIs verwendet.

Kopieren eines AMI

Sie können ein AMI mithilfe der SDKs AWS Management Console, der AWS Command Line Interface SDKs oder der Amazon EC2 EC2-API kopieren, die alle die Aktion unterstützen. `CopyImage`

Console

Um ein AMI zu kopieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Konsolennavigationsleiste die Region mit dem AMI aus.
3. Wählen Sie im Navigationsbereich AMIs aus, um die Liste der AMIs anzuzeigen, die Ihnen in der Region zur Verfügung stehen.
4. Wenn Sie das AMI, das Sie kopieren möchten, nicht sehen, wählen Sie einen anderen Filter. Sie können nach AMIs, die mir gehören, privaten Bildern, öffentlichen Bildern und deaktivierten Bildern filtern.
5. Wählen Sie das zu kopierende AMI und anschließend Aktionen, AMI kopieren aus.
6. Geben Sie auf der Seite AMI kopieren die folgenden Informationen an:

   a. Name der AMI-Kopie: Der Name für das neue AMI. Sie können die Betriebssysteminformationen in den Namen aufnehmen, da Amazon EC2 diese Informationen bei der Anzeige von Details zum AMI nicht bereitstellt.

   b. Beschreibung der AMI-Kopie: Standardmäßig enthält die Beschreibung Informationen zum Quell-AMI zur Unterscheidung der Kopie vom Original. Sie können die Beschreibung bei Bedarf ändern.

   c. Zielregion: Die Region, in die das AMI kopiert werden soll. Weitere Informationen finden Sie unter Regionsübergreifendes Kopieren.

   d. Copy tags (Tags kopieren): Aktivieren Sie dieses Kontrollkästchen, um Ihre benutzerdefinierten AMI-Tags beim Kopieren des AMI einzubeziehen. System-Tags (Präfix mit `aws:`) und benutzerdefinierte Tags, die von anderen AWS-Konten angehängt wurden, werden nicht kopiert.

   e. (Nur EBS-gestützte AMIs) EBS-Snapshots der AMI-Kopie verschlüsseln: Aktivieren Sie dieses Kontrollkästchen, um die Ziel-Snapshots zu verschlüsseln oder um sie mit einem anderen Schlüssel erneut zu verschlüsseln. Wenn die Verschlüsselung standardmäßig aktiviert ist, ist das Kontrollkästchen EBS-Snapshots der AMI-Kopie verschlüsseln aktiviert und kann nicht deaktiviert werden. Weitere Informationen finden Sie unter Verschlüsselung und Kopieren.

   f. (Nur EBS-gestützte AMIs) KMS-Schlüssel: Der KMS-Schlüssel, der zum Verschlüsseln der Ziel-Snapshots verwendet werden soll.

g. Tags: Sie können das neue AMI und die neuen Snapshots mit denselben Tags oder mit unterschiedlichen Tags kennzeichnen.

   - Um das neue AMI und die neuen Snapshots mit denselben Tags zu taggen, wählen Sie Bild und Snapshots zusammen taggen. Dieselben Tags werden auf das neue AMI und jeden Snapshot, der erstellt wird, angewendet.
   - Um das neue AMI und die neuen Snapshots mit unterschiedlichen Tags zu kennzeichnen, wählen Sie Bild und Snapshots separat taggen. Verschiedene Tags werden auf das neue AMI und die erstellten Snapshots angewendet. Beachten Sie jedoch, dass alle neu erstellten Snapshots dieselben Tags erhalten. Sie können nicht jeden neuen Snapshot mit einem anderen Tag kennzeichnen.

   Sie fügen ein Tag (Markierung) hinzu, indem Sie Add Tags (Tag (Markierung) hinzufügen) auswählen und den Schlüssel und den Wert für das Tags (Markierungen) eingeben. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

h. Wenn Sie bereit sind, das AMI zu kopieren, wählen Sie Copy AMI.

   Der ursprüngliche Status des neuen AMI ist `Pending`. Der AMI-Kopiervorgang ist abgeschlossen, wenn der Status `Available` lautet.

AWS CLI

So kopieren Sie ein AMI mit dem AWS CLI

Kopieren Sie ein AMI mit dem copy-image-Befehl. Geben Sie die Quell- und Zielregionen an. Geben Sie die Quellregion mit dem `--source-region`-Parameter an. Geben Sie die Zielregion mit dem `--region`-Parameter oder einer Umgebungsvariablen an. Weitere Informationen finden Sie unter Konfiguration der AWS Befehlszeilenschnittstelle.

(Nur EBS-gestützte AMIs) Wenn Sie einen Ziel-Snapshot beim Kopieren verschlüsseln, müssen Sie die folgenden zusätzlichen Parameter angeben: und. `--encrypted` `--kms-key-id`

Beispielbefehle finden Sie unter den Beispielen in copy-image in der AWS CLI -Befehlsreferenz.

PowerShell

So kopieren Sie ein AMI mit den Tools für Windows PowerShell

Sie können ein AMI mit dem Copy-EC2ImageBefehl kopieren. Geben Sie die Quell- und Zielregionen an. Geben Sie die Quellregion mit dem `-SourceRegion`-Parameter an. Geben Sie die Zielregion mit dem `-Region`-Parameter oder dem `Set-AWSDefaultRegion`-Befehl an. Weitere Informationen finden Sie unter AWS Regionen angeben.

(Nur EBS-gestützte AMIs) Wenn Sie einen Ziel-Snapshot beim Kopieren verschlüsseln, müssen Sie die folgenden zusätzlichen Parameter angeben: und. `-Encrypted -KmsKeyId`

Anhalten eines ausstehenden AMI-Kopiervorgangs

Sie können eine ausstehende AMI-Kopie mit der AWS Management Console oder der Befehlszeile beenden.

Console

Anhalten eines AMI-Kopiervorgangs mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der oberen Navigationsleiste die Zielregion aus der Regionsauswahl aus.
3. Wählen Sie im Navigationsbereich die Option AMIs.
4. Wählen Sie das AMI aus, das Kopieren beendet werden soll, und klicken Sie dann auf Aktionen, AMI deregister.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie AMI abmelden aus.

Command line

Anhalten eines AMI-Kopiervorgangs mittels Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

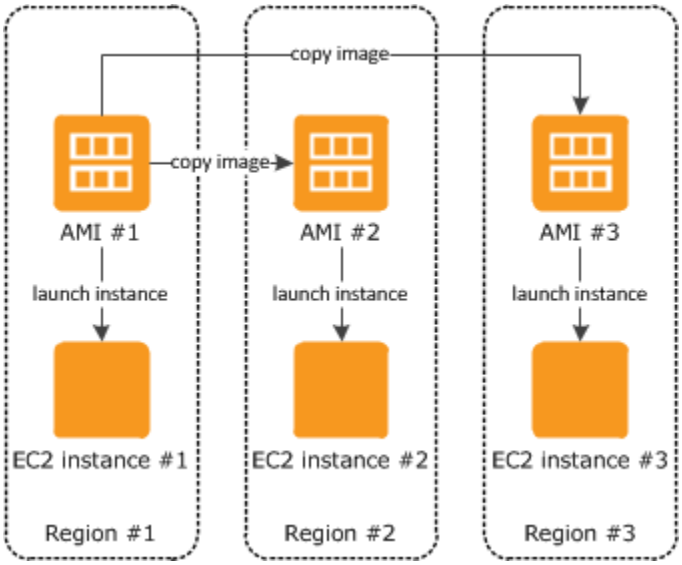
- deregister-image (AWS CLI)
- Unregister-EC2Image (AWS Tools for Windows PowerShell)

Regionsübergreifendes Kopieren

Das Kopieren eines AMI zwischen geografisch unterschiedlichen Regionen bietet folgende Vorteile:

- Einheitliche globale Bereitstellung: Kopieren Sie ein AMI aus einer Region in eine andere, um einheitliche, auf dem gleichen AMI basierende Instances in verschiedenen Regionen zu starten.
- Skalierbarkeit: Entwerfen Sie Anwendungen für den globalen Einsatz, die die Anforderungen Ihrer Benutzer erfüllen, unabhängig davon, wo sie sich befinden.
- Performance: Steigern Sie die Leistung von Anwendungen, indem Sie sie verteilen und kritische Komponenten näher an die Benutzer rücken. Sie können auch regionsspezifische Funktionen wie Instance-Typen oder andere Dienste nutzen. AWS
- Hohe Verfügbarkeit: Sie können Anwendungen entwerfen und zwischen AWS -Regionen übergreifend bereitstellen, um die Verfügbarkeit zu erhöhen.

Das folgende Diagramm zeigt die Beziehung zwischen einem Quell-AMI und zwei kopierten AMIs in verschiedenen Regionen sowie die EC2-Instances, die von jeder Region aus gestartet wurden. Beim Starten einer Instance von einem AMI verbleibt sie in derselben Region, in der sich auch das AMI befindet. Wenn Sie das Quell-AMI verändern und die Änderungen für die AMIs in den Zielregionen übernehmen möchten, kopieren Sie das Quell-AMI in die Zielregionen.



Wenn Sie zuerst ein Instance Store-Backed AMI in eine Region kopieren, erstellen wir einen Amazon S3-Bucket für die in diese Region kopierten AMIs. Alle Instance Store-Backed AMIs, die Sie in diese Region kopieren, werden in diesem Bucket gespeichert. Die Bucket-Namen haben das folgende Format: amis-for-*account*-in-*region*-*hash*. Zum Beispiel: `amis-for-123456789012-in-us-east-2-yhjmxvp6`.

Voraussetzung

Aktualisieren Sie vor dem Kopieren eines AMI die Inhalte des Quell-AMI, damit die Ausführung in einer anderen Region unterstützt wird. Aktualisieren Sie z. B. Datenbankverbindungs-Zeichenfolgen oder ähnliche Anwendungskonfigurationsdaten, sodass sie auf die entsprechenden Ressourcen verweisen. Andernfalls könnten Instances, die über das neue AMI in der Zielregion gestartet werden, weiterhin die Ressourcen aus der Quellregion verwenden, was sich auf Leistung und Kosten auswirken kann.

Einschränkungen

- Die Zielregionen sind auf 100 gleichzeitige AMI-Kopien beschränkt.
- Sie können ein paravirtuelles (PV) AMI nicht in eine Region kopieren, die PV-AMIs nicht unterstützt. Weitere Informationen finden Sie unter AMI-Virtualisierungstypen.

Kontoübergreifendes Kopieren

Sie können ein AMI mit einem anderen AWS Konto teilen. Das Teilen eines AMI wirkt sich nicht auf die Eigentumsrechte des AMI aus. Die Kosten für den Speicher in der Region werden dem Eigentümerkonto angerechnet. Weitere Informationen finden Sie unter Freigeben eines AMI für bestimmte AWS -Konten.

Wenn Sie ein AMI kopieren, das mit Ihrem Konto geteilt wird, sind Sie der Eigentümer des Ziel-AMI in Ihrem Konto. Dem Eigentümer des Quell-AMI werden die standardmäßigen Amazon EBS- bzw. Amazon S3-Übertragungsgebühren in Rechnung gestellt. Die Gebühren für den Speicher des Ziel-AMI in der Zielregion werden Ihnen in Rechnung gestellt.

Ressourcenberechtigungen

Um ein AMI zu kopieren, das mit Ihnen von einem anderen Konto geteilt wurde, muss Ihnen der Besitzer des Quell-AMI Leseberechtigungen für den Speicher zuweisen, der das AMI sichert. Der Speicher ist entweder der zugehörige EBS-Snapshot (für ein Amazon-EBS-gestütztes AMI) oder einen zugehörigen S3-Bucket (für ein Instance-Speicher-gestütztes AMI). Wenn das gemeinsame AMI über verschlüsselte Snapshots verfügt, muss der Besitzer den bzw. die Schlüssel auch für Sie freigeben. Weitere Informationen zur Gewährung von Ressourcenberechtigungen für EBS-Snapshots finden Sie unter Freigeben eines Amazon EBS-Snapshots im Amazon EBS-Benutzerhandbuch und für S3-Buckets unter Identitäts- und Zugriffsmanagement in Amazon S3 im Amazon Simple Storage Service-Benutzerhandbuch.

> **Note**
>
> Um ein AMI mit seinen Tags zu kopieren, benötigen Sie Startberechtigungen für das Quell-AMI.

Verschlüsselung und Kopieren

In der folgenden Tabelle ist der Verschlüsselungssupport für diverse AMI-Kopierszenarien abgebildet. Sie können zwar einen nicht verschlüsselten Snapshot zur Erstellung eines verschlüsselten Snapshots erstellen, umgekehrt ist dies jedoch nicht möglich.

Szenario	Beschreibung	Unterstützt
1	Nicht verschlüsselt zu nicht verschlüsselt	Ja
2	Verschlüsselt zu verschlüsselt	Ja
3	Nicht verschlüsselt zu verschlüsselt	Ja
4	Verschlüsselt zu nicht verschlüsselt	Nein

> **Note**
>
> Die Verschlüsselung während der `CopyImage`-Aktion gilt ausschließlich für Amazon EBS-gestützte AMIs. Da ein Instance Store-Backed AMI keine Snapshots erfordert, können Sie mithilfe des Kopiervorgangs den Verschlüsselungsstatus nicht ändern.

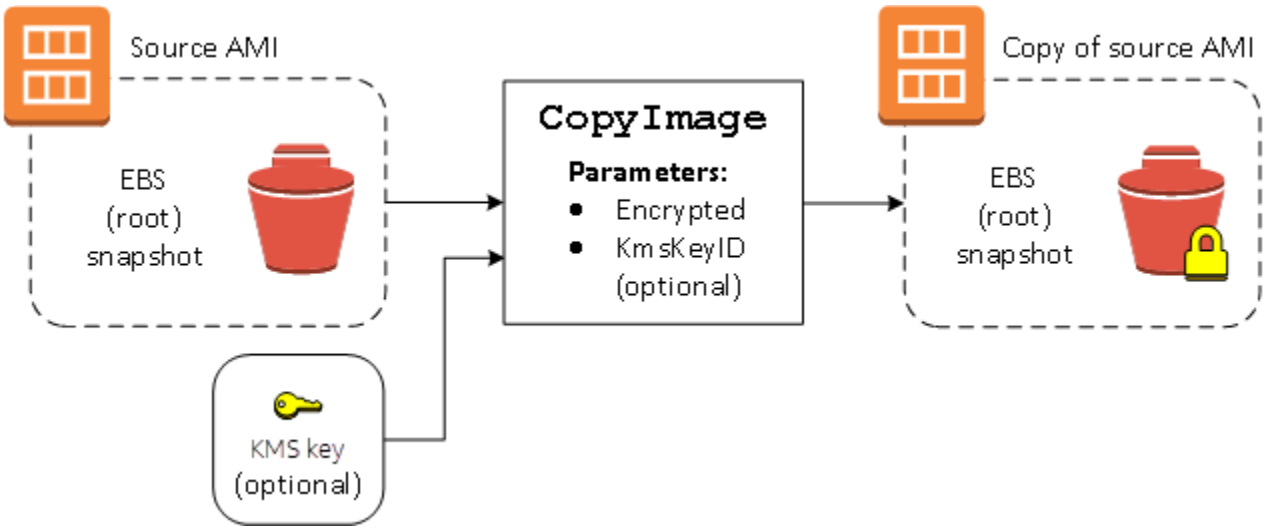
Standardmäßig (d. h. ohne die Verschlüsselungsparameter anzugeben) wird der Backing-Snapshot eines AMI mit dem ursprünglichen Verschlüsselungsstatus kopiert. Beim Kopieren eines AMI, das durch einen nicht verschlüsselten Snapshot gesichert ist, wird ein identischer Ziel-Snapshot erstellt, der ebenfalls nicht verschlüsselt ist. Wenn das Quell-AMI von einem verschlüsselten Snapshot unterstützt wird, führt das Kopieren zu einem identischen Ziel-Snapshot, der mit demselben AWS KMS Schlüssel verschlüsselt ist. Durch das Kopieren eines AMI, das durch mehrere Snapshots gesichert ist, wird der Quell-Verschlüsselungsstatus standardmäßig in jedem Ziel-Snapshot bewahrt.

Wenn Sie beim Kopieren eines AMI Verschlüsselungsparameter angeben, können Sie seine Unterstützungs-Snapshots verschlüsseln oder erneut verschlüsseln. Das folgende Beispiel zeigt einen nicht standardmäßigen Fall, in dem der `CopyImage`-Aktion Verschlüsselungsparameter bereitgestellt werden, um den Verschlüsselungsstatus des Ziel-AMIs zu ändern.

Kopieren eines nicht verschlüsselten Quell-AMI zu einem verschlüsselten Ziel-AMI

In diesem Szenario wird ein von einem unverschlüsselten Stamm-Snapshot unterstütztes AMI in ein AMI mit einem verschlüsselten Stamm-Snapshot kopiert. Die Aktion `CopyImage` wird mit zwei Verschlüsselungsparametern aufgerufen, einschließlich eines vom Kunden verwalteten Schlüssels. Dadurch ändert sich der Verschlüsselungsstatus des Stamm-Snapshots, sodass das Ziel-AMI durch einen Stamm-Snapshot gestützt wird, der dieselben Daten wie der Quell-Snapshot enthält, aber mit dem angegebenen Schlüssel verschlüsselt wird. Für Sie fallen Speicherkosten für die Snapshots in beiden AMIs sowie Gebühren für Instances an, die Sie von einem der AMIs starten.

> **Note**
>
> Die standardmäßige Aktivierung der Verschlüsselung hat dieselbe Wirkung wie das Setzen des `Encrypted` Parameters auf `true` für alle Snapshots im AMI.



Wenn der `Encrypted`-Parameter festgelegt wird, wird der einzige Snapshot für diese Instance verschlüsselt. Wenn Sie den `KmsKeyId`-Parameter nicht angeben, wird der standardmäßige vom Kunden verwaltete Schlüssel zum Verschlüsseln der Snapshot-Kopie verwendet.

Weitere Informationen zum Kopieren von AMIs mit verschlüsselten Snapshots finden Sie unter Verwenden der Verschlüsselung mit EBS-gestützten AMIs.

Speichern und Wiederherstellen eines AMI mit S3

Sie können ein Amazon Machine Image (AMI) in einem Amazon S3-Bucket speichern, das AMI in einen anderen S3-Bucket kopieren und dann aus dem S3-Bucket wiederherstellen. Durch Speichern und Wiederherstellen eines AMI mithilfe von S3-Buckets können Sie AMIs von einer AWS Partition auf eine andere kopieren, z. B. von der kommerziellen Hauptpartition auf die AWS GovCloud (US) Partition. Sie können auch Archivkopien von AMIs erstellen, indem Sie sie in einem S3-Bucket speichern.

Die unterstützten APIs zum Speichern und Wiederherstellen eines AMI mit S3 sind `CreateStoreImageTask`, `DescribeStoreImageTasks` und `CreateRestoreImageTask`.

`CopyImage`ist die empfohlene API für das Kopieren von AMIs innerhalb einer AWS Partition. `CopyImage` kann jedoch kein AMI in eine andere Partition kopieren.

Informationen zu den AWS Partitionen finden Sie unter *`Partition`* auf der Seite Amazon Resource Names (ARNs) im IAM-Benutzerhandbuch.

> **Warning**
>
> Stellen Sie sicher, dass Sie beim Verschieben von Daten zwischen AWS Partitionen oder AWS Regionen alle geltenden Gesetze und Geschäftsanforderungen einhalten, einschließlich, aber nicht beschränkt auf, alle geltenden behördlichen Vorschriften und Anforderungen an die Datenresidenz.

Themen

Anwendungsfälle

Verwenden Sie die Speicher- und Wiederherstellungs-APIs, um Folgendes zu tun:

- Kopieren Sie ein AMI von einer AWS Partition auf eine andere AWS Partition
- Erstellen von Archivkopien von AMIs

Kopieren Sie ein AMI von einer AWS Partition auf eine andere AWS Partition

Durch Speichern und Wiederherstellen eines AMI mithilfe von S3-Buckets können Sie ein AMI von einer AWS Partition auf eine andere oder von einer AWS Region in eine andere kopieren. Im folgenden Beispiel kopieren Sie ein AMI von der kommerziellen Hauptpartition auf die AWS GovCloud (US) Partition, insbesondere von der `us-east-2` Region in die `us-gov-east-1` Region.

Um ein AMI von einer Partition auf eine andere zu kopieren, führen Sie die folgenden Schritte aus:

- Speichern Sie das AMI in einem S3-Bucket in der aktuellen Region mithilfe von `CreateStoreImageTask`. In diesem Beispiel befindet sich der S3-Bucket in `us-east-2`. Ein Beispielbefehl finden Sie unter Speichern eines AMI in einem S3-Bucket.
- Überwachen Sie den Fortschritt der Speicheraufgabe mithilfe von `DescribeStoreImageTasks`. Das Objekt wird im S3-Bucket sichtbar, wenn die Aufgabe abgeschlossen ist. Ein Beispielbefehl finden Sie unter Beschreiben des Fortschritts einer AMI-Speicheraufgabe.
- Kopieren Sie das gespeicherte AMI-Objekt mit einer Prozedur Ihrer Wahl in einen S3-Bucket in der Zielpartition. In diesem Beispiel befindet sich der S3-Bucket in `us-gov-east-1`.

> **Note**
>
> Da Sie für jede Partition unterschiedliche AWS Anmeldeinformationen benötigen, können Sie ein S3-Objekt nicht direkt von einer Partition auf eine andere kopieren. Der Prozess zum Kopieren eines S3-Objekts über Partitionen hinweg liegt außerhalb des Rahmens dieser Dokumentation. Wir stellen die folgenden Kopierprozesse als Beispiele zur Verfügung, aber Sie müssen den Kopierprozess verwenden, der Ihren Sicherheitsanforderungen entspricht.
>
> - Um ein AMI über Partitionen hinweg zu kopieren, kann ein einfacher Kopiervorgang wie der Folgende ausreichen: Erst das Objekt herunterladen (aus dem Quell-Bucket auf einen Zwischen-Host, z. B. eine EC2-Instance oder einen Laptop) und danach das Objekt hochladen (vom Zwischen-Host in den Ziel-Bucket). Verwenden Sie für jede Phase des Prozesses die AWS Anmeldeinformationen für die Partition.

- Für eine nachhaltigere Nutzung sollten Sie erwägen, eine Anwendung zu entwickeln, die die Kopien verwaltet, möglicherweise mithilfe von mehrteiligen S3-Downloads und -Uploads.

- Stellen Sie das AMI aus dem S3-Bucket in der Zielpartition mithilfe von `CreateRestoreImageTask` wieder her. In diesem Beispiel befindet sich der S3-Bucket in `us-gov-east-1`. Ein Beispielbefehl finden Sie unter Wiederherstellen eines AMI aus einem S3-Bucket.
- Überwachen Sie den Fortschritt der Wiederherstellungsaufgabe, indem Sie das AMI beschreiben, um zu überprüfen, wann sein Status verfügbar wird. Sie können auch die Fortschrittsprozentsätze der Snapshots, aus denen das wiederhergestellte AMI besteht, überwachen, indem Sie die Snapshots beschreiben.

Erstellen von Archivkopien von AMIs

Sie können Archivkopien von AMIs erstellen, indem Sie sie in einem S3-Bucket speichern. Ein Beispielbefehl finden Sie unter Speichern eines AMI in einem S3-Bucket.

Das AMI wird in S3 in ein einzelnes Objekt gepackt, und alle AMI-Metadaten (ohne Freigabe-Informationen) bleiben als Teil des gespeicherten AMI erhalten. Die AMI-Daten werden im Rahmen des Speicherprozesses komprimiert. AMIs, die Daten enthalten, die leicht komprimiert werden können, führen zu kleineren Objekten in S3. Um die Kosten zu senken, können Sie günstigere S3-Speicherstufen verwenden. Weitere Informationen finden Sie unter Amazon-S3-Speicherklassen und Amazon-S3-Preisen

Funktionsweise der AMI-Speicher- und -Wiederherstellungs-APIs

Um ein AMI mit S3 zu speichern und wiederherzustellen, verwenden Sie die folgenden APIs:

- `CreateStoreImageTask` – Speichert das AMI in einem S3-Bucket
- `DescribeStoreImageTasks` – Liefert den Fortschritt der AMI-Speicheraufgabe
- `CreateRestoreImageTask` – Stellt das AMI aus einem S3-Bucket wieder her

So funktionieren die APIs

- CreateStoreImageTask
- DescribeStoreImageTasks

- CreateRestoreImageTask

CreateStoreImageTask

Die CreateStoreImageTaskAPI speichert ein AMI als einzelnes Objekt in einem S3-Bucket.

Die API erstellt eine Aufgabe, die alle Daten aus dem AMI und seinen Snapshots liest und dann einen mehrteiligen S3-Upload verwendet, um die Daten in einem S3-Objekt zu speichern. Die API nimmt alle Komponenten des AMI, einschließlich der meisten nicht regionsspezifischen AMI-Metadaten, und aller im AMI enthaltenen EBS-Snapshots und verpackt sie in einem einzigen Objekt in S3. Die Daten werden im Rahmen des Upload-Prozesses komprimiert, um den in S3 verwendeten Speicherplatz zu reduzieren, sodass das Objekt in S3 möglicherweise kleiner ist als die Summe der Größe der Snapshots im AMI.

Wenn für das Konto, das diese API aufruft, AMI- und Snapshot-Tags (Markierungen) sichtbar sind, bleiben diese erhalten.

Das Objekt in S3 hat die gleiche ID wie das AMI, jedoch mit einer `.bin`-Erweiterung. Die folgenden Daten werden auch als S3-Metadaten-Tags (Markierungen) für das S3-Objekt gespeichert: AMI-Name, AMI-Beschreibung, AMI-Registrierungsdatum, AMI-Besitzerkonto und ein Zeitstempel für den Speichervorgang.

Die Zeit, die benötigt wird, um die Aufgabe abzuschließen, hängt von der Größe des AMI ab. Dies hängt auch davon ab, wie viele andere Aufgaben ausgeführt werden, da Aufgaben in die Warteschlange gestellt werden. Sie können den Fortschritt der Aufgabe verfolgen, indem Sie die DescribeStoreImageTasksAPI aufrufen.

Die Summe der Größen aller laufenden AMIs ist auf 600 GB EBS-Snapshot-Daten pro Konto begrenzt. Die weitere Aufgabenerstellung wird abgelehnt, bis die laufenden Aufgaben unter dem Grenzwert liegen. Wenn beispielsweise derzeit ein AMI mit 100 GB Snapshot-Daten und ein anderes AMI mit 200 GB Snapshot-Daten gespeichert wird, wird eine weitere Anforderung akzeptiert, da die laufende Gesamtzahl 300 GB beträgt, was unter dem Limit liegt. Wenn jedoch derzeit ein einzelnes AMI mit 800 GB Snapshot-Daten gespeichert wird, werden weitere Aufgaben abgelehnt, bis die Aufgabe abgeschlossen ist.

DescribeStoreImageTasks

Die DescribeStoreImageTasksAPI beschreibt den Fortschritt der AMI-Speicheraufgaben. Sie können Aufgaben für bestimmte AMIs beschreiben. Wenn Sie keine AMIs angeben, erhalten Sie eine paginierte Liste aller Speicher-Image-Aufgaben, die in den letzten 31 Tagen verarbeitet wurden.

Für jede AMI-Aufgabe gibt die Antwort an, ob die Aufgabe `InProgress`, `Completed` oder `Failed` ist. Bei Aufgaben `InProgress` zeigt die Antwort einen geschätzten Fortschritt in Prozent.

Aufgaben werden in umgekehrter chronologischer Reihenfolge aufgeführt.

Derzeit können nur Aufgaben des Vormonats eingesehen werden.

CreateRestoreImageTask

Die CreateRestoreImageTaskAPI startet eine Aufgabe, die ein AMI aus einem S3-Objekt wiederherstellt, das zuvor mithilfe einer CreateStoreImageTaskAnfrage erstellt wurde.

Die Wiederherstellungsaufgabe kann in derselben oder einer anderen Region ausgeführt werden, in der die Speicheraufgabe ausgeführt wurde.

Der S3-Bucket, aus dem das AMI-Objekt wiederhergestellt wird, muss sich in derselben Region befinden, in der die Wiederherstellungsaufgabe angefordert wird. Das AMI wird in dieser Region wiederhergestellt.

Das AMI wird mit seinen Metadaten wie dem Namen, der Beschreibung und den Blockgeräte-Zuweisungen wiederhergestellt, die den Werten des gespeicherten AMI entsprechen. Der Name muss für AMIs in der Region für dieses Konto eindeutig sein. Wenn Sie keinen Namen angeben, erhält das neue AMI den gleichen Namen wie das ursprüngliche AMI. Das AMI erhält eine neue AMI-ID, die zum Zeitpunkt des Wiederherstellungsprozesses generiert wird.

Die Zeit, die zum Abschließen der AMI-Wiederherstellungsaufgabe benötigt wird, hängt von der Größe des AMI ab. Dies hängt auch davon ab, wie viele andere Aufgaben ausgeführt werden, da Aufgaben in die Warteschlange gestellt werden. Sie können den Fortschritt der Aufgabe anzeigen, indem Sie das AMI (describe-images) oder seine EBS-Snapshots (describe-snapshots) beschreiben. Wenn die Aufgabe fehlschlägt, werden das AMI und die Snapshots in einen fehlgeschlagenen Zustand verschoben.

Die Summe der Größen aller laufenden AMIs ist auf 300 GB (basierend auf der Größe nach der Wiederherstellung) von EBS-Snapshot-Daten pro Konto begrenzt. Die weitere Aufgabenerstellung wird abgelehnt, bis die laufenden Aufgaben unter dem Grenzwert liegen.

Einschränkungen

- Um ein AMI zu speichern, AWS-Konto müssen Sie entweder Eigentümer des AMI und seiner Snapshots sein, oder das AMI und seine Snapshots müssen direkt mit Ihrem Konto geteilt werden. Sie können ein AMI nicht speichern, wenn es nur öffentlich freigegeben ist.

- Nur mit EBS unterstützte AMIs können mit diesen APIs gespeichert werden.
- Paravirtual(PV)-AMIs werden nicht unterstützt.
- Die Größe eines AMI (vor der Komprimierung), das gespeichert werden kann, ist auf 5 000 GB beschränkt.
- Kontingent für store image-Anforderungen: 600 GB Speicherarbeit (Snapshot-Daten) in Bearbeitung.
- Kontingent für restore image-Anforderungen: 300 GB Wiederherstellungsarbeit (Snapshot-Daten) in Bearbeitung.
- Für die Dauer der Speicheraufgabe dürfen die Snapshots nicht gelöscht werden und der IAM-Prinzipal, der die Speicherung durchführt, muss Zugriff auf die Snapshots haben, andernfalls schlägt der Speicherprozess fehl.
- Sie können nicht mehrere Kopien eines AMI im selben S3-Bucket erstellen.
- Ein AMI, das in einem S3-Bucket gespeichert ist, kann mit seiner ursprünglichen AMI-ID nicht wiederhergestellt werden. Sie können dies abschwächen, indem Sie AMI-Aliasingverwenden.
- Derzeit werden die Speicher- und Wiederherstellungs-APIs nur mithilfe der AWS SDKs und der AWS Command Line Interface Amazon EC2 EC2-API unterstützt. Sie können ein AMI nicht mit der Amazon EC2-Konsole speichern und wiederherstellen.

Kosten

Wenn Sie AMIs mit S3 speichern und wiederherstellen, werden Ihnen die Dienste in Rechnung gestellt, die von den Speicher- und Wiederherstellungs-APIs verwendet werden, sowie für die Datenübertragung. Die APIs verwenden S3 und die EBS-Direct-API (die intern von diesen APIs verwendet wird, um auf die Snapshot-Daten zuzugreifen). Weitere Informationen finden Sie unter Amazon S3 – Preise und Amazon EBS – Preise.

Sichern Ihrer AMIs

Um die Speicher- und Wiederherstellungs-APIs zu verwenden, müssen sich das S3-Bucket und das AMI in derselben Region befinden. Es ist wichtig sicherzustellen, dass das S3-Bucket mit ausreichender Sicherheit konfiguriert ist, um den Inhalt des AMI zu sichern, und dass die Sicherheit so lange erhalten bleibt, wie die AMI-Objekte im Bucket verbleiben. Wenn dies nicht möglich ist, wird die Verwendung dieser APIs nicht empfohlen. Stellen Sie sicher, dass der öffentliche Zugriff auf den S3-Bucket nicht erlaubt ist. Wir empfehlen, dass Sie die serverseitige Verschlüsselung für den S3-Bucket aktivieren, in dem Sie die AMIs speichern, obwohl dies nicht erforderlich ist.

Informationen zum Festlegen der geeigneten Sicherheitseinstellungen für Ihre S3-Buckets finden Sie in den folgenden Sicherheitsthemen:

- Blockieren des öffentlichen Zugriffs auf Ihren Amazon S3-Speicher
- Einstellen des Verhaltens der serverseitigen Verschlüsselung für Amazon S3-Buckets
- Welche S3-Bucket-Richtlinie kann ich verwenden, um die AWS Config Regel s3-bucket-ssl-requests-only einzuhalten?
- Aktivieren der Amazon S3-Serverzugriffsprotokollierung

Wenn die AMI-Snapshots in das S3-Objekt kopiert werden, werden die Daten danach über TLS-Verbindungen kopiert. Sie können AMIs mit verschlüsselten Snapshots speichern, aber die Snapshots werden im Rahmen des Speicherprozesses entschlüsselt.

Berechtigungen zum Speichern und Wiederherstellen von AMIs mit S3

Wenn Ihre IAM-Prinzipale AMIs mithilfe von Amazon S3 speichern oder wiederherstellen, müssen Sie ihnen die erforderlichen Berechtigungen erteilen.

Die folgende Beispielrichtlinie enthält alle Aktionen, die erforderlich sind, um einem IAM-Prinzipal die Durchführung der Speicher- und Wiederherstellungsaufgaben zu ermöglichen.

Sie können auch IAM-Richtlinien erstellen, die Prinzipalen nur Zugriff auf bestimmte Ressourcen gewähren. Weitere Beispielrichtlinien finden Sie unter Zugriffsverwaltung für Ressourcen im IAM-Benutzerhandbuch. AWS

> **Note**
>
> Wenn die Snapshots, aus denen das AMI besteht, verschlüsselt sind oder Ihr Konto standardmäßig für Verschlüsselung aktiviert ist, muss Ihr IAM-Prinzipal über die Berechtigung verfügen, den KMS-Schlüssel zu verwenden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:DeleteObject",
```

```
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:PutObjectTagging",
                "s3:AbortMultipartUpload",
                "ebs:CompleteSnapshot",
                "ebs:GetSnapshotBlock",
                "ebs:ListChangedBlocks",
                "ebs:ListSnapshotBlocks",
                "ebs:PutSnapshotBlock",
                "ebs:StartSnapshot",
                "ec2:CreateStoreImageTask",
                "ec2:DescribeStoreImageTasks",
                "ec2:CreateRestoreImageTask",
                "ec2:GetEbsEncryptionByDefault",
                "ec2:DescribeTags",
                "ec2:CreateTags"
            ],
            "Resource": "*"
        }
    ]
}
```

Arbeiten mit den AMI-Speicher- und -Wiederherstellungs-APIs

Themen

- Speichern eines AMI in einem S3-Bucket
- Beschreiben des Fortschritts einer AMI-Speicheraufgabe
- Wiederherstellen eines AMI aus einem S3-Bucket

Speichern eines AMI in einem S3-Bucket

Speichern eines AMI (AWS CLI)

Verwenden Sie den Befehl create-store-image-task . Geben Sie die ID des AMI und den Namen des S3-Buckets an, in dem das AMI gespeichert werden soll.

```
aws ec2 create-store-image-task \
    --image-id ami-1234567890abcdef0 \
    --bucket myamibucket
```

Erwartete Ausgabe

```
{
  "ObjectKey": "ami-1234567890abcdef0.bin"
}
```

Beschreiben des Fortschritts einer AMI-Speicheraufgabe

Beschreiben des Fortschritts einer AMI-Speicheraufgabe (AWS CLI)

Verwenden Sie den Befehl describe-store-image-tasks .

```
aws ec2 describe-store-image-tasks
```

Erwartete Ausgabe

```
{
  "AmiId": "ami-1234567890abcdef0",
  "Bucket": "myamibucket",
  "ProgressPercentage": 17,
  "S3ObjectKey": "ami-1234567890abcdef0.bin",
  "StoreTaskState": "InProgress",
  "StoreTaskFailureReason": null,
  "TaskStartTime": "2021-01-01T01:01:01.001Z"
}
```

Wiederherstellen eines AMI aus einem S3-Bucket

Wiederherstellen eines AMI (AWS CLI)

Verwenden Sie den Befehl create-restore-image-task . Geben Sie unter Verwendung der Werte für `S3ObjectKey` und `Bucket` aus der `describe-store-image-tasks`-Ausgabe den Objektschlüssel des AMI und den Namen des S3-Buckets an, in den das AMI kopiert wurde. Geben Sie auch einen Namen für das wiederhergestellte AMI an. Der Name muss für AMIs in der Region für dieses Konto eindeutig sein.

> **Note**
>
> Das wiederhergestellte AMI erhält eine neue AMI-ID.

```
aws ec2 create-restore-image-task \
    --object-key ami-1234567890abcdef0.bin \
    --bucket myamibucket \
    --name "New AMI Name"
```

Erwartete Ausgabe

```
{
   "ImageId": "ami-0eab20fe36f83e1a8"
}
```

Verwenden Sie Dateipfade in S3

Sie können beim Speichern und Wiederherstellen von AMIs auf folgende Weise Dateipfade verwenden:

- Beim Speichern eines AMI in S3 kann der Dateipfad zum Bucket-Namen hinzugefügt werden. Intern trennt das System den Pfad vom Bucket-Namen und fügt den Pfad dann dem Objektschlüssel hinzu, der zum Speichern des AMI generiert wird. Der vollständige Objektpfad wird in der Antwort auf den API-Aufruf angezeigt.
- Da bei der Wiederherstellung des AMI ein Objektschlüsselparameter verfügbar ist, kann der Pfad am Anfang des Objektschlüsselwerts hinzugefügt werden.

Sie können Dateipfade verwenden, wenn Sie die SDKs AWS CLI und verwenden.

Beispiel: Verwenden Sie einen Dateipfad beim Speichern und Wiederherstellen eines AMI (AWS CLI)

Im folgenden Beispiel wird zunächst ein AMI in S3 gespeichert, wobei der Dateipfad an den Bucket-Namen angehängt wird. Das Beispiel stellt dann das AMI aus S3 wieder her, wobei dem Objektschlüsselparameter der Dateipfad vorangestellt wird.

1. Speichern Sie das AMI. Geben Sie für `--bucket` den Dateipfad nach dem Bucket-Namen wie folgt an:

   ```
   aws ec2 create-store-image-task \
       --image-id ami-1234567890abcdef0 \
       --bucket myamibucket/path1/path2
   ```

   Erwartete Ausgabe

```
{
  "ObjectKey": "path1/path2/ami-1234567890abcdef0.bin"
}
```

2. Speichern Sie das AMI. Für `--object-key` geben Sie den Wert aus der Ausgabe im vorherigen Schritt an, der den Dateipfad enthält.

```
aws ec2 create-restore-image-task \
    --object-key path1/path2/ami-1234567890abcdef0.bin \
    --bucket myamibucket \
    --name "New AMI Name"
```

AMI als veraltet kennzeichnen

Sie können ein AMI verwerfen, um anzuzeigen, dass es veraltet ist und nicht verwendet werden sollte. Sie können auch ein zukünftiges Ablaufdatum für ein AMI angeben, das angibt, wann das AMI veraltet ist. Beispielsweise können Sie ein AMI verwerfen, das nicht mehr aktiv verwaltet wird oder Sie können ein AMI verwerfen, das durch eine neuere Version ersetzt wurde. Standardmäßig werden veraltete AMIs nicht in AMI-Listen angezeigt, wodurch neue Benutzer daran gehindert werden, AMIs zu verwenden out-of-date . Vorhandene Benutzer und Start-Services wie Startvorlagen und Auto-Scaling-Gruppen können jedoch weiterhin ein veraltetes AMI verwenden, indem sie dessen ID angeben. Um das AMI zu löschen, sodass Benutzer und Services es nicht verwenden können, müssen Sie es Abmelden.

Nachdem ein AMI veraltet ist:

- Für AMI-Benutzer erscheint das veraltete AMI nicht in DescribeImagesAPI-Aufrufen, es sei denn, Sie geben seine ID an oder geben an, dass veraltete AMIs erscheinen müssen. AMI-Besitzern werden weiterhin veraltete AMIs in DescribeImagesAPI-Aufrufen angezeigt.
- Für AMI-Benutzer steht das veraltete AMI nicht zur Auswahl über die EC2-Konsole zur Verfügung. Ein veraltetes AMI wird beispielsweise nicht im AMI-Katalog des Launch Instance Wizard angezeigt. AMI-Besitzer sehen weiterhin veraltete AMIs in der EC2-Konsole.
- Wenn Sie für AMI-Benutzer die ID eines veralteten AMI kennen, können Sie weiterhin Instances mit dem veralteten AMI starten, indem Sie die API, CLI oder die SDKs verwenden.
- Start-Services wie Startvorlagen und Auto-Scaling-Gruppen können weiterhin auf veraltete AMIs verweisen.

- EC2-Instances, die mit einem anschließend veralteten AMI gestartet wurden, sind nicht betroffen und können gestoppt, gestartet und neu gestartet werden.

Sie können sowohl private als auch öffentliche AMIs veralten lassen.

Sie können auch Amazon Data Lifecycle Manager EBS-gestützte AMIs erstellen, um die Verweigerung von EBS-gestützten AMIs zu automatisieren. Weitere Informationen finden Sie unter Automatisieren von AMI-Lebenszyklen.

> **Note**
>
> Standardmäßig ist das Veralterungsdatum aller öffentlichen AMIs auf zwei Jahre ab dem AMI-Erstellungsdatum festgelegt. Sie können das Veralterungsdatum auf weniger als zwei Jahre festlegen. Um das Veralterungsdatum zu stornieren oder weiter in die Zukunft zu verschieben, müssen Sie das AMI privat machen, indem Sie es nur für bestimmte AWS -Konten freigeben.

Themen

Kosten

Wenn Sie ein AMI veralten lassen, wird das AMI nicht gelöscht. Der AMI-Besitzer zahlt weiterhin für die Snapshots des AMI. Um die Zahlung für die Schnappschüsse einzustellen, muss der AMI-Besitzer das AMI löschen, indem er es abmeldet.

Einschränkungen

- Um ein AMI veralten zu lassen, müssen Sie der Besitzer des AMI sein.

AMI als veraltet kennzeichnen

Sie können ein AMI an einem bestimmten Datum und einer bestimmten Uhrzeit veralten lassen Sie müssen der AMI-Besitzer sein, um dieses Verfahren durchführen zu können.

Console

AMI an einem bestimmten Datum als veraltet kennzeichnen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich AMIs aus.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Wählen Sie das AMI und dann Actions (Aktionen), Manage AMI Deprecation (AMI-Veralterung verwalten) aus. Sie können mehrere AMIs auswählen, um das gleiche Veralterungsdatum für mehrere AMIs gleichzeitig festzulegen.
5. Wählen Sie das Kontrollkästchen Enable (Aktivieren) aus und geben Sie dann das Datum und die Uhrzeit für die Veralterung ein.

   Die Obergrenze für das Veralterungsdatum liegt bei 10 Jahren ab dem jeweiligen Tag. Eine Ausnahme bilden öffentliche AMIs, bei denen die Obergrenze bei 2 Jahren ab dem Erstellungsdatum liegt. Sie können kein Datum angeben, das in der Vergangenheit liegt.
6. Wählen Sie Speichern.

AWS CLI

AMI an einem bestimmten Datum als veraltet kennzeichnen

Verwenden Sie den Befehl enable-image-deprecation. Geben Sie die ID des AMI sowie das Datum und die Uhrzeit an, zu denen das AMI veraltet sein soll. Wenn Sie einen Wert für Sekunden angeben, rundet Amazon EC2 die Sekunden auf die nächste Minute.

Die Obergrenze für `deprecate-at` liegt bei 10 Jahren ab dem jeweiligen Tag. Eine Ausnahme bilden öffentliche AMIs, bei denen die Obergrenze bei 2 Jahren ab dem Erstellungsdatum liegt. Sie können kein Datum angeben, das in der Vergangenheit liegt.

```
aws ec2 enable-image-deprecation \
    --image-id ami-1234567890abcdef0 \
    --deprecate-at "2021-10-15T13:17:12.000Z"
```

Erwartete Ausgabe

```
{
  "Return": "true"
}
```

Prüfen Sie, wann ein AMI zuletzt verwendet wurde

`LastLaunchedTime` gibt als Zeitstempel an, wann Ihr AMI zuletzt zum Starten einer Instance verwendet wurde. AMIs, die in der letzten Zeit nicht verwendet wurden, um eine Instance zu starten, können möglicherweise gute Kandidaten für eine Veralterung oder Abmeldung sein.

> **Note**
>
> - Wenn ein AMI verwendet wird, um eine Instance zu starten, kommt es zu einer Verzögerung von 24 Stunden, bevor diese Nutzung gemeldet wird.
> - `lastLaunchedTime`-Daten sind seit April 2017 verfügbar.

Console

Uhrzeit des letzten Starts eines AMI anzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich AMIs aus.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Wählen Sie das AMI aus und überprüfen Sie dann das Feld Last launched time (Uhrzeit des letzten Starts). Wenn Sie das Kontrollkästchen neben dem AMI aktiviert haben, befindet es sich auf der Registerkarte Details. Das Feld zeigt das Datum und die Uhrzeit an, bei der das AMI zum letzten Mal zum Starten einer Instance verwendet wurde.

AWS CLI

Uhrzeit des letzten Starts eines AMI anzeigen

Führen Sie den Befehl describe-image-attribute aus und geben Sie `--attribute lastLaunchedTime` an. Sie müssen der AMI-Besitzer sein, um diesen Befehl ausführen zu können.

```
aws ec2 describe-image-attribute \
    --image-id ami-1234567890example \
    --attribute lastLaunchedTime
```

Beispielausgabe

```
{
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    },
    "ImageId": "ami-1234567890example",
}
```

Beschreiben Sie veraltete AMIs

Sie können das Datum und die Uhrzeit der Veralterung eines AMI anzeigen und alle AMIs nach dem Veralterungsdatum filtern. Sie können das auch verwenden AWS CLI , um alle veralteten AMIs zu beschreiben, wobei das Verfallsdatum in der Vergangenheit liegt.

Console

Veralterungsdatum eines AMI anzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigatotionsbereich AMIs und dann das AMI aus.
3. Überprüfen Sie das Feld Deprecation time (Uhrzeit der Veralterung). Wenn Sie das Kontrollkästchen neben dem AMI aktiviert haben, befindet es sich auf der Registerkarte Details. Das Feld zeigt das Datum und die Uhrzeit der Veralterung des AMI. Wenn das Feld leer ist, ist das AMI nicht als veraltet gekennzeichnet.

AMIs nach Datum der Veralterung filtern

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich AMIs aus.

3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) oder Private images (Private Images) aus. (Private Images umfassen sowohl AMIs, die für Sie freigegeben wurden, als auch AMIs, die sich in Ihrem Besitz befinden.)
4. Geben Sie in der Suchleiste **`Deprecation time`** ein (während Sie die Buchstaben eingeben, wird der Filter Deprecation time (Uhrzeit der Veralterung) angezeigt) und wählen Sie dann einen Operator sowie ein Datum und eine Uhrzeit aus.

AWS CLI

Wenn Sie alle AMIs mit dem Befehl describe-images beschreiben, sind die Ergebnisse unterschiedlich, je nachdem, ob Sie AMI-Benutzer oder AMI-Besitzer sind.

- Wenn Sie ein AMI-Benutzer sind:

  Wenn Sie alle AMIs mit dem Befehl describe-images beschreiben, werden standardmäßig veraltete AMIs, die nicht Ihnen gehören, aber mit Ihnen geteilt werden, nicht in den Ergebnissen angezeigt. Dies liegt daran, dass der Standardwert `--no-include-deprecated` ist. Um veraltete AMIs in die Ergebnisse aufzunehmen, müssen Sie den `--include-deprecated`-Parameter angeben.
- Wenn Sie der AMI-Besitzer sind:

  Wenn Sie alle AMIs mit dem Befehl describe-images beschreiben, werden alle AMIs in Ihrem Besitz, einschließlich veralteter AMIs, in den Ergebnissen angezeigt. Sie müssen den `--include-deprecated`-Parameter nicht angeben. Darüber hinaus können Sie veraltete AMIs, deren Eigentümer Sie sind, nicht mithilfe von `--no-include-deprecated` aus den Ergebnissen ausschließen.

Wenn ein AMI veraltet ist, wird das Feld `DeprecationTime` in den Ergebnissen angezeigt.

> **Note**
>
> Ein veraltetes AMI ist ein AMI, dessen Ablaufdatum in der Vergangenheit liegt. Wenn Sie das Ablaufdatum auf ein Datum in der Zukunft gesetzt haben, ist das AMI noch nicht veraltet.

Alle AMIs bei der Beschreibung aller AMIs einschließen

Verwenden Sie den Befehl describe-images und geben Sie den Parameter `--include-deprecated` an, um alle veralteten AMIs, die Ihnen nicht gehören, in die Ergebnisse einzuschließen.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners 123456example
    --include-deprecated
```

Veralterungsdatum eines AMI beschreiben

Verwenden Sie den Befehl describe-images und geben Sie die ID des AMI an.

Beachten Sie, dass das veraltete AMI in den Ergebnissen zurückgegeben wird, wenn Sie `--no-include-deprecated` zusammen mit der AMI-ID angeben.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

Erwartete Ausgabe

Das Feld `DeprecationTime` zeigt das Datum an, an dem das AMI als veraltet festgelegt wird. Wenn das AMI nicht als veraltet festgelegt ist, wird das `DeprecationTime`-Feld nicht in der Ausgabe angezeigt.

```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "available",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2021-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
```

```
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Abbruch der Veraltung eines AMI

Sie können die Veralterung eines AMI abbrechen, wodurch Datum und Uhrzeit aus dem Feld Deprecation time (Uhrzeit der Veralterung) (Konsole) bzw. dem `DeprecationTime`-Feld aus der Ausgabe describe-images (AWS CLI) entfernt werden. Sie müssen der AMI-Besitzer sein, um dieses Verfahren durchführen zu können.

Console

Veralterung eines AMI abbrechen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich AMIs aus.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Wählen Sie das AMI und dann Actions (Aktionen), Manage AMI Deprecation (AMI-Veralterung verwalten) aus. Sie können mehrere AMIs auswählen, um die Veralterung mehrerer AMIs gleichzeitig abzubrechen

5. Deaktivieren Sie das Kontrollkästchen Enable (Aktivieren) und wählen Sie dann Save (Speichern) aus.

AWS CLI

Veralterung eines AMI abbrechen

Verwenden Sie den Befehl disable-image-deprecation und geben Sie die ID des AMI an.

```
aws ec2 disable-image-deprecation \
    --image-id ami-1234567890abcdef0
```

Erwartete Ausgabe

```
{
  "Return": "true"
}
```

Deaktivieren eines AMIs

Sie können ein AMI deaktivieren, um zu verhindern, dass es für Instance-Starts verwendet wird. Sie können keine neuen Instances von einem deaktivierten AMI aus starten. Sie können ein deaktiviertes AMI erneut aktivieren, sodass es wieder für Instance-Starts verwendet werden kann.

> **Warning**
>
> Durch die Deaktivierung eines AMI werden alle Startberechtigungen entfernt.

Wenn ein AMI deaktiviert ist:

- Der Status des AMI ändert sich zu `disabled`.
- Ein deaktiviertes AMI kann nicht freigegeben werden. Wenn ein AMI öffentlich war oder zuvor freigegeben wurde, wird es privat gemacht. Wenn ein AMI mit einer AWS-Konto Organisation oder Organisationseinheit geteilt wurde, verlieren diese den Zugriff auf das deaktivierte AMI.
- Ein deaktiviertes AMI wird standardmäßig nicht in DescribeImages-API-Aufrufen angezeigt.
- Ein deaktiviertes AMI wird nicht unter dem Konsolenfilter Owned by me angezeigt. Um deaktivierte AMIs zu finden, verwenden Sie den Konsolenfilter Deaktivierte Bilder.

- Ein deaktiviertes AMI kann nicht für den Start von Instances in der EC2-Konsole ausgewählt werden. Ein deaktiviertes AMI wird beispielsweise nicht im AMI-Katalog im Launch Instance Wizard oder beim Erstellen einer Startvorlage angezeigt.
- Start-Services wie Startvorlagen und Auto-Scaling-Gruppen können weiterhin auf deaktivierte AMIs verweisen. Nachfolgende Instance-Starts von einem deaktivierten AMI aus schlagen fehl. Wir empfehlen daher, Startvorlagen und Auto-Scaling-Gruppen so zu aktualisieren, dass sie nur auf verfügbare AMIs verweisen.
- EC2-Instances, die zuvor mit einem anschließend deaktivierten AMI gestartet wurden, sind nicht betroffen und können gestoppt, gestartet und neu gestartet werden.
- Sie können keine Snapshots löschen, die mit deaktivierten AMIs verknüpft sind. Der Versuch, einen zugehörigen Snapshot zu löschen, führt zu dem `snapshot is currently in use`-Fehler.

Wenn ein AMI wieder aktiviert wird:

- Der Status des AMI ändert sich auf `available` und es kann zum Starten von Instances verwendet werden.
- Das AMI kann gemeinsam genutzt werden.
- AWS-Konten, Organisationen und Organisationseinheiten, die den Zugriff auf das AMI verloren haben, als es deaktiviert wurde, erhalten nicht automatisch wieder Zugriff, aber das AMI kann wieder mit ihnen geteilt werden.

Sie können sowohl private als auch öffentliche AMIs deaktivieren.

Themen

Kosten

Wenn Sie ein AMI deaktivieren, wird das AMI nicht gelöscht. Wenn es sich bei dem AMI um ein EBS-gestütztes AMI handelt, zahlen Sie weiterhin für die EBS-Snapshots des AMI. Wenn Sie das AMI behalten möchten, können Sie möglicherweise Ihre Speicherkosten senken, indem Sie die Snapshots archivieren. Weitere Informationen finden Sie unter Archivieren von Amazon EBS-Snapshots im Amazon EBS-Benutzerhandbuch. Wenn Sie das AMI und seine Snapshots nicht behalten möchten, müssen Sie das AMI abmelden und die Snapshots löschen. Weitere Informationen finden Sie unter Löschen Sie Ressourcen, die mit Ihrem Amazon EBS-backed AMI verknüpft sind.

Voraussetzungen

Um ein AMI zu deaktivieren oder erneut zu aktivieren, müssen Sie das AMI besitzen.

Erforderliche IAM-Berechtigungen

Sie benötigen die folgenden IAM-Berechtigungen, um ein AMI zu deaktivieren und erneut zu aktivieren:

- `ec2:DisableImage`
- `ec2:EnableImage`

Deaktivieren eines AMIs

Sie können ein AMI deaktivieren, indem Sie die EC2-Konsole oder die AWS Command Line Interface (AWS CLI) verwenden. Sie müssen der AMI-Besitzer sein, um dieses Verfahren durchführen zu können.

Console

So deaktivieren Sie ein AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich AMIs aus.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Wählen Sie das AMI aus, dann Aktionen und anschließend AMI deaktivieren. Sie können mehrere AMIs zur gleichzeitigen Deaktivierung auswählen.
5. Wählen Sie im Fenster AMI deaktivieren die Option AMI deaktivieren aus.

AWS CLI

So deaktivieren Sie ein AMI

Verwenden Sie den Befehl disable-image und geben Sie die AMI-ID an.

```
aws ec2 disable-image --image-id ami-1234567890abcdef0
```

Erwartete Ausgabe

```
{
  "Return": "true"
}
```

Beschreiben deaktivierter AMIs

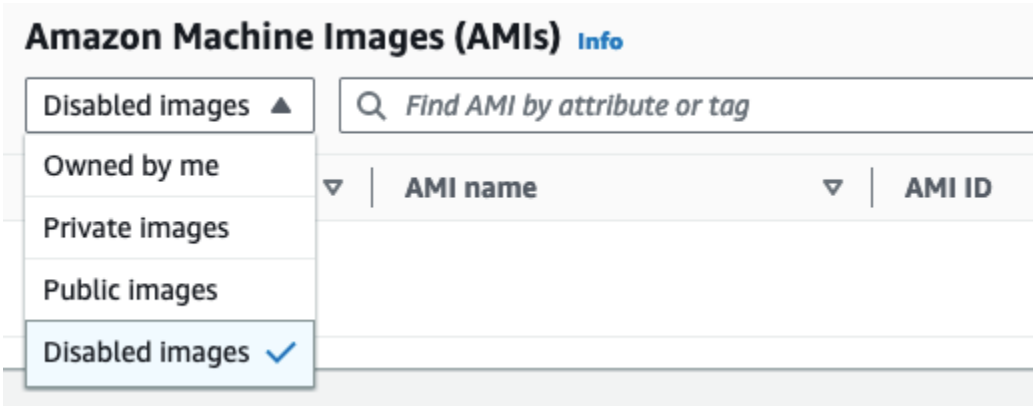
Sie können deaktivierte AMIs in der EC2-Konsole und über die AWS CLI anzeigen.

Sie müssen das AMI besitzen, um deaktivierte AMIs anzeigen zu können. Da deaktivierte AMIs als privat eingestuft werden, können Sie deaktivierte AMIs nicht anzeigen, wenn Sie sie nicht besitzen.

Console

So zeigen Sie deaktivierte AMIs an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich AMIs aus.
3. Wählen Sie in der Filterleiste Deaktivierte Bilder aus.



AWS CLI

Wenn Sie den Befehl describe-images zur Beschreibung aller AMIs verwenden, werden deaktivierte AMIs standardmäßig nicht in den Ergebnissen angezeigt. Dies liegt daran, dass der Standardwert `--no-include-disabled` ist. Um deaktivierte AMIs in die Ergebnisse aufzunehmen, müssen Sie den `--include-disabled`-Parameter angeben.

So schließen Sie alle deaktivierten AMIs bei der Beschreibung aller AMIs ein

Verwenden Sie den Befehl describe-images und geben Sie den Parameter `--include-disabled` an, um deaktivierte AMIs zusätzlich zu allen anderen AMIs abzurufen. Geben Sie optional `--owners self` an, sodass nur die AMIs abgerufen werden, die Sie besitzen.

```
aws ec2 describe-images \
    --region us-east-1 \
    --owners self
    --include-disabled
```

Wenn Sie die ID eines deaktivierten AMI angeben, aber nicht `--include-disabled` angeben, wird das deaktivierte AMI in den Ergebnissen zurückgegeben.

```
aws ec2 describe-images \
    --region us-east-1 \
    --image-ids ami-1234567890EXAMPLE
```

So rufen Sie nur deaktivierte AMIs ab

Geben Sie an `--filters Name=state,Values=disabled`. Sie müssen auch `--include-disabled` angeben, sonst erhalten Sie einen Fehler.

```
aws ec2 describe-images \
    --include-disabled \
    --filters Name=state,Values=disabled
```

Beispielausgabe

Das Feld `State` zeigt den Status eines AMI an. `disabled` zeigt an, dass das AMI deaktiviert ist.

```
{
```

```
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "EnaSupport": true,
            "Hypervisor": "xen",
            "State": "disabled",
            "SriovNetSupport": "simple",
            "ImageId": "ami-1234567890EXAMPLE",
            "DeprecationTime": "2023-05-10T13:17:12.000Z"
            "UsageOperation": "RunInstances:0010",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
            "Public": false,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Ein deaktiviertes AMI erneut aktivieren

Sie können ein zuvor deaktiviertes AMI reaktivieren. Sie müssen der AMI-Besitzer sein, um dieses Verfahren durchführen zu können.

Console

So reaktivieren Sie ein zuvor deaktiviertes AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich AMIs aus.
3. Wählen Sie in der Filterleiste Deaktivierte Bilder aus.
4. Wählen Sie das AMI aus, dann Aktionen und anschließend AMI aktivieren. Sie können mehrere AMIs auswählen, um mehrerer AMIs gleichzeitig zu reaktivieren.
5. Wählen Sie im Fenster AMI aktivieren die Option Aktivieren aus.

AWS CLI

So reaktivieren Sie ein zuvor deaktiviertes AMI

Verwenden Sie den Befehl enable-image und geben Sie die AMI-ID an.

```
aws ec2 enable-image --image-id ami-1234567890abcdef0
```

Erwartete Ausgabe

```
{
  "Return": "true"
}
```

Archivieren von AMI-Snapshots

Sie können die Snapshots archivieren, die Ihren deaktivierten EBS-gestützten AMIs zugeordnet sind. Dies kann Ihnen helfen, die Speicherkosten für Ihre selten verwendeten AMIs zu senken, die über lange Zeiträume aufbewahrt werden müssen. Weitere Informationen finden Sie unter Archivieren von Amazon EBS-Snapshots im Amazon EBS-Benutzerhandbuch.

So archivieren Sie Snapshots, die einem AMI zugeordnet sind

1. Deaktivieren Sie das AMI.
2. Archivieren Sie die Snapshots.

Sie können ein AMI nicht verwenden, solange es deaktiviert ist und die zugehörigen Snapshots archiviert sind.

So stellen Sie ein deaktiviertes AMI mit archivierten Snapshots zur Verwendung wieder her

1. Stellen Sie die archivierten Snapshots wieder her, die dem AMI zugeordnet sind.
2. Aktivieren Sie das AMI.

Ein AMI abmelden (löschen)

Wenn Sie ein AMI abmelden, löscht Amazon EC2 es dauerhaft. Nach der Abmeldung können Sie das AMI nicht mehr verwenden, um neue Instances zu starten. Sie könnten erwägen, ein AMI zu deregistrieren, wenn Sie es nicht mehr verwenden.

Zum Schutz vor versehentlicher oder böswilliger Abmeldung eines AMI können Sie den Abmeldeschutz aktivieren. Wenn Sie versehentlich ein EBS-gestütztes AMI deregistrieren, können Sie es nur dann mit dem Papierkorb wiederherstellen, wenn Sie es innerhalb des zulässigen Zeitraums wiederherstellen, bevor es dauerhaft gelöscht wird.

Die Abmeldung eines AMI hat keine Auswirkungen auf Instances, die über das AMI gestartet wurden. Sie können diese Instances weiterhin verwenden. Die Deregistrierung eines AMI hat auch keine Auswirkungen auf Snapshots, die während des AMI-Erstellungsprozesses erstellt wurden. Es fallen weiterhin Nutzungskosten für diese Instances und Speicherkosten für die Snapshots an. Um unnötige Kosten zu vermeiden, empfehlen wir Ihnen daher, alle Instances zu beenden und alle Snapshots zu löschen, die Sie nicht benötigen. Weitere Informationen finden Sie unter Vermeiden Sie Kosten, die durch ungenutzte Ressourcen entstehen.

Inhalt

Überlegungen

- Sie können ein AMI, das nicht Ihrem Konto gehört, nicht abmelden.

- Sie können Amazon EC2 nicht verwenden, um ein vom Service verwaltetes AMI abzumelden. AWS Backup Verwenden Sie stattdessen, AWS Backup um die entsprechenden Wiederherstellungspunkte im Backup-Tresor zu löschen. Weitere Informationen finden Sie unter Löschen von Backups im AWS Backup Entwickler-Leitfaden.

Ein AMI abmelden

Verwenden Sie eine der folgenden Methoden, um ein EBS-gestütztes AMI oder ein instance store-backed AMI abzumelden.

> **Tip**
>
> Um unnötige Kosten zu vermeiden, sollten Sie alle Ressourcen löschen, die Sie nicht benötigen. Wenn Sie beispielsweise für EBS-gestützte AMIs die mit dem abgemeldeten AMI verknüpften Snapshots nicht benötigen, sollten Sie sie löschen. Weitere Informationen finden Sie unter Vermeiden Sie Kosten, die durch ungenutzte Ressourcen entstehen.

Console

Um ein AMI abzumelden

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie in der Filterleiste Owned by me aus, um Ihre verfügbaren AMIs aufzulisten, oder wählen Sie Disabled images, um Ihre deaktivierten AMIs aufzulisten.
4. Wählen Sie das AMI aus, das Sie abmelden möchten.
5. Wählen Sie Aktionen, AMI abmelden aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Deregister AMI.

   Es kann einige Minuten dauern, bis die Konsole das AMI aus der Liste entfernt. Wählen Sie Refresh (Aktualisieren) aus, um den Status zu aktualisieren.

AWS CLI

Um ein AMI abzumelden

Verwenden Sie den Befehl deregister-image und geben Sie die ID des AMI an, für das die Registrierung aufgehoben werden soll.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

Powershell

Um ein AMI abzumelden

Verwenden Sie das Unregister-EC2ImageCmdlet und geben Sie die ID des AMI an, für das die Registrierung aufgehoben werden soll.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

Prüfen Sie, wann ein AMI zuletzt verwendet wurde

`LastLaunchedTime` gibt als Zeitstempel an, wann Ihr AMI zuletzt zum Starten einer Instance verwendet wurde. AMIs, die in der letzten Zeit nicht verwendet wurden, um eine Instance zu starten, können möglicherweise gute Kandidaten für eine Abmeldung oder Veralterung sein.

> **Note**
>
> - Wenn das AMI verwendet wird, um eine Instance zu starten, kommt es zu einer Verzögerung von 24 Stunden, bevor diese Nutzung gemeldet wird.
> - `lastLaunchedTime`-Daten sind seit April 2017 verfügbar.

Console

Uhrzeit des letzten Starts eines AMI anzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich AMIs aus.
3. Wählen Sie in der Filterleiste Owned by me (In meinem Besitz) aus.
4. Wählen Sie das AMI aus und überprüfen Sie dann das Feld Last launched time (Uhrzeit des letzten Starts). Wenn Sie das Kontrollkästchen neben dem AMI aktiviert haben, befindet es sich auf der Registerkarte Details. Das Feld zeigt das Datum und die Uhrzeit an, bei der das AMI zum letzten Mal zum Starten einer Instance verwendet wurde.

AWS CLI

Sie können entweder den Befehl describe-images oder den Befehl describe-image-attribute verwenden, um die Uhrzeit des letzten Starts eines AMI anzuzeigen.

So zeigen Sie die Uhrzeit des letzten Starts eines AMI mithilfe von describe-images an

Verwenden Sie den Befehl describe-images und geben Sie die ID des AMI an.

```
aws ec2 describe-images --image-id ami-0123456789example
```

Beispielausgabe

> **Note**
>
> Das `LastLaunchedTime` Feld erscheint in der Ausgabe nur für AMIs, die Sie besitzen.

```
{
    "Images": [
       {
           ...
           "LastLaunchedTime": {
               "Value": "2024-04-02T02:03:18Z"
           },
           ...
       }
   ]
}
```

Uhrzeit des letzten Starts eines AMI anzeigen

Verwenden Sie den Befehl describe-image-attribute und geben Sie Folgendes an. `--attribute lastLaunchedTime` Sie müssen Eigentümer des AMI sein, um diesen Befehl ausführen zu können.

```
aws ec2 describe-image-attribute \
    --image-id ami-0123456789example \
    --attribute lastLaunchedTime
```

Beispielausgabe

```
{
    "ImageId": "ami-1234567890example",
    "LastLaunchedTime": {
        "Value": "2022-02-10T02:03:18Z"
    }
}
```

Ein AMI vor der Abmeldung schützen

Sie können den Abmeldeschutz für ein AMI aktivieren, um ein versehentliches oder böswilliges Löschen zu verhindern. Wenn Sie den Abmeldeschutz aktivieren, kann das AMI von keinem Benutzer abgemeldet werden, unabhängig von seinen IAM-Berechtigungen. Wenn Sie das AMI abmelden möchten, müssen Sie zuerst den Abmeldeschutz für das AMI deaktivieren.

Wenn Sie den Abmeldeschutz für ein AMI aktivieren, haben Sie die Möglichkeit, eine 24-stündige Abklingzeit einzuplanen. Diese Abklingzeit ist die Zeit, in der der Abmeldeschutz auch nach dem Ausschalten aktiv bleibt. Während dieser Abklingzeit kann das AMI nicht abgemeldet werden. Nach Ablauf der Abklingzeit kann das AMI deregistriert werden.

Der Abmeldeschutz ist standardmäßig für alle vorhandenen und neuen AMIs deaktiviert.

Schalten Sie den Abmeldeschutz ein

Verwenden Sie eine der folgenden Methoden, um den Abmeldeschutz für ein AMI zu aktivieren. Dazu müssen Sie der Besitzer des AMI sein.

Console

So aktivieren Sie den Abmeldeschutz für ein AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie in der Filterleiste Owned by me aus, um Ihre verfügbaren AMIs aufzulisten, oder wählen Sie Deaktivierte Images, um Ihre deaktivierten AMIs aufzulisten.
4. Wählen Sie das AMI aus, für das Sie den Abmeldeschutz aktivieren möchten, und klicken Sie dann auf Aktionen, AMI-Abmeldeschutz verwalten.
5. Im Dialogfeld AMI-Abmeldeschutz verwalten können Sie den Abmeldeschutz mit oder ohne Abklingzeit aktivieren. Wählen Sie eine der folgenden Optionen:

- Mit einer Abklingzeit von 24 Stunden aktivieren — Bei einer Abklingzeit kann das AMI 24 Stunden lang nicht abgemeldet werden, wenn der Abmeldeschutz ausgeschaltet ist.
- Ohne Abklingzeit aktivieren — Ohne eine Abklingzeit kann das AMI sofort abgemeldet werden, wenn der Abmeldeschutz ausgeschaltet ist.

6. Wählen Sie Speichern.

AWS CLI

So aktivieren Sie den Abmeldeschutz für ein AMI

Verwenden Sie den Befehl enable-image-deregistration-protection und geben Sie die AMI-ID an. Um die optionale 24-stündige Abklingzeit einzubeziehen, setzen Sie Include auf. `--with-cooldown true` Um die Abklingzeit auszuschließen, lassen Sie den Parameter weg. `--with-cooldown`

```
aws ec2 enable-image-deregistration-protection \
    --image-id ami-0123456789example \
    --with-cooldown true
```

Schalten Sie den Abmeldeschutz aus

Verwenden Sie eine der folgenden Methoden, um den Abmeldeschutz für ein AMI zu deaktivieren. Dazu müssen Sie der Besitzer des AMI sein.

> **Note**
>
> Wenn Sie bei der Aktivierung des Abmeldeschutzes für das AMI eine 24-stündige Abklingzeit gewählt haben, können Sie das AMI nicht sofort abmelden, wenn Sie den Abmeldeschutz ausschalten. Die Abklingzeit ist der 24-Stunden-Zeitraum, in dem der Abmeldeschutz auch nach dem Ausschalten aktiv bleibt. Während dieser Abklingzeit kann das AMI nicht abgemeldet werden. Nach Ablauf der Abklingzeit kann das AMI deregistriert werden.

Console

So deaktivieren Sie den Abmeldeschutz für ein AMI

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie in der Filterleiste Owned by me aus, um Ihre verfügbaren AMIs aufzulisten, oder wählen Sie Deaktivierte Images, um Ihre deaktivierten AMIs aufzulisten.
4. Wählen Sie das AMI aus, um den Abmeldeschutz zu deaktivieren, und wählen Sie dann Aktionen, AMI-Abmeldeschutz verwalten aus.
5. Wählen Sie im Dialogfeld AMI-Deregistrierungsschutz verwalten die Option Deaktivieren aus.
6. Wählen Sie Speichern.

AWS CLI

So deaktivieren Sie den Abmeldeschutz für ein AMI

Verwenden Sie den Befehl disable-image-deregistration-protection und geben Sie die AMI-ID an.

```
aws ec2 disable-image-deregistration-protection --image-id ami-0123456789example
```

Vermeiden Sie Kosten, die durch ungenutzte Ressourcen entstehen

Wenn Sie ein AMI deregistrieren, löschen Sie nicht die Ressourcen, die dem AMI zugeordnet sind. Zu diesen Ressourcen gehören die Snapshots für EBS-gestützte AMIs und die Dateien in Amazon S3, beispielsweise speichergestützte AMIs. Wenn Sie ein AMI abmelden, beenden oder stoppen Sie auch keine Instances, die über das AMI gestartet wurden.

Es fallen weiterhin Kosten für das Speichern der Snapshots und Dateien an, und es fallen Kosten für alle laufenden Instances an. Weitere Informationen finden Sie unter Kostenberechnung.

Um unnötige Kosten dieser Art zu vermeiden, empfehlen wir, alle Ressourcen zu löschen, die Sie nicht benötigen.

Informationen darüber, ob Ihr AMI EBS-gestützt oder Instance-Store-gesichert ist, finden Sie unter. Bestimmen des Root-Gerätetyps Ihres AMI

Löschen Sie Ressourcen, die mit Ihrem Amazon EBS-backed AMI verknüpft sind

Verwenden Sie eine der folgenden Methoden, um die Ressourcen zu löschen, die mit Ihrem EBS-gestützten AMI verknüpft sind.

Console

So löschen Sie Ressourcen, die mit Ihrem EBS-gestützten AMI verknüpft sind

1. Melden Sie das AMI ab.

   Notieren Sie sich die AMI-ID — dies kann Ihnen helfen, die Snapshots zu finden, die Sie im nächsten Schritt löschen möchten.

2. Löschen Sie Snapshots, die Sie nicht benötigen.

   Die ID des zugehörigen AMI wird in der Spalte Beschreibung auf dem Bildschirm Snapshots angezeigt.

3. Beenden Sie Instances, die Sie nicht benötigen.

AWS CLI

So löschen Sie Ressourcen, die mit Ihrem EBS-gestützten AMI verknüpft sind

1. Melden Sie das AMI mit dem Befehl deregister-image ab.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Löschen Sie Snapshots, die Sie nicht benötigen, mit dem Befehl delete-snapshot.

```
aws ec2 delete-snapshot --snapshot-id snap-0123456789example
```

3. Beenden Sie Instances, die Sie nicht benötigen, mit dem Befehl terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

PowerShell

So löschen Sie Ressourcen, die mit Ihrem EBS-gestützten AMI verknüpft sind

1. Deregistrieren Sie das AMI mithilfe des Unregister-EC2ImageCmdlets.

```
Unregister-EC2Image -ImageId ami-0123456789example
```

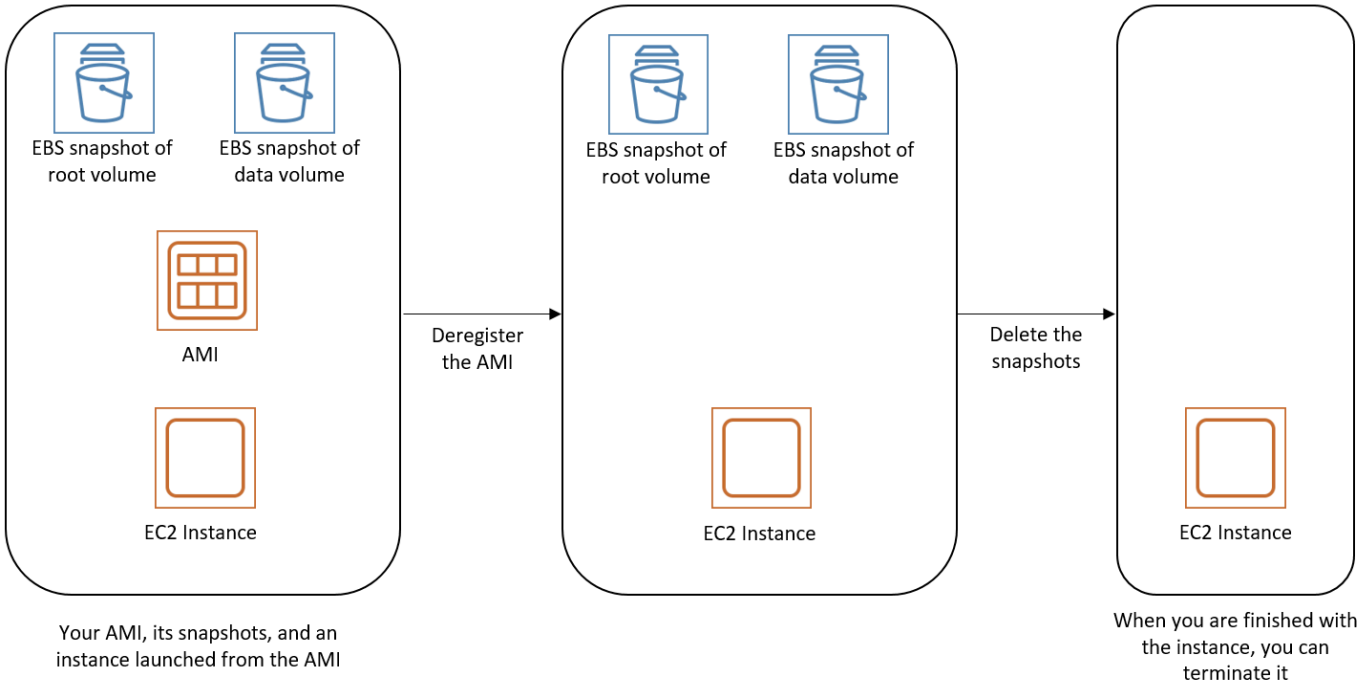
2. Löschen Sie Snapshots, die Sie nicht benötigen, mithilfe des Cmdlets. Remove-EC2Snapshot

```
Remove-EC2Snapshot -SnapshotId snap-0123456789example
```

3. Beenden Sie Instanzen, die Sie nicht benötigen, mithilfe des Cmdlets. Remove-EC2Instance

```
Remove-EC2Instance -InstanceId i-0123456789example
```

Das folgende Diagramm zeigt, wie Sie Ressourcen löschen, die einem EBS-gestützten AMI zugeordnet sind.



Löschen Sie Ressourcen, die mit Ihrem durch den instance store-backed AMI verknüpft sind

Verwenden Sie die folgende Methode, um die Ressourcen zu löschen, die Ihrem durch den instance store-backed AMI zugeordnet sind.

So löschen Sie Ressourcen, die mit Ihrem durch den instance store-backed AMI verknüpft sind

1. Melden Sie das AMI mit dem Befehl deregister-image ab.

```
aws ec2 deregister-image --image-id ami-0123456789example
```

2. Löschen Sie das Bundle in Amazon S3 mithilfe des Befehls ec2-delete-bundle (AMI tools).

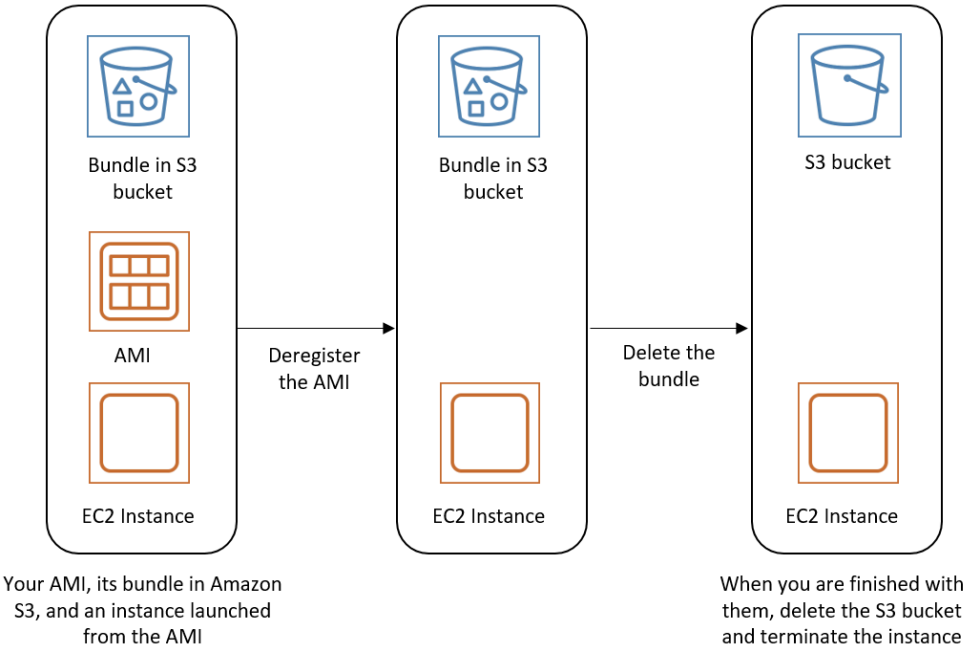
```
ec2-delete-bundle -b myawsbucket/myami -a your_access_key_id -
s your_secret_access_key -p image
```

3. Beenden Sie Instances, die Sie nicht benötigen, mit dem Befehl terminate-instances.

```
aws ec2 terminate-instances --instance-ids i-0123456789example
```

4. Wenn Sie mit dem Amazon S3 S3-Bucket, in den Sie das Bundle hochgeladen haben, fertig sind, können Sie den Bucket löschen. Um einen Amazon S3-Bucket zu löschen, müssen Sie die Amazon S3-Konsole öffnen, den Bucket auswählen und die Option Actions (Aktionen) und anschließend Delete (Löschen) auswählen.

Das folgende Diagramm zeigt, wie Sie Ressourcen löschen, die mit Ihrem durch den instance store-backed AMI verknüpft sind.



Automatisieren des von EBS-unterstützten AMI-Lebenszyklus

Sie können Amazon Data Lifecycle Manager verwenden, um die Erstellung, Aufbewahrung, Kopie, Veraltung und Abmeldung von Amazon EBS-gestützten AMIs und deren unterstützenden Snapshots zu automatisieren. Weitere Informationen finden Sie unter Amazon Data Lifecycle Manager.

Verwenden der Verschlüsselung mit EBS-gestützten AMIs

AMIs, die durch Amazon EBS-Snapshots gestützt werden, können die Amazon EBS-Verschlüsselung nutzen. Snapshots von Daten- und Stamm-Volumes können verschlüsselt und einem AMI zugeordnet werden. Sie können Instances starten und Images mit vollständiger EBS-Verschlüsselungsunterstützung kopieren. Verschlüsselungsparameter für diese Operationen werden in allen Regionen unterstützt, in denen sie AWS KMS verfügbar sind.

EC2-Instances mit verschlüsselten EBS-Volumes werden über AMIs genau wie andere Instances gestartet. Zudem können Sie einige oder alle Volumes während des Starts verschlüsseln, wenn Sie eine Instance von einem AMI starten, das von unverschlüsselten EBS-Snapshots unterstützt wird.

Wie EBS-Volumes können Snapshots in AMIs entweder mit Ihrem Standardschlüssel oder mit einem von Ihnen angegebenen AWS KMS key, vom Kunden verwalteten Schlüssel verschlüsselt werden. In allen Fällen müssen Sie die Berechtigung haben, den ausgewählten Verschlüsselung zu verwenden.

AMIs mit verschlüsselten Snapshots können von mehreren Konten gemeinsam genutzt werden. AWS Weitere Informationen finden Sie unter Gemeinsame AMIs.

Themen zur Verschlüsselung mit EBS-gestützten AMIs

- Instance-startende Szenarien
- Image-kopierende Szenarien

Instance-startende Szenarien

Amazon EC2 EC2-Instances werden von AMIs aus gestartet, wobei die `RunInstances` Aktion mit Parametern verwendet wird, die über die Blockgerätezuweisung bereitgestellt werden, entweder über die Amazon EC2-API AWS Management Console oder CLI oder direkt mithilfe der Amazon EC2 EC2-API oder CLI. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen. Beispiele für die Steuerung der Blockgerätezuweisung über finden Sie unter EC2-Instances starten, auflisten und beenden. AWS CLI

Ohne explizite Verschlüsselungsparameter behält eine `RunInstances`-Aktion standardmäßig den bestehenden Verschlüsselungsstatus der Quell-Snapshots eines AMI bei, während EBS-Volumes von diesen wiederhergestellt werden. Wenn die Verschlüsselung standardmäßig aktiviert ist, werden alle vom AMI erstellten Volumes (unabhängig davon, ob es sich um verschlüsselte oder

unverschlüsselte Snapshots handelt) verschlüsselt. Wenn die Verschlüsselung standardmäßig nicht aktiviert ist, behält die Instance den Verschlüsselungsstatus des AMI bei.

Sie können auch eine Instance starten und gleichzeitig einen neuen Verschlüsselungsstatus auf die sich ergebenden Volumes anwenden, indem Sie Verschlüsselungsparameter angeben. Folglich werden die folgenden Verhaltensweisen beobachtet:

Starten ohne Verschlüsselungsparameter

- Ein unverschlüsselter Snapshot wird in ein unverschlüsseltes Volume wiederhergestellt, es sei denn, die standardmäßige Verschlüsselung ist aktiviert. In diesem Fall werden alle neu erstellten Volumes verschlüsselt.
- Ein verschlüsselter Snapshot, den Sie besitzen, wird in ein Volume wiederhergestellt, das mit demselben Verschlüsselung verschlüsselt wird.
- Ein verschlüsselter Snapshot, der Ihnen nicht gehört (z. B. wenn das AMI mit Ihnen geteilt wird), wird auf einem Volume wiederhergestellt, das mit dem Standard-KMS-Schlüssel Ihres AWS Kontos verschlüsselt ist.

Durch Angeben von Verschlüsselungsparametern können die Standard-Verhaltensweisen überschrieben werden. Die verfügbaren Parameter sind `Encrypted` und `KmsKeyId`. Werden nur die `Encrypted`-Parameter festgelegt, ergibt sich Folgendes:

Instance-Start-Verhaltensweisen, wenn **`Encrypted`** festgelegt, aber keine **`KmsKeyId`** angegeben ist

- Ein unverschlüsselter Snapshot wird in einem EBS-Volume wiederhergestellt, das mit dem Standard-KMS-Schlüssel Ihres AWS -Kontos verschlüsselt wird.
- Ein verschlüsselter Snapshot, den Sie besitzen, wird in ein EBS-Volume wiederhergestellt, das mit demselben Verschlüsselung verschlüsselt wird. (Mit anderen Worten, der `Encrypted`-Parameter ist wirkungslos.)
- Ein verschlüsselter Snapshot, der Ihnen nicht gehört (d. h., das AMI wird mit Ihnen geteilt), wird auf einem Volume wiederhergestellt, das mit dem Standard-KMS-Schlüssel Ihres AWS Kontos verschlüsselt ist. (Mit anderen Worten, der `Encrypted`-Parameter ist wirkungslos.)

Durch Festlegen der Parameter `Encrypted` und `KmsKeyId` können Sie einen nicht standardmäßigen Verschlüsselung für eine Verschlüsselungsoperation angeben. Dadurch ergeben sich die folgenden Verhaltensweisen:

Instance, bei der **`Encrypted`** und **`KmsKeyId`** festgelegt sind

- Ein unverschlüsselter Snapshot wird in ein EBS-Volume wiederhergestellt, das mit dem angegebenen Verschlüsselung verschlüsselt wird.
- Ein verschlüsselter Snapshot wird in ein EBS-Volume wiederhergestellt, das nicht mit dem ursprünglichen Verschlüsselung, sondern mit dem angegebenen Verschlüsselung verschlüsselt wird.

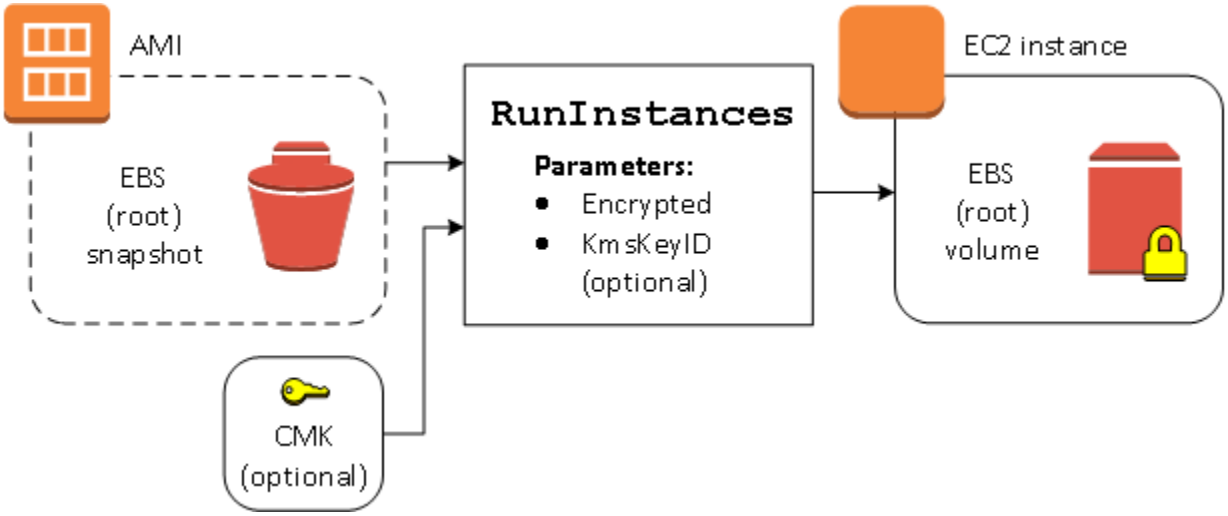
Das Senden einer `KmsKeyId` ohne Festlegen des `Encrypted`-Parameters führt zu einem Fehler.

Die folgenden Abschnitte enthalten Beispiele für das Starten von Instances aus AMIs mithilfe von nicht standardmäßigen Verschlüsselungsparametern. In jedem dieser Szenarien ergibt sich durch die in der `RunInstances`-Aktionen bereitgestellten Parameter eine Änderung des Verschlüsselungsstatus während der Wiederherstellung eines Volumes aus einem Snapshot.

Informationen zur Verwendung der Konsole zum Starten einer Instance von einem AMI aus finden Sie unter Starten Ihrer Instance.

Verschlüsseln eines Volumes während des Startens

In diesem Beispiel wird ein von einem unverschlüsselten Snapshot unterstütztes AMI verwendet, um eine EC2-Instance mit einem verschlüsselten EBS-Volume zu starten.

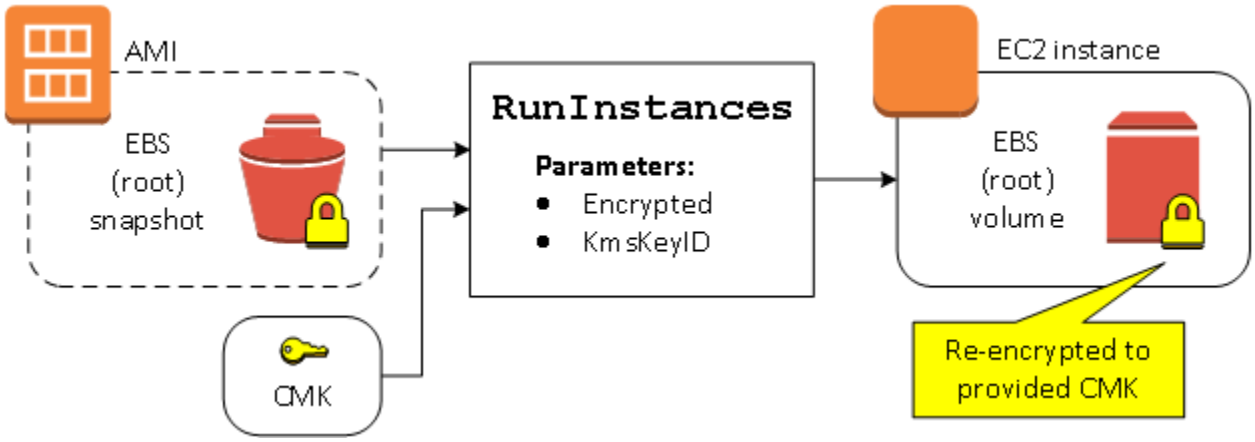


Der Parameter `Encrypted` für sich allein bewirkt, dass das Volume für diese Instance verschlüsselt wird. Die Angabe eines Parameters `KmsKeyId` ist optional. Wenn keine KMS-Schlüssel-ID angegeben ist, wird der Standard-KMS-Schlüssel des AWS Kontos zur Verschlüsselung des Volumes

verwendet. Geben Sie den Parameter `KmsKeyId` an, um das Volume mit einem anderen eigenen Verschlüsselung zu verschlüsseln.

Neuverschlüsseln eines Volumes während des Startens

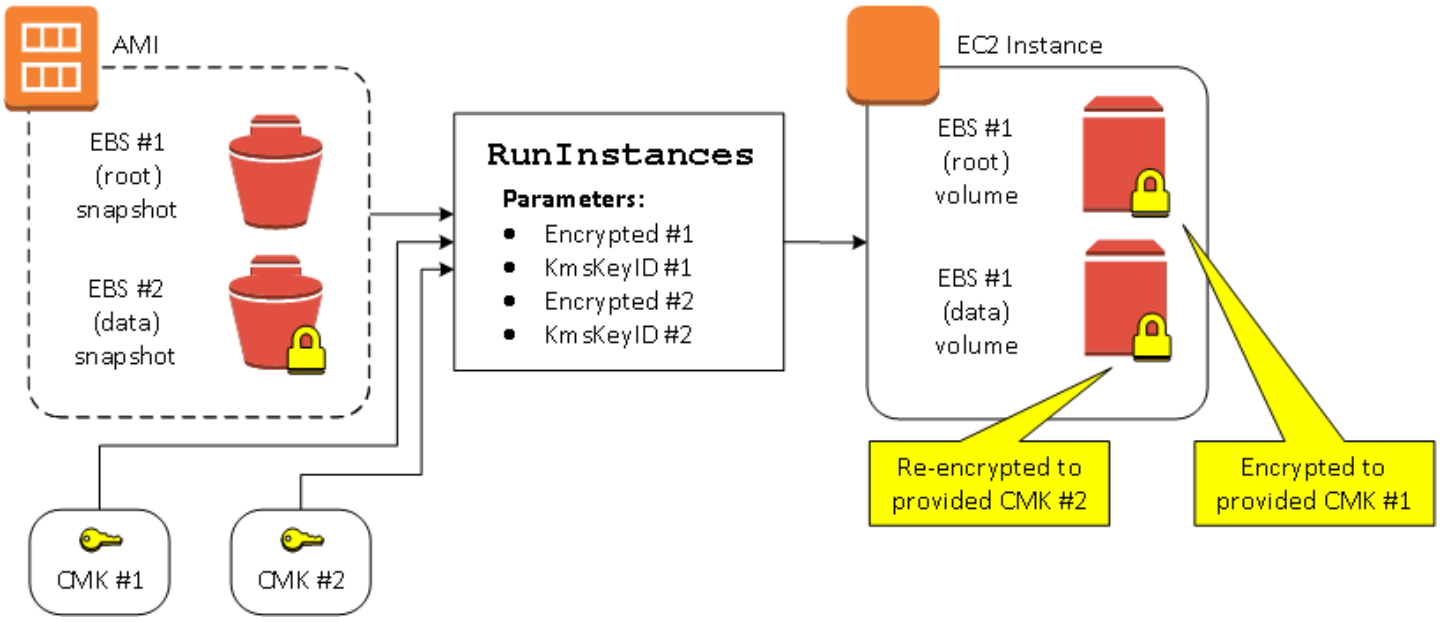
In diesem Beispiel wird ein von einem verschlüsselten Snapshot unterstütztes AMI verwendet, um eine EC2-Instance mit einem EBS-Volume zu starten, das mit einem neuen Verschlüsselung verschlüsselt wird.



Wenn Sie das AMI besitzen und keine Verschlüsselungsparameter angeben, verfügt die resultierende Instance über ein Volume, das mit demselben KMS-Schlüssel wie der Snapshot verschlüsselt wird. Wenn das AMI gemeinsam genutzt wird und nicht Ihnen gehört – und Sie keine Verschlüsselungsparameter angeben – wird das Volume mit Ihrem Standard-Verschlüsselung verschlüsselt. Werden die Verschlüsselungsparameter wie gezeigt angegeben, wird das Volume mit dem angegebenen Verschlüsselung verschlüsselt.

Ändern des Verschlüsselungsstatus mehrerer Volumes während des Startens

In diesem komplexeren Beispiel wird ein von mehreren Snapshots unterstütztes AMI (jedes mit einem eigenen Verschlüsselungsstatus) verwendet, um eine EC2-Instance mit einem neu verschlüsselten und einem erneut verschlüsselten Volume zu starten.



In diesem Szenario wird die `RunInstances`-Aktion mit Verschlüsselungsparametern für jeden der Quell-Snapshots bereitgestellt. Wenn alle möglichen Verschlüsselungsparameter angegeben sind, ist die sich ergebende Instance unabhängig davon, ob Sie die AMI besitzen, identisch.

Image-kopierende Szenarien

Amazon-EC2-AMIs werden mit der `CopyImage`-Aktion kopiert, entweder über die AWS Management Console oder direkt mit der Amazon EC2 API oder CLI.

Ohne explizite Verschlüsselungsparameter behält eine `CopyImage`-Aktion standardmäßig den bestehenden Verschlüsselungsstatus der Quell-Snapshots eines AMI während des Kopierens bei. Sie können auch ein AMI kopieren und gleichzeitig einen neuen Verschlüsselungsstatus auf seine zugeordneten EBS-Snapshots anwenden, indem Sie Verschlüsselungsparameter angeben. Folglich werden die folgenden Verhaltensweisen beobachtet:

Kopieren ohne Verschlüsselungsparameter

- Ein unverschlüsselter Snapshot wird in einen anderen unverschlüsselten Snapshot kopiert, es sei denn, die standardmäßige Verschlüsselung ist aktiviert. In diesem Fall werden alle neu erstellten Snapshots verschlüsselt.
- Ein verschlüsselter Snapshot, den Sie besitzen, wird in einen Snapshot kopiert, der mit demselben Verschlüsselung verschlüsselt wird.
- Ein verschlüsselter Snapshot, der Ihnen nicht gehört (d. h., das AMI wird mit Ihnen geteilt), wird in einen Snapshot kopiert, der mit dem Standard-KMS-Schlüssel Ihres AWS Kontos verschlüsselt ist.

All diese Standard-Verhaltensweisen können durch Angeben von Verschlüsselungsparametern überschrieben werden. Die verfügbaren Parameter sind `Encrypted` und `KmsKeyId`. Werden nur die `Encrypted`-Parameter festgelegt, ergibt sich Folgendes:

Copy-image-Verhaltensweisen, wenn **`Encrypted`** festgelegt, aber keine **`KmsKeyId`** angegeben ist

- Ein unverschlüsselter Snapshot wird in einen Snapshot kopiert, der mit dem Standard-KMS-Schlüssel des AWS -Kontos verschlüsselt wird.
- Ein verschlüsselter Snapshot wird in einen Snapshot kopiert, der mit demselben Verschlüsselung verschlüsselt wird. (Mit anderen Worten, der `Encrypted`-Parameter ist wirkungslos.)
- Ein verschlüsselter Snapshot, der Ihnen nicht gehört (d. h., das AMI wird mit Ihnen geteilt), wird auf ein Volume kopiert, das mit dem Standard-KMS-Schlüssel Ihres AWS Kontos verschlüsselt ist. (Mit anderen Worten, der `Encrypted`-Parameter ist wirkungslos.)

Durch Festlegen der Parameter `Encrypted` und `KmsKeyId` können Sie einen kundenverwalteten Verschlüsselung für eine Verschlüsselungsoperation angeben. Dadurch ergeben sich die folgenden Verhaltensweisen:

Copy-image-Verhaltensweisen, wenn **`Encrypted`** und **`KmsKeyId`** festgelegt sind

- Ein unverschlüsselter Snapshot wird in einen Snapshot kopiert, der mit dem angegebenen Verschlüsselung verschlüsselt wird.
- Ein verschlüsselter Snapshot wird in einen Snapshot kopiert, der nicht mit dem ursprünglichen Verschlüsselung, sondern mit dem angegebenen Verschlüsselung verschlüsselt wird.

Das Senden einer `KmsKeyId` ohne Festlegen des `Encrypted`-Parameters führt zu einem Fehler.

Der folgende Abschnitt enthält ein Beispiel für das Kopieren eines AMI mit nicht standardmäßigen Verschlüsselungsparametern, wodurch sich der Verschlüsselungsstatus ändert.

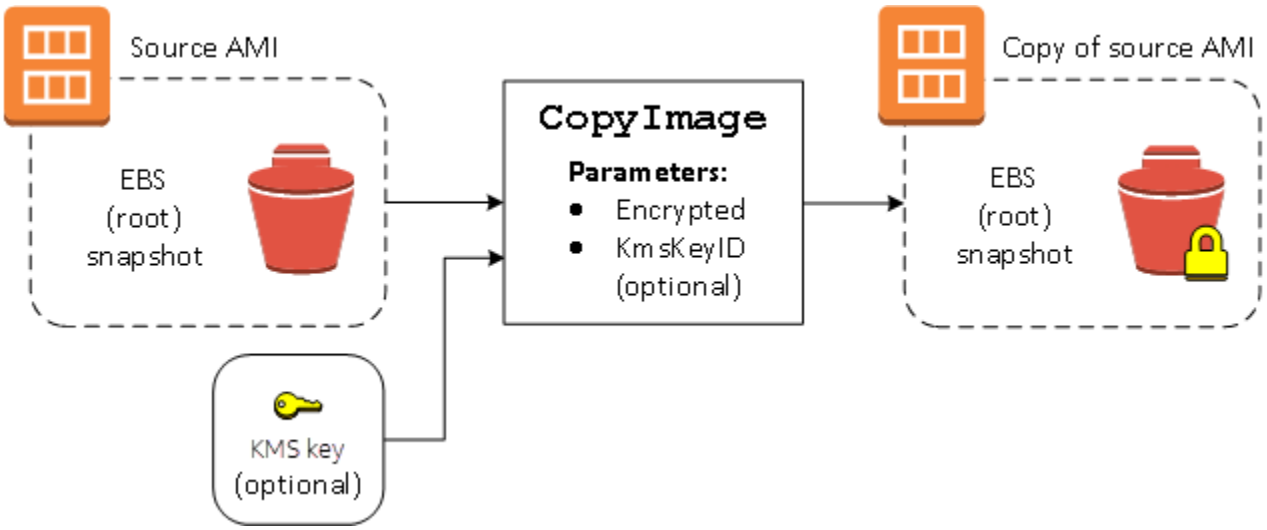
Detaillierte Anweisungen zur Verwendung der Konsole finden Sie unter Kopieren eines AMI.

Verschlüsseln eines unverschlüsselten Images während des Kopierens

In diesem Szenario wird ein von einem unverschlüsselten Stamm-Snapshot unterstütztes AMI in ein AMI mit einem verschlüsselten Stamm-Snapshot kopiert. Die Aktion `CopyImage` wird mit zwei Verschlüsselungsparametern aufgerufen, einschließlich eines vom Kunden verwalteten Schlüssels.

Dadurch ändert sich der Verschlüsselungsstatus des Stamm-Snapshots, sodass das Ziel-AMI durch einen Stamm-Snapshot gestützt wird, der dieselben Daten wie der Quell-Snapshot enthält, aber mit dem angegebenen Schlüssel verschlüsselt wird. Für Sie fallen Speicherkosten für die Snapshots in beiden AMIs sowie Gebühren für Instances an, die Sie von einem der AMIs starten.

> **Note**
>
> Die standardmäßige Aktivierung der Verschlüsselung hat dieselbe Wirkung wie das Setzen des `Encrypted` Parameters auf `true` für alle Snapshots im AMI.



Wenn der `Encrypted`-Parameter festgelegt wird, wird der einzige Snapshot für diese Instance verschlüsselt. Wenn Sie den `KmsKeyId`-Parameter nicht angeben, wird der standardmäßige vom Kunden verwaltete Schlüssel zum Verschlüsseln der Snapshot-Kopie verwendet.

> **Note**
>
> Sie können auch ein Image mit mehreren Snapshots kopieren und den Verschlüsselungsstatus individuell konfigurieren.

Überwachen Sie AMI-Ereignisse mit Amazon EventBridge

Wenn sich der Status eines Amazon Machine Image (AMI) ändert, generiert Amazon EC2 ein Ereignis, das an Amazon gesendet wird EventBridge (früher bekannt als Amazon CloudWatch

Events). Sie können Amazon verwenden EventBridge , um diese Ereignisse zu erkennen und darauf zu reagieren. Sie tun dies, indem Sie Regeln erstellen EventBridge , die als Reaktion auf ein Ereignis eine Aktion auslösen. Sie können beispielsweise eine EventBridge Regel erstellen, die erkennt, wann der AMI-Erstellungsprozess abgeschlossen ist, und dann ein Amazon SNS SNS-Thema aufruft, um Ihnen eine E-Mail-Benachrichtigung zu senden.

Amazon EC2 generiert ein Ereignis, wenn ein AMI einen der folgenden Status eingibt:

- `available`
- `failed`
- `deregistered`
- `disabled`

In der folgenden Tabelle sind die AMI-Vorgänge und die Zustände aufgeführt, in die ein AMI übergehen kann. In der Tabelle gibt Ja die Zustände an, in die das AMI übergehen kann, wenn der entsprechende Vorgang ausgeführt wird.

AMI-Vorgänge	available	failed	deregistered	disabled
CopyImage	Ja	Ja		
CreateImage	Ja	Ja		
CreateRestoreImageTask	Ja	Ja		
DeregisterImage			Ja	
DisableImage				Ja
EnableImage	Ja			
RegisterImage	Ja	Ja		

Ereignisse werden auf bestmögliche Weise ausgegeben.

Themen

- AMI-Ereignisse

- EventBridge Amazon-Regeln erstellen

AMI-Ereignisse

Es gibt vier EC2 AMI State Change-Ereignisse:

- available
- failed
- deregistered
- disabled

Die Ereignisse werden im JSON-Format an den EventBridge Standard-Event-Bus gesendet.

Die folgenden Felder des Ereignisses können verwendet werden, um Regeln zu erstellen, die eine Aktion auslösen:

`"source": "aws.ec2"`

Gibt an, dass das Ereignis aus Amazon EC2 stammt

`"detail-type": "EC2 AMI State Change"`

Identifiziert den Ereignisnamen.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Stellt die folgenden Informationen bereit:

- Die AMI-ID – Wenn Sie ein bestimmtes AMI verfolgen möchten.
- Den Status des AMI (`available`, `failed`, `deregistered` oder `disabled`).

`available`

Im Folgenden finden Sie ein Ereignis, das Amazon EC2 generiert, wenn das AMI nach einem erfolgreichen `CreateImage`-, `CopyImage`-, `RegisterImage`-, `CreateRestoreImageTask`- oder `EnableImage`-Vorgang in den `available`-Status wechselt.

`"State": "available"` zeigt an, dass der Vorgang erfolgreich war.

```
{
```

```
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "available",
        "ErrorMessage": ""
    }
}
```

`failed`

Im Folgenden finden Sie ein Ereignis, das Amazon EC2 generiert, wenn das AMI nach einem fehlgeschlagenen `CreateImage`-, `CopyImage`-, `RegisterImage`- oder `CreateRestoreImageTask`-Vorgang in den `failed`-Status wechselt.

Die folgenden Felder enthalten relevante Informationen:

- `"State": "failed"` – Gibt an, dass ein Vorgang fehlgeschlagen ist.
- `"ErrorMessage": ""` – Gibt den Grund für den fehlgeschlagenen Vorgang an.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "failed",
        "ErrorMessage": "Description of failure"
```

```
    }
}
```

deregistered

Im Folgenden finden Sie ein Ereignis, das Amazon EC2 generiert, wenn das AMI nach einem erfolgreichen `DeregisterImage`-Vorgang in den `deregistered`-Status wechselt. Wenn der Vorgang fehlschlägt, wird kein Ereignis generiert. Jeder Fehler ist sofort bekannt, da `DeregisterImage` ein synchroner Vorgang ist.

`"State": "deregistered"` zeigt an, dass der `DeregisterImage`-Vorgang erfolgreich war.

```
{
    "version": "0",
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "deregistered",
        "ErrorMessage": ""
    }
}
```

disabled

Im Folgenden finden Sie ein Ereignis, das Amazon EC2 generiert, wenn das AMI nach einem erfolgreichen `DisableImage`-Vorgang in den `disabled`-Status wechselt. Wenn der Vorgang fehlschlägt, wird kein Ereignis generiert. Jeder Fehler ist sofort bekannt, da `DisableImage` ein synchroner Vorgang ist.

`"State": "disabled"` zeigt an, dass der `DisableImage`-Vorgang erfolgreich war.

```
{
    "version": "0",
```

```
    "id": "example-9f07-51db-246b-d8b8441bcdf0",
    "detail-type": "EC2 AMI State Change",
    "source": "aws.ec2",
    "account": "012345678901",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-1",
    "resources": ["arn:aws:ec2:us-east-1::image/ami-0123456789example"],
    "detail": {
        "RequestId": "example-9dcc-40a6-aa77-7ce457d5442b",
        "ImageId": "ami-0123456789example",
        "State": "disabled",
        "ErrorMessage": ""
    }
}
```

EventBridge Amazon-Regeln erstellen

Sie können eine EventBridge Amazon-Regel erstellen, die eine Aktion festlegt, die ausgeführt werden soll, wenn ein Ereignis EventBridge empfangen wird, das dem Ereignismuster in der Regel entspricht. Wenn ein Ereignis übereinstimmt, wird das Ereignis an das angegebene Ziel EventBridge gesendet und die in der Regel definierte Aktion ausgelöst.

Ereignismuster haben dieselbe Struktur wie die Ereignisse, mit denen sie übereinstimmen. Ein Ereignismuster stimmt entweder mit einem Ereignis überein oder nicht.

Wenn Sie eine Regel für ein AMI-Statusänderungsereignis erstellen, können Sie die folgenden Felder in das Ereignismuster aufnehmen:

`"source": "aws.ec2“`

Gibt an, dass das Ereignis aus Amazon EC2 stammt

`"detail-type": "EC2 AMI State Change"`

Identifiziert den Ereignisnamen.

`"detail": { "ImageId": "ami-0123456789example", "State": "available", }`

Stellt die folgenden Informationen bereit:

- Die AMI-ID – Wenn Sie ein bestimmtes AMI verfolgen möchten.
- Den Status des AMI (`available`, `failed`, `deregistered` oder `disabled`).

Beispiel: Erstellen Sie eine EventBridge Regel zum Senden einer Benachrichtigung

Im folgenden Beispiel wird eine EventBridge Regel zum Senden einer E-Mail, Textnachricht oder mobilen Push-Benachrichtigung erstellt, wenn sich ein AMI nach erfolgreichem Abschluss des `CreateImage` Vorgangs im `available` Status befindet.

Bevor Sie die EventBridge Regel erstellen, müssen Sie das Amazon SNS SNS-Thema für die E-Mail, Textnachricht oder mobile Push-Benachrichtigung erstellen.

Um eine EventBridge Regel zu erstellen, um eine Benachrichtigung zu senden, wenn ein AMI erstellt wird und sich im **`available`** Status

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:
   a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

      Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
   b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird dieses stets an den standardmäßigen Event Bus Ihres Kontos weitergeleitet.
   c. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
   d. Wählen Sie Weiter aus.
4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:
   a. Wählen Sie als Eventquelle AWS Events oder EventBridge Partnerevents aus.
   b. Bei Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, um mit jedem `EC2 AMI State Change`-Ereignis übereinzustimmen, das generiert wird, wenn ein AMI in den `available`-Status übergeht:

```
{
 "source": ["aws.ec2"],
 "detail-type": ["EC2 AMI State Change"],
 "detail": {"State": ["available"]}
}
```

Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

C. Wählen Sie bei AWS -Service EC2 aus.

D. Bei Event type (Ereignistyp), wählen Sie EC2 AMI State Change (EC2-AMI-Statusänderung) aus.

E. Um die Vorlage anzupassen, wählen Sie Edit pattern (Muster bearbeiten) und nehmen Sie Ihre Änderungen vor, damit sie dem Beispiel-Ereignismuster entsprechen.

ii. Gehen Sie wie folgt vor, um ein benutzerdefiniertes Ereignismuster anzugeben:

A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.

b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.

c. Wählen Sie für Topic (Thema) ein vorhandenes Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge

Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).

e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.
7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

   a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.

   b. Wählen Sie Regel erstellen aus.

Weitere Informationen finden Sie in den folgenden Themen im EventBridge Amazon-Benutzerhandbuch:

- EventBridge Amazon-Veranstaltungen
- EventBridge Amazon-Ereignismuster
- EventBridge Amazon-Regeln

Ein Tutorial zum Erstellen einer Lambda-Funktion und einer EventBridge Regel, die die Lambda-Funktion ausführt, finden Sie unter Tutorial: Den Status einer Amazon EC2 EC2-Instance mithilfe protokollieren EventBridge im AWS Lambda Developer Guide.

Verstehen von AMI-Fakturierungsdaten

Beim Start Ihrer Instances stehen viele Amazon Machine Images (AMIs) zur Auswahl, und sie unterstützen eine Vielzahl von Betriebssystemplattformen und -features. Um zu verstehen, wie sich das AMI, das Sie beim Start Ihrer Instance wählen, auf das Endergebnis Ihrer AWS Rechnung auswirkt, können Sie die zugehörige Betriebssystemplattform und die Abrechnungsinformationen überprüfen. Tun Sie dies, bevor Sie On-Demand oder Spot-Instances starten oder Reserved Instance kaufen.

Hier sind zwei Beispiele dafür, wie die Untersuchung Ihres AMI im Voraus bei der Auswahl des AMI helfen kann, das Ihren Anforderungen am besten entspricht:

- Für Spot-Instances können Sie anhand der AMI-Plattformdetails bestätigen, dass das AMI für Spot-Instances unterstützt wird.

- Beim Kauf eines Reserved Instance können Sie sicherstellen, dass Sie die Betriebssystemplattform (Plattform) auswählen, die den AMI-Plattformdetails zugeordnet ist.

Weitere Informationen zu den Preisen für Instances erhalten Sie unter Amazon EC2 – Preise.

Inhalt

Felder für AMI-Fakturierungsdaten

Die folgenden Felder enthalten Fakturierungsdaten, die einem AMI zugeordnet sind:

Plattformdetails

Die Plattformdetails, die mit dem Fakturierungscode des AMI verknüpft sind. z. B. `Red Hat Enterprise Linux`.

Verwendungsvorgang

Der Betrieb der Amazon-EC2-Instance und der mit dem AMI verknüpfte Abrechnungscode. z. B. `RunInstances:0010`. Der Nutzungsvorgang entspricht der Spalte LineItem/Vorgang in Ihrem AWS Kosten- und Nutzungsbericht (CUR) und in der Preislisten-API.AWS

Sie können diese Felder auf der Seite Instances oder AMIs in der Amazon EC2 EC2-Konsole oder in der Antwort anzeigen, die vom Befehl describe-images oder dem Befehl describe-images zurückgegeben wird. Get-EC2Image

Beispieldaten: Verwendungsvorgang nach Plattform

In der folgenden Tabelle sind einige der Plattformdetails und Nutzungsvorgangswerte aufgeführt, die auf den Instances - oder AMI-Seiten in der Amazon EC2 EC2-Konsole oder in der Antwort angezeigt werden können, die vom Befehl describe-images oder dem Befehl describe-images zurückgegeben wird. Get-EC2Image

Plattformdetails	Verwendungsvorgang 2

Plattformdetails	Verwendungsvorgang 2
Linux/UNIX	RunInstances
Red Hat BYOL Linux	RunInstances:00g0[3]
Red Hat Enterprise Linux	RunInstances:0010
Red Hat Enterprise Linux with HA	RunInstances:1010
Red Hat Enterprise Linux with SQL Server Standard and HA	RunInstances:1014
Red Hat Enterprise Linux with SQL Server Enterprise and HA	RunInstances:1110
Red Hat Enterprise Linux with SQL Server Standard	RunInstances:0014
Red Hat Enterprise Linux with SQL Server Web	RunInstances:0210
Red Hat Enterprise Linux with SQL Server Enterprise	RunInstances:0110
SQL Server Enterprise	RunInstances:0100
SQL Server Standard	RunInstances:0004
SQL Server Web	RunInstances:0200
SUSE Linux	RunInstances:000g
Ubuntu Pro	RunInstances:0g00
Windows	RunInstances:0002

Plattformdetails	Verwendungsvorgang 2
Windows BYOL	RunInstances:0800
Windows with SQL Server Enterprise[1]	RunInstances:0102
Windows with SQL Server Standard[1]	RunInstances:0006
Windows with SQL Server Web[1]	RunInstances:0202

[1] Wenn zwei Softwarelizenzen mit einem AMI verknüpft sind, werden im Feld Plattformdetails beide angezeigt.

[2] Wenn Sie Spot-Instances ausführen, kann sich der in lineitem/OperationIhrem AWS Kosten- und Nutzungsbericht angegebene Wert von dem hier aufgeführten Wert für den Nutzungsvorgang unterscheiden. Wenn beispielsweise `lineitem/Operation` angezeigt wird, bedeutet dies`RunInstances:0010:SV006`, dass Amazon EC2 Red Hat Enterprise Linux Spot Instance-Stunde in der Region USA Ost (Nord-Virginia) in Zone 6 ausführt.

[3] Dies wird wie RunInstances (Linux/UNIX) in Ihren Nutzungsberichten angezeigt.

Informationen zur AMI-Fakturierung und Verwendung finden

In der Konsole Amazon EC2 können Sie die AMI-Fakturierungsdaten auf der Seite AMIs oder auf der Seite Instances anzeigen. Sie können Rechnungsinformationen auch mithilfe des Instanz-Metadatendienstes AWS CLI oder des Instanz-Metadatendienstes finden.

Die folgenden Felder können Ihnen helfen, AMI-Gebühren auf Ihrer Rechnung zu überprüfen:

- Plattformdetails
- Verwendungsvorgang
- AMI-ID

AMI-Fakturierungsdaten (Konsole) finden

Befolgen Sie diese Schritte, um AMI-Fakturierungsdaten in der Konsole Amazon EC2 anzuzeigen:

Schlagen Sie AMI-Fakturierungsdaten auf der AMIS-Seite nach

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich AMIs und dann ein AMI aus.
3. Überprüfen Sie auf der Registerkarte Details die Werte für Platform details (Plattformdetails) und Usage operation (Verwendungsvorgang).

Suchen Sie auf der Seite Instances nach AMI-Fakturierungsdaten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann eine Instance aus.
3. Überprüfen Sie auf der Registerkarte Details (oder auf der Registerkarte Description (Beschreibung), wenn Sie die vorherige Version der Konsole verwenden) die Werte für Platform details (Plattformdetails) und den Usage operation (Verwendungsvorgang).

Felder für AMI-Fakturierungsdaten (AWS CLI)

Um die AMI-Rechnungsinformationen mithilfe von zu finden AWS CLI, müssen Sie die AMI-ID kennen. Wenn Sie die AMI-ID nicht kennen, können Sie sie mit dem Befehl describe-instances von der Instance abrufen.

Finden der AMI-ID

Wenn Sie die Instance-ID kennen, können Sie die AMI-ID für die Instance mit dem Befehl describe-instances abrufen.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

In der Ausgabe wird die AMI-ID im Feld `ImageId` angegeben.

```
..."Instances": [
{
    "AmiLaunchIndex": 0,
    "ImageId": "ami-0123456789EXAMPLE",
    "InstanceId": "i-123456789abcde123",
    ...
}]
```

Finden der AMI-Fakturierungsdaten

Wenn Sie die AMI-ID kennen, können Sie den Befehl describe-images verwenden, um Details zum AMI-Plattform- und Verwendungsvorgang abzurufen:

```
$ aws ec2 describe-images --image-ids ami-0123456789EXAMPLE
```

Die folgende Beispielausgabe zeigt die Felder `PlatformDetails` und `UsageOperation`. In diesem Beispiel ist die ami-0123456789EXAMPLE-Plattform `Red Hat Enterprise Linux` und der Verwendungsvorgangs- und der Abrechnungscode ist `RunInstances:0010`.


```
{
    "Images": [
        {
            "VirtualizationType": "hvm",
            "Description": "Provided by Red Hat, Inc.",
            "Hypervisor": "xen",
            "EnaSupport": true,
            "SriovNetSupport": "simple",
            "ImageId": "ami-0123456789EXAMPLE",
            "State": "available",
            "BlockDeviceMappings": [
                {
                    "DeviceName": "/dev/sda1",
                    "Ebs": {
                        "SnapshotId": "snap-111222333444aaabb",
                        "DeleteOnTermination": true,
                        "VolumeType": "gp2",
                        "VolumeSize": 10,
                        "Encrypted": false
                    }
                }
            ],
            "Architecture": "x86_64",
            "ImageLocation": "123456789012/RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-
GP2",
            "RootDeviceType": "ebs",
            "OwnerId": "123456789012",
            "PlatformDetails": "Red Hat Enterprise Linux",
            "UsageOperation": "RunInstances:0010",
            "RootDeviceName": "/dev/sda1",
            "CreationDate": "2019-05-10T13:17:12.000Z",
```

```
            "Public": true,
            "ImageType": "machine",
            "Name": "RHEL-8.0.0_HVM-20190618-x86_64-1-Hourly2-GP2"
        }
    ]
}
```

Überprüfen Sie die AMI-Gebühren auf Ihrer Rechnung

Um sicherzustellen, dass Ihnen keine ungeplanten Kosten entstehen, können Sie überprüfen, ob die Rechnungsinformationen für eine Instance in Ihrem AWS Kosten- und Nutzungsbericht (CUR) mit den Abrechnungsinformationen übereinstimmen, die dem AMI zugeordnet sind, das Sie zum Starten der Instance verwendet haben.

Um die Fakturierungsdaten zu bestätigen, suchen Sie die Instance-ID in Ihrem CUR und überprüfen Sie den entsprechenden Wert in der Spalte `lineitem/Operation`. Der Wert sollte mit dem Wert für Usage operation (Verwendungsvorgang) übereinstimmen, der dem AMI zugeordnet ist.

Zum Beispiel hat das AMI `ami-0123456789EXAMPLE` die folgenden Fakturierungsdaten:

- Plattformdetails = `Red Hat Enterprise Linux`
- Verwendungsvorgang = `RunInstances:0010`

Wenn Sie eine Instance mit diesem AMI gestartet haben, können Sie die Instance-ID in Ihrem CUR finden und den entsprechenden Wert in der Spalte `lineitem/Operation` überprüfen. In diesem Beispiel sollte der Wert `RunInstances:0010` sein.

AMI-Kontingente

Die folgenden Kontingente gelten für das Erstellen und Freigeben von AMIs. Die Kontingente gelten pro AWS-Region.

Kontingentname	Beschreibung	Standardkontingent pro Region
AMIs	Die maximal zulässige Anzahl öffentlicher und privater AMIs	50 000

Kontingentname	Beschreibung	Standardkontingent pro Region
	pro Region. Dazu gehören verfügbare, ausstehende und deaktivierte AMIs sowie AMIs im Papierkorb.	
Öffentliche AMIs	Die maximal zulässige Anzahl öffentlicher AMIs, einschließlich öffentlicher AMIs im Papierkorb, pro Region.	5
Freigeben von AMIs	Die maximale Anzahl von Entitäten (Organisationen, Organisationseinheiten (OUs) und Konten), mit denen ein AMI in einer Region gemeinsam genutzt werden kann. Beachten Sie, dass bei Freigabe eines AMI für eine Organisation oder Organisationseinheit die Anzahl der Konten in der Organisation oder Organisationseinheit nicht auf das Kontingent angerechnet wird.	1.000

Wenn Sie Ihre Kontingente überschreiten und weitere AMIs erstellen oder freigeben möchten, können Sie Folgendes tun:

- Wenn Sie Ihr Gesamtkontingent an AMIs oder öffentlichen AMIs überschreiten, sollten Sie erwägen, nicht verwendete Images abzumelden.
- Wenn Sie Ihr Kontingent an öffentlichen AMIs überschreiten, sollten Sie eine oder mehrere öffentliche AMIs als privat einstufen.
- Wenn Sie Ihr AMI-Freigabekontingent überschreiten, sollten Sie erwägen, Ihre AMIs für eine Organisation oder Organisationseinheit anstelle von separaten Konten freizugeben.

- Beantragen Sie eine Kontingenterhöhung für AMIs.

Beantragung einer Kontingenterhöhung für AMIs

Wenn Sie mehr als das standardmäßige Kontingent für AMIs benötigen, können Sie eine Kontingenterhöhung beantragen.

So beantragen Sie eine Kontingenterhöhung für AMIs

1. Öffnen Sie die Service-Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/.
2. Wählen Sie im Navigationsbereich AWS -Services.
3. Wählen Sie Amazon Elastic Compute Cloud (Amazon EC2) aus der Liste aus oder geben Sie den Namen des Service in das Suchfeld ein.
4. Wählen Sie das AMI-Kontingent, um eine Erhöhung zu beantragen. Sie können folgende AMI-Kontingente auswählen:
   - AMIs
   - Öffentliche AMIs
   - Freigeben von AMIs
5. Wählen Sie Kontingenterhöhung anfordern.
6. Geben Sie unter Change quota value (Kontingentwert ändern) den neuen Kontingentwert ein und wählen Sie dann Request (Anforderung) aus.

Um ausstehende oder kürzlich genehmigte Anfragen anzuzeigen, wählen Sie im Navigationsbereich die Option Dashboard . Wählen Sie für ausstehende Anfragen den Status der Anfrage, um die Anfrage zu öffnen. Der Anfangsstatus einer Anfrage ist Pending (Ausstehend). Nachdem sich der Status in Quota requested (Kontingent beantragt) geändert hat, wird Ihnen die Fallnummer unter Support Center case number (Support-Center-Fallnummer) angezeigt. Wählen Sie die Fallnummer, um das Ticket für Ihre Anfrage zu öffnen.

Nachdem die Anfrage genehmigt wurde, wird Applied quota value (Angewandter Kontingentwert) für das Kontingent auf den neuen Wert eingestellt.

Weitere Informationen zu diesem Service finden Sie im Benutzerhandbuch für Service Quotas.

Amazon EC2-Instances

Bevor Sie eine produktive Umgebung starten, sollten Sie unbedingt die folgenden Fragen beantworten.

F:. Welcher Instance-Typ ist für meine Anforderungen am besten geeignet?

In Amazon EC2 können Sie zwischen verschiedenen Instance-Typen wählen; diese unterscheiden sich in Bezug auf CPU, Arbeitsspeicher, Speicher und Netzwerkkapazität, die Sie zur Ausführung Ihrer Anwendungen verwenden können. Weitere Informationen finden Sie unter Amazon EC2-Instance-Typen.

F.: Welche Kaufoption ist für meine Anforderungen am besten geeignet?

Amazon EC2 unterstützt On-Demand-Instances (den Standard), Spot-Instances, und Reserved Instances. Weitere Informationen finden Sie unter Instance-Kaufoptionen.

F.: Welche Art von Root-Volume ist für meine Anforderungen geeignet?

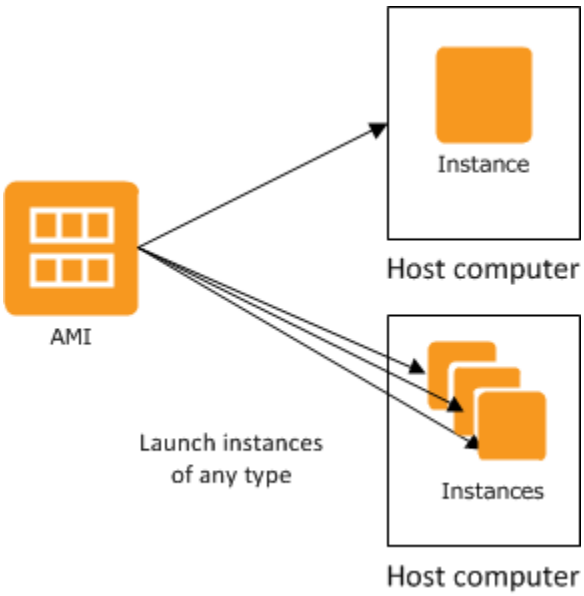
Jede Instance ist entweder Amazon EBS-gestützt oder Instance-Speicher-gestützt. Wählen Sie ein AMI danach aus, welche Art von Root-Volume Sie benötigen. Weitere Informationen finden Sie unter Speicher für das Root-Gerät.

F. Kann ich eine Flotte von EC2-Instances und PCs in meiner hybriden Umgebung per Fernzugriff verwalten?

AWS Systems Manager ermöglicht es Ihnen, die Konfiguration Ihrer Amazon EC2 EC2-Instances und Ihrer lokalen Instances und virtuellen Maschinen (VMs) in Hybridumgebungen, einschließlich VMs von anderen Cloud-Anbietern, remote und sicher zu verwalten. Weitere Informationen finden Sie im AWS Systems Manager -Benutzerhandbuch.

Instances und AMIs

Ein Amazon Machine Image (AMI) ist eine Vorlage, die eine Softwarekonfiguration enthält (z. B. ein Betriebssystem, einen Anwendungsserver und Anwendungen). Über ein AMI starten Sie eine Instance. Hierbei handelt es sich um eine Kopie des AMI, die als virtueller Server in der Cloud ausgeführt wird. Sie können auch mehrere Instances eines AMI starten, wie in der folgenden Abbildung gezeigt.



Ihre Instances werden so lange ausgeführt, bis Sie sie in den Ruhezustand versetzen, sie beenden oder bis sie ausfallen. Wenn eine Instance ausfällt, können Sie eine neue aus dem AMI starten.

Instances

Eine Instance ist ein virtueller Server in der Cloud. Ihre Konfiguration zur Startzeit ist eine Kopie des AMI, das Sie beim Starten der Instance angegeben haben.

Sie können verschiedene Instance-Typen eines einzelnen AMI starten. Mit dem Instance-Typ wird im Wesentlichen die Hardware des Host-Computers bestimmt, der für Ihre Instance verwendet wird. Jeder Instance-Typ bietet andere Fähigkeiten in Bezug auf Datenverarbeitung und Arbeitsspeicher. Wählen Sie einen Instance-Typ basierend auf der Größe des benötigten Speichers und der Datenverarbeitungsleistung für die Anwendung oder die Software aus, die auf der Instance ausgeführt werden soll. Detaillierte Spezifikationen für Instance-Typen finden Sie unter Spezifikationen im Amazon EC2 Instance Types Guide. Preisinformationen finden Sie unter Amazon EC2 On-Demand-Preise.

Wenn Sie eine Instance launchen, sieht sie wie ein herkömmlicher Host aus, und Sie können mit ihr wie mit jedem anderen Computer arbeiten. Sie haben die vollständige Kontrolle über Ihre Instances. Mit dem Befehl sudo führen Sie Befehle aus, die Root-Berechtigungen erfordern.

In Ihrem AWS Konto ist die Anzahl der Instances, die Sie ausführen können, begrenzt. Weitere Informationen zu dieser Begrenzung und zur Erhöhung dieser Anzahl erhalten Sie in den häufig gestellten Fragen (FAQ) zu Amazon EC2 unter Wie viele Instances kann ich in Amazon Amazon EC2ausführen.

Speicher für Ihre Instance

Das Root-Gerät Ihrer Instance enthält das Image, das zum Starten der Instance verwendet wird. Das Stamm-Gerät ist entweder ein Amazon Elastic Block Store (Amazon EBS)-Volume oder ein Instance-Speicher-Volume. Weitere Informationen finden Sie unter Root-Volume der Amazon-EC2-Instance.

Ihre Instance enthält möglicherweise lokale Speicher-Volumes, die sogenannten Instance-Speicher-Volumes, die Sie beim Start der Instance mit Blockgerät-Zuweisung konfigurieren können. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen. Nach dem Hinzufügen dieser Volumes und Zuweisen auf Ihrer Instance können sie gemountet und verwendet werden. Wenn Ihre Instance ausfällt, angehalten oder beendet wird, gehen die Daten auf diesen Volumes verloren. Daher sind diese Volumes am besten für temporäre Daten geeignet. Um wichtige Daten sicher zu halten, sollten Sie eine Replikationsstrategie über mehrere Instances hinweg verwenden oder Ihre persistenten Daten in Amazon S3 oder Amazon EBS Volumes speichern. Weitere Informationen finden Sie unter Speicheroptionen für Ihre Amazon-EC2-Instances.

Bewährte Methoden für die Gewährleistung der Sicherheit

- Verwenden Sie AWS Identity and Access Management (IAM), um den Zugriff auf Ihre AWS Ressourcen, einschließlich Ihrer Instanzen, zu kontrollieren. Weitere Informationen finden Sie unter Identity and Access Management für Amazon EC2.
- Beschränken Sie den Zugriff, indem Sie ausschließlich vertrauenswürdige Hosts und Netzwerke auf Ihre Instance zugreifen lassen. Sie können beispielsweise den SSH-Zugriff einschränken, indem Sie eingehenden Datenverkehr auf Port 22 beschränken. Weitere Informationen finden Sie unter Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances.
- Überprüfen Sie regelmäßig die Regeln in Ihren Sicherheitsgruppen und wenden Sie unbedingt das Prinzip der geringstmöglichen Berechtigungen an — öffnen Sie ausschließlich erforderliche Berechtigungen. Sie können zudem verschiedene Sicherheitsgruppen für Instances mit unterschiedlichen Sicherheitsanforderungen erstellen. Ziehen Sie das Erstellen einer Bastion-Sicherheitsgruppe in Erwägung, die externe Anmeldungen erlaubt, und fassen Sie die restlichen Instances in einer Gruppe zusammen, die keine externen Anmeldungen erlaubt.
- Deaktivieren Sie passwortbasierte Anmeldungen für Instances, die über Ihr AMI gestartet werden. Passwörter können entschlüsselt oder geknackt werden und stellen daher ein Sicherheitsrisiko dar. Weitere Informationen finden Sie unter Deaktivieren von passwortbasierten Fernanmeldungen für den Stammbenutzer. Weitere Informationen zum sichereren Teilen von AMIs finden Sie unter Gemeinsame AMIs.

Stoppen und Beenden von Instances

Sie können eine laufende Instance jederzeit anhalten oder beenden.

Anhalten einer Instance

Wenn eine Instance angehalten wird, führt sie einen normalen Shutdown durch und wechselt in den Zustand `stopped`. Alle ihre Amazon EBS-Volumes bleiben angehängt. Sie können die Instance zu einem späteren Zeitpunkt erneut starten.

Während die Instance angehalten ist, wird Ihnen keine zusätzlichen Instance-Nutzung berechnet. Ihnen wird jeder Übergang von einem angehaltenen Zustand in einen laufenden Zustand in Rechnung gestellt. Wenn sich der Instance-Typ geändert hat, während die Instance gestoppt wurde, wird Ihnen der Tarif für den neuen Instance-Typ nach dem Start der Instance in Rechnung gestellt. Ihnen wird auch der zugehörige Amazon EBS-Speicher für Ihre Instance in Rechnung gestellt, einschließlich des Root-Geräte-Volumes.

Wenn sich eine Instance in einem angehaltenen Zustand befindet, können Sie Amazon EBS-Volumes hinzufügen oder entfernen. Sie können ein AMI auch über die Instance erstellen und den Kernel, RAM-Datenträger und Instance-Typ ändern.

Beenden einer Instance

Wenn eine Instance beendet wird, führt die Instance den normalen Prozess zum Herunterfahren aus. Der Root-Gerät-Volume wird standardmäßig gelöscht, aber alle angefügten Amazon EBS-Volumes bleiben standardmäßig erhalten, abhängig von der Einstellung für das `deleteOnTermination`-Attribut des jeweiligen Volumes. Die Instance selbst wird ebenfalls gelöscht und kann zu einem späteren Zeitpunkt nicht erneut gestartet werden.

Um versehentliches Beenden einer Instance zu vermeiden, kann das Beenden von Instances deaktiviert werden. Beachten Sie dabei, dass das `disableApiTermination`-Attribut für die Instance auf `true` festgelegt sein muss. Um das Verhalten des Shutdown einer Instance zu kontrollieren, wie beispielsweise `shutdown -h` in Linux oder `shutdown` in Windows, setzen Sie das `instanceInitiatedShutdownBehavior`-Attribut der Instances entweder auf `stop` oder `terminate`. Instances mit Amazon EBS-Volumes, deren Root-Gerät standardmäßig auf `stop` festgelegt ist, und Instances mit Instance-Speicher-Root-Geräten werden nach einem Instance-Shutdown immer beendet.

Weitere Informationen finden Sie unter Instance-Lebenszyklus.

> **Note**
>
> Für einige AWS Ressourcen, wie Amazon EBS-Volumes und Elastic IP-Adressen, fallen unabhängig vom Status der Instance Gebühren an. Weitere Informationen finden Sie unter Unerwartete Gebühren vermeiden im AWS Billing -Benutzerhandbuch. Weitere Information zu Amazon EBS-Kosten finden Sie unter Amazon EBS – Preise.

AMIs

Amazon Web Services (AWS) veröffentlicht Amazon Machine Images (AMIs), die gängige Softwarekonfigurationen für den öffentlichen Gebrauch enthalten. Darüber hinaus haben Mitglieder der AWS Entwickler-Community ihre eigenen benutzerdefinierten AMIs veröffentlicht. Sie können auch Ihre eigenen benutzerdefinierten AMIs erstellen. Auf diese Weise können Sie schnell und einfach neue Instances starten, die alles bieten, was Sie benötigen. Wenn es sich bei Ihrer Anwendung beispielsweise um eine Website oder einen Webservice handelt, kann Ihr AMI einen Webserver, den dazugehörigen statischen Inhalt und den Code für die dynamischen Seiten enthalten. Nach dem Start einer Instance über dieses AMI und Ihres Webservers kann Ihre Anwendung Anfragen akzeptieren.

Alle AMIs sind in zwei Kategorien unterteilt: Entweder Amazon EBS-gestützt, was bedeutet, dass das Root-Gerät für eine Instance, die über ein AMI gestartet wurde, ein Amazon EBS-Volume ist oder Instance Store-Backed, was bedeutet, dass das Root-Gerät für eine Instance, die über ein AMI gestartet wurde, ein Instance-Speicher-Volume ist, der aus einer in Amazon S3 gespeicherten Vorlage erstellt wurde.

Die Beschreibung eines AMI bestimmt den Typ eines Root-Geräts (entweder `ebs` oder `instance store`). Dies ist wichtig, weil zwischen den jeweiligen Möglichkeiten mit den AMI-Typen erhebliche Unterschiede bestehen. Weitere Informationen zu diesen Unterschieden erhalten Sie unter Speicher für das Root-Gerät.

Sie können ein AMI abmelden (Aufheben der Registrierung), wenn Sie es nicht mehr benötigen. Nachdem Sie ein AMI abgemeldet haben, können Sie es nicht mehr verwenden, um neue Instances zu starten. Vorhandene Instances, die über das AMI gestartet wurden, werden davon nicht beeinflusst. Wenn Sie also auch mit den Instances fertig sind, die von diesen AMIs gestartet werden, sollten Sie sie daher beenden.

Amazon EC2-Instance-Typen

Wenn Sie eine Instance starten, bestimmt der von Ihnen angegebene Instance-Typ die Hardware der Host-Computer für die Instance. Jeder Instance-Typ bietet unterschiedliche Rechenleistung, Arbeitsspeicher- und Speicher-Kapazität und wird abhängig von diesen Eigenschaften in Instance-Familien eingeordnet. Wählen Sie einen Instance-Typ den Anforderungen der Anwendung oder Software entsprechend aus, die Sie in Ihrer Instance ausführen möchten.

Einige Ressourcen des Host-Computers, wie z. B. CPU, Arbeitsspeicher und Instance-Speicher, werden von Amazon EC2 einer bestimmten Instance zugewiesen. Amazon EC2 teilt andere Ressourcen des Host-Computers, z. B. das Netzwerk und das Datenträgersubsystem, zwischen mehreren Instances. Wenn die Instances eines Host-Computers jeweils möglichst viele Ressourcen nutzen möchten, wird die Ressource gleichmäßig aufgeteilt. Wenn eine Ressource jedoch nicht voll ausgelastet ist, kann eine Instance einen höheren Anteil der verfügbaren Ressource nutzen.

Jeder Instance-Typ stellt Leistung von einer gemeinsamen Ressource je nach Anforderung bereit. Instance-Typen mit hoher I/O-Leistung wird beispielsweise ein höherer Anteil der gemeinsamen Ressourcen zugewiesen. Durch die Zuweisung eines größeren Anteils gemeinsamer Ressourcen werden außerdem Abweichungen der I/O-Leistung verringert. Für die meisten Anwendungen ist mittlere I/O-Leistung vollkommen ausreichend. Für Anwendungen, die mehr oder einheitlichere I/O-Leistung erfordern, sollten Sie jedoch einen Instance-Typ mit höherer I/O-Leistung in Erwägung ziehen.

Inhalt

Verfügbare Instance-Typen

Amazon EC2 bietet eine große Auswahl an Instance-Typen, die für verschiedene Anwendungsfälle optimiert sind. Die Instance-Typen umfassen unterschiedliche Kombinationen von CPU-, Arbeitsspeicher-, Speicher- und Netzwerkkapazitäten und geben Ihnen die nötige Flexibilität, um die richtige Mischung von Ressourcen für Ihre Anwendungen zu wählen. Jeder Instance-Typ umfasst eine oder mehrere Instance-Größen, sodass Sie Ihre Ressourcen an die Anforderungen Ihres Ziel-Workloads anpassen können. Weitere Informationen zu Funktionen und Anwendungsfällen finden Sie unter Details zu Amazon EC2 EC2-Instance-Typen.

Benennungskonventionen für Instance-Typen

Die Namen basieren auf Instanzfamilie, Generation, Prozessorfamilie, Funktionen und Größe. Weitere Informationen finden Sie unter Namenskonventionen im Amazon EC2 Instance Types Guide.

Suchen eines -Instance-Typs

Informationen darüber, welche Instance-Typen Ihren Anforderungen entsprechen, wie z. B. unterstützte Regionen, Rechenressourcen oder Speicherressourcen, finden Sie unter Suchen eines Amazon EC2-Instance-Typs Amazon EC2 EC2-Instance-Typenspezifikationen im Amazon EC2 EC2-Instance-Types-Handbuch.

Instances der aktuellen Generation

- Universell einsetzbar: M5 | M5a | M5ad | M5d | M5dn | M5Zn | M6a | M6g | M6g | M6gd | M6i | M6id | M6idn | M6in | M7in | M7a | M7g | M7gd | M7i | M7i-Flex | Mac1 | Mac2 | Mac2-m2 | Mac2-M2Pro | T2 | T2 3 | T3a | T4g
- Computeroptimiert: C5 | C5a | C5ad | C5d | C5n | C6a | C6g | C6GD | C6Gn | C6i | C6id | C6in | C7a | C7g | C7GD | C7Gn | C7i | C7i-Flex
- Speicheroptimiert: R5 | R5a | R5ad | R5b | R5d | R5dn | R5n | R6a | R6g | R6gd | R6i | R6idn | R6in | R6id | R7a | R7g | R7g | R7gd | R7i | R7iz | U-3 tb1 | U-6 tb1 | U-9 tb1 | U-12 tb1 | U-18 TB1 | U-24 TB1 | U7i-12 TB | U7-in-16 TB | U7-in-24 TB | U7-in-32 TB | X1 | X2GD | X2IDN | X2iEDN | X2IEZN | X1e | z1d
- Speicheroptimiert: D2 | D3 | D3en | H1 | I3 | i3EN | i4G | i4I | i4GN | IS4Gen
- Beschleunigtes Rechnen: DL1 | DL2q | F1 | G4ad | G4dn | G5 | G5g | G6 | Gr6 | Inf1 | Inf2 | P2 | P3 | P3dn | P4d | P4de | P5 | Trn1 | Trn1n | VT1
- Hochleistungsrechnen: HPC6a | HPC6id | HPC7a | HPC7G

Instances der vorherigen Generation

- Allgemeiner Zweck: A1 | M1 | M2 | M3 | M4 | T1
- Für Berechnungen optimiert: C1 | C3 | C4
- Speicheroptimiert: R3 | R4
- Speicheroptimiert: I2
- Beschleunigtes Rechnen: G3

Hardwarespezifikationen

Detaillierte Spezifikationen für Instance-Typen finden Sie unter Spezifikationen im Amazon EC2 Instance Types Guide. Preisinformationen finden Sie unter Amazon EC2 On-Demand-Preise.

Um die richtigen Instance-Typen für Ihre Anforderungen zu bestimmen, empfehlen wir, eine Instance zu starten und Ihre eigene Benchmarkanwendung zu verwenden. Da Instances pro Sekunde abgerechnet werden, können Sie mehrere Instance-Typen bequem und ohne großen Kostenaufwand testen, bevor Sie eine Entscheidung treffen. Falls sich Ihre Anforderungen ändern, können Sie selbst nach der Entscheidung den Instance-Typ anpassen. Weitere Informationen finden Sie unter Ändern des Instance-Typs.

Intel-Prozessorfeatures

Amazon EC2-Instances, die auf Intel-Prozessoren laufen, können die folgenden Features enthalten. Nicht alle der folgenden Prozessorfeatures werden von allen Instance-Typen unterstützt. Detaillierte Informationen darüber, welche Funktionen für jeden Instance-Typ verfügbar sind, finden Sie unter Amazon EC2 EC2-Instance-Typen.

- Intel AES New Instructions (AES-NI) – Der Befehlssatz für Intel AES-NI-Verschlüsselung verbessert den Originalalgorithmus Advanced Encryption Standard (AES) in Hinblick auf schnelleren Datenschutz und bessere Sicherheit. Alle EC2-Instances der aktuellen Generation unterstützten dieses Prozessorfeature.
- Intel Advanced Vector Extensions (Intel AVX, Intel AVX2 und Intel AVX-512) – Intel AVX und Intel AVX2 sind Erweiterungen des 256-Bit-Befehlssatzes und Intel AVX-512 ist eine Erweiterung des 512-Bit-Befehlssatzes für Anwendungen mit vielen Gleitkommaoperationen (FP). Intel AVX-Befehle verbessern die Leistung von Anwendungen für beispielsweise Image-, Audio- und Videobearbeitung, wissenschaftliche Simulationen, Finanzanalysen sowie 3D-Modellierung und

-Analysen. Diese Features stehen nur für Instances zur Verfügung, die mit HVM-AMIs gestartet wurden.

- Intel Turbo Boost Technology — Prozessoren der Intel Turbo Boost Technology führen Kerne automatisch schneller als die Basisbetriebsfrequenz aus.
- Intel Deep Learning Boost (Intel DL Boost) — beschleunigt KI-Deep-Learning-Anwendungsfälle. Intel Xeon Scalable-Prozessoren der 2. Generation erweitern Intel AVX-512 mit einer neuen Vector Neural Network Instruction (VNNI/INT8), welche die Deep-Learning-Inferenzleistung im Vergleich zur vorherigen Generation von Intel-Xeon-Scalable-Prozessoren (mit FP32) deutlich übertrifft. Dies ist unter anderem für die Bereiche Image-Erkennung/-segmentierung, Objekterkennung, Spracherkennung, Sprachübersetzung, Empfehlungssysteme und Reinforcement Learning und mehr vorgesehen. VNNI ist möglicherweise nicht mit allen Linux-Distributionen kompatibel.

  Die folgenden Instances unterstützen VNNI: `M5n`, `R5n`, `M5dn`, `M5zn`, `R5b`, `R5dn`, `D3`, `D3en` und `C6i`. Die Instances `C5` und `C5d` unterstützen VNNI nur für `12xlarge`-, `24xlarge`- und `metal`-Instances.

Die brancheninternen Namenskonventionen für 64-Bit-CPUs können zu Verwirrung führen. Prozessorhersteller Advanced Micro Devices (AMD) stellte die erste kommerziell erfolgreiche 64-Bit-Architektur basierend auf dem x86-Befehlssatz von Intel vor. Entsprechend wird die Architektur gemeinläufig als „AMD64“ bezeichnet, unabhängig vom Prozessorhersteller. Windows und diverse Linux-Distributionen folgen dieser Konvention. Darum wird in den internen Systeminformationen einer Instance, auf der Ubuntu oder Windows ausgeführt wird, für die CPU-Architektur „AMD64“ angegeben, obwohl die Instances auf Intel-Hardware ausgeführt werden.

AWS Graviton-Prozessoren

AWS Graviton ist eine Prozessorfamilie, die darauf ausgelegt ist, das beste Preis-Leistungs-Verhältnis für Ihre Workloads zu bieten, die auf Amazon EC2 EC2-Instances ausgeführt werden.

Weitere Informationen finden Sie unter Erste Schritte mit Graviton.

AWS Trainium

Von AWS Trainium betriebene Instances wurden speziell für leistungsstarke, kostengünstige Deep-Learning-Schulungen entwickelt. Sie können diese Instances verwenden, um natürliche Sprachverarbeitung, Computer Vision und Empfehlungsmodelle zu trainieren, die in einer Vielzahl von Anwendungen eingesetzt werden, z. B. Spracherkennung, Empfehlung, Betrugserkennung

und Bild- und Videoklassifizierung. Verwenden Sie Ihre vorhandenen Workflows in gängigen ML-Frameworks wie PyTorch und TensorFlow.

AWS Inferenz

Von AWS Inferentia betriebene Instances wurden entwickelt, um maschinelles Lernen zu beschleunigen. Sie bieten Inferenz für maschinelles Lernen mit hoher Leistung und geringer Latenz. Diese Instances sind für die Bereitstellung von Deep-Learning-(DL)-Modellen für Anwendungen wie natürliche Sprachverarbeitung, Objekterkennung und -klassifizierung, Inhaltspersonalisierung und -filterung sowie Spracherkennung optimiert.

Es gibt eine Vielzahl von Möglichkeiten für den Einstieg:

- Verwenden Sie SageMaker, einen vollständig verwalteten Dienst, der der einfachste Weg ist, mit Modellen für maschinelles Lernen zu beginnen. Weitere Informationen finden Sie unter Erste Schritte mit SageMaker im Amazon SageMaker Developer Guide.
- Starten Sie eine Inf1- oder Inf2-Instance mit dem Deep-Learning-AMI. Weitere Informationen finden Sie unter AWS Inferentia with DLAMI im AWS Deep Learning AMI -Developer-Handbuch.
- Starten Sie eine Inf1- oder Inf2-Instance mit Ihrem eigenen AMI und installieren Sie den AWS Neuron SDK, mit dem Sie Deep-Learning-Modelle für AWS Inferentia kompilieren, ausführen und profilieren können.
- Starten Sie eine Container-Instance mit einer Inf1- oder Inf2-Instance und einem Amazon-ECS-optimierten AMI. Weitere Informationen finden Sie unter Amazon Linux 2-(Inferentia)-AMIs im Amazon Elastic Container Service Developer Guide.
- Erstellen Sie einen Amazon EKS-Cluster mit Knoten, auf denen Inf1-Instances ausgeführt werden. Weitere Informationen finden Sie unter Inferentia-Support im Amazon EKS-Benutzerhandbuch.

AMI-Virtualisierungstypen

Der Virtualisierungstyp Ihrer Instance wird durch das AMI bestimmt, das zum Starten der Instance verwendet wird. Instance-Typen der aktuellen Generation unterstützen nur eine Hardware Virtual Machine (HVM). Einige Instance-Typen der vorherigen Generation unterstützen paravirtual (PV) und einige AWS Regionen unterstützen PV-Instances. Weitere Informationen finden Sie unter AMI-Virtualisierungstypen.

Um optimale Leistung zu erzielen, empfehlen wir die Verwendung eines HVM-AMI. Außerdem sind HVM-AMIs erforderlich, um die verbesserte Netzwerkleistung nutzen zu können. Die HVM-

Virtualisierung nutzt die von der Plattform bereitgestellte hardwaregestützte Technologie. AWS Mit HVM-Virtualisierung kann die VM wie auf einer nativen Hardwareplattform ausgeführt werden. Es werden jedoch weiterhin PV-Netzwerk- und Speicher-Treiber für bestmögliche Leistung eingesetzt.

Suchen eines Amazon EC2-Instance-Typs

Bevor Sie eine Instance starten können, müssen Sie einen Instance-Typ auswählen, der verwendet werden soll. Der von Ihnen gewählte Instance-Typ hängt unter Umständen von den Ressourcen ab, die Ihre Workload benötigt, z. B. Computing-, Speicher- oder Storage-Ressourcen. Es kann von Vorteil sein, mehrere Instance-Typen zu identifizieren, die zu Ihrer Workload passen, und deren Leistung in einer Testumgebung zu bewerten. Es gibt keinen Ersatz für die Messung der Leistung Ihrer Anwendung unter Last.

Wenn Sie bereits EC2-Instances ausführen, können Sie hier Empfehlungen AWS Compute Optimizer zu den Instance-Typen abrufen, die Sie verwenden sollten, um die Leistung zu verbessern, Geld zu sparen oder beides zu tun. Weitere Informationen finden Sie unter the section called “Für bestehende Workloads”.

Aufgaben

- Suchen eines Instance-Typs mithilfe der Konsole
- Suchen Sie einen Instanztyp mithilfe der AWS CLI

Suchen eines Instance-Typs mithilfe der Konsole

Mit der Amazon EC2-Konsole finden Sie einen Instance-Typ, der Ihren Anforderungen entspricht.

So suchen Sie einen Instance-Typ mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der Sie Ihre Instances starten möchten. Sie können unabhängig von Ihrem Standort jede verfügbare Region auswählen.
3. Wählen Sie im Navigationsbereich Instance Types (Instance-Typen) aus.
4. (Optional) Wählen Sie das Einstellungssymbol (Zahnrad) aus, um festzulegen, welche Attribute des Instance-Typs angezeigt werden sollen (z. B. On-Demand-Linux-Preise), und wählen Sie dann Bestätigen aus. Wählen Sie alternativ den Namen eines Instance-Typs, um die Detailseite zu öffnen und alle über die Konsole verfügbaren Attribute anzuzeigen. Die Konsole zeigt nicht alle Attribute an, die über die API oder die Befehlszeile verfügbar sind.

5. Verwenden Sie die Instance-Typ-Attribute, um die Liste der angezeigten Instance-Typen nur nach den Instance-Typen zu filtern, die Ihren Anforderungen entsprechen. Sie können beispielsweise nach den folgenden Attributen filtern:

   - Availability Zone – Der Name der Availability Zone, der lokalen Zone oder der Wavelength-Zone. Weitere Informationen finden Sie unter the section called “Regionen und Zonen”.
   - vCPUs oder Kerne – Die Anzahl an vCPUs oder Kernen.
   - Arbeitsspeicher (GiB) – Die Speichergröße in GiB
   - Netzwerkleistung – Die Netzwerkleistung in Gigabit.
   - Lokaler Instance-Speicher – Gibt an, ob der Instance-Typ über lokalen Instance-Speicher verfügt (`true` | `false`).

6. (Optional) Um einen side-by-side Vergleich zu sehen, aktivieren Sie das Kontrollkästchen für mehrere Instance-Typen. Der Vergleich wird unten auf dem Bildschirm angezeigt.
7. (Optional) Um die Liste der Instance-Typen zur weiteren Überprüfung in einer CSV-Datei zu speichern, wählen Sie Actions (Aktionen), Download List CSV (Liste als CSV herunterladen). Die Datei enthält alle Instance-Typen, die den von Ihnen festgelegten Filtern entsprechen.
8. (Optional) Um Instances mit einem Instance-Typ zu starten, der Ihren Anforderungen entspricht, aktivieren Sie das Kontrollkästchen für den Instance-Typ und wählen Sie Actions (Aktionen), Launch Instance (Instance starten). Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Suchen Sie einen Instanztyp mithilfe der AWS CLI

Sie können AWS CLI Befehle für Amazon EC2 verwenden, um einen Instance-Typ zu finden, der Ihren Anforderungen entspricht.

Um einen Instance-Typ zu finden, verwenden Sie den AWS CLI

1. Falls Sie dies noch nicht getan haben, installieren Sie das. AWS CLI Weitere Informationen finden Sie im AWS Command Line Interface Benutzerhandbuch.
2. Verwenden Sie den Befehl describe-instance-types, um Instance-Typen basierend auf Instance-Attributen zu filtern. Sie können beispielsweise den folgenden Befehl verwenden, um nur Instance-Typen der aktuellen Generation mit 64 GiB (65536 MiB) Speicher anzuzeigen.

```
aws ec2 describe-instance-types --filters "Name=current-generation,Values=true"
 "Name=memory-info.size-in-mib,Values=65536" --query "InstanceTypes[*].
[InstanceType]" --output text | sort
```

3. Verwenden Sie den Befehl describe-instance-type-offerings, um Instance-Typen zu filtern, die nach Standort (Region oder Zone) angeboten werden. Beispielsweise können Sie den folgenden Befehl verwenden, um die Instance-Typen anzuzeigen, die in der angegebenen Zone angeboten werden.

```
aws ec2 describe-instance-type-offerings --location-type "availability-
zone" --filters Name=location,Values=us-east-2a --region us-east-2 --query
 "InstanceTypeOfferings[*].[InstanceType]" --output text | sort
```

4. Nachdem Sie Instance-Typen gefunden haben, die Ihren Anforderungen entsprechen, speichern Sie die Liste, damit Sie diese Instance-Typen beim Starten von Instances verwenden können. Weitere Informationen zum Starten einer Instance finden Sie im AWS Command Line Interface - Benutzerhandbuch.

Erhalten von Empfehlungen für einen Instance-Typ

Die folgenden Tools können Ihnen bei der Auswahl der optimalen Instance-Typen für Ihre neuen oder vorhandenen Workloads helfen:

- Neue Workloads — Der EC2-Instance-Typ-Finder berücksichtigt Ihren Anwendungsfall, den Workload-Typ, die Präferenz des CPU-Herstellers und Ihre Priorisierung von Preis und Leistung sowie zusätzliche Parameter, die Sie angeben können. Anschließend werden anhand dieser Daten Vorschläge und Anleitungen für Amazon EC2 EC2-Instance-Typen bereitgestellt, die für Ihre neuen Workloads am besten geeignet sind.
- Bestehende Workloads — AWS Compute Optimizer analysiert Ihre bestehenden Instance-Spezifikationen und Nutzungskennzahlen. Danach verwendet die Funktion die kompilierten Daten, um zu empfehlen, welche Amazon-EC2-Instance-Typen hinsichtlich Kosten oder Leistung oder beides für Ihre bestehenden Workloads optimiert sind.

Empfehlungen für Instance-Typen erhalten:

- Empfehlungen für Instance-Typen für einen neuen Workload erhalten:
- Empfehlungen für Instance-Typen für einen vorhandenen Workload erhalten:

Empfehlungen für Instance-Typen für einen neuen Workload erhalten:

Der EC2-Instance-Typ-Finder berücksichtigt Ihren Anwendungsfall, den Workload-Typ, die Präferenz des CPU-Herstellers und Ihre Priorisierung von Preis und Leistung sowie zusätzliche Parameter, die Sie angeben können. Anschließend werden anhand dieser Daten Vorschläge und Anleitungen für Amazon EC2 EC2-Instance-Typen bereitgestellt, die für Ihre neuen Workloads am besten geeignet sind.

Bei so vielen verfügbaren Instance-Typen kann es zeitaufwändig und komplex sein, die richtigen Instance-Typen für Ihre Arbeitslast zu finden. Mithilfe des EC2-Instance-Typ-Finders können Sie über die neuesten Instance-Typen auf dem Laufenden bleiben und das beste Preis-Leistungs-Verhältnis für Ihre Workloads erzielen.

In diesem Thema wird beschrieben, wie Sie über die Amazon EC2-Konsole Vorschläge und Anleitungen für EC2-Instance-Typen erhalten. Sie können auch direkt zu Amazon Q gehen, um eine Beratung zu Instance-Typen zu erhalten. Weitere Informationen finden Sie im Amazon Q Developer User Guide.

Wenn Sie nach Empfehlungen zum Instance-Typ für einen bestehenden Workload suchen, verwenden Sie AWS Compute Optimizer. Weitere Informationen finden Sie unter Empfehlungen für Instance-Typen für einen vorhandenen Workload erhalten:.

Verwenden Sie den EC2-Instance-Typ-Finder

In der Amazon EC2 EC2-Konsole können Sie Vorschläge zu Instance-Typen über den EC2-Instance-Typ-Finder im Launch-Instance-Assistenten, beim Erstellen einer Startvorlage oder auf der Seite Instance-Typen abrufen.

Verwenden Sie die folgenden Anweisungen, um Vorschläge und Anleitungen für EC2-Instance-Typen mithilfe des EC2-Instance-Typ-Finders in der Amazon EC2 EC2-Konsole zu erhalten. Eine Animation der Schritte finden Sie unter. Animation anzeigen: Mithilfe des EC2-Instance-Typ-Finders erhalten Sie Vorschläge für Instance-Typen

So rufen Sie mithilfe des EC2-Instance-Typ-Finders Vorschläge zu Instanztypen ab

1. Starten Sie Ihren Prozess mit einer der folgenden Methoden:

   - Befolgen Sie das Verfahren zum Starten einer Instance. Wählen Sie neben Instance-Typ die Verknüpfung Tipps einholen.

- Gehen Sie wie folgt vor, um eine Startvorlage zu erstellen. Wählen Sie neben Instance-Typ die Verknüpfung Tipps einholen.
- Wählen Sie im Navigationsbereich die Option Instance-Typen und anschließend die Finder-Schaltfläche für den Instanztyp aus.

2. Gehen Sie auf dem Bildschirm „Tipps zur Auswahl des Instanztyps erhalten“ wie folgt vor:

   a. Geben Sie Ihre Anforderungen an den Instance-Typ an, indem Sie Optionen für Workload-Typ, Anwendungsfall, Priorität und CPU-Hersteller auswählen.

   b. (Optional) Gehen Sie wie folgt vor, um detailliertere Anforderungen für Ihren Workload anzugeben:

      i. Erweitern Sie Erweiterte Parameter.

      ii. Um einen Parameter hinzuzufügen, wählen Sie einen Parameter aus, klicken Sie auf Hinzufügen und geben Sie einen Wert für den Parameter an. Wiederholen Sie den Vorgang für jeden weiteren Parameter, den Sie hinzufügen möchten. Wenn Sie keinen Mindest- oder Höchstwert angeben möchten, lassen Sie das Feld leer.

      iii. Um einen Parameter nach dem Hinzufügen zu entfernen, wählen Sie das X neben dem Parameter aus.

   c. Wählen Sie Tipps zu Instance-Typen einholen.

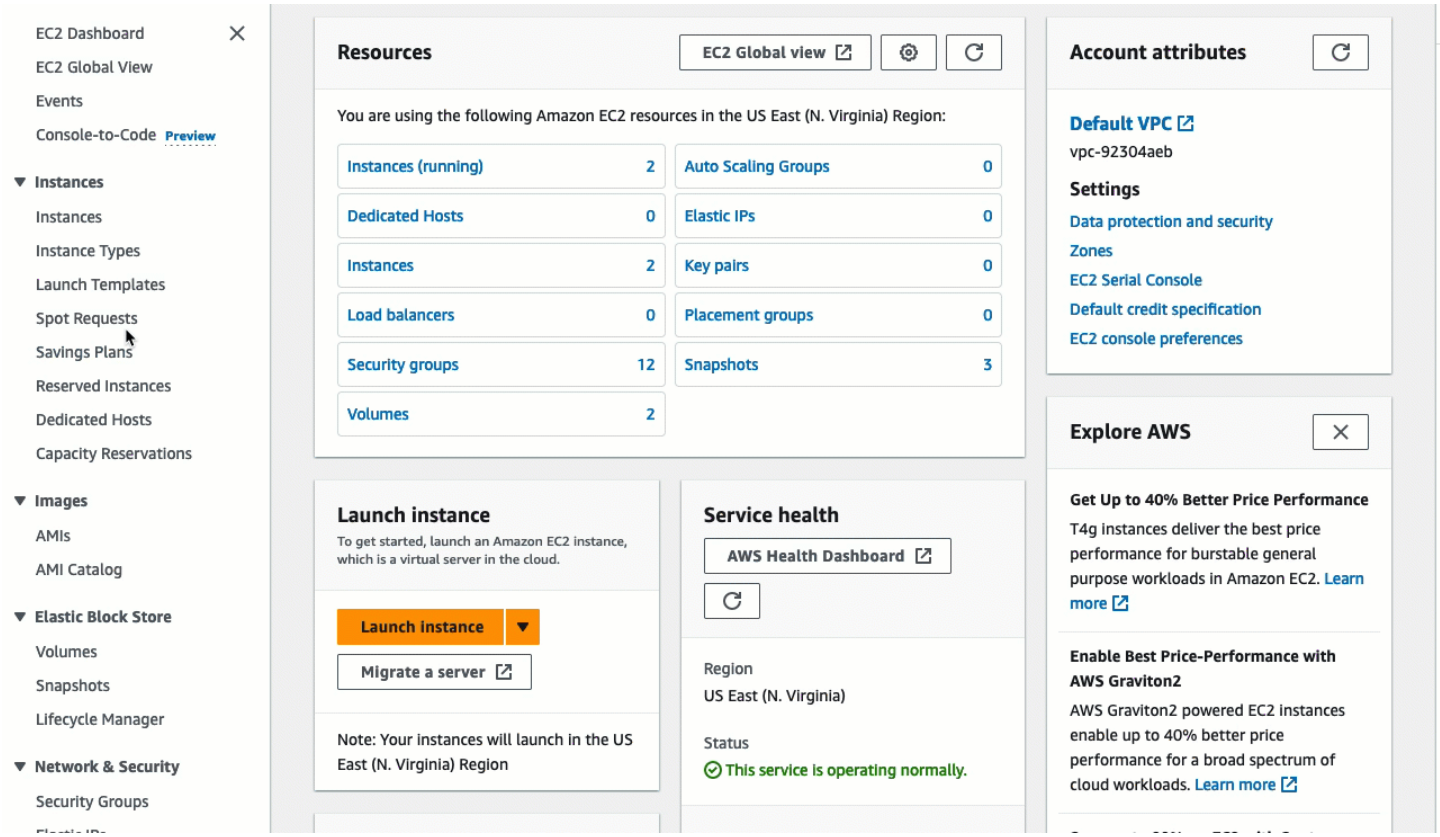
      Amazon EC2 bietet Ihnen Vorschläge für Instance-Familien, die Ihren spezifischen Anforderungen entsprechen.

3. Um die Details der einzelnen Instance-Typen innerhalb der vorgeschlagenen Instance-Familien anzuzeigen, wählen Sie Empfohlene Instance-Familiendetails anzeigen.

4. Wählen Sie einen Instance-Typ aus, der Ihren Anforderungen entspricht, und wählen Sie dann Aktionen, Instanz starten oder Aktionen, Startvorlage erstellen.

   Wenn Sie den Vorgang alternativ im Launch-Instance-Assistenten oder auf der Launch-Vorlagenseite gestartet haben und lieber zu Ihrem ursprünglichen Flow zurückkehren möchten, notieren Sie sich den Instance-Typ, den Sie verwenden möchten. Wählen Sie dann im Launch-Instance-Assistenten oder in der Startvorlage unter Instance-Typ den Instance-Typ aus und schließen Sie das Verfahren ab, um eine Instance zu starten oder eine Startvorlage zu erstellen.

Animation anzeigen: Mithilfe des EC2-Instance-Typ-Finders erhalten Sie Vorschläge für Instance-Typen



Empfehlungen für Instance-Typen für einen vorhandenen Workload erhalten:

AWS Compute Optimizer bietet Amazon EC2 EC2-Instance-Empfehlungen, um Ihnen zu helfen, die Leistung zu verbessern, Geld zu sparen oder beides. Mit diesen Empfehlungen können Sie entscheiden, ob Sie zu einem neuen Instance-Typ wechseln möchten.

Zur Abgabe von Empfehlungen analysiert Compute Optimizer Ihre vorhandenen Instance-Spezifikationen und Auslastungsmetriken. Die kompilierten Daten werden dann für die Empfehlung verwendet, welche Amazon EC2-Instance-Typen den vorhandenen Workload am besten bewältigen können. Empfehlungen werden zusammen mit den Preisen der Instance pro Stunde zurückgegeben.

In diesem Thema wird beschrieben, wie Empfehlungen über die Amazon EC2-Konsole angezeigt werden. Weitere Informationen finden Sie im AWS Compute Optimizer -Benutzerhandbuch.

> **Note**
>
> Um Empfehlungen von Compute Optimizer zu erhalten, müssen Sie sich zunächst bei Compute Optimizer anmelden. Weitere Informationen finden Sie unter Erste Schritte in AWS Compute Optimizer im AWS Compute Optimizer -Benutzerhandbuch.

Wenn Sie nach Empfehlungen für den Instance-Typ für einen neuen Workload suchen, verwenden Sie den Amazon Q EC2 Instance Type Selector. Weitere Informationen finden Sie unter Empfehlungen für Instance-Typen für einen neuen Workload erhalten:.

Inhalt

Einschränkungen

Compute Optimizer generiert derzeit Empfehlungen für C-, D-, H-, I-, M-, R-, T-, X- and z-Instance-Typen. Andere Instance-Typen werden von Compute Optimizer nicht berücksichtigt. Wenn Sie andere Instance-Typen verwenden, werden diese nicht in der Compute Optimizer-Empfehlungsansicht aufgeführt. Weitere Informationen zu den unterstützten und nicht unterstützten Instance-Typen finden Sie unterAmazon-EC2-Instance-Anforderungen im AWS Compute Optimizer -Benutzerhandbuch.

Funde

Compute Optimizer klassifiziert seine Ergebnisse für EC2-Instances wie folgt:

- Unterdimensioniert– Eine EC2-Instance gilt als unterdimensioniert, wenn mindestens eine Spezifikation Ihrer Instance, z. B. CPU, Arbeitsspeicher oder Netzwerk, die Leistungsanforderungen für Ihre Verarbeitungslast (Workload) nicht erfüllt. Unterdimensionierte EC2-Instances führen möglicherweise zu einer schlechten Anwendungsleistung.
- Überdimensioniert – Eine EC2-Instance gilt als überdimensioniert, wenn mindestens eine Spezifikation Ihrer Instance, z. B. CPU, Arbeitsspeicher oder Netzwerk, verringert werden kann und

dabei nach wie vor die Leistungsanforderungen für Ihr Workload erfüllt werden und wenn keine Spezifikation mangelhaft erfüllt wird. Überdimensionierte EC2-Instances können zu überflüssigen Infrastrukturkosten führen.

- Optimiert– Eine EC2-Instance gilt als optimiert, wenn alle Spezifikationen Ihrer Instance, z. B. CPU, Arbeitsspeicher und Netzwerk, die Leistungsanforderungen für Ihr Workload erfüllen und die Instance nicht überdimensioniert wird. Eine optimierte EC2-Instance führt Ihre Workloads mit optimalen Leistungs- und Infrastrukturkosten aus. Für optimierte Instances empfiehlt Compute Optimizer mitunter einen Instance-Typ einer neuen Generation.
- Keine– Für diese Instance liegen keine Empfehlungen vor. Dies kann vorkommen, wenn Sie bei Compute Optimizer weniger als 12 Stunden angemeldet waren oder die Instance weniger als 30 Stunden ausgeführt wurde oder wenn der Instance-Typ von Compute Optimizer nicht unterstützt wird. Weitere Informationen finden Sie unter Einschränkungen im vorhergehenden Abschnitt.

Anzeigen von Empfehlungen

Nachdem Sie sich bei Compute Optimizer angemeldet haben, können Sie die Ergebnisse, die Compute Optimizer für Ihre EC2-Instances generiert, in der EC2-Konsole anzeigen. Anschließend können Sie auf die Compute Optimizer-Konsole zugreifen, um die Empfehlungen anzuzeigen. Wenn Sie sich vor kurzem angemeldet haben, werden die Ergebnisse möglicherweise bis zu 12 Stunden lang nicht in der EC2-Konsole angezeigt.

So lassen Sie sich eine Empfehlung für eine EC2-Instance über die EC2-Konsole anzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann die Instance-ID .
3. Wählen Sie auf der Instance-Übersichtsseite im AWS Compute Optimizer-Banner unten auf der Seite die Option Details anzeigen aus.

   Die Instance wird in Compute Optimizer geöffnet, wo sie als Current (Aktuelle) Instance bezeichnet wird. Es werden bis zu drei verschiedene Empfehlungen für Instance-Typen gegeben, die als Option 1, Option 2 und Option 3 bezeichnet werden. In der unteren Hälfte des Fensters werden aktuelle CloudWatch Metrikdaten für die aktuelle Instance angezeigt: CPU-Auslastung, Speicherauslastung, Netzwerkeingang und Netzwerkausgang.
4. (Optional) Wählen Sie in der Compute Optimizer Optimizer-Konsole Einstellungen (),

um die sichtbaren Spalten in der Tabelle zu ändern oder um die öffentlichen Preisinformationen für eine andere Kaufoption für die aktuellen und empfohlenen Instance-Typen anzuzeigen.

> **Note**
>
> Wenn Sie eine Reserved Instance erworben haben, wird Ihnen Ihre On-Demand-Instance möglicherweise als Reserved Instance in Rechnung gestellt. Bevor Sie den aktuellen Instance-Typ ändern, sollten Sie zunächst die Auswirkungen auf die Nutzung und Abdeckung der Reserved Instance bewerten.

Legen Sie fest, ob Sie eine der Empfehlungen verwenden möchten. Entscheiden Sie, ob Sie die Leistungssteigerung, Kostensenkung oder beides optimieren möchten. Weitere Informationen finden Sie unter Anzeigen von Ressourcenempfehlungen im AWS Compute Optimizer -Benutzerhandbuch.

So zeigen Sie Empfehlungen für alle EC2-Instances in allen Regionen über die Compute Optimizer-Konsole an:

1. Öffnen Sie die Compute-Optimizer-Konsole unter https://console.aws.amazon.com/compute-optimizer/.
2. Wählen Sie View recommendations for all EC2 instances (Empfehlungen für alle EC2-Instances anzeigen).
3. Auf der Empfehlungsseite können Sie die folgenden Aktionen ausführen:

   a. Um Empfehlungen nach einer oder mehreren AWS Regionen zu filtern, geben Sie den Namen der Region in das Textfeld Nach einer oder mehreren Regionen filtern ein oder wählen Sie in der angezeigten Dropdownliste eine oder mehrere Regionen aus.

   b. Um sich Empfehlungen für Ressourcen in einem anderen Konto anzeigen zu lassen, wählen Sie Account (Konto) und dann eine andere Konto-ID aus.

      Diese Option ist nur verfügbar, wenn Sie bei einem Verwaltungskonto einer Organisation angemeldet sind und Sie sich für alle Mitgliedskonten innerhalb der Organisation angemeldet haben.

   c. Um die ausgewählten Filter zu löschen, wählen Sie Clear filters (Filter löschen) aus.

   d. Um die Kaufoption zu ändern, die für die aktuellen und empfohlenen Instance-Typen angezeigt wird, wählen Sie Einstellungen (⚙)

und dann On-Demand-Instances, Reserved Instances, Standard 1 Jahr ohne Vorauszahlung oder Reserved Instances, Standard 3 Jahre ohne Vorauszahlung.

e. Um Details anzuzeigen, wie z. B. zusätzliche Empfehlungen und einen Vergleich der Auslastungsmetriken, wählen Sie das Ergebnis (Under-provisioned (Unterdimensioniert), Over-provisioned (Überdimensioniert) oder Optimized (Optimiert)) aus, das neben der gewünschten Instance aufgeführt ist. Weitere Informationen finden Sie unter Anzeigen von Ressourcendetails im AWS Compute Optimizer -Benutzerhandbuch.

Überlegungen zur Bewertung von Empfehlungen

Bevor Sie einen Instance-Typ ändern, sollten Sie Folgendes beachten:

- Die Empfehlungen prognostizieren nicht Ihre Nutzung. Die Empfehlungen basieren auf Ihrer bisherigen Nutzung während des letzten 14-Tage-Zeitraums. Stellen Sie sicher, dass Sie einen Instance-Typ auswählen, der Ihren künftigen Ressourcenanforderungen entspricht.
- Konzentrieren Sie sich auf die grafisch dargestellten Metriken, um zu ermitteln, ob die tatsächliche Nutzung geringer als die Instance-Kapazität ist. Sie können auch Metrikdaten (Durchschnitt, Spitze, Perzentil) einsehen, CloudWatch um Ihre EC2-Instance-Empfehlungen weiter auszuwerten. Beachten Sie zum Beispiel, wie sich die prozentualen CPU-Prozentsatzmetriken im Laufe des Tages verändern und ob es Datenverkehrsspitzen gibt, die berücksichtigt werden müssen. Weitere Informationen finden Sie unter Verfügbare Metriken anzeigen im CloudWatch Amazon-Benutzerhandbuch.
- Compute Optimizer bietet möglicherweise Empfehlungen für Instances mit Spitzenlastleistung, bei denen es sich um T3-, T3a- und T2-Instances handelt. Wenn Sie regelmäßig über die Basisleistung hinausgehen, stellen Sie sicher, dass Sie dies weiterhin auf der Grundlage der vCPUs des neuen Instance-Typs tun können. Weitere Informationen finden Sie unter Schlüsselkonzepte und Definitionen für Burstable Performance Instance.
- Wenn Sie eine Reserved Instance erworben haben, wird Ihnen Ihre On-Demand-Instance möglicherweise als Reserved Instance in Rechnung gestellt. Bevor Sie den aktuellen Instance-Typ ändern, sollten Sie zunächst die Auswirkungen auf die Nutzung und Abdeckung der Reserved Instance bewerten.
- Ziehen Sie nach Möglichkeit einen Umstieg auf Instances der neueren Generation in Betracht.
- Bei der Migration auf eine andere Instance-Familie ist darauf zu achten, dass der aktuelle Instance-Typ und der neue Instance-Typ miteinander kompatibel sind, z. B. in Bezug auf Virtualisierung, Architektur oder Netzwerktyp. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

- Berücksichtigen Sie abschließend die Bewertung des Leistungsrisikos, die für jede Empfehlung angegeben ist. Das Leistungsrisiko gibt den Aufwand an, den Sie möglicherweise aufwenden müssen, um zu überprüfen, ob der empfohlene Instance-Typ den Leistungsanforderungen Ihrem Workload entspricht. Darüber hinaus empfehlen wir, vor und nach jeder Änderung Last- und Leistungstests durchzuführen.

Es gibt noch weitere Überlegungen, die beim Ändern der Größe einer EC2-Instance anzustellen sind. Weitere Informationen finden Sie unter Ändern des Instance-Typs.

Weitere Ressourcen

Weitere Informationen:

- Amazon EC2-Instance-Typen
- AWS Compute Optimizer Benutzerhandbuch

Ändern des Instance-Typs

Wenn sich Ihre Anforderungen ändern, wird Ihre Instance möglicherweise überlastet (der Instance-Typ ist zu klein) oder wird nicht voll ausgelastet (der Instance-Typ ist zu groß). In diesem Fall können Sie die Größe Ihrer Instance ändern, indem Sie ihren Instance-Typ ändern. Beispiel: Wenn Ihre `t2.micro`-Instance zu klein für den Workload ist, können Sie die Größe erhöhen, indem Sie sie in einen größeren T2-Instance-Typ ändern, z. B. `t2.large`. Oder Sie ändern sie in einen anderen Instance-Typ wie z. B. `m5.large`. Möglicherweise möchten Sie auch von einem Instance-Typ der vorherigen Generation zu einem Instance-Typ der aktuellen Generation migrieren, um einige Features zu nutzen, z. B. den Support für IPv6.

Wenn Sie eine Empfehlung für einen Instance-Typ wünschen, der Ihren vorhandenen Workload am besten verarbeiten kann, können Sie AWS Compute Optimizer nutzen. Weitere Informationen finden Sie unter Empfehlungen für Instance-Typen für einen vorhandenen Workload erhalten:.

Wenn Sie den Instance-Typ ändern, zahlen Sie ab dann den Tarif des neuen Instance-Typs. Informationen zu den On-Demand-Preisen aller Instance-Typen finden Sie unter On-Demand-Preise für Amazon EC2.

Um Ihrer Instance zusätzlichen Speicher hinzuzufügen, ohne den Instance-Typ zu ändern, fügen Sie der Instance ein EBS-Volume hinzu. Weitere Informationen finden Sie unter Anhängen eines Amazon EBS-Volumes an eine Instance im Amazon EBS-Benutzerhandbuch.

Welche Anweisungen müssen Sie befolgen?

Zum Ändern des Instance-Typs sind verschiedene Anweisungen verfügbar. Die zu verwendenden Anweisungen hängen vom Root-Volume der Instance ab und davon, ob der Instance-Typ mit der aktuellen Konfiguration der Instance kompatibel ist. Weitere Informationen zur Bestimmung der Kompatibilität finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

Bestimmen Sie anhand der nachstehenden Tabelle, welche Anweisungen zu befolgen sind.

Root-Volume	Kompatibilität	Diese Anweisungen befolgen
EBS	Kompatibel	Ändern Sie den Instance-Typ einer EBS-gestützten Instance
EBS	Nicht kompatibel	Ändern des Instance-Typs durch Starten einer neuen Instance
Instance-Speicher	Nicht zutreffend	Instance-Typ einer Instance-Speicher-gestützten Instance ändern

Überlegungen zu kompatiblen Instance-Typen

Beachten Sie beim Ändern des Typs einer vorhandenen Instance Folgendes:

- Sie müssen eine Amazon EBS-gestützte Instance anhalten, bevor Sie den Instance-Typ ändern können. Planen Sie Stillstandzeiten ein, während Ihre Instance angehalten ist. Das Anhalten der Instance und die Änderung des Instance-Typs können ein paar Minuten dauern. Der Neustart Ihrer Instance kann je nach den Startup-Skripten Ihrer Anwendung unterschiedlich lange dauern. Weitere Informationen finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.
- Wenn Sie eine Instance anhalten und wieder starten, wird sie auf neue Hardware verschoben. Wenn Ihre Instance über eine öffentliche IPv4-Adresse verfügt, geben wir diese Adresse frei und vergeben eine neue öffentliche IPv4-Adresse. Wenn Sie eine öffentliche IPv4-Adresse benötigen, die sich nicht ändert, verwenden Sie eine elastische IP-Adresse.
- Sie können den Instance-Typ einer Spot-Instance nicht ändern.
- [Windows-Instances] Wir empfehlen, dass Sie das AWS PV-Treiberpaket aktualisieren, bevor Sie den Instance-Typ ändern. Weitere Informationen finden Sie unter the section called “Upgrade für PV-Treiber”.

- Wenn sich die Instance in einer Auto Scaling-Gruppe befindet, kennzeichnet der Amazon EC2 Auto Scaling-Dienst die angehaltene Instance als fehlerhaft, beendet sie ggf. und startet eine Ersatz-Instance. Um dies zu verhindern, können Sie die Skalierungsprozesse für die Gruppe anhalten, während Sie den Instance-Typ ändern. Weitere Informationen finden Sie unter Anhalten und Fortsetzen eines Prozesses für eine Auto-Scaling-Gruppe im Benutzerhandbuch für Amazon EC2 Auto Scaling.
- Wenn Sie den Instance-Typ einer Instance mit NVMe-Instance-Speicher-Volumes ändern, verfügt die aktualisierte Instance möglicherweise über zusätzliche Instance-Speicher-Volumes, da alle NVMe-Instance-Speicher-Volumes verfügbar sind, auch wenn sie nicht in der AMI- oder Instance-Blockgerät-Zuweisung angegeben sind. Anderenfalls weist die aktualisierte Instance die gleiche Anzahl von Instance-Speicher-Volumes auf, die Sie beim Starten der ursprünglichen Instance angegeben haben.
- Die maximale Anzahl von Amazon-EBS-Volumes, die Sie einer Instance anfügen können, hängt vom Instance-Typ und der Instance-Größe ab. Sie können nicht zu einem Instance-Typ oder einer Instance-Größe wechseln, die nicht die Anzahl der Volumes unterstützt, die bereits an Ihre Instance angefügt sind. Weitere Informationen finden Sie unter Volume-Limits für Instances.

Ändern Sie den Instance-Typ einer EBS-gestützten Instance

Verwenden Sie die folgenden Anweisungen, um den Instance-Typ einer EBS-gestützten Instance zu ändern, wenn der gewünschte Instance-Typ mit der aktuellen Konfiguration der Instance kompatibel ist.

So ändern Sie den Instance-Typ einer Amazon-EBS-gestützten Instance

1. (Optional) Wenn für den neuen Instance-Typ Treiber erforderlich sind, die nicht auf der vorhandenen Instance installiert sind, müssen Sie eine Verbindung zu Ihrer Instance einrichten und zuerst die Treiber installieren. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.
2. [Windows-Instanzen] Wenn Sie Ihre Windows-Instance für die Verwendung statischer IP-Adressierung konfiguriert haben und Sie von einem Instance-Typ, der Enhanced Networking nicht unterstützt, zu einem Instance-Typ wechseln, der Enhanced Networking unterstützt, erhalten Sie möglicherweise eine Warnung vor einem potenziellen IP-Adresskonflikt, wenn Sie die statische IP-Adressierung neu konfigurieren. Sie können das verhindern, indem Sie DHCP für die Netzwerkschnittstelle der Instance aktivieren, bevor Sie den Instance-Typ ändern. Öffnen Sie in Ihrer Instance das Network and Sharing Center und die Internet Protocol Version 4 (TCP/IPv4) Properties für die Netzwerkschnittstelle und wählen Sie die Option Obtain an IP

address automatically. Ändern Sie den Instance-Typ und konfigurieren Sie die statische IP-Adresszuweisung für die Netzwerkschnittstelle neu.

3. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
4. Wählen Sie im Navigationsbereich Instances aus.
5. Wählen Sie die Instance und dann Instance-Status, Instance anhalten aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus. Das Anhalten der Instance kann einige Minuten dauern.
6. Während die Instance noch ausgewählt ist, wählen Sie Aktionen, Instance-Einstellungen, Instance-Typ ändern aus. Diese Option ist deaktiviert, wenn der Status der Instance nicht lautet `stopped`.
7. Gehen Sie auf der Seite Ändern des Instance-Typs wie folgt vor:

   a. Wählen Sie unter Instance-Typ den gewünschten Instance-Typ aus.

      Wenn der Instance-Typ nicht in der Liste enthalten ist, ist er nicht mit der Konfiguration Ihrer Instance kompatibel. Befolgen Sie stattdessen die nachstehenden Anweisungen: Ändern des Instance-Typs durch Starten einer neuen Instance.

   b. (Optional) Wenn der ausgewählte Instance-Typ EBS-Optimierung unterstützt, wählen Sie EBS-optimiert aus, um die EBS-Optimierung zu aktivieren oder löschen Sie EBS-optimiert, um die Optimierung zu deaktivieren. Wenn der ausgewählte Instance-Typ standardmäßig EBS-optimiert ist, ist die Option EBS-optimiert bereits ausgewählt und Sie können sie nicht deaktivieren.

   c. Wählen Sie Apply, um die neuen Einstellungen zu übernehmen.
8. Um die Instance zu starten, wählen Sie die Instance aus und wählen Sie Instance state (Instance-Status), Start instance (Instance starten). Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht. Wenn Ihre Instance nicht startet, finden Sie weitere Informationen unter Problembehandlung beim Ändern des Instance-Typs.
9. [Windows-Instanzen] Wenn auf Ihrer Instance Windows Server 2016 oder Windows Server 2019 mit EC2Launch v1 ausgeführt wird, stellen Sie eine Verbindung zu Ihrer Windows-Instance her und führen Sie das folgende PowerShell EC2Launch-Skript aus, um die Instance zu konfigurieren, nachdem der Instance-Typ geändert wurde.

   > **Important**
   >
   > Das Administratorpasswort wird zurückgesetzt, wenn Sie das EC2-Launch-Skript zum Initialisieren der Instance aktivieren. Sie können die Konfigurationsdatei bearbeiten,

um das Zurücksetzen des Administratorpassworts zu deaktivieren, indem Sie es in den Einstellungen für die Initialisierungsaufgaben festlegen. Schritte zum Deaktivieren des Kennwortzurücksetzens finden Sie unter Initialisierungsaufgaben konfigurieren (EC2Launch) oder Einstellungen ändern (EC2Launch v2).

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Ändern des Instance-Typs durch Starten einer neuen Instance

Wenn die aktuelle Konfiguration Ihrer EBS-gestützten Instance nicht mit dem neuen gewünschten Instance-Typ kompatibel ist, können den Instance-Typ der ursprünglichen Instance nicht ändern. Stattdessen müssen Sie eine neue Instance mit einer Konfiguration starten, die mit dem neuen gewünschten Instance-Typ kompatibel ist, und Ihre Anwendung zur neuen Instance migrieren. Wenn Sie beispielsweise Ihre ursprüngliche Instance von einem PV-AMI aus gestartet haben, aber zu einem Instance-Typ der aktuellen Generation wechseln möchten, für den ein HVM-AMI erforderlich ist, müssen Sie eine neue Instance von einem HVM-AMI aus starten. Weitere Informationen zur Bestimmung der Kompatibilität finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

Um Ihre Anwendung zu einer neuen Instance zu migrieren, gehen Sie wie folgt vor:

- Sichern Sie die Daten Ihrer ursprünglichen Instance.
- Starten Sie eine neue Instance mit einer Konfiguration, die mit dem neuen gewünschten Instance-Typ kompatibel ist, und fügen Sie alle EBS-Volumes an, die an Ihre ursprüngliche Instance angehängt waren.
- Installieren Sie Ihre Anwendung und jegliche Software auf Ihrer neuen Instance.
- Stellen Sie alle Daten wieder her.
- Wenn Ihre ursprüngliche Instance über eine elastische IP-Adresse verfügt und Sie sicherstellen möchten, dass die Benutzer die Anwendungen auf Ihrer neuen Instance weiterhin ohne Unterbrechung verwenden können, müssen Sie die elastische IP-Adresse Ihrer neuen Instance zuordnen. Weitere Informationen finden Sie unter Elastische IP-Adressen.

So ändern Sie den Instance-Typ für eine neue Instance-Konfiguration

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Sichern Sie Daten, die Sie behalten müssen, wie folgt:
   - Sichern Sie Daten Ihrer Instance-Speicher-Volumes im persistenten Speicher.
   - Für Daten auf Ihren EBS-Volumes erstellen Sie einen Snapshot der Volumes oder trennen Sie die Volumes von der Instance, sodass Sie sie später an die neue Instance anhängen können.
3. Wählen Sie im Navigationsbereich Instances aus.
4. Wählen Sie Launch Instances aus. Gehen Sie beim Konfigurieren der Instance wie folgt vor:
   a. Wählen Sie ein AMI aus, das den gewünschten Instance-Typ unterstützt. Beachten Sie, dass Instance-Typen der aktuellen Generation ein HVM-AMI benötigen.
   b. Wählen Sie den neuen Instance-Typ aus, den Sie starten möchten. Wenn der gewünschte Instance-Typ nicht verfügbar ist, ist er nicht mit der Konfiguration des ausgewählten AMI kompatibel.
   c. Wenn Sie eine elastische IP-Adresse verwenden, wählen Sie die VPC aus, in der die ursprüngliche Instance zurzeit ausgeführt wird.
   d. Wenn Sie erlauben wollen, dass der gleiche Datenverkehr die neue Instance erreicht, wählen Sie die Sicherheitsgruppe aus, die der ursprünglichen Instance zugeordnet ist.
   e. Wenn Sie mit der Konfiguration Ihrer neuen Instance fertig sind, wählen Sie ein Schlüsselpaar aus und starten Sie Ihre Instance. Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht.
5. Fügen Sie bei Bedarf alle neuen EBS-Volumes basierend auf den erstellten Snapshots oder alle EBS-Volumes, die Sie von der ursprünglichen Instance getrennt haben, an die neue Instance an.
6. Installieren Sie Ihre Anwendung und benötigte Software auf der neuen Instance.
7. Stellen Sie alle Daten wieder her, die Sie von den Instance-Speicher-Volumes der ursprünglichen Instance gesichert haben.
8. Wenn Sie eine elastische IP-Adresse verwenden, weisen Sie sie der neuen Instance wie folgt zu:
   a. Wählen Sie im Navigationsbereich Elastic IPs.
   b. Wählen Sie die Elastic IP-Adresse aus, die der ursprünglichen Instance zugeordnet ist, und wählen Sie dann Aktionen, Elastic IP-Adresszuordnung aufheben aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Zuordnung aufheben.
   c. Wählen Sie bei noch ausgewählter Elastic IP-Adresse Aktionen, Elastic IP-Adresse zuordnen aus.
   d. Wählen Sie für Resource type (Ressourcentyp) die Option Instance aus.

e. Wählen Sie unter Instance die neue Instance aus, der die elastische IP-Adresse zugeordnet werden soll.

f. (Optional) Geben Sie für Private IP address (Private IP-Adresse) eine private IP-Adresse an, mit der die Elastic IP-Adresse verknüpft werden soll.

g. Wählen Sie Associate aus.

9. (Optional) Sie können die ursprüngliche Instance beenden, wenn sie nicht länger benötigt wird. Wählen Sie die Instance aus, stellen Sie sicher, dass Sie im Begriff sind, die ursprüngliche Instance und nicht die neue Instance zu beenden (überprüfen Sie beispielsweise den Namen oder die Startzeit), und wählen Sie dann Instance-Status, Instance beenden aus.

Kompatibilität zum Ändern des Instance-Typs

Sie können den Instance-Typ nur ändern, wenn die aktuelle Konfiguration der Instance mit dem gewünschten Instance-Typ kompatibel ist. Wenn der gewünschte Instance-Typ nicht mit der aktuellen Konfiguration der Instance kompatibel ist, müssen Sie eine neue Instance mit einer Konfiguration starten, die mit dem Instance-Typ kompatibel ist, und dann Ihre Anwendung auf die neue Instance migrieren.

[Linux-Instanzen] Sie können das `AWSSupport-MigrateXenToNitroLinux` Runbook verwenden, um kompatible Linux-Instances von einem Xen-Instance-Typ zu einem Nitro-Instance-Typ zu migrieren. Weitere Informationen finden Sie unter `AWSSupport-MigrateXenToNitroLinux` runbook in der Referenz zum AWS Systems Manager -Automation-Runbook.

[Windows-Instanzen] Weitere Anleitungen zur Migration kompatibler Windows-Instances von einem Xen-Instance-Typ zu einem Nitro-Instance-Typ finden Sie unter Migration zu Instance-Typen der neuesten Generation.

Die Kompatibilität wird folgendermaßen ermittelt:

Virtualisierungstyp

Linux-AMIs verwenden einen dieser zwei Virtualisierungstypen: Paravirtual (PV) oder Hardware Virtual Machine (HVM). Wenn eine Instance von einem PV-AMI gestartet wurde, können Sie nicht zu einem Instance-Typ wechseln, der nur HVM ist. Weitere Informationen finden Sie unter AMI-Virtualisierungstypen. Den Virtualisierungstyp Ihrer Instance können Sie dem Wert Virtualization im Detailbereich des Bildschirms Instances in der Amazon-EC2-Konsole entnehmen.

Architektur

AMIs sind spezifisch für die Architektur des Prozessors. Daher müssen Sie einen Instance-Typ mit der Prozessorarchitektur des aktuellen Instance-Typs auswählen. Zum Beispiel:

- Wenn der aktuelle Instance-Typ einen auf der ARM-Architektur basierenden Prozessor hat, sind Sie auf die Instance-Typen beschränkt, die einen auf der ARM-Architektur basierenden Prozessor unterstützen, z. B. C6g und M6g.
- Die folgenden Instance-Typen sind die einzigen Instance-Typen, die 32-Bit-AMIs unterstützen: `t2.nano`, `t2.micro`, `t2.small`, `t2.medium`, `c3.large`, `t1.micro`, `m1.small`, `m1.medium` und `c1.medium`. Wenn Sie den Instance-Typ einer 32-Bit-Instance ändern, sind Sie auf diese Instance-Typen beschränkt.

Netzwerkadapter

Wenn Sie von einem Treiber für einen Netzwerkadapter zu einem anderen wechseln, werden die Netzwerkadaptereinstellungen zurückgesetzt, wenn das Betriebssystem den neuen Adapter erstellt. Um die Einstellungen neu zu konfigurieren, benötigen Sie möglicherweise Zugriff auf ein lokales Konto mit Administratorberechtigungen. Nachfolgend finden Sie Beispiele für den Wechsel von einem Netzwerkadapter zu einem anderen:

- AWS PV (T2-Instances) auf Intel 82599 VF (M4-Instances)
- Intel 82599 VF (die meisten M4-Instances) zu ENA (M5-Instances)
- ENA (M5-Instances) zu ENA mit hoher Bandbreite (M5n-Instances)

Netzwerkkarten

Einige Instance-Typen unterstützen mehrere Netzwerkkarten. Sie müssen einen Instance-Typ auswählen, der dieselbe Anzahl von Netzwerkkarten unterstützt wie der aktuelle Instance-Typ.

Enhanced Networking

Instance-Typen, die Enhanced Networking unterstützen, erfordern die Installation der notwendigen Treiber. Instances, die auf dem AWS Nitro System basieren, benötigen beispielsweise EBS-gestützte AMIs, auf denen die Elastic Network Adapter (ENA) -Treiber installiert sind. Um von einem Instance-Typ, der Enhanced Networking nicht unterstützt, zu einem Instance-Typ zu wechseln, der es unterstützt, müssen Sie die ENA-Treiber oder ixgbevf-Treiber entsprechend auf der Instance installieren.

> **Note**
>
> Wenn Sie die Größe einer Instance ändern, bei der ENA Express aktiviert ist, muss der neue Instance-Typ auch ENA Express unterstützen. Eine Liste mit Instance-Typen, die ENA Express unterstützen, finden Sie unter Unterstützte Instance-Typen für ENA Express.
> Wenn Sie von einem Instance-Typ, der ENA Express unterstützt, zu einem Instance-Typ wechseln möchten, der ENA Express nicht unterstützt, stellen Sie sicher, dass ENA Express nicht aktiviert ist, bevor Sie die Größe der Instance ändern.

NVMe

EBS-Volumes werden als NVMe-Blockgeräte auf Instances bereitgestellt, die auf dem Nitro System basieren. AWS Wenn Sie von einem Instance-Typ, der NVMe nicht unterstützt, zu einem Instance-Typ wechseln, der NVMe unterstützt, müssen Sie zuerst die NVMe-Treiber auf Ihrer Instance installieren. Außerdem werden die Gerätenamen für Geräte, die Sie in der Blockgerätezuordnung angeben, mithilfe von NVMe-Gerätenamen () umbenannt. `/dev/nvme[0-26]n1`

[Linux-Instanzen] Um Dateisysteme beim Booten mithilfe zu mounten`/etc/fstab`, müssen Sie daher UUID/Label anstelle von Gerätenamen verwenden.

Volumes-Limits

Die maximale Anzahl von Amazon-EBS-Volumes, die Sie einer Instance anfügen können, hängt vom Instance-Typ und der Instance-Größe ab. Weitere Informationen finden Sie unter Volume-Limits für Instances.

Sie können nur zu einem Instance-Typ oder einer Instance-Größe wechseln, der/die dieselbe oder eine größere Anzahl von Volumes unterstützt, als derzeit an die Instance angefügt ist. Wenn Sie zu einem Instance-Typ oder einer Instance-Größe wechseln, die die Anzahl der aktuell angefügten Volumes nicht unterstützt, schlägt die Anfrage fehl. Wenn Sie beispielsweise von einer `m7i.4xlarge`-Instance mit 32 angefügten Volumes zu einer `m6i.4xlarge`-Instance wechseln, die maximal 27 Volumes unterstützt, schlägt die Anfrage fehl.

Problembehandlung beim Ändern des Instance-Typs

Verwenden Sie die folgenden Informationen, um Probleme zu diagnostizieren und zu beheben, die beim Ändern des Instance-Typs auftreten können.

Die Instance startet nach dem Ändern des Instance-Typs nicht

Mögliche Ursache: Anforderungen für neuen Instance-Typ nicht erfüllt

Wenn Ihre Instance nicht startet, ist es möglich, dass eine der Anforderungen für den neuen Instance-Typ nicht erfüllt wurde. Weitere Informationen finden Sie unter Warum startet meine Linux-Instance nicht, nachdem ich ihren Typ geändert habe?

Mögliche Ursache: AMI unterstützt den Instance-Typ nicht

Wenn Sie die EC2-Konsole verwenden, um den Instance-Typ zu ändern, stehen nur die Instance-Typen zur Verfügung, die vom ausgewählten AMI unterstützt werden. Wenn Sie jedoch die verwenden, AWS CLI um eine Instance zu starten, können Sie ein inkompatibles AMI und einen Instance-Typ angeben. Wenn das AMI und der Instance-Typ nicht kompatibel sind, kann die Instance nicht gestartet werden. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

Mögliche Ursache: Instance befindet sich in Cluster-Placement-Gruppe

Wenn sich Ihre Instance in einer Cluster-Placement-Gruppe befindet und die Instance nach dem Ändern des Instance-Typs nicht startet, versuchen Sie Folgendes:

1. Beenden Sie alle Instances in der Cluster-Placement-Gruppe.
2. Ändern Sie den Instance-Typ der betroffenen Instance.
3. Starten Sie alle Instances in der Cluster-Placement-Gruppe.

Anwendung oder Website nach Änderung des Instance-Typs nicht aus dem Internet erreichbar

Mögliche Ursache: Öffentliche IPv4-Adresse wird freigegeben

Wenn Sie den Instance-Typ ändern, müssen Sie zuerst die Instance beenden. Wenn Sie eine Instance beenden, geben wir die öffentliche IPv4-Adresse frei und weisen Ihrer Instance eine neue öffentliche IPv4-Adresse zu.

Um die öffentliche IPv4-Adresse während des Beendens und Startens einer Instance beizubehalten, empfehlen wir Ihnen, eine elastische IP-Adresse ohne zusätzliche Kosten zu

verwenden, sofern Ihre Instance ausgeführt wird. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

Instance-Typ einer Instance-Speicher-gestützten Instance ändern

Eine per Instance-Speicher gestützte Instance ist eine Instance, die über ein Instance-Speicher-Root-Volume verfügt. Sie können den Instance-Typ einer Instance mit einem Instance-Speicher-Root-Volume nicht ändern. Stattdessen müssen Sie ein AMI von Ihrer Instance erstellen, eine neue Instance von diesem AMI aus starten, den gewünschten Instance-Typ auswählen und dann Ihre Anwendung auf die neue Instance migrieren. Beachten Sie, dass der gewünschte Instance-Typ mit dem erstellten AMI kompatibel sein muss. Weitere Informationen zur Bestimmung der Kompatibilität finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

Prozessübersicht

- Sichern Sie die Daten Ihrer ursprünglichen Instance.
- Erstellen Sie ein AMI aus Ihrer ursprünglichen Instance.
- Starten Sie eine neue Instance von diesem AMI aus und wählen Sie den gewünschten Instance-Typ aus.
- Installieren Sie Ihre Anwendung auf der neuen Instance.
- Wenn Ihre ursprüngliche Instance über eine elastische IP-Adresse verfügt und Sie sicherstellen möchten, dass die Benutzer die Anwendungen auf Ihrer neuen Instance weiterhin ohne Unterbrechung verwenden können, müssen Sie die elastische IP-Adresse Ihrer neuen Instance zuordnen. Weitere Informationen finden Sie unter Elastische IP-Adressen.

So ändern Sie den Instance-Typ einer Instance-Speicher-gestützten Instance

1. Sichern Sie Daten, die Sie behalten müssen, wie folgt:
   - Sichern Sie Daten Ihrer Instance-Speicher-Volumes im persistenten Speicher.
   - Erstellen Sie für Daten auf Ihren EBS-Volumes einen Snapshot der Volumes oder trennen Sie das Volume von der Instance, sodass Sie es später an die neue Instance anhängen können.
2. Erstellen Sie ein AMI von der Instance, indem Sie die Voraussetzungen erfüllen und die Verfahren in Erstellen einer Instance-Speicher-Backed Linux-AMI befolgen. Wenn Sie mit dem Erstellen eines AMI von Ihrer Instance fertig sind, kehren Sie zu diesem Verfahren zurück.
3. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

4. Wählen Sie im Navigationsbereich die Option AMIs. Wählen Sie aus den Filterlisten In meinem Besitz aus und wählen Sie das Image aus, das Sie in Schritt 2 erstellt haben. Beachten Sie, dass AMI Name der Name ist, den Sie beim Registrieren des Images angegeben haben, und dass Source Ihr Amazon-S3-Bucket ist.

   > **Note**
   >
   > Wenn das in Schritt 2 erstellte AMI nicht angezeigt wird, überprüfen Sie, ob die Region ausgewählt ist, in der Sie das AMI erstellt haben.

5. Wählen Sie bei ausgewähltem AMI Instance aus dem Image starten. Gehen Sie beim Konfigurieren der Instance wie folgt vor:

   a. Wählen Sie den neuen Instance-Typ aus, den Sie starten möchten. Wenn der gewünschte Instance-Typ nicht verfügbar ist, ist er nicht mit der Konfiguration des erstellten AMI kompatibel. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.

   b. Wenn Sie eine elastische IP-Adresse verwenden, wählen Sie die VPC aus, in der die ursprüngliche Instance zurzeit ausgeführt wird.

   c. Wenn Sie erlauben wollen, dass der gleiche Datenverkehr die neue Instance erreicht, wählen Sie die Sicherheitsgruppe aus, die der ursprünglichen Instance zugeordnet ist.

   d. Wenn Sie mit der Konfiguration Ihrer neuen Instance fertig sind, wählen Sie ein Schlüsselpaar aus und starten Sie Ihre Instance. Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht.

6. Fügen Sie bei Bedarf alle neuen EBS-Volumes basierend auf den erstellten Snapshots oder alle EBS-Volumes, die Sie von der ursprünglichen Instance getrennt haben, an die neue Instance an.

7. Installieren Sie Ihre Anwendung und benötigte Software auf der neuen Instance.

8. Wenn Sie eine elastische IP-Adresse verwenden, weisen Sie sie der neuen Instance wie folgt zu:

   a. Wählen Sie im Navigationsbereich Elastic IPs.

   b. Wählen Sie die Elastic IP-Adresse aus, die der ursprünglichen Instance zugeordnet ist, und wählen Sie dann Aktionen, Elastic IP-Adresszuordnung aufheben aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Zuordnung aufheben.

   c. Wählen Sie bei noch ausgewählter Elastic IP-Adresse Aktionen, Elastic IP-Adresse zuordnen aus.

   d. Wählen Sie für Resource type (Ressourcentyp) die Option Instance aus.

e. Wählen Sie unter Instance die neue Instance aus, der die elastische IP-Adresse zugeordnet werden soll.

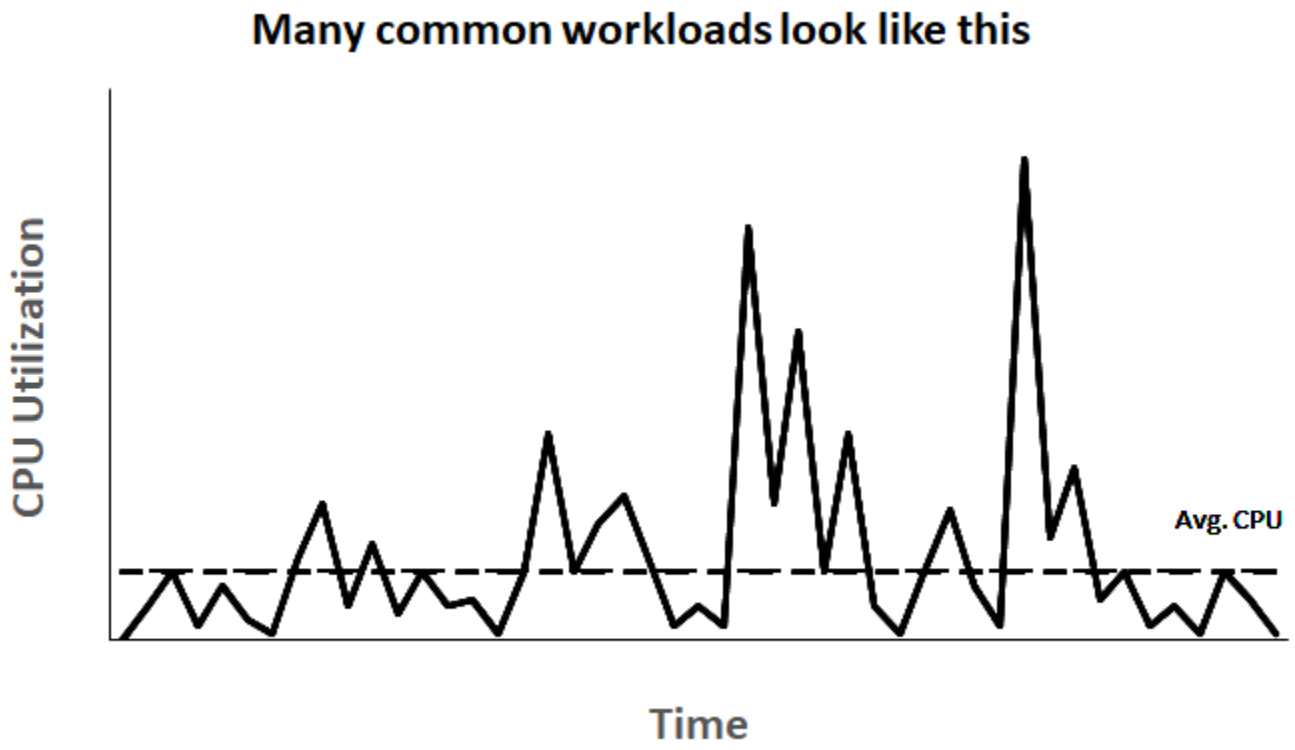
f. (Optional) Geben Sie für Private IP address (Private IP-Adresse) eine private IP-Adresse an, mit der die Elastic IP-Adresse verknüpft werden soll.

g. Wählen Sie Associate aus.

9. (Optional) Sie können die ursprüngliche Instance beenden, wenn sie nicht länger benötigt wird. Wählen Sie die Instance aus, stellen Sie sicher, dass Sie im Begriff sind, die ursprüngliche Instance und nicht die neue Instance zu beenden (überprüfen Sie beispielsweise den Namen oder die Startzeit), und wählen Sie dann Instance-Status, Instance beenden aus.

Burstable Performance Instances

Viele allgemeine Workloads sind im Durchschnitt nicht ausgelastet und erfordern keine hohe anhaltende CPU-Leistung. Die folgende Grafik veranschaulicht die CPU-Auslastung für viele gängige Workloads, die Kunden heute in der AWS Cloud ausführen.



Diese low-to-moderate CPU-Auslastung führt zu einer Verschwendung von CPU-Zyklen, sodass Sie für mehr bezahlen, als Sie nutzen. Um dies zu überwinden, können Sie die kostengünstigen universellen Burstable-Instances, die T-Instances, nutzen.

Die T-Instance-Familie bietet eine Baseline-CPU-Leistung mit der Möglichkeit, jederzeit und so lange wie erforderlich über die Baseline zu springen. Die Baseline-CPU ist so definiert, dass sie die Anforderungen der meisten universellen Workloads erfüllt, einschließlich großer Mikrodienste, Webserver, kleiner und mittlerer Datenbanken, Datenprotokollierung, Code-Repositorys, virtueller Desktops, Entwicklungs- und Testumgebungen sowie Geschäfts-kritische Anwendungen. Die T-Instances bieten ein ausgewogenes Verhältnis von Rechen-, Arbeitsspeicher- und Netzwerkressourcen und bieten Ihnen die kostengünstigste Möglichkeit, ein breites Spektrum an Allzweckanwendungen mit low-to-moderate CPU-Auslastung auszuführen. Sie können Ihnen im Vergleich zu M-Instances bis zu 15 % Kosten einsparen und können mit kleineren, kostengünstigeren Instance-Größen, die nur 2 vCPUs und 0,5 GiB Arbeitsspeicher bieten, zu noch mehr Kosteneinsparungen führen. Die kleineren T-Instance-Größen wie Nano, Micro, Small und Medium eignen sich gut für Workloads, die wenig Arbeitsspeicher benötigen und keine hohe CPU-Auslastung erwarten.

> **Note**
>
> In diesem Thema wird die Burst-fähige CPU beschrieben. Informationen zu Burst-fähiger Netzwerkleistung finden Sie unter Netzwerkbandbreite für Amazon EC2-Instances.

EC2-Burstable-Instance-Typen

Die EC2-Burstable-Instances bestehen ausT4g,T3a- und T3-Instance-Typen sowie die T2-Instance-Typen der vorherigen Generation.

Die T4G-Instance-Typen sind die neueste Generation von Burstable-Instances. Sie bieten das beste Preis-Leistungs-Verhältnis und die niedrigsten Kosten aller EC2-Instance-Typen. Die T4g-Instance-Typen werden von ARM-basierten AWS Graviton2-Prozessoren angetrieben und bieten umfassende Ökosystemunterstützung durch Betriebssystemanbieter, unabhängige Softwareanbieter und beliebte Dienste und Anwendungen. AWS

Die folgende Tabelle fasst die wichtigsten Unterschiede zwischen den Burstable-Instance-Typen zusammen.

Typ	Beschreibung	Prozessorfamilie
Neueste Generation		

Typ	Beschreibung	Prozessorfamilie
T4g	Kostengünstigster EC2-Instance-Typ mit bis zu 40 % höherem Preis-/Leistungsverhältnis und 20 % niedrigeren Kosten im Vergleich zu T3	AWS Graviton2-Prozessoren mit Arm Neoverse N1-Kernen
T3a	Kostengünstigste x86-basierte Instances mit 10 % geringeren Kosten im Vergleich zu T3-Instances	AMD-EPYC-Prozessoren der 1. Generation
T3	Bestes Spitzenpreis-/Leistungsverhältnis für x86-Workloads mit bis zu 30 % niedrigerem Preis-/Leistungsverhältnis im Vergleich zu T2-Instances der vorherigen Generation	Intel Xeon Scalable (Skylake, Cascade-Lake-Prozessoren)
Vorherige Generation		
T2	Burstable-Instances der vorherigen Generation	Intel-Xeon-Prozessoren

Informationen zu den Preisen für Instances sowie zusätzliche Angaben finden Sie unter Amazon-EC2-Preise und Amazon-EC2-Instance-Typen. Informationen zu Burst-fähiger Netzwerkleistung finden Sie unter Netzwerkbandbreite für Amazon EC2-Instances.

Wenn Ihr Konto weniger als 12 Monate alt ist, können Sie innerhalb bestimmter Nutzungslimits eine `t2.micro`-Instance kostenlos (oder eine `t3.micro`-Instance in Regionen, in denen `t2.micro` nicht verfügbar ist) verwenden. Weitere Informationen finden Sie unter Kostenloses Kontingent für AWS.

Unterstützte Kaufoptionen für T-Instances

- On-Demand Instances
- Reserved Instances
- Dedicated Instances (nur T3)

- Dedicated Hosts (nur T3, nur in `standard`-Modus)
- Spot-Instances

Weitere Informationen finden Sie unter Instance-Kaufoptionen.

Inhalt

Bewährte Methoden

Folgen Sie diesen bewährten Methoden, um Burstable Performance Instances mit größtmöglichem Nutzen zu verwenden.

- Stellen Sie sicher, dass die gewählte Größe der Instance die Speicher-Mindestanforderungen Ihres Betriebssystems und Ihrer Anwendungen erfüllt. Betriebssysteme mit grafischen Benutzeroberflächen, die deutlich mehr Speicher und CPU-Ressourcen verbrauchen (z. B. Windows), erfordern möglicherweise eine `t3.micro`- oder eine noch größere Instance-Größe für viele Anwendungsfälle. Da die Speicher- und CPU-Anforderungen Ihrer Workload im Laufe der Zeit wachsen, haben Sie mit den T-Instances die Flexibilität, auf größere Instance-Größen desselben Instance-Typs zu skalieren oder einen anderen Instance-Typ auszuwählen.
- Aktivieren Sie AWS Compute Optimizer für Ihr Konto und überprüfen Sie die Compute-Optimizer-Empfehlungen für Ihre Workload. Compute Optimizer kann bei der Beurteilung helfen, ob Instances zur Verbesserung der Leistung vergrößert oder zur Kosteneinsparung verkleinert werden sollten. Compute Optimizer empfiehlt möglicherweise auch einen anderen Instance-Typ basierend auf Ihrem Szenario. Weitere Informationen finden Sie unter Anzeigen von EC2-Instance-Empfehlungen im AWS Compute Optimizer -Benutzerhandbuch.

Schlüsselkonzepte und Definitionen für Burstable Performance Instance

Herkömmliche Amazon EC2-Instance-Typen bieten feste CPU-Ressourcen während Burstable Performance Instances eine Basisebene der CPU-Auslastung bieten, die über die Basisebene hinaus gesteigert werden kann. Dadurch wird sichergestellt, dass Sie nur für die Basis-CPU zuzüglich einer zusätzlichen Burst-CPU-Nutzung zahlen, was zu geringeren Rechenkosten führt. Die Basisauslastung und die Steigerbarkeit werden über das CPU-Guthaben verwaltet. Burstable Performance Instances sind die einzigen Instance-Typen, die CPU-Guthaben für die CPU-Nutzung verwenden.

Jede Burstable Performance Instance erhält kontinuierlich Guthaben, wenn sie unter der CPU-Baseline bleibt, und gibt kontinuierlich Guthaben aus, wenn sie über der Baseline liegt. Die Höhe des verdienten oder ausgegebenen Guthabens hängt von der CPU-Auslastung der Instance ab:

- Wenn die CPU-Auslastung unter dem Ausgangswert liegt, sind die verdienten Guthaben höher als die ausgegebenen Guthaben.
- Wenn die CPU-Auslastung der Baseline entspricht, entsprechen die verdienten Guthaben den ausgegebenen Guthaben.
- Wenn die CPU-Auslastung höher als der Basiswert ist, sind die ausgegebenen Guthaben höher als die verdienten Guthaben

Wenn das verdiente Guthaben höher ist als das ausgegebene Guthaben, wird die Differenz als aufgelaufenes Guthaben bezeichnet, das später verwendet werden kann, um die CPU-Basisauslastung zu überschreiten. Wenn das ausgegebene Guthaben höher ist als das verdiente Guthaben, hängt das Verhalten der Instance ebenfalls vom Guthaben-Konfigurationsmodus ab – Standardmodus oder unbegrenzter Modus.

Wenn im Standardmodus das ausgegebene Guthaben höher ist als das verdiente Guthaben, verwendet die Instance das angesammelte Guthaben, um die CPU-Basisauslastung zu überschreiten. Wenn keine angesammelten Guthaben mehr vorhanden sind, sinkt die Instance allmählich auf die Baseline-CPU-Auslastung und kann nicht über die Baseline hinausgehen, bis mehr Guthaben angesammelt wird.

Wenn die Instance im unbegrenzten Modus über die Baseline-CPU-Auslastung hinausgeht, verwendet die Instance zuerst die aufgelaufenen Guthaben für das Burst. Wenn keine angesammelten Guthaben übrig sind, gibt die Instance das überschüssige Guthaben für das Burst aus. Wenn ihre CPU-Nutzung die Baseline unterschreitet, verwendet sie die verdienten CPU-Guthaben, um die zuvor verbrauchten überzähligen Guthaben wieder zurückzuzahlen. Die Fähigkeit

zum Verdienen von CPU-Guthaben und zum Abzahlen von überzähligem Guthaben ermöglicht Amazon EC2, die CPU-Nutzung einer Instance in einem 24-Stunden-Zeitraum anzugleichen. Wenn die durchschnittliche CPU-Auslastung über einen Zeitraum von 24 Stunden die Grundkapazität übersteigt, wird der Instance die zusätzliche Nutzung zu einer pauschalen Zusatzgebühr pro vCPU-Stunde in Rechnung gestellt.

Inhalt

Die wichtigsten Konzepte und Definitionen

Die folgenden Schlüsselkonzepte und Definitionen gelten für Burstable Performance Instances.

CPU-Auslastung

Die CPU-Auslastung ist der Prozentsatz der zugeordneten EC2-Recheneinheiten, die gegenwärtig auf der Instance verwendet werden. Diese Metrik misst den Prozentsatz der zugewiesenen CPU-Zyklen, die auf einer Instance verwendet werden. Die CloudWatch Metrik zur CPU-Auslastung zeigt die CPU-Auslastung pro Instanz und nicht die CPU-Auslastung pro Kern. Die Baseline-CPU-Spezifikation einer Instance basiert auch auf der CPU-Auslastung pro Instance. Informationen zur Messung der CPU-Auslastung mit dem AWS Management Console oder dem AWS CLI finden Sie unterAbrufen von Statistiken für eine bestimmte Instance.

CPU-Guthaben

Eine Einheit von vCPU-Zeit.

Beispiele:

1 CPU-Guthaben = 1 vCPU * 100 % Auslastung * 1 Minute.

1 CPU-Guthaben = 1 vCPU * 50 % Auslastung * 2 Minuten.

1 CPU-Guthaben = 2 vCPU * 25 % Auslastung * 2 Minuten.

Basisauslastung

Die Basisauslastung ist die Ebene, auf der die CPU für ein Nettoguthaben von Null genutzt werden kann, wenn die Anzahl der verdienten CPU-Guthaben mit der Anzahl der verwendeten CPU-Guthaben übereinstimmt. Die Basisauslastung wird auch als Baseline bezeichnet. Die Basisauslastung wird als Prozentsatz der vCPU-Auslastung ausgedrückt, die wie folgt berechnet wird: Basis-Auslastung in % = (Höhe des erworbenen Guthabens / Anzahl der vCPUs) / 60 Minuten.

Informationen zur Basisauslastung der einzelnen Burstable Performance Instances finden Sie in der Guthabentabelle.

Erworbenes Guthaben

Guthaben, die von einer Instance kontinuierlich gesammelt werden, wenn sie ausgeführt wird.

Anzahl der pro Stunde verdienten Guthaben = % Basis-Auslastung * Anzahl der vCPUs * 60 Minuten

Beispiel:

T3.nano mit 2 vCPUs und einer Basisauslastung von 5 % verdient 6 Guthaben pro Stunde, berechnet wie folgt:

2 vCPUs * 5 % Baseline * 60 Minuten = 6 Guthaben pro Stunde

Ausgelaufene oder genutzte Guthaben

Guthaben, die von einer Instance kontinuierlich genutzt werden, wenn sie ausgeführt wird.

CPU-Guthaben pro Minute = Anzahl der vCPUs * CPU-Auslastung * 1 Minute

Angesammelte Guthaben

Nicht ausgegebene CPU-Guthaben, wenn eine Instance weniger Guthaben benötigt, als für die Baseline-Auslastung erforderlich ist. Mit anderen Worten, aufgelaufene Guthaben = (verdiente Guthaben – Verwendete Guthaben) unterhalb der Basislinie.

Beispiel:

Wenn ein t3.nano mit einer CPU-Auslastung von 2 % läuft, die für eine Stunde unter der Baseline von 5 % liegt, werden die aufgelaufenen Guthaben wie folgt berechnet:

Angesammelte CPU-Guthaben = (verdiente Guthaben pro Stunde – verwendete Guthaben pro Stunde) = 6 – 2 vCPUs * 2 % CPU-Auslastung * 60 Minuten = 6 – 2,4 = 3,6 aufgelaufene Guthaben pro Stunde

Guthabenansammlungslimit

Hängt von der Instance-Größe ab, ist aber im Allgemeinen gleich der Anzahl der maximalen Guthaben, die in 24 Stunden verdient wurden.

Beispiel:

Für t3.nano, das Kreditabgrenzungslimit = 24 * 6 = 144 Guthaben

Startguthaben

Gilt nur für T2-Instances, die für den Standardmodus konfiguriert sind. Startguthaben sind eine begrenzte Anzahl von CPU-Guthaben, die einer neuen T2-Instance zugewiesen werden, damit sie beim Start im Standardmodus über die Baseline hinausgehen kann.

Überschüssiges Guthaben

Guthaben, die von einer Instance ausgegeben werden, nachdem sie ihr angesammeltes Guthaben aufgebraucht hat. Das überschüssige Guthaben ist für Burstable-Instances ausgelegt, um eine hohe Leistung über einen längeren Zeitraum aufrechtzuerhalten und werden nur im unbegrenzten Modus verwendet. Das überschüssige Guthaben wird verwendet, um zu bestimmen, wie viele Guthaben von der Instance für Burst im unbegrenzten Modus verwendet wurden.

Standardmodus

Der Guthaben-Konfigurationsmodus, der es einer Instance ermöglicht, über die Baseline zu springen, indem sie Guthaben ausgibt, die sie in ihrem Guthabenstand angesammelt hat.

Unbegrenzter Modus

Guthaben-Konfigurationsmodus, der es einer Instance ermöglicht, über die Baseline zu springen, indem sie bei Bedarf eine hohe CPU-Auslastung für einen beliebigen Zeitraum aufrechterhält. Der Instance-Stundenpreis deckt alle CPU-Nutzungsspitzen automatisch ab, wenn die durchschnittliche CPU-Nutzung der Instance in einem fortlaufendem 24-Stunden-Zeitraum oder über die Lebensdauer der Instance hinweg (es gilt der jeweils kürzere Zeitraum) bei oder unterhalb der Baseline liegt. Wenn die Instance für einen längeren Zeitraum mit einer höheren CPU-Nutzung ausgeführt wird, kann sie dies für eine pauschale Zusatzgebühr pro vCPU-Stunde tun.

In der folgenden Tabelle werden die wichtigsten Guthaben-Unterschiede zwischen den Burstable-Instance-Typen zusammengefasst.

Typ	Art der unterstützten CPU-Guthaben	Modi zur Konfiguration des Guthabens	Die Lebensdauer des aufgelaufenen CPU-Guthabens zwischen Instance- Starts und -Stopps
Neueste Generation			
T4g	Verdiente Guthaben, aufgelaufene Guthaben, ausgegebene Guthaben, überschüssige Guthaben (nur im unbegrenzten Modus)	Standard, Unbegrenzt (Standard)	7 Tage (Guthaben bleiben 7 Tage lang bestehen, nachdem eine Instance gestoppt wurde)
T3a	Verdiente Guthaben, aufgelaufene Guthaben, ausgegebene Guthaben, überschüssige Guthaben (nur im unbegrenzten Modus)	Standard, Unbegrenzt (Standard)	7 Tage (Guthaben bleiben 7 Tage lang bestehen, nachdem eine Instance gestoppt wurde)
T3	Verdiente Guthaben, aufgelaufene Guthaben, ausgegebene Guthaben, überschüssige Guthaben (nur im unbegrenzten Modus)	Standard, Unbegrenzt (Standard)	7 Tage (Guthaben bleiben 7 Tage lang bestehen, nachdem eine Instance gestoppt wurde)
Vorherige Generation			

Typ	Art der unterstützten CPU-Guthaben	Modi zur Konfiguration des Guthabens	Die Lebensdauer des aufgelaufenen CPU-Guthabens zwischen Instance- Starts und -Stopps
T2	Verdiente Guthaben, aufgelaufene Guthaben, ausgegebene Guthaben, Startguthaben (nur im Standardmodus), überschüssige Guthaben (nur im unbegrenzten Modus)	Standard (standard), Unbegrenzt	0 Tage (Guthaben gehen verloren, wenn eine Instance stoppt)

> **Note**
>
> Unbegrenzter Modus wird für T3-Instances, die auf einem Dedicated Host gestartet werden, nicht unterstützt.

Verdienen von CPU-Guthaben

Jede Burstable Performance Instance erhält kontinuierlich (mit einer Auflösung in Millisekunden) einen festgelegten Satz an CPU-Guthaben pro Stunde, der von der Instance-Größe abhängt. Der Berechnungsprozess dafür, ob Guthaben angesammelt oder verbraucht wird, geschieht ebenfalls in Millisekunden. Sie müssen sich also keine Sorgen machen, dass Sie zu viel CPU-Guthaben verbrauchen; durch eine kurzzeitige CPU-Steigerung wird nur ein Bruchteil des CPU-Guthabens verbraucht.

Wenn eine Burstable Performance Instance weniger CPU-Ressourcen verwendet, als für die Basisauslastung erforderlich ist (z. B. im Leerlauf), werden die nicht verbrauchten CPU-Guthaben dem CPU-Guthabenkonto gutgeschrieben. Benötigt eine Burstable Performance Instance eine höhere als die Basisauslastung, gibt sie die angesammelten Guthaben aus. Je mehr Guthaben sich für Ihre Burstable Performance Instance angesammelt hat, desto länger kann die Leistung über die Basisleistung hinaus gesteigert werden, wenn mehr CPU-Auslastung benötigt wird.

In der folgenden Tabelle sind die Burstable Performance Instances, die Rate, in der CPU-Guthaben pro Stunde verdient werden, die maximale Anzahl an CPU-Guthaben, die eine Instance ansammeln kann, die Anzahl der vCPUs pro Instance und die Basisauslastung als Prozentsatz eines vollständigen Kerns (unter Verwendung einer einzelnen vCPU) aufgelistet.

Instance-Typ	Pro Stunde erworbenes CPU-Guthaben	Maximal verdiente Guthaben, die angesammelt werden können*	vCPUs***	Basisauslastung pro vCPU
T2				
t2.nano	3	72	1	5 %
t2.micro	6	144	1	10 %
t2.small	12	288	1	20 %
t2.medium	24	576	2	20 %**
t2.large	36	864	2	30 %**
t2.xlarge	54	1 296	4	22,5 %**
t2.2xlarge	81,6	1 958,4	8	17 %**
T3				
t3.nano	6	144	2	5 %**
t3.micro	12	288	2	10 %**
t3.small	24	576	2	20 %**
t3.medium	24	576	2	20 %**
t3.large	36	864	2	30 %**
t3.xlarge	96	2 304	4	40 %**
t3.2xlarge	192	4 608	8	40 %**

Instance-Typ	Pro Stunde erworbenes CPU-Guthaben	Maximal verdiente Guthaben, die angesammelt werden können*	vCPUs***	Basisauslastung pro vCPU
T3a				
t3a.nano	6	144	2	5 %**
t3a.micro	12	288	2	10 %**
t3a.small	24	576	2	20 %**
t3a.medium	24	576	2	20 %**
t3a.large	36	864	2	30 %**
t3a.xlarge	96	2 304	4	40 %**
t3a.2xlarge	192	4 608	8	40 %**
T4g				
t4g.nano	6	144	2	5 %**
t4g.micro	12	288	2	10 %**
t4g.small	24	576	2	20 %**
t4g.medium	24	576	2	20 %**
t4g.large	36	864	2	30 %**
t4g.xlarge	96	2 304	4	40 %**
t4g.2xlarge	192	4 608	8	40 %**

* Die Anzahl der Guthaben, die angesammelt werden können, entspricht dem Guthaben, das in einem 24-Stunden-Zeitraum verdient werden kann.

** Die prozentuale Basisauslastung in der Tabelle angegeben pro vCPU In wird CloudWatc h die CPU-Auslastung pro vCPU angezeigt. Beispielsweise wird die CPU-Auslastung für eine `t3.large` Instanz, die auf der Basisebene betrieben wird, in den CloudWatch CPU-Metriken mit 30% angegeben. Weitere Informationen zum Berechnen der Basisauslastung finden Sie unter Basisauslastung.

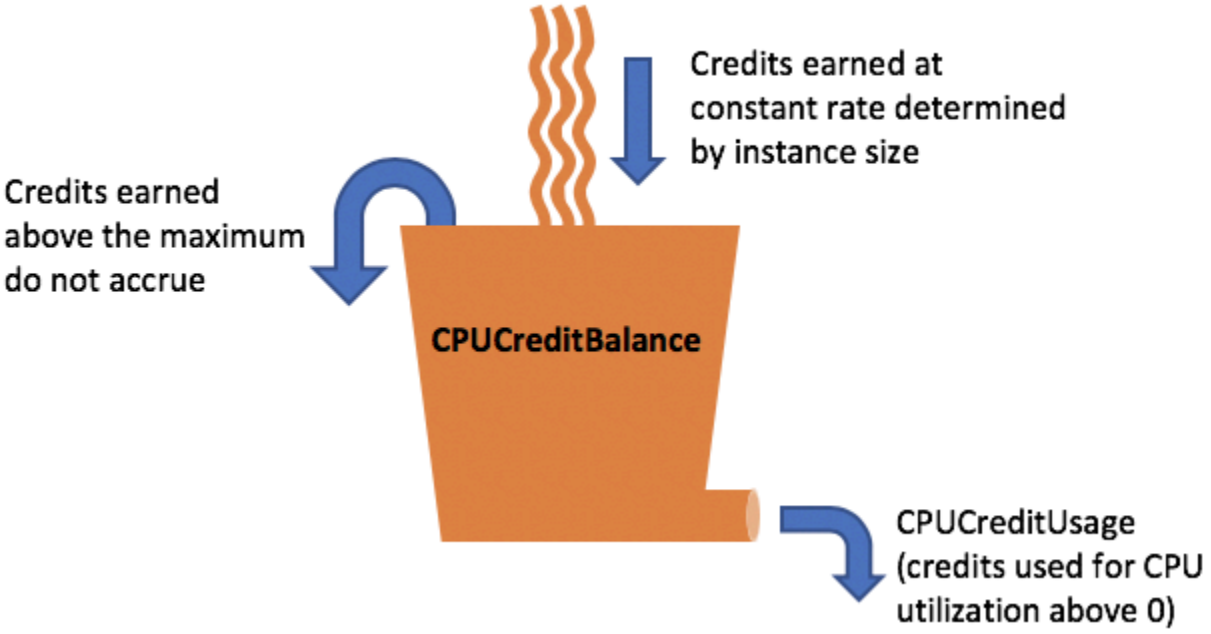
*** Jede vCPU ist ein Thread entweder eines Intel-Xeon-Kerns oder eines AMD-EPYC-Kerns, mit Ausnahme von T2- -Instances.

Erwerbsrate von CPU-Guthaben

Die Anzahl des pro Stunde erworbenen CPU-Guthabens wird anhand der Instance-Größe bestimmt. So erwirbt ein `t3.nano` z. B. sechs Guthaben pro Stunde, während ein `t3.small` 24 Guthaben pro Stunde erwirbt. Die oben stehende Tabelle listet die Guthaben-Erwerbsrate für alle Instances auf.

Limit für die Ansammlung von CPU-Guthaben

Während verdiente Guthaben für eine in Ausführung befindliche Instance nie ablaufen können, gibt es ein Limit für die Anzahl von Guthaben, die eine Instance ansammeln kann. Das Limit wird durch das CPU-Guthaben-Kontostand-Limit festgelegt. Nach Erreichen des Limits werden neu verdiente Guthaben verworfen, wie in folgendem Image angegeben. Der volle Bucket zeigt das CPU-Guthaben-Kontostand-Limit an, und der Überlauf zeigt neu verdiente Guthaben an, die das Limit überschreiten.



Das Limit für das CPU-Guthabenkonto ist von der jeweiligen Größe der jeweiligen -Instance abhängig. Beispielsweise kann eine `t3.micro`-Instance maximal 288 verdiente CPU-Guthaben auf dem CPU-Guthaben-Konto ansammeln. Die oben stehende Tabelle listet die Höchstzahl der verdienten Guthaben auf, die jede -Instance ansammeln kann.

T2-Standard-Instances verdienen zudem Startguthaben. Das Startguthaben wird dem Limit für das CPU-Guthaben-Konto nicht angerechnet. Wenn eine T2-Instance ihr Startguthaben nicht ausgegeben hat und für einen Zeitraum von 24 Stunden im Leerlauf verbleibt, während verdiente Guthaben angesammelt werden, erscheint sein CPU-Guthaben-Konto über dem Limit. Weitere Informationen finden Sie unter Startguthaben.

T4g-, T3a- und T3-Instances verdienen keine Startguthaben. Diese Instances werden standardmäßig als `unlimited` gestartet und können daher die Leistung sofort beim Start steigern, ohne dass Startguthaben erforderlich wäre. T3-Instances, die auf einem Dedicated Host standardmäßig als `standard` gestartet werden; `unlimited`-Modus wird für T3-Instances auf einem Dedicated Host nicht unterstützt.

Lebensdauer des angefallenen CPU-Guthabens

CPU-Guthaben für eine laufende Instance verfallen nicht.

Der CPU-Guthaben-Kontostand bleibt zwischen dem Anhalten und Starten einer Instance für T2 jedoch nicht erhalten. Wenn Sie eine T2-Instance anhalten, verliert die Instance alle angesammelten Guthaben.

Für T4g, T3a und T3 bleibt der CPU-Guthaben-Kontostand sieben Tage nach dem Anhalten einer Instance erhalten. Danach verfällt das Guthaben. Falls Sie die Instance innerhalb von sieben Tagen starten, geht kein Guthaben verloren.

Weitere Informationen finden Sie `CPUCreditBalance` in der CloudWatch Metriktabelle.

Basisauslastung

Die Basisauslastung ist die Ebene, auf der die CPU für ein Nettoguthaben von Null genutzt werden kann, wenn die Anzahl der verdienten CPU-Guthaben mit der Anzahl der verwendeten CPU-Guthaben übereinstimmt. Die Basisauslastung wird auch als Baseline bezeichnet.

Die Basisauslastung wird als Prozentsatz der vCPU-Auslastung ausgedrückt, die wie folgt berechnet wird:

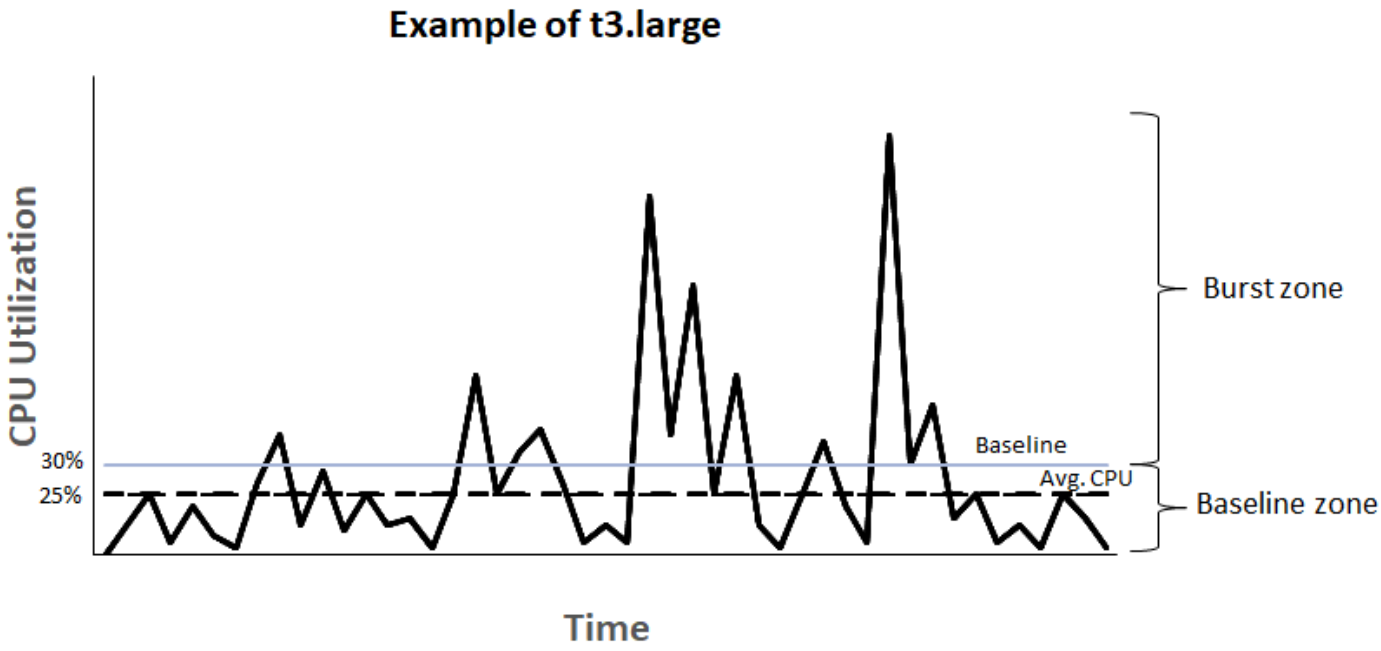
```
(number of credits earned/number of vCPUs)/60 minutes = % baseline utilization
```

Beispielsweise verdient eine `t3.nano`-Instance mit 2 vCPUs 6 Guthaben pro Stunde, was eine Basisauslastung von 5 % ergibt, die wie folgt berechnet wird:

```
(6 credits earned/2 vCPUs)/60 minutes = 5% baseline utilization
```

Eine `t3.large` Instance mit 2 vCPUs verdient 36 Credits pro Stunde, was einer Basisauslastung von 30% () entspricht. `(36/2)/60`

Das folgende Diagramm zeigt ein Beispiel für eine, `t3.large` bei der die durchschnittliche CPU-Auslastung unter dem Basiswert liegt.



Unbegrenzter Modus für Burstable Performance Instances

Eine als `unlimited` konfigurierte Burstable Performance Instance kann eine hohe CPU-Auslastung je nach Bedarf in jedem erforderlichen Zeitraum aufrechterhalten. Der Instance-Stundenpreis deckt alle CPU-Nutzungsspitzen automatisch ab, wenn die durchschnittliche CPU-Nutzung der Instance in einem fortlaufendem 24-Stunden-Zeitraum oder über die Lebensdauer der Instance hinweg (es gilt der jeweils kürzere Zeitraum) bei oder unterhalb der Baseline liegt.

Für eine Mehrzahl von allgemeinen Workloads bieten als `unlimited` konfigurierte Instances ausreichend Leistung ohne zusätzliche Gebühren. Wenn die Instance für einen längeren Zeitraum mit einer höheren CPU-Nutzung ausgeführt wird, kann sie dies zu einer pauschalen Zusatzgebühr pro vCPU-Stunde tun. Informationen zu den Preisen finden Sie unter Amazon EC2-Preise und Preise für unbegrenzten T2/T3/T4-Modus.

Wenn Sie eine `t2.micro`- oder `t3.micro`-Instance im Rahmen des Angebots Kostenloses Kontingent für AWS verwenden und sie im `unlimited`-Modus verwenden, können Gebühren anfallen, wenn Ihre durchschnittliche Auslastung in einem fortlaufendem 24-Stunden-Zeitraum die Basisauslastung der Instance überschreitet.

T4g-, T3a- und T3-Instances werden `unlimited` standardmäßig gestartet (sofern Sie die Standardeinstellung nicht ändern). Wenn die durchschnittliche CPU-Auslastung über einen Zeitraum von 24 Stunden den Basiswert überschreitet, werden ebenso Gebühren für überschüssiges

Guthaben anfallen. Wenn Sie Spot-Instances als `unlimited` starten und planen, sie sofort und für eine kurze Dauer ohne Leerlaufzeit für die Anrechnung von CPU-Guthaben zu verwenden, werden Gebühren für überschüssiges Guthaben entstehen. Wir empfehlen Ihnen, Spot-Instances im Standardmodus zu starten, um höhere Kosten zu vermeiden. Weitere Informationen finden Sie unter Für überzähliges Guthaben können Gebühren anfallen und Burstable Performance Instances.

> **Note**
>
> T3-Instances, die auf einem Dedicated Host standardmäßig als `standard` gestartet werden; `unlimited`-Modus wird für T3-Instances auf einem Dedicated Host nicht unterstützt.

Inhalt

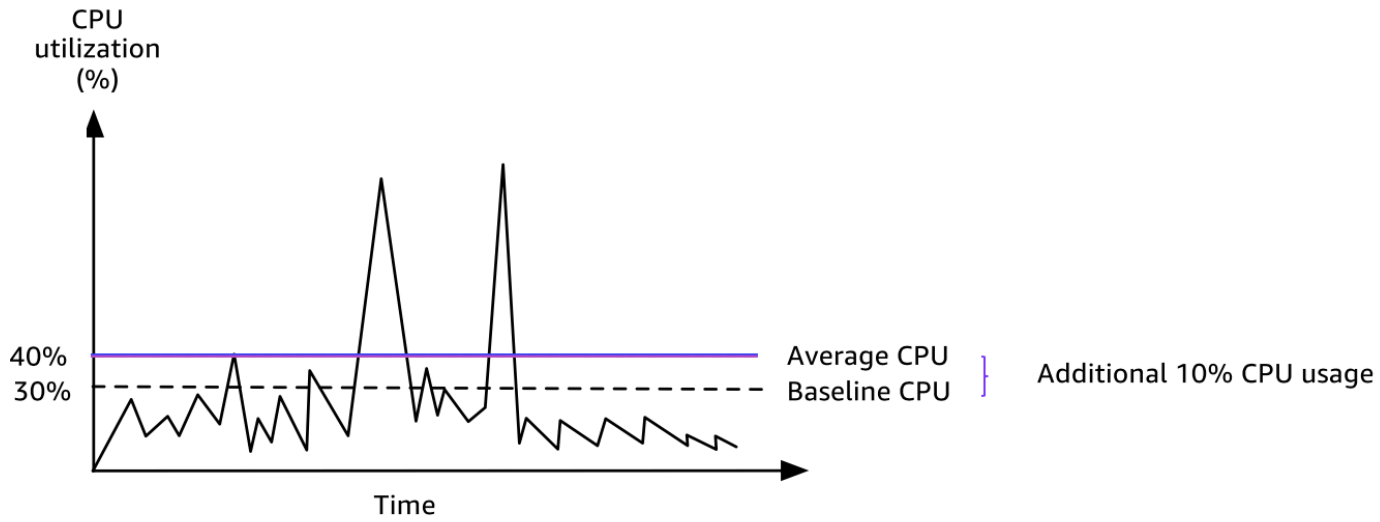
Konzepte für den unbegrenzten Modus

Der `unlimited`-Modus ist eine Guthabenkonfigurationsoption für Burstable Performance Instances. Er kann jederzeit für eine laufende oder angehaltene Instance aktiviert oder deaktiviert werden. Sie können diese Option auf Kontoebene pro AWS Region und pro Instance-Familie mit Burstable Performance `unlimited` als Standard-Kreditoption festlegen, sodass alle neuen Burstable-Performance-Instances im Konto mit der Standard-Kreditoption gestartet werden.

Funktionsweise der Unlimited Burstable Performance Instances

Wenn eine Burstable Performance Instance, die als `unlimited` konfiguriert ist, ihr CPU-Guthaben aufgebraucht hat, kann sie überzählige Guthaben verbrauchen, um die Leistung über die Baseline hinaus zu steigern. Wenn ihre CPU-Nutzung die Baseline unterschreitet, verwendet sie die verdienten CPU-Guthaben, um die zuvor verbrauchten überzähligen Guthaben wieder zurückzuzahlen. Die Fähigkeit zum Verdienen von CPU-Guthaben und zum Abzahlen von überzähligem Guthaben ermöglicht Amazon EC2, die CPU-Nutzung einer Instance in einem 24-Stunden-Zeitraum anzugleichen. Wenn die durchschnittliche CPU-Auslastung über einen Zeitraum von 24 Stunden die Grundkapazität übersteigt, wird der Instance die zusätzliche Nutzung zu einer pauschalen Zusatzgebühr pro vCPU-Stunde in Rechnung gestellt.

Das folgende Diagramm zeigt die CPU-Nutzung einer `t3.large`. Die CPU-Basisnutzung für eine `t3.large` ist 30 %. Wenn die Instance über einen Zeitraum von 24 Stunden mit einer CPU-Basisnutzung von durchschnittlich 30 % oder weniger ausgeführt wird, fallen keine zusätzlichen Gebühren an, da die Kosten bereits vom Stundenpreis der Instance abgedeckt werden. Wenn die Instance über einen Zeitraum von 24 Stunden jedoch mit einer CPU-Basisnutzung von durchschnittlich 40 % ausgeführt wird (siehe Diagramm), wird der Instance die zusätzliche CPU-Auslastung von 10 % zu einer pauschalen Zusatzgebühr pro vCPU-Stunde in Rechnung gestellt.



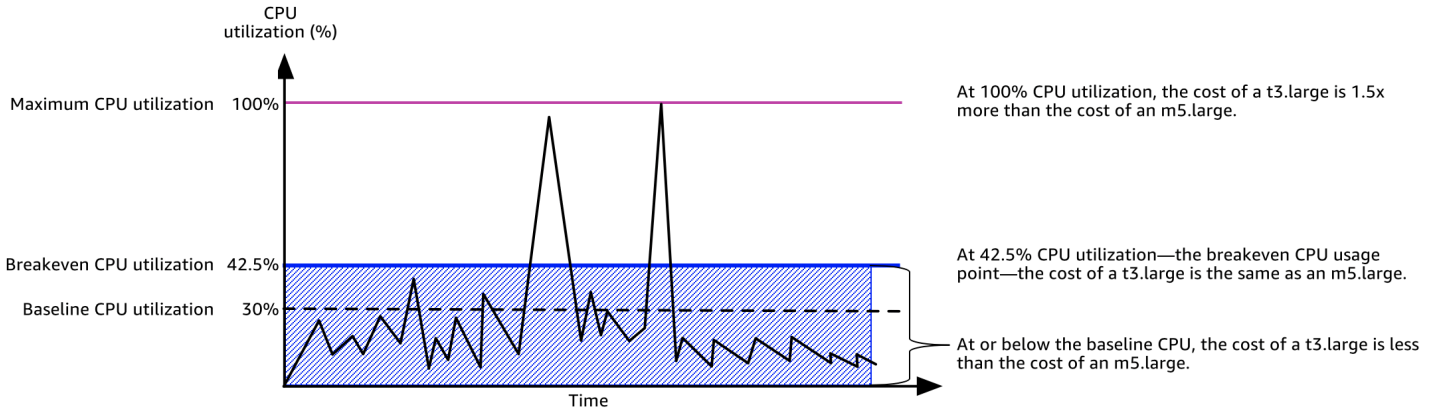
Weitere Informationen zur Basisauslastung pro vCPU für jeden Instance-Typ und dazu, wie viel Guthaben jeder Instance-Typ erwirbt, finden Sie in der Guthabentabelle.

Verwendung des unbegrenzten Modus im Vergleich zu einer festen CPU

Bei der Entscheidung, ob eine Burstable Performance Instances im `unlimited`-Modus, wie eine T3 oder eine Instance mit fester Leistung, wie eine M5, verwendet werden soll, müssen Sie den Break Even der CPU-Auslastung bestimmen. Der Break Even der CPU-Nutzung für eine Burstable Performance Instance ist der Punkt, an dem eine Burstable Performance Instance genauso günstig ist wie eine Instance mit fester Leistung. Anhand des Break Even der CPU-Nutzung können Sie Folgendes bestimmen:

- Wenn die durchschnittliche CPU-Nutzung in einem Zeitraum von 24 Stunden beim oder unterhalb des Break Even der CPU-Nutzung liegt, verwenden Sie eine Burstable Performance Instance im `unlimited`-Modus, sodass Sie vom niedrigeren Preis einer Burstable Performance Instance profitieren können, während Sie die gleiche Leistung wie bei einer Instance mit fester Leistung erhalten.
- Wenn die durchschnittliche CPU-Nutzung über einen Zeitraum von 24 Stunden oberhalb des Break Even der CPU-Nutzung liegt, kostet die Burstable Performance Instance mehr als die Instance mit fester Leistung gleicher Größe. Wenn eine T3-Instance kontinuierlich Spitzen bei 100 % CPU erreicht, zahlen etwa 1,5 Mal mehr als für eine M5-Instance der gleichen Größe.

Das folgende Diagramm zeigt den Break Even-CPU-Nutzungspunkt, an dem eine `t3.large` gleich viel kostet wie eine `m5.large`. Der Break Even-CPU-Nutzungspunkt für eine `t3.large` ist 42,5 %. Wenn die durchschnittliche CPU-Nutzung bei 42,5 % liegt, kostet das Ausführen von `t3.large` und `m5.large` das Gleiche, und es ist teurer, wenn die durchschnittliche CPU-Nutzung über 42,5 % liegt. Wenn der Workload weniger als die durchschnittliche CPU-Nutzung von 42,5 % erfordert, können Sie vom niedrigeren Preis der `t3.large` profitieren, während Sie die gleiche Leistung wie bei einer `m5.large` erhalten.



In der folgenden Tabelle wird gezeigt, wie Sie den Schwellenwert für den Break Even der CPU-Nutzung berechnen, sodass Sie bestimmen können, wann es weniger teuer ist, eine Burstable Performance Instance im `unlimited`-Modus oder eine Instance mit fester Leistung zu verwenden. Die Spalten in der Tabelle sind von A bis K gekennzeichnet.

Instance-Typ	vCPUs	T3 Preis*/ Stunde	M5 Preis*/ Stunde	Preisunterschied	T3-Basisauslastung pro vCPU (%)	Gebühr pro vCPU-Stunde für überzählige Guthaben	Gebühr pro vCPU-Minute	Zusätzliche verfügbare Steigerungsminuten pro vCPU	Zusätzliche CPU % verfügbar	Break Even CPU %
A	B	C	D	E = D - C	F	G	H = G / 60	I = E/H	J = (I / 60) / B	K = F + J
t3.large	2	0,0835 US$	0,096 US$	0,0125 US	30 %	0.05 USD	0,000833 US	15	12,5%	42,5 %

* Preis basiert auf us-east-1 und Linux OS.

Die Tabelle bietet die folgenden Informationen:

- Spalte A zeigt den Instance-Typ `t3.large`.
- Spalte B zeigt die Anzahl der vCPUs für die `t3.large`.
- Spalte C zeigt den Preis einer `t3.large` pro Stunde.
- Spalte D zeigt den Preis einer `m5.large` pro Stunde.
- Spalte E zeigt den Preisunterschied zwischen der `t3.large` und der `m5.large`.
- Spalte F zeigt die Basisauslastung pro vCPU der `t3.large`, d. h. 30 %. Auf Baseline-Stufe deckt der Stundenpreis der Instance die Kosten der CPU-Nutzung ab.

- Spalte G zeigt die pauschale Zusatzgebühr pro vCPU-Stunde, die einer Instance in Rechnung gestellt wird, wenn sie ihre CPU-Nutzung auf 100 % steigert, nachdem sie ihr verdientes Guthaben aufgebraucht hat.
- Spalte H zeigt die pauschale Zusatzgebühr pro vCPU-Minute, die einer Instance in Rechnung gestellt wird, wenn sie ihre CPU-Nutzung auf 100 % steigert, nachdem sie ihr verdientes Guthaben aufgebraucht hat.
- Spalte I zeigt die Anzahl der zusätzlichen Minuten, die die `t3.large` pro Stunde bei 100 % CPU steigern kann, während der gleiche Preis pro Stunde wie bei einer `m5.large` bezahlt wird.
- Spalte J zeigt die zusätzliche CPU-Nutzung (in %) oberhalb der Baseline, die die Instance steigern kann, während der gleiche Preis pro Stunde wie bei einer `m5.large` bezahlt wird.
- Spalte K zeigt den Break Even der CPU-Nutzung (in %), den die `t3.large` steigern kann, ohne mehr zu bezahlen als bei der `m5.large`. Bei allem, was darüber hinausgeht, kostet die `t3.large` mehr als die `m5.large`.

Die folgende Tabelle zeigt den Break Even der CPU-Nutzung (in %) für T3-Instance-Typen im Vergleich zu M5-Instance-Typen ähnlicher Größe.

T3-Instance-Typ	Break Even der CPU-Nutzung (in %) für T3 im Vergleich zu M5
`t3.large`	42,5%
`t3.xlarge`	52,5 %
`t3.2xlarge`	52,5 %

Für überzähliges Guthaben können Gebühren anfallen

Wenn die durchschnittliche CPU-Nutzung einer Instance bei oder unterhalb der Baseline liegt, werden für die Instance keine zusätzlichen Gebühren erhoben. Da eine Instance in einem 24-Stunden-Zeitraum eine Höchstzahl von Guthaben verdient (eine `t3.micro`-Instance kann z. B. in einem 24-Stunden-Zeitraum eine Höchstzahl von 288 Guthaben verdienen), kann sie überzählige Guthaben bis zu dieser Höchstzahl verbrauchen, ohne dass diese sofort in Rechnung gestellt werden.

Wenn die CPU-Nutzung jedoch oberhalb der Baseline verbleibt, kann die Instance nicht genügend Guthaben verdienen, um die verbrauchten überzähligen Guthaben zurückzuzahlen. Die überzähligen Guthaben, die nicht zurückgezahlt werden, werden zu einer pauschalen Zusatzgebühr pro vCPU-Stunde in Rechnung gestellt. Informationen zum Tarif finden Sie unter Preise für unbegrenzten T2/T3/T4g-Modus.

Überzählige Guthaben, die zuvor ausgegeben wurden, werden in Rechnung gestellt, wenn einer der folgenden Fälle auftritt:

- Die ausgegebenen überzähligen Guthaben überschreiten die maximale Anzahl an Guthaben, die die Instance in einem 24-Stunden-Zeitraum verdienen kann. Über das Maximum hinaus ausgegebene überzählige Guthaben werden am Ende der Stunde abgerechnet.
- Die Instance wird angehalten oder beendet.
- Die Instance wird von `unlimited` in `standard` geändert.

Verbrauchte überschüssige Credits werden anhand der CloudWatch Metrik erfasst. `CPUSurplusCreditBalance` Überschüssige Gutschriften, die in Rechnung gestellt werden, werden anhand der CloudWatch Kennzahl erfasst`CPUSurplusCreditsCharged`. Weitere Informationen finden Sie unter Zusätzliche CloudWatch Metriken für Instances mit hoher Leistung.

Kein Startguthaben für T2 Unlimited-Instances

T2-Standard-Instances erhalten Startguthaben, T2 Unlimited-Instances erhalten jedoch keines. Bei einer T2 Unlimited-Instance kann die Leistung jederzeit ohne zusätzliche Gebühren über die Basisleistung hinaus gesteigert werden, solange ihre durchschnittliche CPU-Nutzung in einem fortlaufendem 24-Stunden-Zeitraum oder über die Lebensdauer der Instance hinweg (es gilt der jeweils kürzere Zeitraum) bei oder unterhalb der Baseline liegt. Daher benötigen T2 Unlimited-Instances keine Startguthaben, um sofort nach dem Start eine hohe Leistung zu erzielen.

Wenn eine T2-Instance von `standard` in `unlimited` geändert wird, werden alle angesammelten Startguthaben vom `CPUCreditBalance` entfernt, bevor der verbleibende `CPUCreditBalance` übertragen wird.

T4g,T3a- und T3-Instances erhalten nie Startguthaben, da sie den unbegrenzten Modus unterstützen. Die Guthabenkonfiguration im unbegrenzten Modus ermöglicht es T4g-, T3a- und T3-Instances, so viel CPU wie nötig zu verwenden, um über die Baseline hinaus und so lange wie nötig zu gehen.

Unbegrenzten Modus aktivieren

Sie können für eine laufende oder angehaltene Instance jederzeit von `unlimited` zu `standard` und von `standard` zu `unlimited` wechseln. Weitere Informationen finden Sie unter Starten einer Burstable Performance Instance als Unlimited oder Standard und Ändern der Guthabenspezifikation einer Burstable Performance Instance.

Sie können auf Kontoebene pro AWS Region und pro Instance-Familie mit Burstable Performance die Standard-Kreditoption `unlimited` als Standard-Kreditoption festlegen, sodass alle neuen Burstable-Performance-Instances im Konto mit der Standard-Kreditoption gestartet werden. Weitere Informationen finden Sie unter Festlegen der standardmäßigen Guthaben-Spezifikation für das Konto.

Sie können überprüfen, ob Ihre Burstable Performance Instance als `unlimited` oder `standard` konfiguriert ist, über die Amazon-EC2-Konsole oder die AWS CLI. Weitere Informationen finden Sie unter Anzeigen der Guthabenspezifikation einer Burstable Performance Instance und Anzeigen der standardmäßigen Guthaben-Spezifikation.

Was passiert mit dem Guthaben beim Wechsel zwischen unbegrenzt und Standard?

`CPUCreditBalance`ist eine CloudWatch Metrik, die die Anzahl der von einer Instance gesammelten Credits erfasst. `CPUSurplusCreditBalance`ist eine CloudWatch Metrik, die die Anzahl der überschüssigen Credits erfasst, die von einer Instance ausgegeben wurden.

Wenn Sie eine als `unlimited` konfigurierte Instance in `standard` ändern, passiert Folgendes:

- Der `CPUCreditBalance`-Wert bleibt unverändert und wird übertragen.
- Der `CPUSurplusCreditBalance`-Wert wird sofort in Rechnung gestellt.

Wenn eine `standard`-Instance in `unlimited` geändert wird, passiert Folgendes:

- Der `CPUCreditBalance`-Wert, der das angesammelte verdiente Guthaben enthält, wird übertragen.
- Für T2 Standard-Instances werden alle Startguthaben vom `CPUCreditBalance`-Wert entfernt, und der verbleibende `CPUCreditBalance`-Wert mit angesammelten verdienten Guthaben wird übertragen.

Überwachen der Guthabennutzung

Um zu sehen, ob Ihre Instance mehr Credits ausgibt, als der Basiswert vorsieht, können Sie die Nutzung anhand von CloudWatch Metriken verfolgen und stündliche Alarme einrichten, um über die Nutzung des Guthabens informiert zu werden. Weitere Informationen finden Sie unter Überwachen des CPU-Guthabens auf Instances mit Spitzenlastleistung.

Beispiele für den unbegrenzten Modus

In den folgenden Beispielen wird die Guthabennutzung für Instances erläutert, die als `unlimited` konfiguriert sind.

Beispiele

- Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Unlimited
- Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Unlimited

Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Unlimited

Dieses Beispiel veranschaulicht die CPU-Auslastung einer als `t3.nano` gestarteten `unlimited`-Instance und die Verwendung von verdienten und überzähligen Guthaben zur Aufrechterhaltung der CPU-Auslastung.

Eine `t3.nano`-Instance verdient 144 CPU-Guthaben in einem rollierenden 24-Stunden-Zeitraum, mit denen sie 144 Minuten an vCPU-Nutzung einlösen kann. Wenn ihr CPU-Guthabenguthaben aufgebraucht ist (dargestellt durch die CloudWatch Metrik`CPUCreditBalance`), kann sie überschüssige CPU-Guthaben — die sie noch nicht verdient hat — ausgeben, um sie so lange zu nutzen, wie sie benötigt. Da eine `t3.nano`-Instance in einem 24-Stunden-Zeitraum eine Höchstzahl von 144 Guthaben verdient, kann sie überzählige Guthaben bis zu dieser Höchstzahl verbrauchen, ohne dass diese sofort in Rechnung gestellt werden. Wenn sie mehr als 144 CPU-Guthaben verbraucht, wird ihr am Ende der Stunde die Differenz in Rechnung gestellt.

Das Beispiel soll anhand der folgenden Kurve veranschaulichen, wie eine Instance ihre Leistung sogar nach Verbrauch ihres `CPUCreditBalance` mithilfe überzähliger Guthaben steigern kann. Der folgende Workflow bezieht sich auf die nummerierten Endpunkte in der Kurve:

P1 – Bei 0 Stunden auf dem Graphen wird die Instance als `unlimited` gestartet und beginnt sofort, Guthaben zu verdienen. Die Instance bleibt ab dem Zeitpunkt, an dem sie gestartet wird, ungenutzt – die CPU-Auslastung beträgt 0 % – und es werden keine Guthabenpunkte ausgegeben. Alle nicht

verbrauchten Guthabenpunkt werden im Guthaben gesammelt. Die ersten 24 Stunden liegt die `CPUCreditUsage` bei 0 und der `CPUCreditBalance`-Wert erreicht den Höchstwert von 144.

P2 – In den nächsten 12 Stunden liegt die CPU-Nutzung bei 2,5 %, was unter der Baseline von 5 % liegt. Die Instance verdient mehr Guthaben, als sie verbraucht, `CPUCreditBalance`-Wert kann allerdings den Höchstwert von 144 Guthaben nicht übersteigen.

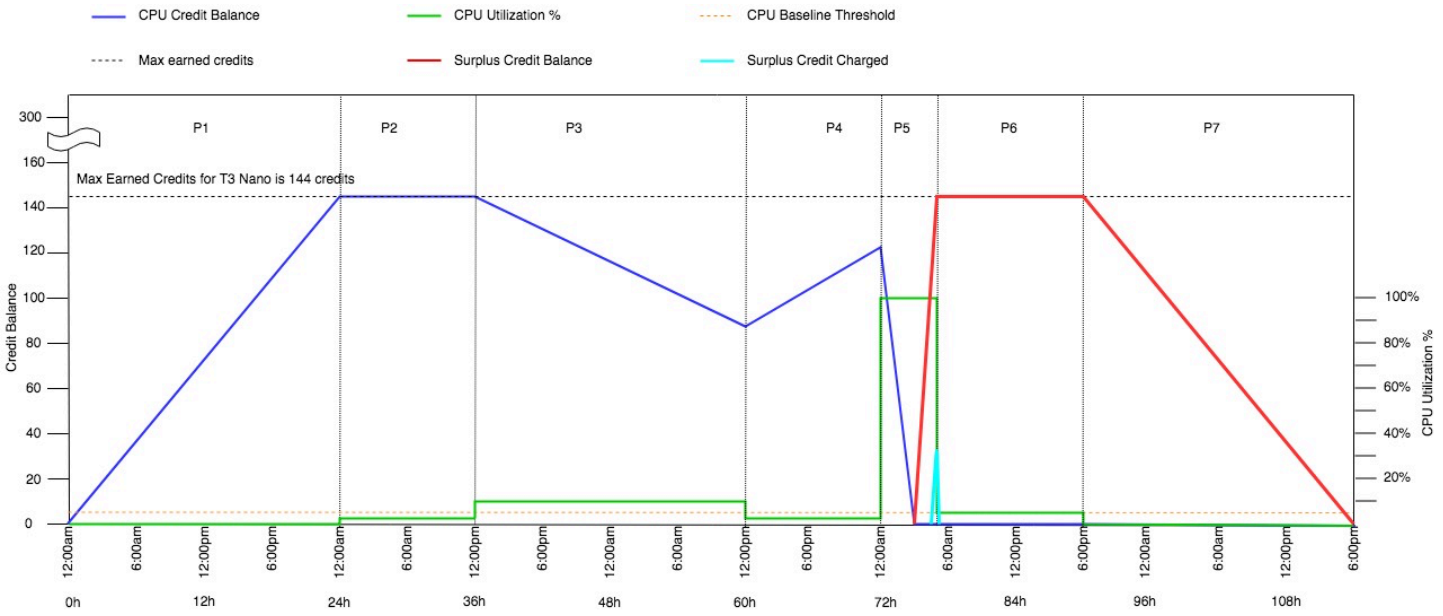
P3 – In den nächsten 24 Stunden liegt die CPU-Nutzung bei 7 % (über der Baseline), wodurch 57,6 Guthaben benötigt werden. Die Instance benötigt mehr Guthaben, als sie verdient, und der `CPUCreditBalance`-Wert wird auf 86,4 Guthaben reduziert.

P4 – In den nächsten 12 Stunden sinkt die CPU-Nutzung auf 2.5 % (unter der Baseline), wodurch 36 Guthaben benötigt werden. In dieser Zeit verdient die Instance 72 Guthaben. Die Instance verdient mehr Guthaben, als sie verbraucht, und der `CPUCreditBalance`-Wert steigt auf 122 Guthaben.

P5 – In den nächsten 5 Stunden steigert die Instance ihre CPU-Nutzung auf 100 % und verbraucht insgesamt 570 Guthaben, um die Laststeigerung aufrechtzuerhalten. Nach etwa einer Stunde hat die Instance ihr gesamtes `CPUCreditBalance`-Guthaben in Höhe von 122 aufgebraucht und benötigt überzähliges Guthaben, um die hohe CPU-Auslastung aufrechtzuerhalten. Dafür fallen 448 überzählige Guthaben in diesem Zeitraum an (570-122=448). Wenn der `CPUSurplusCreditBalance`-Wert 144 CPU-Guthaben erreicht (der Höchstwert, den eine `t3.nano`-Instance im Zeitraum von 24 Stunden verdienen kann), können keine überzähligen Guthaben, die danach verbraucht werden, durch verdiente Guthaben verrechnet werden. Für die danach verbrauchten überzähligen Guthaben in Summe von 304 Guthaben (448-144=304) fällt eine geringfügige zusätzliche Gebühr am Ende des Zeitraums in Höhe von 304 Guthaben an.

P6 – In den nächsten 13 Stunden liegt die CPU-Nutzung bei 5 % (Baseline). Die Instance verdient so viele Guthaben, wie sie ausgibt, ohne Überschuss zu Bezahlen des `CPUSurplusCreditBalance`. Der `CPUSurplusCreditBalance`-Wert verbleibt bei 144 Guthaben.

P7 – Für die letzten 24 Stunden in diesem Beispiel bleibt die Instance im Leerlauf und die CPU-Nutzung beträgt 0 %. Während dieser Zeit verdient die Instance 144 Guthaben, die zum Bezahlen des `CPUSurplusCreditBalance` verwendet werden.



Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Unlimited

Dieses Beispiel veranschaulicht die CPU-Auslastung einer als `t2.nano` gestarteten `unlimited`-Instance und die Verwendung von verdienten und überzähligen Guthaben zur Aufrechterhaltung der CPU-Auslastung.

Eine `t2.nano`-Instance verdient 72 CPU-Guthaben in einem rollierenden 24-Stunden-Zeitraum, mit denen sie 72 Minuten an vCPU-Nutzung einlösen kann. Wenn das CPU-Guthaben aufgebraucht ist (dargestellt durch die CloudWatch Metrik`CPUCreditBalance`), kann es überschüssige CPU-Guthaben — die es noch nicht verdient hat — ausgeben, um es so lange wie nötig zu nutzen. Da eine `t2.nano`-Instance in einem 24-Stunden-Zeitraum eine Höchstzahl von 72 Guthaben verdient, kann sie überzählige Guthaben bis zu dieser Höchstzahl verbrauchen, ohne dass diese sofort in Rechnung gestellt werden. Wenn sie mehr als 72 CPU-Guthaben verbraucht, wird ihr am Ende der Stunde die Differenz in Rechnung gestellt.

Das Beispiel soll anhand der folgenden Kurve veranschaulichen, wie eine Instance ihre Leistung sogar nach Verbrauch ihres `CPUCreditBalance` mithilfe überzähliger Guthaben steigern kann. Es wird davon ausgegangen, dass die Instance am Anfang des Zeitstrahls im Graphen die Höchstzahl des Guthabens verdient hat, die sie in 24 Stunden verdienen kann. Der folgende Workflow bezieht sich auf die nummerierten Endpunkte in der Kurve:

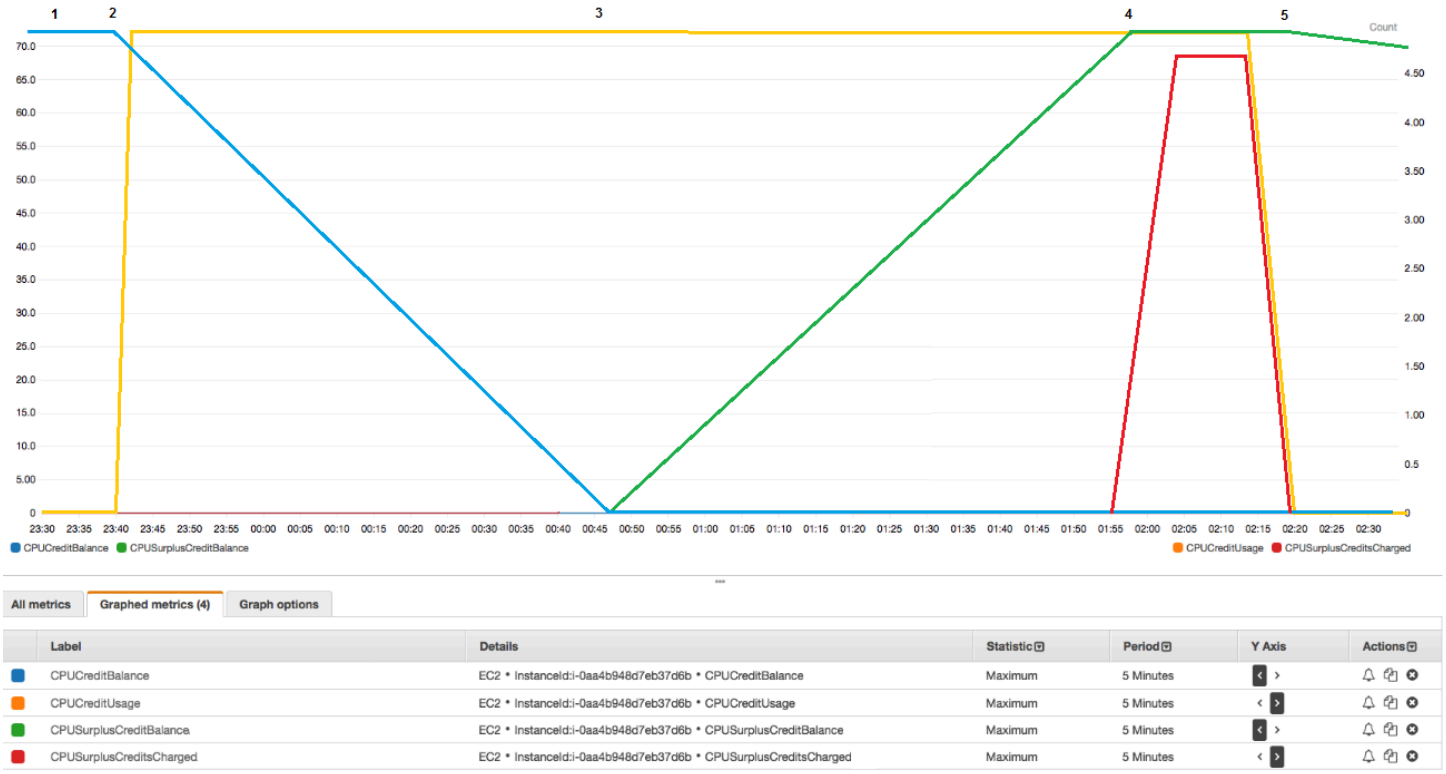
1 – In den ersten 10 Minuten beläuft sich `CPUCreditUsage` auf 0, und der `CPUCreditBalance`-Wert befindet sich weiterhin bei der Höchstzahl 72.

2 – Um 23.40 Uhr verbraucht die Instance mit zunehmender CPU-Nutzung CPU-Guthaben, und der `CPUCreditBalance`-Wert verringert sich.

3 – Gegen 00:47 Uhr hat die Instance ihr gesamtes `CPUCreditBalance` aufgebraucht und verbraucht nun überzählige Guthaben, um die hohe CPU-Auslastung aufrechtzuhalten.

4 – Überzählige Guthaben werden bis um 01.55 Uhr verwendet. Zu diesem Zeitpunkt erreicht der `CPUSurplusCreditBalance`-Wert 72 CPU-Guthaben. Dies entspricht der Höchstzahl, die eine `t2.nano`-Instance in einem 24-Stunden-Zeitraum verdienen kann. Alle danach verwendeten überzähligen Guthaben können innerhalb des 24-Stunden-Zeitraums nicht durch verdiente Guthaben ausgeglichen werden. Dies führt zu einer geringen zusätzlichen Gebühr am Ende der Stunde.

5 – Die Instance verwendet fortgesetzt überzählige Guthaben bis gegen 02.20 Uhr. Jetzt fällt die CPU-Nutzung unter die Baseline, und die Instance beginnt, 3 Guthaben pro Stunde (oder 0,25 Guthaben pro 5 Minuten) zu verdienen, die sie verwendet, um den `CPUSurplusCreditBalance` zurückzuzahlen. Nachdem der `CPUSurplusCreditBalance`-Wert auf 0 verringert wurde, beginnt die Instance, mit 0,25 Guthaben pro 5 Minuten, verdiente Guthaben in `CPUCreditBalance` anzusammeln.



Berechnung der Rechnung (Linux-Instanz)

Überschüssige Credits kosten 0,05$ pro vCPU-Stunde. Die Instance verbrauchte zwischen 01.55 Uhr und 02.20 Uhr ca. 25 überzählige Guthaben. Dies entspricht 0,42 vCPU-Stunden. Die zusätzlichen Gebühren für diese Instanz betragen 0,42 vCPU-Stunden x 0,05 USD/vCPU-Stunde = 0,021 USD, gerundet auf 0,02 USD. Hier ist die Abrechnung am Monatsende für diese T2 Unlimited-Instance:

Amazon Elastic Compute Cloud running Linux/UNIX		
$0.0058 per On Demand Linux t2.nano Instance Hour	720.000 Hrs	$4.18

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.05 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.02

Berechnung der Rechnung (Windows-Instanz)

Überschüssige Credits kosten 0,096$ pro vCPU-Stunde. Die Instance verbrauchte zwischen 01.55 Uhr und 02.20 Uhr ca. 25 überzählige Guthaben. Dies entspricht 0,42 vCPU-Stunden. Die zusätzlichen Gebühren für diese Instanz betragen 0,42 vCPU-Stunden x 0,096 USD/vCPU-Stunde = 0,04032 USD, gerundet auf 0,04 USD. Hier ist die Abrechnung am Monatsende für diese T2 Unlimited-Instance:

Amazon Elastic Compute Cloud running Windows		
$0.0081 per On Demand Windows t2.nano Instance Hour	720.000 Hrs	$5.83

Amazon Elastic Compute Cloud T2 CPU Credits		
$0.096 per vCPU-Hour of T2 CPU credits	0.420 vCPU-Hours	$0.04

Sie können Gebührenlimit-Warnungen einrichten, damit Sie jede Stunde über anfallende Gebühren benachrichtigt werden und ggf. Maßnahmen ergreifen können.

Standardmodus für Instances mit Spitzenlastleistung

Eine als `standard` konfigurierte Burstable Performance Instance ist für Workloads mit durchschnittlicher CPU-Auslastung geeignet, die dauerhaft unter der CPU-Basisauslastung der Instance liegt. Um die Basisleistung zu übersteigen, gibt die Instance Guthaben aus, die sie in ihrem CPU-Guthaben-Konto angesammelt hat. Wenn die Instance nicht mehr viele angesammelte Guthaben aufweist, wird die CPU-Auslastung schrittweise auf die Basisebene reduziert, sodass bei der Instance kein starker Leistungsrückgang auftritt, wenn ihr angesammelter CPU-Guthaben-Kontostand aufgebraucht ist. Weitere Informationen finden Sie unter Schlüsselkonzepte und Definitionen für Burstable Performance Instance.

Inhalt

Konzepte für den Standardmodus

Der `standard`-Modus ist eine Konfigurationsoption für Instances mit Spitzenleistung. Er kann jederzeit für eine laufende oder angehaltene Instance aktiviert oder deaktiviert werden. Sie können auf Kontoebene pro AWS Region und Instance-Familie mit Burstable Performance die Standard-Kreditoption `standard` als Standard-Kreditoption festlegen, sodass alle neuen Burstable-Performance-Instances im Konto mit der Standard-Kreditoption gestartet werden.

Funktionsweise der Standard-Instances mit Spitzenlastleistung

Wenn sich eine Burstable Performance Instance, die als `standard` konfiguriert ist, in einem Ausführungsstatus befindet, verdient sie kontinuierlich (mit einer Auflösung in Millisekunden) einen festgelegten Satz an verdientem Guthaben pro Stunde. Wenn eine T2-Standard-Instance beendet wird, verliert sie das gesamte angefallene Guthaben, und das Guthabenkonto wird auf Null zurückgesetzt. Wenn sie erneut gestartet wird, erhält sie einen neuen Satz an Startguthaben, und beginnt mit dem Sammeln von verdientem Guthaben. Für T4g-, T3a- und T3-Standard-Instances bleibt der CPU-Guthaben-Kontostand sieben Tage nach dem Anhalten einer Instance erhalten.

Danach verfällt das Guthaben. Falls Sie die Instance innerhalb von sieben Tagen starten, geht kein Guthaben verloren.

T2-Standard-Instances erhalten zwei Arten von CPU-Guthaben: erworbenes Guthaben und Startguthaben. Wenn sich eine T2 Standard-Instance in einem Ausführungsstatus befindet, verdient sie kontinuierlich (mit einer Auflösung in Millisekunden) einen festgelegten Satz an verdientem Guthaben pro Stunde. Beim Start hat sie noch kein Guthaben für eine gute Startuperfahrung verdient; daher erhält sie für einen gute Startuperfahrung Startguthaben, das sie zuerst ausgibt, während verdientes Guthaben gesammelt wird.

T4g,T3a- und T3-Instances erhalten kein Startguthaben, da sie den unbegrenzten Modus unterstützen. Die Guthabenkonfiguration im unbegrenzten Modus ermöglicht es T4g-, T3a- und T3-Instances, so viel CPU wie nötig zu verwenden, um über die Baseline hinaus und so lange wie nötig zu gehen.

Startguthaben

T2 Standard-Instances erhalten 30 Startguthaben pro vCPU beim Start oder Start, und T1 Standard-Instances erhalten 15 Startguthaben. So erhält z. B. eine `t2.micro`-Instance mit einer vCPU 30 Startguthaben, während ein `t2.xlarge`-Instance mit vier vCPUs 120 Startguthaben erhält. Das Startguthaben wurde für eine gute Startuperfahrung entwickelt, um die Steigerung der Leistung von Instances unmittelbar nach dem Start zu ermöglichen, bevor sie verdientes Guthaben angesammelt haben.

Das Startguthaben wird vor dem verdienten Guthaben verwendet. Nicht ausgegebenes Startguthaben wird auf dem CPU-Guthaben-Konto angesammelt, zählt aber nicht zum Limit für das CPU-Guthaben-Konto. Eine `t2.micro`-Instance hat beispielsweise ein Limit von 144 verdienten Guthaben für das CPU-Guthaben-Konto. Wenn sie gestartet und dann 24 Stunden lang nicht genutzt wird, erreicht ihr CPU-Guthaben-Kontostand den Wert 174 (30 Startguthaben + 144 verdiente Guthaben), womit das Limit überschritten ist. Nachdem die Instance jedoch die 30 Startguthaben verbraucht hat, darf der Guthaben-Kontostand 144 nicht überschreiten. Weitere Informationen zum Limit für das CPU-Guthaben-Konto für jede Instance-Größe finden Sie in der Guthabentabelle.

Die folgende Tabelle listet die anfängliche CPU-Guthabenzuordnung beim Start und die Anzahl der vCPUs auf.

Instance-Typ	Startguthaben	vCPUs
`t1.micro`	15	1

Instance-Typ	Startguthaben	vCPUs
t2.nano	30	1
t2.micro	30	1
t2.small	30	1
t2.medium	60	2
t2.large	60	2
t2.xlarge	120	4
t2.2xlarge	240	8

Startguthaben-Limits

Die Häufigkeit, mit der T2-Standard-Instances Startguthaben erhalten können, ist eingeschränkt. Das Standardlimit liegt bei 100 Startvorgängen aller T2-Standard-Instances zusammengenommen pro Konto, pro Region und pro rollierendem 24-Stunden-Zeitraum. Das Limit wird beispielsweise erreicht, wenn eine Instance innerhalb eines 24-Stunden-Zeitraums 100-mal angehalten und gestartet wird oder wenn 100 Instances innerhalb eines 24-Stunden-Zeitraums gestartet werden oder andere Kombinationen erfolgen, die 100 Starts entsprechen. Neue Konten weisen möglicherweise ein geringeres Limit auf, welches sich basierend auf Ihrer Nutzung im Laufe der Zeit erhöht.

> **Tip**
>
> Um sicherzustellen, dass Ihre Workloads immer die erforderliche Leistung erhalten, wechseln Sie zu Unbegrenzter Modus für Burstable Performance Instances oder erwägen die Verwendung einer größeren Instance-Größe.

Unterschiede zwischen Startguthaben und erworbenem Guthaben

Die folgende Tabelle führt die Unterschiede zwischen Startguthaben und erworbenem Guthaben auf.

	Startguthaben	Erworbenes Guthaben
Erwerbsrate von Guthaben	T2-Standard-Instances erhalten beim Start ein Startguthaben von 30 pro vCPU. Wenn eine T2-Instance von `unlimited` in `standard` geändert wird, erhält es beim Wechsel keine Startguthaben.	Jede T2-Instance erhält kontinuierlich (mit einer Auflösung in Millisekunden) einen festgelegten Satz an CPU-Guthaben pro Stunde, der von der Instance-Größe abhängt. Weitere Informationen zur Anzahl des CPU-Guthabens, das für jede Instance-Größe erworben wurde, finden Sie in der Guthabentabelle.
Erwerbslimit von Guthaben	Das Limit für den Erhalt von Startguthaben liegt bei 100 Startvorgängen aller T2-Standard-Instances zusammengenommen pro Konto, pro Region und pro rollierendem 24-Stunden-Zeitraum. Neue Konten weisen möglicherweise ein geringeres Limit auf, welches sich basierend auf Ihrer Nutzung im Laufe der Zeit erhöht.	Eine T2-Instance kann nicht mehr Guthaben ansammeln, als durch das Limit für das CPU-Guthaben-Konto zugelassen. Wenn das CPU-Guthaben-Konto sein Limit erreicht hat, werden alle Guthaben, die nach dem Erreichen des Limits verdient wurden, verworfen. Das Startguthaben wird dem Limit nicht angerechnet. Weitere Informationen zum Limit für das CPU-Guthaben-Konto für jede T2-Instance-Größe finden Sie in der Guthabentabelle.
Verwendung des Guthabens	Das Startguthaben wird vor dem verdienten Guthaben verwendet.	Verdientes Guthaben wird erst verwendet, nachdem das gesamte Startguthaben verbraucht wurde.
Ablauf des Guthabens	Wenn eine T2 Standard-Instance ausgeführt wird, verfällt das Startguthaben nicht. Wenn eine T2 Standard-Instance angehalten oder auf T2 Unlimited umgestellt wird, gehen alle Startguthaben verloren.	Wenn eine T2-Instance ausgeführt wird, verfällt das angesammelte verdiente Guthaben nicht. Wenn die T2-Instance beendet wird, geht das gesamte angesammelte verdiente Guthaben verloren.

Die Anzahl der aufgelaufenen Start-Credits und der aufgelaufenen verdienten Credits wird anhand der Metrik erfasst. CloudWatch `CPUCreditBalance` Weitere Informationen finden Sie `CPUCreditBalance` in der Tabelle mit den Kennzahlen. CloudWatch

Beispiele für den Standardmodus

In den folgenden Beispielen wird die Guthabennutzung für Instances erläutert, die als `standard` konfiguriert sind.

Beispiele

- Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Standard
- Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Standard

Beispiel 1: Beschreiben des Guthabenverbrauchs mit T3 Standard

In diesem Beispiel sehen Sie, wie eine als `t3.nano` gestartete `standard`-Instance earned-Guthaben verdient, sammelt und ausgibt. Der Guthaben-Kontostand zeigt die angesammelten earned-Guthaben an.

Eine ausgeführte `t3.nano`-Instance verdient alle 24 Stunden 144 Guthaben. Das Limit für den Guthaben-Kontostand beträgt 144 verdiente Guthaben. Nachdem das Limit erreicht ist, werden alle neu verdienten Guthabenpunkte verworfen. Weitere Informationen zur Anzahl des Guthabens, das sich verdienen und ansammeln lässt, finden Sie in der Guthabentabelle.

Sie können eine T3-Standard-Instance starten und sofort verwenden. Oder Sie können eine T3 Standard-Instance starten und sie für einige Tage inaktiv lassen, bevor Sie Anwendungen darauf ausführen. Ob eine Instance genutzt wird oder ungenutzt bleibt, entscheidet darüber, ob Punkte ausgegeben oder angesammelt werden. Falls eine Instance nach ihrem Start 24 Stunden lang im Leerlauf verbleibt, erreicht der Guthaben-Kontostand sein Limit, die maximale Anzahl verdienter Guthaben, die angesammelt werden kann.

Dieses Beispiel beschreibt eine Instance, die nach dem Start 24 Stunden lang untätig bleibt, und führt Sie durch sieben Zeitabschnitte über einen Zeitraum von 96 Stunden, wobei die Rate, mit der Punkte für das Guthaben verdient, aufgelaufen, ausgegeben und verworfen werden, und der Wert des Guthabens am Ende jeder Zeitraum angezeigt werden.

Der folgende Workflow bezieht sich auf die nummerierten Endpunkte in der Kurve:

P1 – Bei 0 Stunden auf dem Graphen wird die Instance als `standard` gestartet und beginnt sofort, Guthaben zu verdienen. Die Instance bleibt ab dem Zeitpunkt, an dem sie gestartet wird, ungenutzt –

die CPU-Auslastung beträgt 0 % – und es werden keine Guthabenpunkte ausgegeben. Alle nicht verbrauchten Guthabenpunkt werden im Guthaben gesammelt. Die ersten 24 Stunden liegt die `CPUCreditUsage` bei 0 und der `CPUCreditBalance`-Wert erreicht den Höchstwert von 144.

P2 – In den nächsten 12 Stunden liegt die CPU-Nutzung bei 2,5 %, was unter der Baseline von 5 % liegt. Die Instance verdient mehr Guthaben, als sie verbraucht, `CPUCreditBalance`-Wert kann allerdings den Höchstwert von 144 Guthaben nicht übersteigen. Sämtliche verdienten Guthaben über das Limit hinaus verfallen.

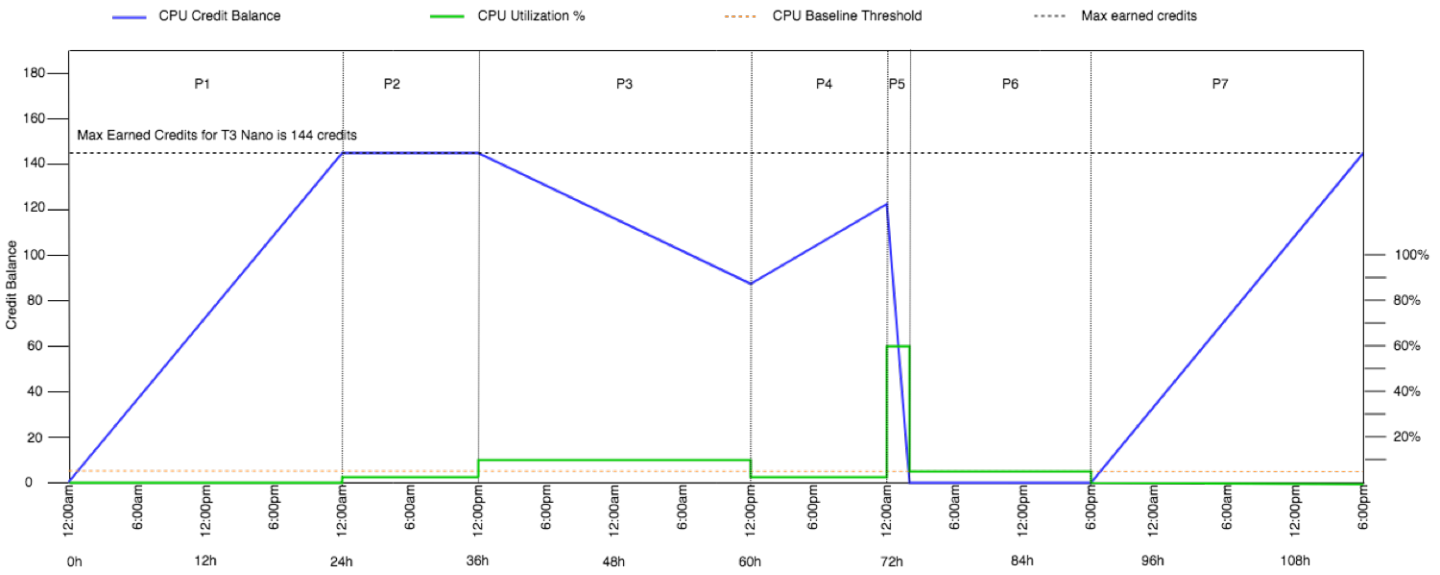
P3 – In den nächsten 24 Stunden liegt die CPU-Nutzung bei 7 % (über der Baseline), wodurch 57,6 Guthaben benötigt werden. Die Instance benötigt mehr Guthaben, als sie verdient, und der `CPUCreditBalance`-Wert wird auf 86,4 Guthaben reduziert.

P4 – In den nächsten 12 Stunden sinkt die CPU-Nutzung auf 2.5 % (unter der Baseline), wodurch 36 Guthaben benötigt werden. In dieser Zeit verdient die Instance 72 Guthaben. Die Instance verdient mehr Guthaben, als sie verbraucht, und der `CPUCreditBalance`-Wert steigt auf 122 Guthaben.

P5 – In den nächsten zwei Stunden steigert die Instance ihre CPU-Nutzung auf 60 % und verbraucht den gesamten `CPUCreditBalance`-Wert von 122 Guthaben. Am Ende dieses Zeitraums, wenn `CPUCreditBalance` gleich Null ist, wird ein Absinken der CPU-Auslastung auf die Basisauslastung von 5 % erzwungen. Auf Baseline-Stufe verdient die Instance so viel Guthaben, wie sie verbraucht.

P6 – In den nächsten 14 Stunden liegt die CPU-Nutzung bei 5 % (Baseline). Die Instance verdient so viele Guthaben, wie sie verbraucht. Der `CPUCreditBalance`-Wert verbleibt bei 0.

P7 – Für die letzten 24 Stunden in diesem Beispiel bleibt die Instance im Leerlauf und die CPU-Nutzung beträgt 0 %. Während dieser Zeit verdient die Instance 144 Guthaben, die im `CPUCreditBalance` angesammelt werden.



Beispiel 2: Beschreiben des Guthabenverbrauchs mit T2 Standard

In diesem Beispiel sehen Sie, wie eine als `t2.nano` gestartete `standard`-Instance launch- und earned-Guthaben verdient, sammelt und ausgibt. Sie sehen, wie das Guthaben nicht nur aufgelaufenes earned-Guthaben widerspiegelt, sondern auch aufgelaufenes launch-Guthaben.

Eine `t2.nano`-Instance erhält 30 Punkte Startguthaben, wenn sie gestartet wird, und verdient alle 24 Stunden 72 Punkte. Ihr Guthabenlimit beträgt 72 verdiente Punkte; Startguthaben wird nicht auf das Limit angerechnet. Nachdem das Limit erreicht ist, werden alle neu verdienten Guthabenpunkte verworfen. Weitere Informationen zur Anzahl des Guthabens, das sich verdienen und ansammeln lässt, finden Sie in der Guthabentabelle. Weitere Informationen zu Limits finden Sie unter Startguthaben-Limits.

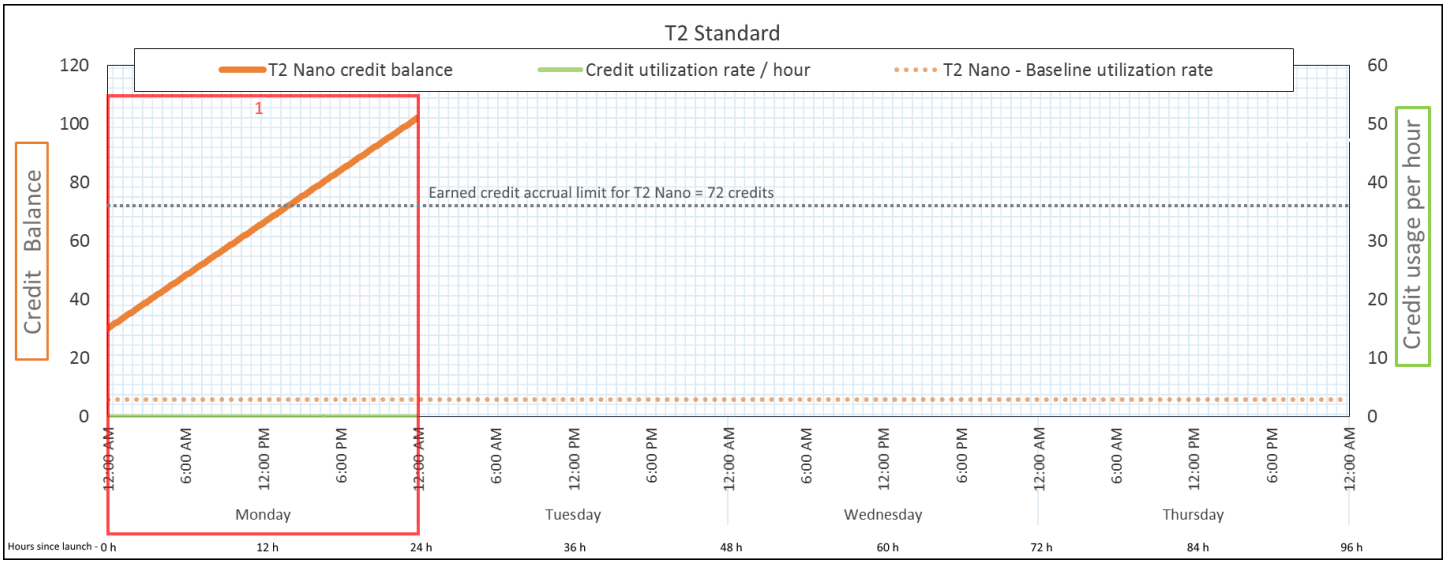
Sie können eine T2-Standard-Instance starten und sofort verwenden. Oder Sie können eine T2 Standard-Instance starten und sie für einige Tage inaktiv lassen, bevor Sie Anwendungen darauf ausführen. Ob eine Instance genutzt wird oder ungenutzt bleibt, entscheidet darüber, ob Punkte ausgegeben oder angesammelt werden. Wenn eine Instance nach dem Start 24 Stunden lang inaktiv bleibt, scheint das Guthaben sein Limit zu überschreiten, da das Guthaben sowohl die aufgelaufenen verdienten Punkte als auch das aufgelaufene Startguthaben widerspiegelt. Nach der Nutzung der CPU wird jedoch zuerst das Startguthaben ausgegeben. Danach spiegelt das Limit immer die maximale Anzahl des verdienten Startguthabens wider, die angesammelt werden können.

Dieses Beispiel beschreibt eine Instance, die nach dem Start 24 Stunden lang untätig bleibt, und führt Sie durch sieben Zeitabschnitte über einen Zeitraum von 96 Stunden, wobei die Rate, mit der

Punkte für das Guthaben verdient, aufgelaufen, ausgegeben und verworfen werden, und der Wert des Guthabens am Ende jeder Zeitraum angezeigt werden.

Zeitraum 1: 1–24 Stunden

Bei 0 Stunden auf dem Graphen wird die T2-Instance als `standard` gestartet und bekommt sofort 30 Punkte Startguthaben. Sie verdient Guthabenpunkte im laufenden Betrieb. Die Instance bleibt ab dem Zeitpunkt, an dem sie gestartet wird, ungenutzt – die CPU-Auslastung beträgt 0 % – und es werden keine Guthabenpunkte ausgegeben. Alle nicht verbrauchten Guthabenpunkt werden im Guthaben gesammelt. Etwa 14 Stunden nach dem Start beträgt das Guthaben 72 (30 Punkte Startguthaben + 42 Punkte verdientes Guthaben), was dem entspricht, was die Instance in 24 Stunden verdienen kann. 24 Stunden nach dem Start übersteigt das Guthaben 72 Punkte, da das nicht verbrauchte Startguthaben aufgelaufen ist. Es beträgt— nun 102 Punkte: 30 Punkte Startguthaben + 72 verdiente Punkte.



Ausgabe-Rate von Guthaben	0 Punkte pro 24 Stunden (0 % CPU-Auslastung)
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden
Verfall-Rate von Guthaben	0 Punkte pro 24 Stunden
Guthaben	102 Punkte (30 Punkte Startguthaben + 72 verdiente Punkte)

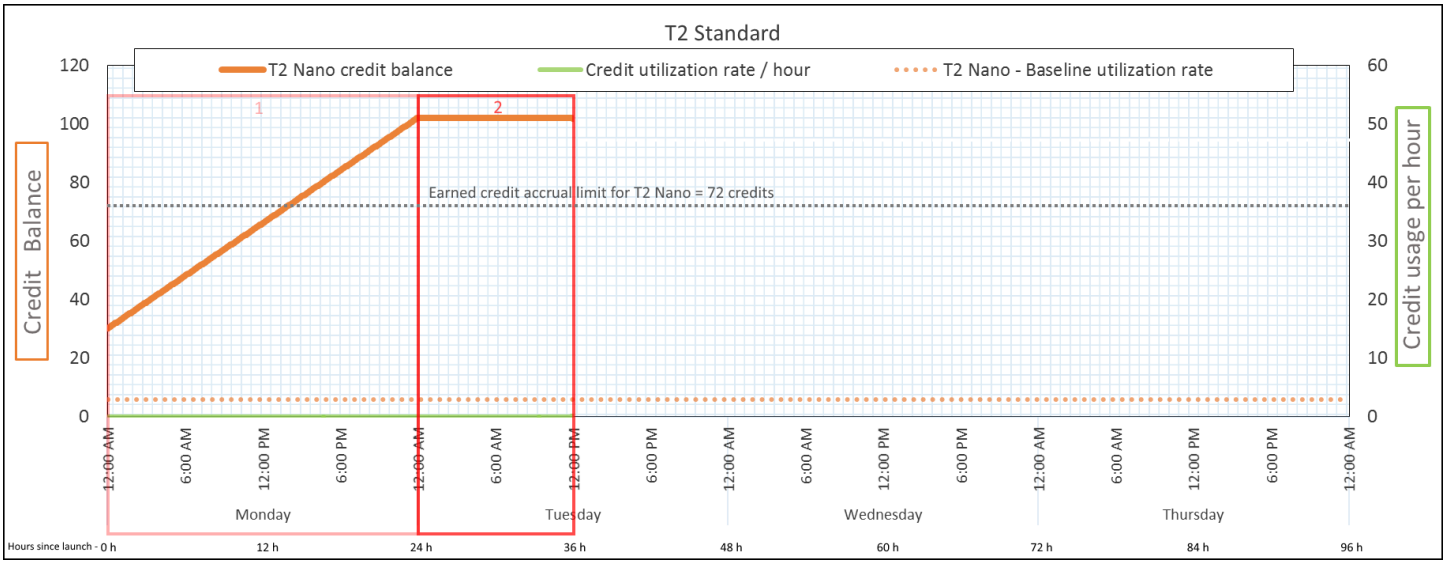
Schlussfolgerung

Wenn es nach dem Start keine CPU-Auslastung gibt, sammelt die Instance mehr Punkte, als sie in 24 Stunden verdienen kann (30 Punkte Startguthaben + 72 verdiente Punkte = 102 Punkte).

In einem realen Szenario verbraucht eine EC2 Instance während des Starts und des Betriebs geringfügig Punkte, was verhindert, dass das Guthaben den maximalen theoretischen Wert in diesem Beispiel erreicht.

Zeitraum 2: 25–36 Stunden

Für die nächsten 12 Stunden bleibt die Instance ungenutzt und verdient Punkte, aber das Guthaben erhöht sich nicht. Es verbleibt bei 102 Punkten (30 Punkte Startguthaben + 72 verdiente Punkte). Das Guthaben hat seine Grenze von 72 aufgelaufenen verdienten Punkten erreicht, sodass neu verdientes Guthaben verworfen wird.



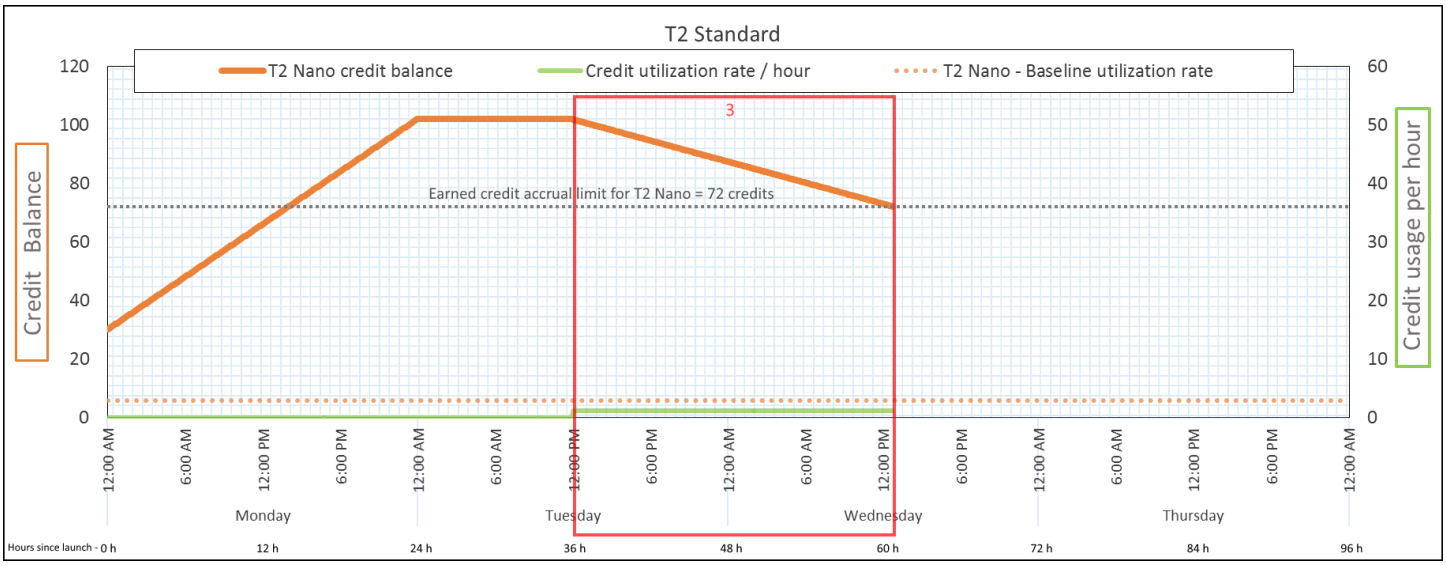
Ausgabe-Rate von Guthaben	0 Punkte pro 24 Stunden (0 % CPU-Auslastung)
Erwerbsrate von Guthaben	72 Credits pro 24 Stunden (3 Credits pro Stunde)
Verfall-Rate von Guthaben	72 Punkte pro 24 Stunden (100 % der Erwerbsrate von Guthaben)
Guthaben	102 Credits (30 Punkte Startguthaben + 72 verdiente Credits) — Saldo ist unverändert

Schlussfolgerung

Eine Instance verdient ständig Punkte, kann aber keine weiteren Punkte mehr sammeln, wenn das Guthaben sein Limit erreicht hat. Nach Erreichen des Limits werden neu verdiente Punkte verworfen. Das Startguthaben wird nicht auf das Guthabenlimit angerechnet. Wenn der Saldo aufgelaufenes Startguthaben enthält, scheint der Saldo über dem Limit zu liegen.

Zeitraum 3: 37–61 Stunden

Für die nächsten 25 Stunden verbraucht die Instance 2 % CPU, was 30 Punkte erfordert. Im gleichen Zeitraum verdient sie 75 Punkte, aber das Guthaben nimmt ab. Der Saldo verringert sich, weil das aufgelaufene Startguthaben zuerst verbraucht wird, während neu erworbenes Guthaben verworfen wird, weil das Guthaben bereits an der Grenze von 72 verdienten Punkten liegt.



Ausgabe-Rate von Guthaben	28,8 Credits pro 24 Stunden (1,2 Credits pro Stunde, 2 % CPU-Auslastung, 40 % der Kreditverdienstquote) — 30 Punkte über 25 Stunden
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden
Verfall-Rate von Guthaben	72 Punkte pro 24 Stunden (100 % der Erwerbsrate von Guthaben)

Guthaben	72 Punkte (30 Punkte Startguthaben wurden ausgegeben; 72 verdiente Punkte bleiben ungenutzt)

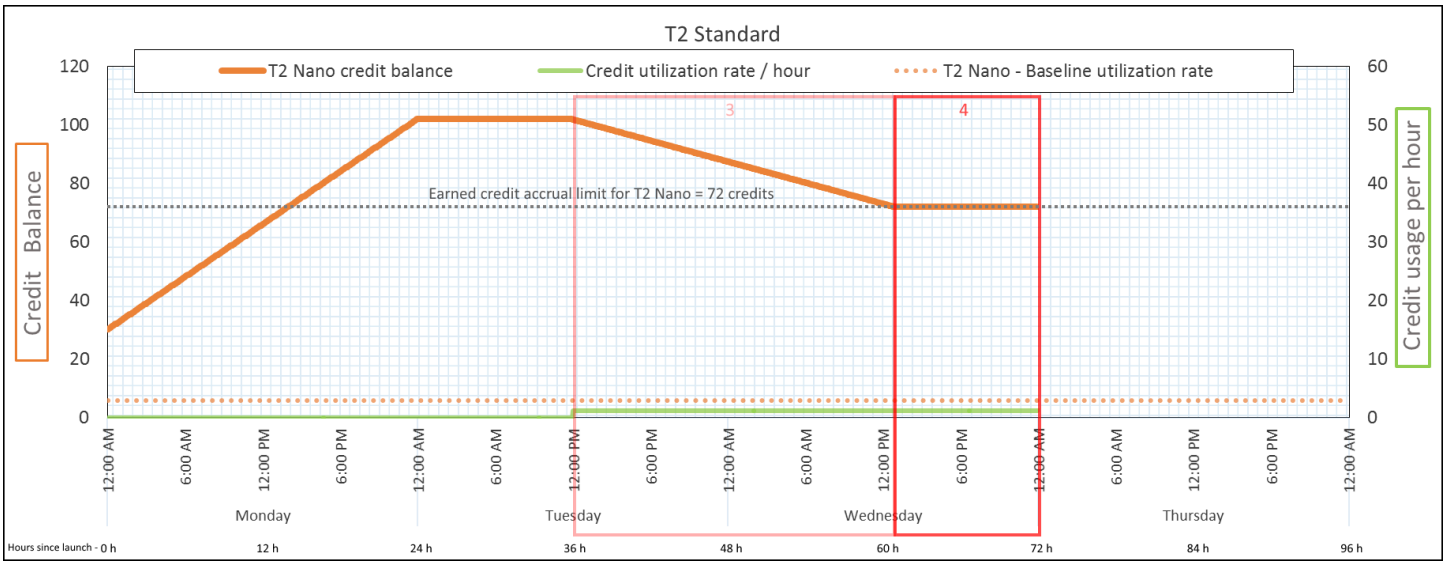
Schlussfolgerung

Eine Instance gibt zuerst das Startguthaben aus, bevor sie das verdiente Guthaben ausgibt. Das Startguthaben wird nicht auf das Guthabenlimit angerechnet. Nachdem das Startguthaben verbraucht ist, kann das Guthaben niemals höher sein als das, was in 24 Stunden verdient werden kann. Außerdem kann eine Instance, während sie läuft, kein weiteres Startguthaben erhalten.

Zeitraum 4: 62–72 Stunden

Für die nächsten 11 Stunden verbraucht die Instance 2 % CPU, was 13.2 Punkte erfordert. Dies ist die gleiche CPU-Auslastung wie im vorherigen Zeitraum, aber der Saldo sinkt nicht. Er bleibt bei 72 Punkten.

Der Saldo verringert sich nicht, da die Erwerbsrate von Guthaben höher ist als die Rate, mit der das Guthaben ausgegeben wird. In der Zeit, in der die Instance 13.2 Punkte ausgibt, verdient sie auch 33 Punkte. Das Saldo-Limit beträgt jedoch 72 Punkte, sodass alle verdienten Punkte, die das Limit überschreiten, verworfen werden. Der Saldo verbleibt bei 72 Punkten, die sich vom Stand von 102 Punkten in Zeitraum 2 unterscheiden, da es kein aufgelaufenes Startguthaben gibt.



Ausgabe-Rate von Guthaben	28,8 Credits pro 24 Stunden (1,2 Credits pro Stunde, 2 % CPU-Auslastung, 40 % der

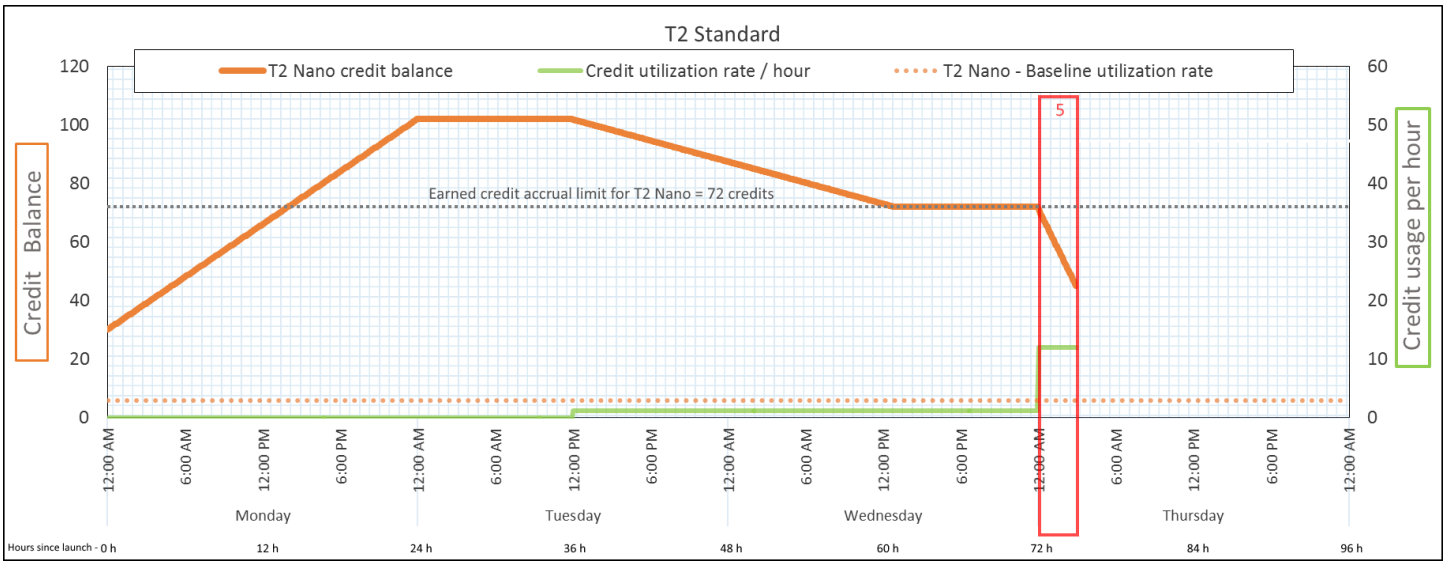
	Kreditverdienstquote) — 13,2 Punkte über 11 Stunden
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden
Verfall-Rate von Guthaben	43.2 Punkte pro 24 Stunden (60 % der Erwerbsrate von Guthaben)
Guthaben	72 Punkte (0 Punkte Startguthaben, 72 verdiente Punkte) — der Saldo ist am Limit

Schlussfolgerung

Nachdem das Startguthaben verbraucht ist, wird das Guthaben durch die Anzahl der Punkte bestimmt, die eine Instance innerhalb von 24 Stunden verdienen kann. Wenn die Instance mehr Punkte verdient, als sie ausgibt, werden neu verdiente Punkte über dem Limit verworfen.

Zeitraum 5: 73–75 Stunden

Für die nächsten drei Stunden verbraucht die Instance plötzlich 20 % CPU-Auslastung, was 36 Punkte erfordert. Die Instance verdient neun Punkte in den gleichen drei Stunden, was zu einer Verringerung des Nettosaldos um 27 Punkte führt. Am Ende von drei Stunden beträgt das Guthaben 45 aufgelaufene Punkte.



Ausgabe-Rate von Guthaben	288 Credits pro 24 Stunden (12 Credits pro Stunde, 20 % CPU-Auslastung, 400 % der

	Kreditverdienstquote) — 36 Punkte über 3 Stunden
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden (9 Punkte über 3 Stunden)
Verfall-Rate von Guthaben	0 Punkte pro 24 Stunden
Guthaben	45 Punkte (vorheriger Saldo [72] – verbrauchte Punkte [36] + verdiente Punkte [9]) — der Saldo sinkt mit einer Rate von 216 Punkten pro 24 Stunden (Ausgabenrate 288/24 + Erwerbsrate 72/24 = Saldoabnahmequote 216/24)

Schlussfolgerung

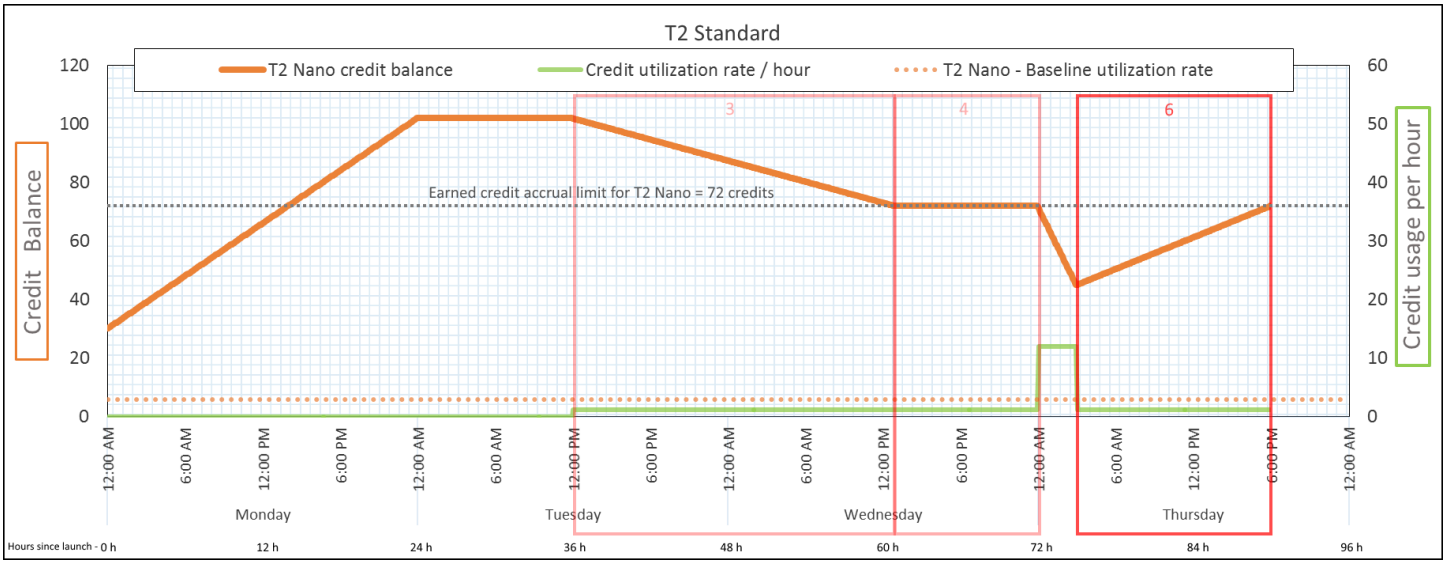
Wenn eine Instance mehr Punkte ausgibt, als sie verdient, verringert sich ihr Guthaben.

Zeitraum 6: 76–90 Stunden

Für die nächsten 15 Stunden verbraucht die Instance 2 % CPU, was 18 Punkte erfordert. Dies ist die gleiche CPU-Auslastung wie in den Zeiträumen 3 und 4. Allerdings steigt der Saldo in diesem Zeitraum an, während er im Zeitraum 3 zurückging und in Zeitraum 4 einen Höchstwert erreichte.

In Zeitraum 3 wurde das aufgelaufene Startguthaben verbraucht und alle verdienten Punkte, die das Guthaben-Limit überschritten haben, verworfen, was zu einem Rückgang des Guthabens führte. In Zeitraum 4 hat die Instance weniger Guthaben ausgegeben als sie verdient hat. Das verdiente Guthaben, das das Limit überschritt, wurde verworfen, so dass die Bilanz auf ihr Guthaben-Maximum von 72 stieg.

In diesem Zeitraum gibt es kein aufgelaufenes Startguthaben, und die Anzahl der aufgelaufenen verdienten Punkte im Saldo liegt unter dem Limit. Verdiente Punkte werden nicht verworfen. Außerdem verdient die Instance mehr Guthaben, als sie ausgibt, was zu einer Erhöhung des Guthabens führt.



Ausgabe-Rate von Guthaben	28,8 Credits pro 24 Stunden (1,2 Credits pro Stunde, 2 % CPU-Auslastung, 40 % der Kreditverdienstquote) — 18 Punkte über 15 Stunden
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden (45 Punkte über 15 Stunden)
Verfall-Rate von Guthaben	0 Punkte pro 24 Stunden
Guthaben	72 Punkte (Saldo steigt um 43,2 Punkte pro 24 Stunden — Änderungsrate = Ausgaberate 28,8/24 + Erwerbsrate 72/24)

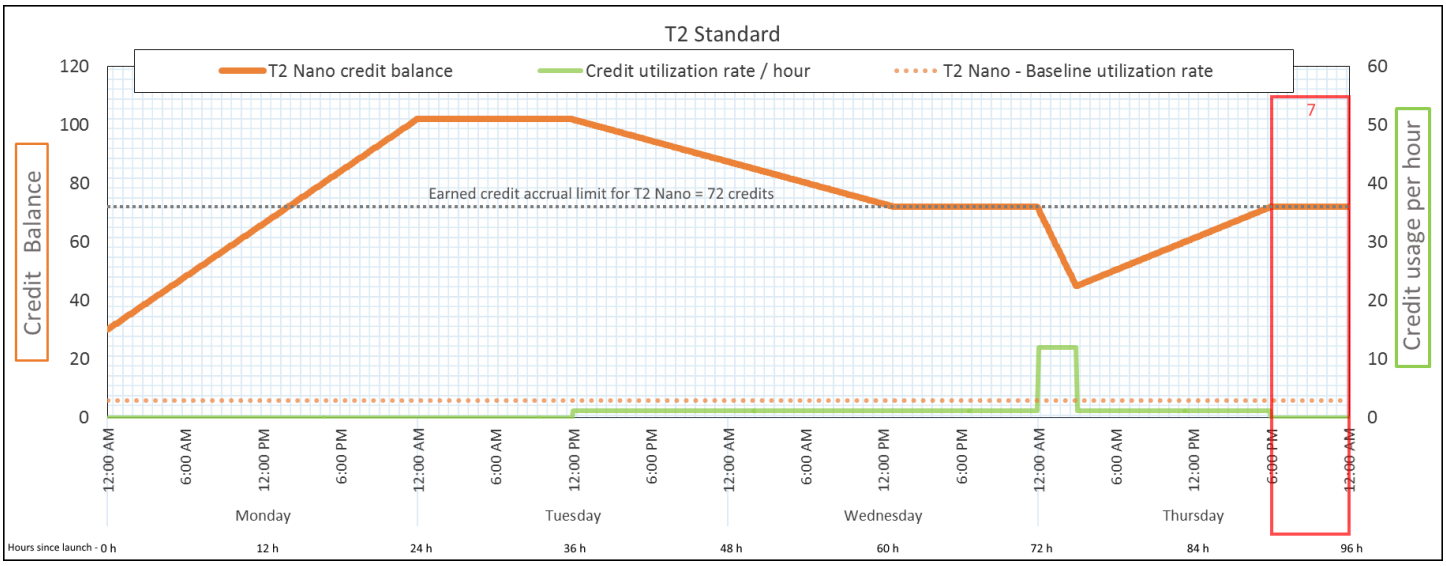
Schlussfolgerung

Wenn eine Instance weniger Punkte ausgibt, als sie verdient, erhöht sich ihr Guthaben.

Zeitraum 7: 91–96 Stunden

Für die nächsten sechs Stunden bleibt die Instance im Leerlauf, die CPU—Auslastung beträgt 0 % und es werden —keine Punkte ausgegeben. Dies ist die gleiche CPU-Auslastung wie im Zeitraum 2, aber der Saldo erreicht nicht 102 Punkte, sondern 72 Punkte, denn —dies ist das Guthabenlimit für die Instance.

Im Zeitraum 2 enthielt das Guthaben 30 aufgelaufene Punkte des Startguthabens. Das Startguthaben wurde in Zeitraum 3 ausgegeben. Eine laufende Instance kann kein weiteres Startguthaben erhalten. Nach Erreichen des Guthabenlimits werden alle verdienten Punkte, die das Limit überschreiten, verworfen.



Ausgabe-Rate von Guthaben	0 Punkte pro 24 Stunden (0 % CPU-Auslastung)
Erwerbsrate von Guthaben	72 Punkte pro 24 Stunden
Verfall-Rate von Guthaben	72 Punkte pro 24 Stunden (100 % der Erwerbsrate von Guthaben)
Guthaben	72 Punkte (0 Punkte Startguthaben, 72 verdiente Punkte)

Schlussfolgerung

Eine Instance verdient ständig Punkte, kann aber keine weiteren Punkte mehr sammeln, wenn das Guthabenlimit erreicht ist. Nach Erreichen des Limits werden neu verdiente Punkte verworfen. Das Guthabenlimit wird durch die Anzahl der Punkte bestimmt, die eine Instance in 24 Stunden verdienen kann. Weitere Informationen zu Guthabenlimits finden Sie in der Guthabentabelle.

Arbeiten mit Instances mit Spitzenlastleistung

Die Schritte zum Starten, Überwachen und Ändern von Burstable-Performance-Instances (T-Instances) sind ähnlich. Der wichtigste Unterschied ist die standardmäßige Guthaben-Festlegung beim Start.

Jede T-Instance-Familie verfügt über die folgende Standard-Kreditspezifikation:

- T4g-, T3a- und T3-Instances werden gestartet als `unlimited`
- T3-Instances auf einem Dedicated Host können nur als `standard` gestartet werden
- T2-Instances starten als `standard`

Sie können die standardmäßige Guthaben-Spezifikation für das Konto ändern.

Inhalt

Starten einer Burstable Performance Instance als Unlimited oder Standard

Sie können Ihre T-Instances als `unlimited` oder `standard` mit der Amazon EC2 EC2-Konsole, einem AWS SDK, einem Befehlszeilentool oder mit einer Auto Scaling Scaling-Gruppe starten.

Die folgenden Verfahren beschreiben, wie Sie die EC2-Konsole oder die verwenden. AWS CLI Informationen zur Verwendung einer Auto Scaling Scaling-Gruppe finden Sie unterVerwenden einer Auto Scaling-Gruppe zum Starten einer Burstable Performance Instance als Unlimited.

Console

So starten Sie eine T-Instance als Unlimited oder Standard

1. Befolgen Sie das Verfahren zum Starten einer Instance.

2. Wählen Sie unter Instance type (Instance-Typ) einen T-Instance-Typ aus.
3. Erweitern Sie Advanced details (Erweiterte Details) und wählen Sie für Credit specification (Gutschriftspezifikation) eine Gutschriftspezifikation aus. Wenn Sie keine Auswahl treffen, wird der Standard verwendet, der für T2 und `standard` für T4g, T3a und `unlimited` T3 gilt.
4. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

AWS CLI

Um eine T-Instance als Unlimited oder Standard zu starten

Starten Sie Ihre Instance mit dem Befehl run-instances (Instances ausführen). Geben Sie mit dem Parameter `--credit-specification CpuCredits=` die Guthaben-Spezifikation an. Gültige Guthaben-Spezifikation sind `unlimited` und `standard`.

- Wenn Sie für T4g, T3a und T3 den `--credit-specification` Parameter nicht angeben, wird die Instance standardmäßig `unlimited` gestartet.
- Wenn Sie für T2 den Parameter `--credit-specification` nicht einschließen, wird die Instance standardmäßig als `standard` gestartet.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --credit-specification "CpuCredits=unlimited"
```

Verwenden einer Auto Scaling-Gruppe zum Starten einer Burstable Performance Instance als Unlimited

Wenn T-Instances gestartet oder gestartet werden, benötigen sie CPU-Guthaben für ein gutes Bootstrapping-Erlebnis. Wenn Sie zum Starten Ihrer Instances eine Auto Scaling-Gruppe verwenden, empfehlen wir Ihnen, Ihre Instances als `unlimited` zu konfigurieren. Wenn Sie dies tun, verwenden die Instances überschüssige Guthaben, wenn sie von der Gruppe Auto Scaling automatisch gestartet oder neu gestartet werden. Mithilfe von überzähligen Guthaben lassen sich Leistungseinschränkungen verhindern.

Erstellen einer Startvorlage

Sie müssen eine launch template (Startvorlage) zum Starten von Instances als `unlimited` in einer Auto Scaling-Gruppe verwenden. Eine Startkonfiguration unterstützt das Starten von Instances als `unlimited` nicht.

> **Note**
>
> `unlimited`-Modus wird für T3-Instances, die auf einem Dedicated Host gestartet werden, nicht unterstützt.

Console

So erstellen Sie eine Startvorlage, die Instances als Unlimited startet

1. Folgen Sie dem Verfahren Erstellen einer Startvorlage mithilfe erweiterter Einstellungen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
2. Wählen Sie unter Inhalt der Startvorlage für Instance-Typ eine Instance-Größe aus.
3. Um Instances in einer Auto Scaling-Gruppe als `unlimited` zu starten, wählen Sie unter Erweiterte Details für Credit specification (Guthabenspezifikation) die Option Unbegrenzt aus.
4. Wenn Sie die Parameter der Startvorlage definiert haben, wählen Sie Create launch template.

AWS CLI

So erstellen Sie eine Startvorlage, die Instances als Unlimited startet

Verwenden Sie den Befehl create-launch-template und legen Sie `unlimited` als Guthaben-Spezifikation an.

- Wenn Sie für T4g, T3a und T3 den `CreditSpecification={CpuCredits=unlimited}` Wert nicht angeben, wird die Instance standardmäßig gestartet. `unlimited`
- Wenn Sie für T2 den Wert `CreditSpecification={CpuCredits=unlimited}` nicht einschließen, wird die Instance standardmäßig als `standard` gestartet.

```
aws ec2 create-launch-template \
    --launch-template-name MyLaunchTemplate \
```

```
    --version-description FirstVersion \
    --launch-template-data
ImageId=ami-8c1be5f6,InstanceType=t3.medium,CreditSpecification={CpuCredits=unlimited}
```

Zuordnen einer Auto Scaling-Gruppe zu einer Startvorlage

Um die Startvorlage einer Auto Scaling-Gruppe zuzuordnen, erstellen Sie die Auto Scaling-Gruppe mit der Startvorlage oder fügen Sie die Startvorlage einer vorhandenen Auto Scaling-Gruppe hinzu.

Console

So erstellen Sie eine Auto-Scaling-Gruppe mithilfe einer Startvorlage

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste oben auf dem Bildschirm dieselbe Region aus, die Sie bei der Erstellung der Startvorlage angegeben haben.
3. Wechseln Sie im Navigationsbereich zu Auto Scaling Groups und klicken Sie auf Create Auto Scaling Group.
4. Wählen Sie Launch Template (Startvorlage), Ihre Startvorlage und anschließend Next Step (Nächster Schritt) aus.
5. Füllen Sie die Felder für die Auto Scaling-Gruppe aus. Wenn Sie mit der Überprüfung Ihrer Konfigurationseinstellung auf der Seite Review (Überprüfung) fertig sind, wählen Sie Create Auto Scaling group (Auto Scaling-Gruppe erstellen). Weitere Informationen finden Sie unter Erstellen einer Auto Scaling -Gruppe mithilfe einer Startvorlage im Amazon EC2 Auto Scaling-Benutzerhandbuch.

AWS CLI

So erstellen Sie eine Auto-Scaling-Gruppe mithilfe einer Startvorlage

Verwenden Sie den AWS CLI Befehl create-auto-scaling-group und geben Sie den Parameter an. `--launch-template`

Console

So fügen Sie einer vorhandenen Auto-Scaling-Gruppe eine Startvorlage hinzu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie auf der Navigationsleiste oben auf dem Bildschirm dieselbe Region aus, die Sie bei der Erstellung der Startvorlage angegeben haben.
3. Wählen Sie im Navigationsbereich die Option Auto Scaling Groups (Gruppen).
4. Wählen Sie in der Liste der Auto Scaling-Gruppen eine Auto Scaling-Gruppe und dann die Optionen Actions (Aktionen) und Edit (Bearbeiten) aus.
5. Wählen Sie auf der Registerkarte Details für Launch Template (Startvorlage) eine Startvorlage und dann Save (Speichern).

AWS CLI

So fügen Sie einer vorhandenen Auto-Scaling-Gruppe eine Startvorlage hinzu

Verwenden Sie den AWS CLI Befehl update-auto-scaling-group und geben Sie den Parameter an. `--launch-template`

Anzeigen der Guthabenspezifikation einer Burstable Performance Instance

Sie können die Kreditspezifikation (`unlimited`oder`standard`) einer laufenden oder angehaltenen T-Instance einsehen.

Console

Um die Kreditspezifikation einer T-Instance einzusehen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie Details und zeigen Sie das Feld Credit specification (Guthaben-Spezifikation) an. Der Wert ist entweder `unlimited` oder `standard`.

AWS CLI

Um die Kreditspezifikation einer T-Instance zu beschreiben

Verwenden Sie den Befehl describe-instance-credit-specifications. Wenn Sie keine oder mehrere Instance-IDs angeben, werden alle Instances mit der Guthabenspezifikation `unlimited` sowie Instances zurückgegeben, die zuvor mit der Guthabenspezifikation `unlimited` konfiguriert

wurden. Wenn Sie beispielsweise die Größe einer T3-Instance auf eine M4-Instance ändern, während sie als `unlimited` konfiguriert ist, gibt Amazon EC2 die M4-Instance zurück.

```
aws ec2 describe-instance-credit-specifications --instance-id i-1234567890abcdef0
```

Beispielausgabe

```
{
  "InstanceCreditSpecifications": [
    {
        "InstanceId": "i-1234567890abcdef0",
        "CpuCredits": "unlimited"
    }
  ]
}
```

Ändern der Guthabenspezifikation einer Burstable Performance Instance

Sie können die Kreditspezifikation einer laufenden oder angehaltenen T-Instance jederzeit zwischen `unlimited` und ändern`standard`.

Beachten Sie, dass eine Instance im `unlimited`-Modus überschüssiges Guthaben einsetzen kann, wofür eine zusätzliche Gebühr anfallen kann. Weitere Informationen finden Sie unter Für überzähliges Guthaben können Gebühren anfallen.

Console

Um die Kreditspezifikation einer T-Instance zu ändern

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus. Um die Guthaben-Spezifikation für mehrere Instances auf einmal zu ändern, wählen Sie alle entsprechenden Instances aus.
4. Wählen Sie Aktionen, Instance-Einstellungen, Change credit specification (Guthabenspezifikation ändern). Diese Option ist nur aktiviert, wenn Sie eine T-Instance ausgewählt haben.

5. Um die Guthabenspezifikation auf `unlimited` zu ändern, aktivieren Sie das Kontrollkästchen neben der Instance-ID. Um die Guthabenspezifikation auf `standard` zu ändern, deaktivieren Sie das Kontrollkästchen neben der Instance-ID.

AWS CLI

Um die Kreditspezifikation einer T-Instance zu ändern

Verwenden Sie den Befehl modify-instance-credit-specification. Geben Sie die Instance und ihre Guthaben-Spezifikation mit dem Parameter `--instance-credit-specification` an. Gültige Guthaben-Spezifikation sind `unlimited` und `standard`.

```
aws ec2 modify-instance-credit-specification \
    --region us-east-1 \
    --instance-credit-specification
 "InstanceId=i-1234567890abcdef0,CpuCredits=unlimited"
```

Beispielausgabe

```
{
  "SuccessfulInstanceCreditSpecifications": [
    {
      "InstanceId": "i- 1234567890abcdef0"
    }
  ],
  "UnsuccessfulInstanceCreditSpecifications": []
}
```

Festlegen der standardmäßigen Guthaben-Spezifikation für das Konto

Jede T-Instance-Familie verfügt über eine Standard-Kreditspezifikation. Sie können die Standard-Kreditspezifikation für jede T-Instance-Familie auf Kontoebene pro AWS Region ändern.

Wenn Sie den Launch Instance Wizard in der EC2-Konsole verwenden, um Instances zu starten, überschreibt der Wert, den Sie für die Guthaben-Spezifikation auswählen, die standardmäßige Guthaben-Spezifikation auf Kontoebene. Wenn Sie die AWS CLI zum Starten von Instances verwenden, werden alle neuen T-Instances im Konto mit der Standard-Kreditspezifikation gestartet. Die Guthaben-Spezifikation für vorhandene laufende oder gestoppte Instances ist nicht davon betroffen.

Überlegungen

Die standardmäßige Guthaben-Spezifikation für eine Instance-Familie kann nur einmal in einem fortlaufenden 5-Minuten-Zeitraum und bis zu viermal in einem fortlaufenden 24-Stunden-Zeitraum geändert werden.

Console

So legen Sie die standardmäßige Guthaben-Spezifikation auf Kontoebene pro Region fest

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
4. Wählen Sie unter Kontoattribute die Option Standard-Guthaben-Spezifikation aus.
5. Wählen Sie Manage (Verwalten).
6. Wählen Sie für jede Instance-Familie Unlimited oder Standard und dann Update.

AWS CLI

So legen Sie die standardmäßige Guthaben-Spezifikation auf Kontoebene fest (AWS CLI)

Verwenden Sie den Befehl modify-default-credit-specification. Geben Sie mithilfe des `--cpu-credits`-Parameters die AWS -Region, die Instance-Familie und die standardmäßige Guthaben-Spezifikation an. Gültige standardmäßige Guthaben-Spezifikationen sind `unlimited` und `standard`.

```
aws ec2 modify-default-credit-specification \
    --region us-east-1 \
    --instance-family t2 \
    --cpu-credits unlimited
```

Anzeigen der standardmäßigen Guthaben-Spezifikation

Sie können die Standard-Kreditspezifikation einer T-Instance-Familie auf Kontoebene pro Region einsehen. AWS

Console

Um die Standard-Kreditspezifikation auf Kontoebene anzuzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Um die zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.
3. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
4. Wählen Sie unter Kontoattribute die Option Standard-Guthaben-Spezifikation aus.

AWS CLI

Um die Standard-Kreditspezifikation auf Kontoebene anzuzeigen

Verwenden Sie den Befehl get-default-credit-specification. Geben Sie die AWS -Region und die Instance-Familie an.

```
aws ec2 get-default-credit-specification --region us-east-1 --instance-family t2
```

Überwachen des CPU-Guthabens auf Instances mit Spitzenlastleistung

EC2 sendet Metriken an Amazon CloudWatch. Sie können die CPU-Guthabenmetriken in den Amazon EC2-Metriken pro Instance der CloudWatch Konsole einsehen oder indem Sie die AWS CLI Metriken für jede Instance auflisten. Weitere Informationen finden Sie unter Auflisten von Metriken mit der Konsole und Listen Sie Metriken auf, indem Sie AWS CLI.

Inhalt

Zusätzliche CloudWatch Metriken für Instances mit hoher Leistung

Burstable Performance-Instances verfügen über diese zusätzlichen CloudWatch Metriken, die alle fünf Minuten aktualisiert werden:

- `CPUCreditUsage` – Die Anzahl des während des Messzeitraums verbrauchten CPU-Guthabens.

- `CPUCreditBalance` – Die Anzahl von CPU-Guthaben, die eine Instance angesammelt hat. Dieser Saldo wird während der Steigerung der CPU-Leistung aufgebraucht, da die CPU-Guthaben schneller verbraucht als erworben werden.
- `CPUSurplusCreditBalance` – Die Anzahl der überzähligen CPU-Guthaben, die zur Aufrechterhaltung der CPU-Auslastung verwendet werden, wenn der `CPUCreditBalance`-Wert gleich Null ist.
- `CPUSurplusCreditsCharged` – Die Anzahl des überzähligen CPU-Guthabens, das die Höchstzahl des CPU-Guthabens überschritten hat, das in einem 24-Stunden-Zeitraum erworben werden kann, und für das daher eine zusätzliche Gebühr erhoben wird.

Die beiden letzten Metriken treffen nur auf Instances zu, die als `unlimited` konfiguriert wurden.

In der folgenden Tabelle werden die CloudWatch Metriken für Burstable-Performance-Instances beschrieben. Weitere Informationen finden Sie unter Listet die verfügbaren CloudWatch Metriken für Ihre Instances auf.

Metrik	Beschreibung
`CPUCreditUsage`	Die Anzahl der von der Instance für die CPU-Nutzung verbrauchten CPU-Guthaben. Ein CPU-Guthaben entspricht einer vCPU mit einer Auslastung von 100 % und einer Nutzungsdauer von einer Minute oder einer äquivalenten Kombination von vCPUs, Auslastung und Nutzungsdauer (z. B. eine vCPU mit einer Auslastung von 50 % mit einer Nutzungsdauer von zwei Minuten oder zwei vCPUs mit einer Auslastung von 25 % und einer Nutzungsdauer von zwei Minuten). Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar. Wenn Sie ein größeres Intervall als 5 Minuten angeben, verwenden Sie die Statistik `Sum` anstelle der Statistik `Average`. Einheiten: Guthaben (vCPU-Minuten)
`CPUCreditBalance`	Die Anzahl verdienter CPU-Guthaben, die eine Instance angesammelt hat, seit sie gestartet wurde. Für T2 Standard

Metrik	Beschreibung
	beinhaltet `CPUCreditBalance` auch die Anzahl der angesammelten Startguthaben. Guthaben werden auf dem Guthaben-Konto angesammelt, nachdem sie verdient wurden, und davon entfernt, wenn sie verbraucht werden. Der Guthaben-Kontostand hat ein maximales Limit, das anhand der Instance-Größe bestimmt wird. Nachdem das Limit erreicht ist, verfallen alle neu verdienten Guthabenpunkte. Für T2 Standard zählen Startguthaben nicht zum Limit. Die Guthaben in `CPUCreditBalance` sind verfügbar, um die Leistung der Instance über die Baseline ihrer CPU-Nutzung hinaus zu steigern. Wenn eine Instance ausgeführt wird, verfallen Guthaben im `CPUCreditBalance` nicht. Wenn eine T4g-, T3a- oder T3-Instance angehalten wird, bleibt der `CPUCreditBalance` Wert sieben Tage lang bestehen. Danach verfallen alle angesammelten Guthaben. Wenn eine T2-Instance beendet wird, bleibt der `CPUCreditBalance` -Wert nicht erhalten, und alle angesammelten Guthaben gehen verloren. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar. Einheiten: Guthaben (vCPU-Minuten)

Metrik	Beschreibung
`CPUSurplusCreditBalance`	Die Anzahl überzähliger Guthaben, die von einer `unlimited` -Instance verbraucht wurden, wenn ihr `CPUCreditBalance` -Wert null ist. Der `CPUSurplusCreditBalance` -Wert wird durch erworbene CPU-Guthaben abgezahlt. Wenn die Anzahl überzähliger Guthaben die Höchstzahl der Guthaben überschreitet, die die Instance in einem 24-Stunden-Zeitraum verdienen kann, fallen für die verbrauchten überzähligen Guthaben zusätzliche Gebühren an. Einheiten: Guthaben (vCPU-Minuten)
`CPUSurplusCreditsCharged`	Die Anzahl verbrauchter überzähliger Guthaben, die nicht durch verdiente CPU-Guthaben zurückgezahlt wurden, und für die deshalb eine zusätzliche Gebühr anfällt. Verbrauchte überzählige Guthaben werden in Rechnung gestellt, wenn einer der folgenden Fälle auftritt: • Die ausgegebenen überzähligen Guthaben überschreiten die maximale Anzahl an Guthaben, die die Instance in einem 24-Stunden-Zeitraum verdienen kann. Über das Maximum hinaus ausgegebene überzählige Guthaben werden am Ende der Stunde abgerechnet. • Die Instance wird angehalten oder beendet. • Die Instance wird von `unlimited` in `standard` geändert. Einheiten: Guthaben (vCPU-Minuten)

Berechnung der CPU-Guthabennutzung

Die CPU-Guthabenauslastung von Instances wird anhand der in der vorherigen Tabelle beschriebenen CloudWatch Instance-Metriken berechnet.

Amazon EC2 sendet die Metriken CloudWatch alle fünf Minuten. Ein Verweis auf einen vorherigen Wert einer Metrik an einem beliebigen Zeitpunkt setzt den vorherigen Wert der Metrik voraus, der vor fünf Minuten gesendet wurde.

Berechnen der CPU-Guthaben-Nutzung für Standard-Instances

- Der CPU-Guthaben-Kontostand erhöht sich, wenn die CPU-Nutzung unterhalb der Baseline liegt und weniger Guthaben verbraucht werden, als im vorherigen Fünf-Minuten-Zeitraum verdient wurden.
- Der CPU-Guthaben-Kontostand verringert sich, wenn die CPU-Nutzung oberhalb der Baseline liegt und mehr Guthaben verbraucht werden, als im vorherigen Fünf-Minuten-Zeitraum verdient wurden.

Mathematisch wird dies durch die folgende Gleichung erfasst:

Example

```
CPUCreditBalance = prior CPUCreditBalance + [Credits earned per hour * (5/60) -
 CPUCreditUsage]
```

Die Größe der Instance bestimmt die Anzahl der Guthaben, die die Instance pro Stunde verdienen kann, sowie der Anzahl der verdienten Guthaben, die sie auf dem Guthaben-Konto ansammeln kann. Weitere Informationen zur Anzahl der pro Stunde verdienten Guthaben, sowie zum Guthaben-Konto-Limit für die verschiedenen Instance-Größen finden Sie in der Guthabentabelle.

Beispiel

Dieses Beispiel verwendet eine `t3.nano`-Instance. Um den `CPUCreditBalance`-Wert der Instance zu berechnen, verwenden Sie folgendermaßen die obige Gleichung:

- `CPUCreditBalance` – Der aktuelle zu berechnende Guthaben-Kontostand.
- `prior CPUCreditBalance` – Der Guthaben-Kontostand vor fünf Minuten. In diesem Beispiel hat die Instance zwei Guthaben angesammelt.
- `Credits earned per hour` – Eine `t3.nano`-Instance erwirbt sechs Guthaben pro Stunde.
- `5/60`— Stellt das Fünf-Minuten-Intervall zwischen der Veröffentlichung der CloudWatch Metriken dar. Multiplizieren Sie die pro Stunde erworbenen Guthaben mit 5/60 (fünf Minuten), um die Anzahl der Guthaben zu erhalten, die die Instance in den letzten fünf Minuten erworben hat. Eine `t3.nano`-Instance erwirbt alle fünf Minuten 0,5 Guthaben.

- `CPUCreditUsage` – Wie viele Guthaben die Instance in den letzten fünf Minuten verbraucht hat. In diesem Beispiel verbrauchte die Instance in den letzten fünf Minuten ein Guthaben.

Anhand dieser Werte können Sie den `CPUCreditBalance`-Wert berechnen:

Example

```
CPUCreditBalance = 2 + [0.5 - 1] = 1.5
```

Berechnen der CPU-Guthaben-Nutzung für Unlimited-Instances

Wenn eine Burstable Performance Instance ihre Leistung über die Baseline hinaus steigern muss, verbraucht sie immer zuerst die verdienten Guthaben, bevor sie die überzähligen Guthaben verbraucht. Wenn ihr angesammeltes CPU-Guthaben aufgebraucht ist, kann sie so lange wie nötig zur CPU-Leistungssteigerung überzählige Guthaben verbrauchen. Wenn die CPU-Nutzung die Baseline unterschreitet, werden immer zuerst überzählige Guthaben abgezahlt, bevor die Instance erworbene Guthaben ansammelt.

Wir verwenden den Begriff `Adjusted balance` in den folgenden Gleichungen zur Bezeichnung der Aktivität, die in diesem Fünf-Minuten-Intervall stattfindet. Wir verwenden diesen Wert, um die Werte für die `CPUSurplusCreditBalance` CloudWatch Metriken `CPUCreditBalance` und zu ermitteln.

Example

```
Adjusted balance = [prior CPUCreditBalance - prior CPUSurplusCreditBalance] + [Credits
 earned per hour * (5/60) - CPUCreditUsage]
```

Ein Wert von `0` für `Adjusted balance` bedeutet, dass die Instance alle ihre verdienten Guthaben für die Leistungssteigerung verbraucht hat und keine überzähligen Guthaben verwendet wurden. Dies hat zur Folge, dass sowohl `CPUCreditBalance` als auch `CPUSurplusCreditBalance` auf `0` eingestellt werden.

Ein Wert von `Adjusted balance` bedeutet, dass die Instance erworbene Guthaben angesammelt hat und dass vorherige überzählige Guthaben, sofern vorhanden, abgezahlt wurden. Dies hat zur Folge, dass der `Adjusted balance`-Wert `CPUCreditBalance` zugewiesen und `CPUSurplusCreditBalance` auf `0` eingestellt wird. Die Instance-Größe bestimmt die maximale Anzahl an Guthaben, die die Instance ansammeln kann.

Example

```
CPUCreditBalance = min [max earned credit balance, Adjusted balance]
CPUSurplusCreditBalance = 0
```

Ein negativer Wert für `Adjusted balance` bedeutet, dass die Instance alle verdienten, angesammelte Guthaben verbraucht und zudem überzählige Guthaben für die Leistungssteigerung ausgegeben hat. Dies hat zur Folge, dass der `Adjusted balance`-Wert `CPUSurplusCreditBalance` zugewiesen und `CPUCreditBalance` auf `0` eingestellt wird. Auch hier bestimmt die Instance-Größe die maximale Anzahl an Guthaben, die die Instance ansammeln kann.

Example

```
CPUSurplusCreditBalance = min [max earned credit balance, -Adjusted balance]
CPUCreditBalance = 0
```

Wenn die ausgegebenen überzähligen Guthaben die Höchstzahl der Guthaben überschreiten, die die Instance ansammeln kann, wird der überzählige Guthaben-Kontostand wie in der obigen Gleichung veranschaulicht auf die Höchstzahl eingestellt. Für die restlichen überzähligen Guthaben werden wie von der `CPUSurplusCreditsCharged`-Metrik repräsentiert Gebühren berechnet.

Example

```
CPUSurplusCreditsCharged = max [-Adjusted balance - max earned credit balance, 0]
```

Wenn die Instance beendet wird, werden schließlich für alle im `CPUSurplusCreditBalance` nachverfolgten überzähligen Guthaben Gebühren berechnet. Wenn die Instance von `unlimited` in `standard` geändert wird, werden für den gesamten verbleibenden `CPUSurplusCreditBalance` ebenfalls Gebühren berechnet.

Leistungsbeschleunigung mit GPU-Instanzen

GPU-basierte Instances bieten Zugriff auf NVIDIA-GPUs mit Tausenden von Recheneinheiten. Mit diesen Instances können Sie wissenschaftliche, technische und Rendering-Anwendungen beschleunigen, indem Sie das CUDA- oder OpenCL-Framework (Open Computing Language) für die parallele Datenverarbeitung verwenden. Sie können sie außerdem für Grafikanwendungen verwenden, u. a. das Streamen von Spielen und 3-D-Anwendungen sowie andere Grafik-Workloads.

Bevor Sie eine GPU-basierte Instance aktivieren oder optimieren können, müssen Sie die entsprechenden Treiber wie folgt installieren:

- Informationen zur Installation von NVIDIA-Treibern auf einer Instanz mit angeschlossener NVIDIA-GPU, z. B. einer P3- oder G4dn-Instanz, finden Sie unter. Installieren Sie NVIDIA-Treiber
- Informationen zur Installation von AMD-Treibern auf einer Instanz mit angeschlossener AMD-GPU, z. B. einer G4ad-Instanz, finden Sie unter. Installieren Sie AMD-Treiber

Inhalt

Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 EC2-GPU-basierten Instances

Um die virtuellen GRID-Anwendungen auf GPU-basierten Instances mit NVIDIA-GPUs zu aktivieren (NVIDIA GRID Virtual Workstation ist standardmäßig aktiviert), müssen Sie den Produkttyp für den Treiber wie folgt definieren.

Aktivieren Sie virtuelle GRID-Anwendungen auf Linux-Instanzen

1. Erstellen Sie die Datei `/etc/nvidia/gridd.conf` aus der bereitgestellten Vorlagendatei.

   ```
   [ec2-user ~]$ sudo cp /etc/nvidia/gridd.conf.template /etc/nvidia/gridd.conf
   ```

2. Öffnen Sie die Datei `/etc/nvidia/gridd.conf` in Ihrem bevorzugten Texteditor.
3. Suchen Sie die Zeile `FeatureType` und setzen Sie den Wert auf `0`. Fügen Sie dann eine Zeile mit `IgnoreSP=TRUE` hinzu.

   ```
   FeatureType=0 IgnoreSP=TRUE
   ```

4. Speichern Sie die Datei und schließen Sie sie.
5. Starten Sie die Instance neu, damit die neue Konfiguration übernommen und angezeigt wird.

```
[ec2-user ~]$ sudo reboot
```

Aktivieren Sie virtuelle GRID-Anwendungen auf Windows-Instanzen

Aktivieren Sie virtuelle GRID-Anwendungen auf Windows-Instanzen

1. Führen Sie regedit.exe aus, um den Registrierungs-Editor zu öffnen.
2. Navigieren Sie zu `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global\GridLicensing`.
3. Öffnen Sie im rechten Bereich das Kontextmenü (Rechtsklick) und wählen Sie Neu und DWORD aus.
4. Geben Sie als Namen ein FeatureTypeund geben Sie ein`Enter`.
5. Öffnen Sie das Kontextmenü (Rechtsklick) FeatureTypeund wählen Sie Ändern.
6. Geben Sie für Wertdaten den Wert `0` for NVIDIA GRID Virtual Applications ein und wählen Sie OK.
7. Öffnen Sie im rechten Bereich das Kontextmenü (Rechtsklick) und wählen Sie Neu und DWORD aus.
8. Geben sie unter Name den Wert IgnoreSP und danach `Enter` ein.
9. Öffnen Sie das Kontextmenü (Rechtsklick) für IgnoreSP und wählen Sie Ändern aus.
10. Geben Sie für Wertdaten `1` ein und wählen Sie OK.
11. Schließen Sie den Registrierungs-Editor.

Optimieren Sie die GPU-Einstellungen auf Amazon EC2 EC2-Instances

Sie können verschiedene Optimierungen an den GPU-Einstellungen vornehmen, um die bestmögliche Leistung in Ihren NVIDIA-GPU-Instances zu erzielen. Bei einigen dieser Instance-Typen verwendet der NVIDIA-Treiber ein Autoboost-Feature, das die GPU-Taktfrequenzen variiert. Wenn Sie die Autoboost-Funktion deaktivieren und die GPU-Taktfrequenzen auf den maximalen Wert einstellen, können Sie in Ihren GPU-Instances permanent die maximale Leistung abrufen.

Optimieren Sie die GPU-Einstellungen unter Linux

1. Konfigurieren Sie die GPU für persistente Leistung. Die Ausführung dieses Befehls kann mehrere Minuten in Anspruch nehmen.

```
[ec2-user ~]$ sudo nvidia-persistenced
```

2. [Nur G3- und P2-Instances] Deaktivieren Sie die Autoboost-Funktion für alle GPUs auf der Instanz.

```
[ec2-user ~]$ sudo nvidia-smi --auto-boost-default=0
```

3. Setzen Sie alle GPU-Taktfrequenzen auf den Maximalwert. Verwenden Sie die in den folgenden befehlen angegebenen Speicher- und Grafik-Taktraten.

   Einige Versionen des NVIDIA-Treibers unterstützen keine Einstellung der Taktrate der Anwendung und werfen den `"Setting applications clocks is not supported for GPU..."`-Fehler auf, den Sie ignorieren können.

   - G3-Instances:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,1177
     ```

   - G4dn-Instances:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 5001,1590
     ```

   - G5-Instances:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 6250,1710
     ```

   - G6- und Gr6-Instanzen:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 6251,2040
     ```

   - P2-Instances:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 2505,875
     ```

   - P3- und P3dn-Instances:

     ```
     [ec2-user ~]$ sudo nvidia-smi -ac 877,1530
     ```

   - P4d-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- P4de-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- P5-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Optimieren Sie die GPU-Einstellungen unter Windows

1. Öffnen Sie ein PowerShell Fenster und navigieren Sie zum NVIDIA-Installationsordner.

```
cd "C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\"
```

2. [Nur G3- und P2-Instances] Deaktivieren Sie die Autoboost-Funktion für alle GPUs auf der Instanz.

```
.\nvidia-smi --auto-boost-default=0
```

3. Setzen Sie alle GPU-Taktfrequenzen auf den Maximalwert. Verwenden Sie die in den folgenden befehlen angegebenen Speicher- und Grafik-Taktraten.

   Einige Versionen des NVIDIA-Treibers unterstützen keine Einstellung der Taktrate der Anwendung und werfen den `"Setting applications clocks is not supported for GPU..."`-Fehler auf, den Sie ignorieren können.

   - G3-Instances:

```
.\nvidia-smi -ac "2505,1177"
```

   - G4dn-Instances:

```
.\nvidia-smi -ac "5001,1590"
```

   - G5-Instances:

```
.\nvidia-smi -ac "6250,1710"
```

- G6- und Gr6-Instanzen:

```
.\nvidia-smi -ac "6251,2040"
```

- P2-Instances:

```
.\nvidia-smi -ac "2505,875"
```

- P3- und P3dn-Instances:

```
.\nvidia-smi -ac "877,1530"
```

- P4d-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1215,1410
```

- P4de-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 1593,1410
```

- P5-Instances:

```
[ec2-user ~]$ sudo nvidia-smi -ac 2619,1980
```

Richten Sie zwei 4K-Displays auf G4ad-Linux-Instances ein

Eine G4ad-Instance launchen

1. Stellen Sie eine Verbindung zu Ihrer Linux-Instance her, um die PCI-Bus-Adresse der GPU zu erhalten, die Sie für Dual 4K (2x4k) anzielen möchten:

   ```
   lspci -vv | grep -i amd
   ```

   Sie erhalten eine Ausgabe, die dem Folgenden ähnelt:

   ```
   00:1e.0 Display controller: Advanced Micro Devices, Inc. [*AMD*/ATI] Device 7362 (rev
    c3)
   ```

```
Subsystem: Advanced Micro Devices, Inc. [AMD/ATI] Device 0a34
```

2. Beachten Sie, dass die PCI-Bus-Adresse in der obigen Ausgabe 00:1e.0 lautet. Erstellen Sie eine Datei mit dem Namen `/etc/modprobe.d/amdgpu.conf` und fügen Sie Folgendes hinzu:

```
options amdgpu virtual_display=0000:00:1e.0,2
```

3. Informationen zur Installation der AMD-Treiber unter Linux finden Sie unterInstallieren Sie AMD-Treiber auf Ihrer Amazon EC2 EC2-Instance. Wenn Sie den AMD-GPU-Treiber bereits installiert haben, müssen Sie die amdgpu-Kernelmodule über dkms neu erstellen.

4. Verwenden Sie die folgende xorg.conf-Datei, um die duale (2x4K) Bildschirmtopologie zu definieren, und speichern Sie die Datei in `/etc/X11/xorg.conf`:

```
~$ cat /etc/X11/xorg.conf
Section "ServerLayout"
    Identifier     "Layout0"
    Screen          0 "Screen0"
    Screen        1 "Screen1"
    InputDevice     "Keyboard0" "CoreKeyboard"
    InputDevice     "Mouse0" "CorePointer"
    Option          "Xinerama" "1"
EndSection
Section "Files"
    ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
    ModulePath "/opt/amdgpu/lib/xorg/modules"
    ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
    ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
    ModulePath "/usr/lib64/xorg/modules"
    ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Mouse0"
    Driver         "mouse"
    Option         "Protocol" "auto"
    Option         "Device" "/dev/psaux"
    Option         "Emulate3Buttons" "no"
    Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
    # generated from default
    Identifier     "Keyboard0"
```

```
    Driver         "kbd"
EndSection

Section "Monitor"
    Identifier     "Virtual"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "Primary" "true"
EndSection

Section "Monitor"
    Identifier     "Virtual-1"
    VendorName     "Unknown"
    ModelName      "Unknown"
    Option         "RightOf" "Virtual"
EndSection

Section "Device"
    Identifier     "Device0"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Device"
    Identifier     "Device1"
    Driver         "amdgpu"
    VendorName     "AMD"
    BoardName      "Radeon MxGPU V520"
    BusID          "PCI:0:30:0"
EndSection

Section "Extensions"
    Option         "DPMS" "Disable"
EndSection

Section "Screen"
    Identifier     "Screen0"
    Device         "Device0"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
```

```
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection

Section "Screen"
    Identifier     "Screen1"
    Device         "Device1"
    Monitor        "Virtual"
    DefaultDepth   24
    Option         "AllowEmptyInitialConfiguration" "True"
    SubSection "Display"
        Virtual    3840 2160
        Depth      32
    EndSubSection
EndSection
```

5. Richten Sie DCV ein, indem Sie die Anweisungen zum Einrichten eines interaktiven Desktops befolgen.
6. Nachdem die DCV-Einrichtung abgeschlossen ist, starten Sie neu.
7. Vergewissern Sie sich, dass der Treiber funktioniert:

```
dmesg | grep amdgpu
```

   Die Antwort sollte wie folgt aussehen:

```
Initialized amdgpu
```

8. Sie sollten in der Ausgabe für `DISPLAY=:0 xrandr -q` sehen, dass Sie 2 virtuelle Displays angeschlossen haben:

```
~$ DISPLAY=:0 xrandr -q
Screen 0: minimum 320 x 200, current 3840 x 1080, maximum 16384 x 16384
Virtual connected primary 1920x1080+0+0 (normal left inverted right x axis y axis)
 0mm x 0mm
 4096x3112  60.00
 3656x2664  59.99
 4096x2160  60.00
 3840x2160  60.00
 1920x1200  59.95
 1920x1080  60.00
```

```
   1600x1200  59.95
   1680x1050  60.00
   1400x1050  60.00
   1280x1024  59.95
   1440x900 59.99
   1280x960 59.99
   1280x854 59.95
   1280x800 59.96
   1280x720 59.97
   1152x768 59.95
   1024x768 60.00 59.95
   800x600  60.32 59.96 56.25
   848x480  60.00 59.94
   720x480  59.94
   640x480  59.94 59.94
Virtual-1 connected 1920x1080+1920+0 (normal left inverted right x axis y axis) 0mm x
   0mm
   4096x3112  60.00
   3656x2664  59.99
   4096x2160  60.00
   3840x2160  60.00
   1920x1200  59.95
   1920x1080  60.00
   1600x1200  59.95
   1680x1050  60.00
   1400x1050  60.00
   1280x1024  59.95
   1440x900 59.99
   1280x960 59.99
   1280x854 59.95
   1280x800 59.96
   1280x720 59.97
   1152x768 59.95
   1024x768 60.00 59.95
   800x600  60.32 59.96 56.25
   848x480  60.00 59.94
   720x480  59.94
  640x480  59.94 59.94
```

9. Wenn Sie eine Verbindung zu DCV herstellen, ändern Sie die Auflösung auf 2x4K, um sicherzustellen, dass die Unterstützung für zwei Monitore von DCV registriert wird.

Erste Schritte mit P5-Instances für Linux

P5-Instances bieten 8 NVIDIA H100-GPUs mit 640 GB GPU-Speicher mit hoher Bandbreite. Sie verfügen über AMD-EPYC-Prozessoren der 3. Generation und bieten 2 TB Systemspeicher, 30 TB lokalen NVMe-Instance-Speicher, eine aggregierte Netzwerkbandbreite von 3 200 Gbit/s und GPUDirect-RDMA-Unterstützung. P5-Instances unterstützen auch die Amazon EC2 UltraCluster EC2-Technologie, die mithilfe von EFA eine geringere Latenz und eine verbesserte Netzwerkleistung bietet.

Die folgende Tabelle enthält eine Zusammenfassung der Spezifikationen von `p5.48xlarge`.

vCPUs	Systemarbeitsspeicher	GPUs	GPU-Arbeitsspeicher	Netzwerkbandbreite	GPUDirect-RDMA	GPU-Peer-to-Peer	Instance-Speicher
192	2 TiB	8 NVIDIA-H100-GPUs	640 GB HBM3	3 200 Gbit/s mit eFAV2	Unterstützt	NV-Switch mit 900 Gbit/s	8 x NVMe-SSD-Volumes mit 3 800 GB

Softwarekonfiguration

Die einfachste Möglichkeit für die ersten Schritte mit P5-Instances besteht darin, eine Instance mit einem AWS Deep Learning AMI zu starten, das mit der gesamten erforderlichen Software vorkonfiguriert ist. Die neuesten Informationen AWS Deep Learning AMI zur Verwendung mit P5-Instances finden Sie im AWS Deep Learning Base GPU AMI (Ubuntu 20.04).

Wenn Sie ein benutzerdefiniertes AMI für den Einsatz mit P5-Instances erstellen müssen, sollten Sie die folgenden Mindest-Softwareversionen installieren:

- NVIDIA-Treiber 535.54.03 oder höher

- CUDA 12.1 oder höher
- NVIDIA GDRCopy 2.3 oder höher
- EFA-Installationsprogramm 1.24.1 oder höher
- NCCL 2.18.3 oder höher
- aws-ofi-nccl Plugin 1.7.2-aws oder höher

Außerdem empfiehlt es sich, die Instance so zu konfigurieren, dass keine tieferen Ruhezustände verwendet werden. Weitere Informationen finden Sie unter Hohe Leistung und niedrige Latenz durch Begrenzung tieferer C-States im Amazon Linux 2-Benutzerhandbuch. Das neueste AWS Deep Learning Base GPU AMI ist so vorkonfiguriert, dass es keine tieferen C-States verwendet.

Spezifische Empfehlungen für Ubuntu 20.04

Die folgenden Empfehlungen für Ubuntu 20.04 tragen dazu bei, unvorhersehbare Schnittstellenbenennungen beim Booten zu verhindern:

- Vergewissern Sie sich, dass Sie `systemd 245.4-4ubuntu3.19` oder eine neuere Version verwenden, indem Sie den folgenden Befehl eingeben:

  ```
  systemd --version
  ```

- Stellen Sie sicher, dass Sie GRUB konfiguriert haben:
  - Öffnen Sie die `/etc/default/grub`-Konfigurationsdatei in einem Texteditor.
  - Bearbeiten Sie den `GRUB_CMDLINE_LINUX_DEFAULT`-Eintrag so, dass er `net.naming-scheme=v247` einschließt.
  - Starten Sie Ihre Instance neu, indem Sie `sudo update-grub` ausführen.

Netzwerk- und EFA-Konfiguration

P5-Instances bieten durch den Einsatz mehrerer EFA-Schnittstellen 3 200 Gbit/s Netzwerkbandbreite. P5-Instances unterstützen 32 Netzwerkkarten. Es empfiehlt sich, pro Netzwerkkarte eine einzige EFA-Netzwerkschnittstelle zu definieren. Um diese Schnittstellen beim Start zu konfigurieren, empfehlen sich die folgenden Einstellungen:

- Für die Netzwerkschnittstelle `0` geben Sie den Geräteindex `0` an.
- Für die Netzwerkschnittstellen 1 bis 31 geben Sie den Geräteindex 1 an.

Weitere Informationen zur Konfiguration von P5-Instances für EFA finden Sie unter Erste Schritte mit P5-Instances und EFA.

Amazon EC2-Mac-Instances

Mac-Instances von Amazon EC2 unterstützen von Haus aus das Betriebssystem macOS.

- x86-Mac-Instances von EC2 (`mac1.metal`) werden auf 2018-Mac-mini-Hardware mit 3,2 GHz Intel-Core-i7-Prozessoren der achten Generation (Coffee Lake) betrieben.
- M1-Mac-Instances von EC2 (`mac2.metal`) basieren auf Mac-mini-Hardware 2020, die von Apple-Silicon-M1-Prozessoren angetrieben wird.
- M2-Mac-Instances von EC2 (`mac2-m2.metal`) basieren auf Mac-mini-Hardware 2023, die von Apple-Silicon-M2-Prozessoren angetrieben wird.
- M2-Pro-Instances von EC2 (`mac2-m2pro.metal`) basieren auf Mac-mini-Hardware 2023, die von Prozessoren vom Typ Apple Silicon M2 Pro angetrieben wird.

EC2-Mac-Instances eignen sich ideal zum Entwickeln, Erstellen, Testen und Signieren von Anwendungen für Apple-Plattformen wie iPhone, iPad, Mac, Vision Pro, Apple Watch, Apple TV und Safari. Sie können über SSH oder Apple Remote Desktop (ARD) eine Verbindung mit Ihrer Mac-Instance herstellen.

> **Note**
>
> Die Fakturierungseinheit ist der Dedicated Host. Für die Instances, die auf diesem Host laufen, entstehen keine zusätzlichen Gebühren.

Inhalt

- Starten einer Mac-Instance
- Herstellen einer Verbindung zu Ihrer Mac-Instance
- Aktualisieren Sie das Betriebssystem und die Software auf Mac-Instanzen
- Erhöhen Sie die Größe eines EBS-Volumes auf Ihrer Mac-Instance
- Stoppen und beenden Sie Ihre Mac-Instance
- Finden Sie unterstützte macOS-Versionen für Ihren Amazon EC2 Mac Dedicated Host
- So abonnieren Sie macOS-AMI-Benachrichtigungen
- Versionshinweise zu Amazon EC2 macOS AMIs

Überlegungen

Die folgenden Überlegungen gelten für Mac-Instances:

- Mac-Instances sind auf Dedicated Hosts nur als Bare-Metal-Instances mit einer Mindestzuweisungsdauer von 24 Stunden verfügbar, bevor Sie den Dedicated Host freigeben können. Sie können eine Mac-Instance pro Dedicated Host starten. Sie können den Dedicated Host für die AWS Konten oder Organisationseinheiten innerhalb Ihrer AWS Organisation oder für die gesamte AWS Organisation gemeinsam nutzen.
- Mac-Instanzen sind in verschiedenen Varianten verfügbar AWS-Regionen. Eine Liste der Verfügbarkeit von Mac-Instances in den AWS-Regionen einzelnen Regionen finden Sie unter Amazon EC2 EC2-Instance-Typen nach Regionen.
- Mac-Instances sind nur als On-Demand-Instances verfügbar. Sie sind nicht als Spot-Instances oder Reserved Instances verfügbar. Sie können Geld für Mac-Instances sparen, indem Sie einen Savings Plan erwerben.
- Mac-Instances können eines der folgenden Betriebssysteme ausführen:
  - macOS Mojave (Version 10.14) (nur x86-Mac-Instances)
  - macOS Catalina (Version 10.15) (nur x86-Mac-Instances)
  - macOS Big Sur (Version 11) (x86- und M1-Mac-Instances)
  - macOS Monterey (Version 12) (x86- und M1-Mac-Instances)
  - macOS Ventura (Version 13) (alle Mac-Instances, M2- und M2-Pro-Mac-Instances unterstützen macOS-Ventura-Version 13.2 oder höher)
  - macOS Sonoma (Version 14) (alle Mac-Instances)
- EBSHotplug wird unterstützt.

- AWS verwaltet oder unterstützt die interne SSD auf der Apple-Hardware nicht. Wir empfehlen dringend, stattdessen Amazon EBS-Volumes zu verwenden. EBSVolumes bieten auf Mac-Instances dieselben Elastizitäts-, Verfügbarkeits- und Haltbarkeitsvorteile wie auf jeder anderen EC2-Instance.
- Wir empfehlen die Verwendung von Allzweck-SSDs (`gp2`und`gp3`) und Bereitgestellten IOPS-SSDs (`io1`und`io2`) mit Mac-Instances, um eine optimale Leistung zu erzielen. EBS
- Mac-Instances unterstützen Amazon EC2 Auto Scaling.
- Auf x86-Mac-Instances sind automatische Softwareupdates deaktiviert. Wir empfehlen, dass Sie Updates anwenden und auf Ihrer Instance testen, bevor Sie die Instance in Produktion nehmen. Weitere Informationen finden Sie unter Aktualisieren Sie das Betriebssystem und die Software auf Mac-Instanzen.
- Wenn Sie eine Mac-Instance anhalten oder beenden, wird ein Scrubbing-Workflow auf Dedicated Host ausgeführt. Weitere Informationen finden Sie unter Stoppen und beenden Sie Ihre Mac-Instance.

> **Warning**
>
> Nicht verwenden. FileVault Die Aktivierung FileVault führt dazu, dass der Host aufgrund der gesperrten Partitionen nicht gestartet werden kann. Wenn Datenverschlüsselung erforderlich ist, verwenden Sie die Amazon EBS-Verschlüsselung, um Startprobleme und Leistungseinbußen zu vermeiden. Bei der Amazon EBS-Verschlüsselung finden Verschlüsselungsvorgänge auf den Servern statt, die Instances hosten, wodurch die Sicherheit sowohl data-at-rest einer Instance als auch data-in-transit zwischen einer Instance und ihrem angeschlossenen EBS-Speicher gewährleistet wird. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung im Amazon EBS-Benutzerhandbuch.

Instance-Bereitschaft

Nachdem Sie eine Mac-Instance gestartet haben, müssen Sie warten, bis die Instance bereit ist, bevor Sie eine Verbindung zu ihr herstellen können. Für ein AWS verkauftes AMI mit einer x86-Mac-Instance oder einer Apple-Silicon-Mac-Instance kann die Startzeit zwischen etwa 6 Minuten und 20 Minuten liegen. Die Startzeit kann sich je nach den ausgewählten Größen von Amazon-EBS-Volumes, der Einbindung zusätzlicher Skripts in Benutzerdaten oder zusätzlich geladener Software in einem benutzerdefinierten macOS-AMI verlängern.

Sie können ein kleines Shell-Skript wie das unten stehende verwenden, um die describe-instance-status API abzufragen, um zu erfahren, wann die Instance bereit ist, eine Verbindung herzustellen. Ersetzen Sie im folgenden Befehl die Beispiel-Instance-ID mit Ihrer eigenen.

```
for i in $(seq 1 200); do aws ec2 describe-instance-status --instance-
ids=i-0123456789example \
    --query='InstanceStatuses[0].InstanceStatus.Status'; sleep 5; done;
```

EC2-macOS-AMIs

Amazon EC2 macOS bietet eine stabile, sichere und leistungsstarke Umgebung für Developer-Workloads, die auf Amazon EC2-Mac-Instances ausgeführt werden. EC2-macOS-AMIs enthalten Pakete, die eine einfache Integration ermöglichen AWS, z. B. Startkonfigurationstools und beliebte AWS Bibliotheken und Tools.

Weitere Informationen zu EC2 macOS-AMIs finden Sie unterVersionshinweise zu Amazon EC2 macOS AMIs.

AWS stellt regelmäßig aktualisierte EC2 macOS-AMIs bereit, die Updates für Pakete enthalten, die Eigentum von AWS und der neuesten vollständig getesteten macOS-Version sind. AWS bietet außerdem aktualisierte AMIs mit den neuesten Nebenversionsupdates oder Hauptversionsupdates, sobald sie vollständig getestet und überprüft werden können. Wenn Sie keine Daten oder Anpassungen an Ihren Mac-Instances beibehalten müssen, können Sie die neuesten Updates erhalten, indem Sie eine neue Instance mit dem aktuellen AMI starten und dann die vorherige Instance beenden. Andernfalls können Sie auswählen, welche Updates auf Ihre Mac-Instances angewendet werden sollen.

Informationen zum Abonnieren von macOS AMI-Benachrichtigungen finden Sie unterSo abonnieren Sie macOS-AMI-Benachrichtigungen.

EC2-macOS-Init

EC2macOS Init wird verwendet, um EC2 Mac-Instanzen beim Start zu initialisieren. Es verwendet Prioritätsgruppen, um logische Aufgabengruppen gleichzeitig auszuführen.

Die launchd-plist-Datei ist `/Library/LaunchDaemons/com.amazon.ec2.macos-init.plist`. Die Dateien für EC2-macOS-Init befinden sich in `/usr/local/aws/ec2-macos-init`.

Weitere Informationen finden Sie unter https://github.com/aws/ec2-macos-init.

Amazon EC2-Systemmonitor für macOS

Amazon EC2 System Monitor für macOS stellt Amazon CloudWatch Metriken zur CPU-Auslastung zur Verfügung. Es sendet diese Messwerte innerhalb von 1 Minute an CloudWatch mehr als ein benutzerdefiniertes serielles Gerät. Sie können diesen Agenten wie folgt aktivieren oder deaktivieren. Er ist standardmäßig aktiviert.

```
sudo setup-ec2monitoring [enable | disable]
```

> **Note**
>
> Amazon EC2 System Monitor für macOS wird derzeit nicht auf Apple Silicon Mac-Instances unterstützt.

Zugehörige Ressourcen

Informationen zu Preisen erhalten Sie unter -Preise.

Weitere Informationen über Mac-Instances finden Sie unter Amazon EC2 Mac-Instances.

Weitere Informationen zu den Hardware-Spezifikationen und der Netzwerkleistung von Mac-Instances finden Sie unter Allzweck-Instances.

Starten einer Mac-Instance

EC2-Mac-Instances benötigen einen Dedicated Host. Sie müssen Ihrem Konto zuerst einen Host zuweisen und dann die Instance über den Host starten.

Sie können eine Mac-Instance mit dem AWS Management Console oder dem AWS CLI starten.

Starten einer Mac-Instance mit der Konsole

Starten einer Mac-Instance auf einem Dedicated Host

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Weisen Sie den Dedicated Host wie folgt zu:
   a. Wählen Sie im Navigationsbereich Dedicated Hosts aus.

b. Wählen Sie Dedicated Host zuweisen und gehen Sie wie folgt vor:

   i. Wählen Sie als Instance-Familie die Optionen mac1, mac2, mac2-m2 oder mac2-m2pro aus. Wenn die Instance-Familie nicht in der Liste erscheint, wird sie in der aktuell ausgewählten Region nicht unterstützt.

   ii. Wählen Sie als Instance-Typ die Optionen mac1.metal, mac2.metal, mac2-m2.metal oder mac2-m2pro.metal basierend auf der ausgewählten Instance-Familie.

   iii. Wählen Sie in Availability Zone die Availability Zone für Dedicated Host aus.

   iv. Für Quantity (Menge) behalten Sie 1.

   v. Wählen Sie Allocate aus.

3. Starten Sie die Instance über den Host wie folgt:

   a. Wählen Sie die von Ihnen erstellte Dedicated Host aus, und klicken Sie dann auf Folgendes:

      i. Wählen Sie Actions (Aktionen), Launch instances onto host (Instances auf Host starten).

      ii. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) ein macOS-AMI.

      iii. Wählen Sie unter Instance-Typ den entsprechenden Instance-Typ aus (mac1.metal, mac2.metal, mac2-m2.metal oder mac2-m2pro.metal).

      iv. Stellen Sie unter Advanced details (Erweiterte Details) sicher, dass Tenancy, Tenancy Host by und Tenancy-Host-ID basierend auf dem von Ihnen erstellten Dedicated Host vorkonfiguriert sind. Aktualisieren Sie die Tenancy affinity (Tenancy-Affinität), wenn nötig.

      v. Schließen Sie den Assistenten ab und geben Sie nach Bedarf EBS-Volumes, Sicherheitsgruppen und Schlüsselpaare an.

      vi. Wählen Sie in der Übersicht Launch instance (Instance starten) aus.

   b. Auf einer Bestätigungsseite wird Ihnen mitgeteilt, dass die Instance gestartet wird. Wählen Sie View all Instances (Alle Instances anzeigen) aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren. Der anfängliche Status einer Instance ist `pending`. Die Instance ist bereit, wenn sich ihr Status in `running` ändert und Statusprüfungen besteht.

Starten Sie eine Mac-Instanz mit dem AWS CLI

Zuweisen eines Dedicated Hosts

Verwenden Sie folgenden Befehl allocate-hosts, um einen Dedicated Host für Ihre Mac-Instance zuzuweisen, wobei der `instance-type` entweder durch `mac1.metal`, `mac2.metal`, `mac2-m2.metal` oder `mac2-m2pro.metal` und der `region` und `availability-zone` durch die für Ihre Umgebung passenden ersetzt wird.

```
aws ec2 allocate-hosts --region us-east-1 --instance-type mac1.metal --availability-
zone us-east-1b --auto-placement "on" --quantity 1
```

Starten der Instance über den Host

Verwenden Sie den folgenden Befehl run-instances, um eine Mac-Instance zu starten, wobei erneut `instance-type` entweder durch `mac1.metal`, `mac2.metal`, `mac2-m2.metal` oder `mac2-m2pro.metal` und `region` und `availability-zone` durch die zuvor verwendeten ersetzt wird.

```
aws ec2 run-instances --region us-east-1 --instance-type mac1.metal --placement
 Tenancy=host --image-id ami_id --key-name my-key-pair
```

Der anfängliche Status einer Instance ist `pending`. Die Instance ist bereit, wenn sich ihr Status in `running` ändert und Statusprüfungen besteht. Verwenden Sie den folgenden Befehl describe-instance-status, um Statusinformationen für Ihre Instance anzuzeigen.

```
aws ec2 describe-instance-status --instance-ids i-017f8354e2dc69c4f
```

Im Folgenden finden Sie eine Beispielausgabe für eine Instance, die ausgeführt wird und Statusprüfungen bestanden hat.

```
{
    "InstanceStatuses": [
        {
            "AvailabilityZone": "us-east-1b",
            "InstanceId": "i-017f8354e2dc69c4f",
            "InstanceState": {
                "Code": 16,
                "Name": "running"
            },
            "InstanceStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
```

```
                    }
                ],
                "Status": "ok"
            },
            "SystemStatus": {
                "Details": [
                    {
                        "Name": "reachability",
                        "Status": "passed"
                    }
                ],
                "Status": "ok"
            }
        }
    ]
}
```

Herstellen einer Verbindung zu Ihrer Mac-Instance

Sie können per SSH oder per grafischer Benutzeroberfläche eine Verbindung mit Ihrer Mac-Instance herstellen.

Herstellung einer Verbindung zu Ihrer Instance mit SSH

> **Important**
>
> Mehrere Benutzer können gleichzeitig auf das Betriebssystem zugreifen. In der Regel gibt es eine 1:1 user:GUI-Sitzung aufgrund des integrierten Bildschirmfreigabedienstes an Port 5900. Die Verwendung von SSH in macOS unterstützt mehrere Sitzungen bis zum Limit „Max. Sitzungen“ in der Datei „sshd_config“.

Amazon EC2-Mac-Instances lassen standardmäßig keinen Root-Fernzugriff über SSH zu. Die Passwort-Authentifizierung ist deaktiviert, um Brute-Force-Angriffe zu verhindern. Das ec2-Benutzerkonto ist für die Remote-Anmeldung mit SSH konfiguriert. Das ec2-Benutzerkonto hat auch sudo-Privilegien. Nachdem Sie eine Verbindung zu Ihrer Instance hergestellt haben, können Sie weitere Benutzer hinzufügen.

Um die Verbindung mit Ihrer Instance mithilfe von SSH zu unterstützen, starten Sie die Instance mit einem Schlüsselpaar und einer Sicherheitsgruppe, die SSH-Zugriff ermöglicht, und stellen Sie

sicher, dass die Instance über eine Internetverbindung verfügt. Sie geben die `.pem`-Datei für das Schlüsselpaar an, wenn Sie eine Verbindung mit der Instance herstellen.

Verwenden Sie die folgende Vorgehensweise, um per SSH-Client eine Verbindung mit Ihrer Mac-Instance herzustellen. Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

So stellen Sie per SSH eine Verbindung mit Ihrer Instance her

1. Stellen Sie sicher, dass auf Ihrem lokalen Computer ein SSH-Client installiert ist, indem Sie ssh über die Befehlszeile eingeben. Wenn Ihr Computer den Befehl nicht erkennt, suchen Sie nach einem SSH-Client für Ihr Betriebssystem und installieren Sie ihn.
2. Holen Sie sich den öffentlichen DNS-Namen Ihrer Instance. Über die Amazon EC2-Konsole finden Sie den öffentlichen DNS-Namen auf den Registerkarten Details und Networking. Mithilfe von können Sie den öffentlichen DNS-Namen mithilfe des Befehls describe-instances finden. AWS CLI
3. Suchen Sie die `.pem`-Datei für das Schlüsselpaar, das Sie beim Starten der Instance angegeben haben.
4. Stellen Sie mithilfe des folgenden Befehls ssh unter Angabe des öffentlichen DNS-Namens der Instance und der `.pem`-Datei eine Verbindung zu Ihrer Instance her.

```
ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
```

Eine Verbindung mit der grafischen Benutzerschnittstelle (GUI) Ihrer Instance herstellen

Verwenden Sie die folgende Vorgehensweise, um per VNC, Apple Remote Desktop (ARD) oder die Apple Screen Sharing-Anwendung (im Lieferumfang von macOS enthalten) eine Verbindung mit der GUI Ihrer Instance herzustellen.

> **Note**
>
> macOS 10.14 und höher erlaubt die Steuerung nur, wenn die Bildschirmfreigabe in den Systemeinstellungen aktiviert ist.

Herstellen einer Verbindung zu Ihrer Instance per ARD- oder VNC-Client

1. Stellen Sie sicher, dass auf Ihrem lokalen Computer ein ARD-Client oder ein VNC-Client installiert ist, der ARD installiert hat. Unter macOS können Sie die integrierte Screen-Sharing-Anwendung nutzen. Andernfalls suchen Sie nach ARD für Ihr Betriebssystem und installieren Sie es.
2. Verbinden Sie sich mit Ihrer Instance über SSH von Ihrem lokalen Computer aus.
3. Richten Sie mit dem passwd-Befehl wie folgt ein Passwort für das ec2-Benutzerkonto ein.

   ```
   [ec2-user ~]$ sudo passwd ec2-user
   ```

4. Installieren und starten Sie macOS Screen Sharing mit dem folgenden Befehl.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

5. Trennen Sie die Verbindung zur Instance, indem Sie exit eingeben und die Eingabetaste drücken.
6. Stellen Sie von Ihrem Computer aus mit dem folgenden ssh-Befehl eine Verbindung zu Ihrer Instance her. Verwenden Sie zusätzlich zu den im vorherigen Abschnitt gezeigten Optionen die -L-Option, um die Port-Weiterleitung zu aktivieren und den gesamten Datenverkehr auf dem lokalen Port 5900 an den ARD-Server auf der Instance weiterzuleiten.

   ```
   ssh -L 5900:localhost:5900 -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

7. Verwenden Sie auf Ihrem lokalen Computer den ARD- oder VNC-Client, der ARD unterstützt, um eine Verbindung zu `localhost:5900` herzustellen. Verwenden Sie beispielsweise die Screen-Sharing-Anwendung unter macOS wie folgt:

   a. Öffnen Sie den Finder und wählen Sie Go.

   b. Wählen Sie Mit Server verbinden aus.

   c. Geben Sie `vnc://localhost:5900` in das Feld Serveradresse ein.

   d. Melden Sie sich wie aufgefordert an und verwenden Sie **`ec2-user`** als Benutzernamen und das Passwort, das Sie für das ec2-Benutzerkonto erstellt haben.

Ändern der macOS-Bildschirmauflösung auf Mac-Instances

Nachdem Sie eine Verbindung zu Ihrer EC2-Mac-Instance über ARD oder einen VNC-Client herstellen, der die ARD unterstützt, können Sie die Bildschirmauflösung Ihrer macOS-Umgebung mit einem der öffentlich verfügbaren macOS-Tools oder -Serviceprogrammen wie dem displayplacer ändern.

So ändern Sie die Bildschirmauflösung mit displayplacer

1. Installieren Sie displayplacer.

```
[ec2-user ~]$ brew tap jakehilborn/jakehilborn && brew install displayplacer
```

2. Zeigen Sie die aktuellen Bildschirminformationen und mögliche Bildschirmauflösungen an.

```
[ec2-user ~]$ displayplacer list
```

3. Wenden Sie die gewünschte Bildschirmauflösung an.

```
[ec2-user ~]$ displayplacer "id:<screenID> res:<width>x<height> origin:(0,0)
 degree:0"
```

   Beispielsweise:

```
RES="2560x1600"
displayplacer "id:69784AF1-CD7D-B79B-E5D4-60D937407F68 res:${RES} scaling:off
 origin:(0,0) degree:0"
```

Aktualisieren Sie das Betriebssystem und die Software auf Mac-Instanzen

Warning

Die Installation von Beta- oder Vorschauversionen von macOS ist nur auf M1-Mac-Instances von Amazon EC2 verfügbar. Amazon EC2 qualifiziert sich nicht für Beta- oder Vorschauversionen von macOS und stellt nicht sicher, dass Instances nach einer Aktualisierung auf eine macOS-Vorproduktionsversion funktionsfähig bleiben.
Der Versuch, Beta- oder Vorabversionen von macOS auf Amazon EC2 x86 Mac-Instances zu installieren, führt zu einer Beeinträchtigung Ihres Mac Dedicated Host auf Amazon EC2, wenn

Sie Ihre Instances stoppen oder beenden, und verhindert, dass Sie eine neue Instance auf diesem Host starten oder einrichten können.

Schritte zum Aktualisieren der Software in x86-Mac-Instances und Apple–Silicon-Mac-Instances.

- Software auf x86-Mac-Instances aktualisieren
- Software in Apple-Silicon-Instances aktualisieren

Software auf x86-Mac-Instances aktualisieren

Auf x86-Mac-Instances können Sie Betriebssystem-Updates von Apple mit dem `softwareupdate`-Befehl installieren.

So installieren Sie Betriebssystem-Updates von Apple auf x86-Mac-Instances

1. Listen Sie die Pakete mit verfügbaren Updates mit dem folgenden Befehl auf.

   ```
   [ec2-user ~]$ softwareupdate --list
   ```

2. Installieren Sie alle Updates oder nur bestimmte Updates. Verwenden Sie den folgenden Befehl, um bestimmte Updates zu installieren.

   ```
   [ec2-user ~]$ sudo softwareupdate --install label
   ```

   Verwenden Sie den folgenden Befehl, um stattdessen alle Updates zu installieren.

   ```
   [ec2-user ~]$ sudo softwareupdate --install --all --restart
   ```

Systemadministratoren können AWS Systems Manager damit vorab genehmigte Betriebssystemupdates auf x86-Mac-Instanzen bereitstellen. Weitere Informationen finden Sie im AWS Systems Manager -Benutzerhandbuch.

Sie können Homebrew verwenden, um Updates für Pakete in den EC2 macOS-AMIs zu installieren, sodass Sie die neueste Version dieser Pakete auf Ihren Instances haben. Sie können Homebrew auch verwenden, um gängige macOS-Anwendungen unter Amazon EC2-macOS zu installieren und auszuführen. Weitere Informationen finden Sie in der Homebrew-Dokumentation.

Installieren von Updates mit Homebrew

1. Aktualisieren Sie Homebrew mit dem folgenden Befehl.

```
[ec2-user ~]$ brew update
```

2. Listen Sie die Pakete mit verfügbaren Updates mit dem folgenden Befehl auf.

```
[ec2-user ~]$ brew outdated
```

3. Installieren Sie alle Updates oder nur bestimmte Updates. Verwenden Sie den folgenden Befehl, um bestimmte Updates zu installieren.

```
[ec2-user ~]$ brew upgrade package name
```

   Verwenden Sie den folgenden Befehl, um stattdessen alle Updates zu installieren.

```
[ec2-user ~]$ brew upgrade
```

Software in Apple-Silicon-Instances aktualisieren

Überlegungen

Elastic Network Adapter (ENA)-Treiber

Aufgrund eines Updates in der Netzwerktreiberkonfiguration ist die ENA-Treiberversion 1.0.2 nicht mit macOS 13.3 oder höher kompatibel. Wenn Sie eine Beta-, Vorschau- oder Produktionsversion von macOS 13.3 oder höher installieren möchten und nicht den neuesten ENA-Treiber installiert haben, gehen Sie folgendermaßen vor, um eine neue Version des Treibers zu installieren.

Installieren einer neuen Version des ENA-Treibers

1. Stellen Sie in einem Terminal-Fenster über SSH eine Verbindung mit Ihrer Apple-Silicon-Mac-Instance her.
2. Laden Sie die ENA-Anwendung mit dem folgenden Befehl in die `Applications`-Datei herunter:

```
[ec2-user ~]$ brew install amazon-ena-ethernet-dext
```

> **Tipp zur Problembehebung**
>
> Wenn Sie die Warnung `No available formula with the name amazon-ena-ethernet-dext` erhalten, führen Sie den folgenden Befehl aus:
>
> ```
> [ec2-user ~]$ brew update
> ```

3. Trennen Sie die Verbindung zur Instance, indem Sie exit eingeben und die Eingabetaste drücken.
4. Verwenden Sie den VNC-Client, um die ENA-Anwendung zu aktivieren.
   a. Richten Sie den VNC-Client mit Eine Verbindung mit der grafischen Benutzerschnittstelle (GUI) Ihrer Instance herstellen ein.
   b. Sobald Sie mithilfe der Bildschirmfreigabe-Anwendung eine Verbindung zu Ihrer Instance hergestellt haben, wechseln Sie zum Ordner Anwendungen und öffnen Sie die ENA-Anwendung.
   c. Wählen Sie Activate.
   d. Führen Sie den folgenden Befehl im Terminalfenster aus, um sicherzustellen, dass der Treiber korrekt aktiviert wurde. Die Ausgabe des Befehls zeigt, dass sich der alte Treiber im Status „Wird beendet“ und der neue Treiber im Status „Aktiviert“ befindet.

      ```
      systemextensionsctl list;
      ```

   e. Nach dem Neustart der Instance ist nur der neue Treiber vorhanden.

Software-Update in Apple-Silicon-Mac-Instances

In Apple-Silicon-Mac-Instances müssen Sie mehrere Schritte ausführen, um ein direktes Betriebssystem-Update durchzuführen. Greifen Sie zunächst mithilfe der GUI mit einem VNC-Client (Virtual Network Computing) auf die interne Festplatte der Instance zu. Dieses Verfahren verwendet macOS Screen Sharing, den integrierten VNC-Client. Delegieren Sie dann die Eigentümerschaft an den administrativen Benutzer (`ec2-user`), indem Sie sich als `aws-managed-user` auf dem Amazon EBS Volume anmelden.

Während Sie dieses Verfahren durcharbeiten, erstellen Sie zwei Passwörter. Ein Passwort ist für den administrativen Benutzer (`ec2-user`) und das andere Passwort ist für einen speziellen

administrativen Benutzer (`aws-managed-user`). Merken Sie sich diese Passwörter, da Sie sie im weiteren Verlauf des Verfahrens verwenden werden.

> **Note**
>
> Mit diesem Verfahren auf macOS Big Sur können Sie nur kleinere Aktualisierungen durchführen, z. B. die Aktualisierung von macOS Big Sur 11.7.3 zu macOS Big Sur 11.7.4. Für macOS Monterey oder höher können Sie größere Softwareupdates durchführen.

Für den Zugriff auf die interne Festplatte

1. Stellen Sie von Ihrem lokalen Computer aus im Terminal mit dem folgenden Befehl über SSH eine Verbindung zu Ihrer Apple-Silicon-Mac-Instance her. Weitere Informationen finden Sie unter Herstellung einer Verbindung zu Ihrer Instance mit SSH.

   ```
   ssh -i /path/key-pair-name.pem ec2-user@instance-public-dns-name
   ```

2. Installieren und starten Sie macOS Screen Sharing mit dem folgenden Befehl.

   ```
   [ec2-user ~]$ sudo launchctl enable system/com.apple.screensharing
   sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
   ```

3. Legen Sie ein Passwort für `ec2-user` mit dem folgenden Befehl fest. Merken Sie sich das Passwort, da Sie es später verwenden werden.

   ```
   [ec2-user ~]$ sudo /usr/bin/dscl . -passwd /Users/ec2-user
   ```

4. Trennen Sie die Verbindung zur Instance, indem Sie exit eingeben und die Rücktaste drücken.
5. Verbinden Sie sich von Ihrem lokalen Computer aus im Terminal erneut mit Ihrer Instance mit einem SSH-Tunnel zum VNC-Port, indem Sie den folgenden Befehl eingeben.

   ```
   ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 ec2-user@instance-public-dns-name
   ```

> **Note**
>
> Beenden Sie diese SSH-Sitzung erst, wenn die folgenden VNC-Verbindungs- und GUI-Schritte abgeschlossen sind. Wenn die Instance neu gestartet wird, wird die Verbindung automatisch geschlossen.

6. Verbinden Sie sich von Ihrem lokalen Computer aus mit `localhost:5900`, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie den Finder und wählen Sie Go.

   b. Wählen Sie Mit Server verbinden aus.

   c. Geben Sie `vnc://localhost:5900` in das Feld Serveradresse ein.

7. Stellen Sie im macOS-Fenster eine Verbindung zur Remote-Sitzung der Apple-Silicon-Mac-Instance als `ec2-user` mit dem Passwort her, das Sie in Schritt 3 erstellt haben.

8. Greifen Sie mit einer der folgenden Optionen auf InternalDiskdas interne Laufwerk mit dem Namen zu.

   a. Für macOS Ventura oder höher: Öffnen Sie die Systemeinstellungen, wählen Sie im linken Bereich Allgemein und dann unten rechts im Bereich Startup-Diskette aus.

   b. Für macOS Monterey oder darunter: Öffnen Sie die Systempräferenzen, wählen Sie Startup-Diskette und entsperren Sie den Bereich dann, indem Sie das Schlosssymbol unten links im Fenster auswählen.

> **Tipp zur Problembehebung**
>
> Wenn Sie die interne Festplatte mounten müssen, führen Sie den folgenden Befehl im Terminal aus.
>
> ```
> APFSVolumeName="InternalDisk" ; SSDContainer=$(diskutil list | grep
>  "Physical Store disk0" -B 3 | grep "/dev/disk" | awk {'print $1'} ) ;
>  diskutil apfs addVolume $SSDContainer APFS $APFSVolumeName
> ```

9. Wählen Sie das interne Laufwerk mit dem Namen InternalDiskaus und klicken Sie auf Neu starten. Wählen Sie erneut Neu starten, wenn Sie dazu aufgefordert werden.

> **Important**
>
> Wenn die interne Festplatte statt Macintosh HD heißt InternalDisk, muss Ihre Instanz gestoppt und neu gestartet werden, damit der dedizierte Host aktualisiert werden kann. Weitere Informationen finden Sie unter Stoppen und beenden Sie Ihre Mac-Instance.

Gehen Sie wie folgt vor, um den Besitz an den administrativen Benutzer zu delegieren. Wenn Sie sich mit SSH wieder mit Ihrer Instance verbinden, starten Sie von der internen Festplatte unter Verwendung des speziellen administrativen Benutzers (`aws-managed-user`). Das ursprüngliche Passwort für `aws-managed-user` ist leer, daher müssen Sie es bei Ihrer ersten Verbindung überschreiben. Dann müssen Sie die Schritte wiederholen, um macOS Screen Sharing zu installieren und zu starten, da sich das Startvolume geändert hat.

Die Inhaberschaft auf einem Amazon-EBS-Volume an den Administrator zu delegieren

1. Stellen Sie von Ihrem lokalen Computer aus im Terminal mit dem folgenden Befehl eine Verbindung zu Ihrer Apple-Silicon-Mac-Instance her.

   ```
   ssh -i /path/key-pair-name.pem aws-managed-user@instance-public-dns-name
   ```

2. Verwenden Sie einen der folgenden Befehle, um das Problem zu beheben, wenn Sie die Warnung `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!` erhalten.

   a. Löschen Sie die bekannten Hosts mit dem folgenden Befehl. Wiederholen Sie dann den vorherigen Schritt.

      ```
      rm ~/.ssh/known_hosts
      ```

   b. Fügen Sie dem SSH-Befehl im vorherigen Schritt Folgendes aus.

      ```
      -o UserKnownHostsFile=/dev/null -o StrictHostKeyChecking=no
      ```

3. Legen Sie das Passwort für `aws-managed-user` mit dem folgenden Befehl fest. Das ursprüngliche `aws-managed-user` Passwort ist leer, daher müssen Sie es bei Ihrer ersten Verbindung überschreiben.

a.
```
[aws-managed-user ~]$ sudo /usr/bin/dscl . -passwd /Users/aws-managed-user password
```

b. Wenn Sie die Eingabeaufforderung `Permission denied. Please enter user's old password:` erhalten, drücken Sie die Eingabetaste.

> **Tipp zur Problembehebung**
>
> Wenn Sie den Fehler `passwd: DS error: eDSAuthFailed` erhalten, verwenden Sie den folgenden Befehl.
>
> ```
> [aws-managed-user ~]$ sudo passwd aws-managed-user
> ```

4. Installieren und starten Sie macOS Screen Sharing mit dem folgenden Befehl.

```
[aws-managed-user ~]$ sudo launchctl enable system/com.apple.screensharing
sudo launchctl load -w /System/Library/LaunchDaemons/com.apple.screensharing.plist
```

5. Trennen Sie die Verbindung zur Instance, indem Sie exit eingeben und die Rücktaste drücken.
6. Verbinden Sie sich von Ihrem lokalen Computer aus im Terminal erneut mit Ihrer Instance mit einem SSH-Tunnel zum VNC-Port, indem Sie den folgenden Befehl eingeben.

```
ssh -i /path/key-pair-name.pem -L 5900:localhost:5900 aws-managed-user@instance-public-dns-name
```

7. Verbinden Sie sich von Ihrem lokalen Computer aus mit `localhost:5900`, indem Sie die folgenden Schritte ausführen:

   a. Öffnen Sie den Finder und wählen Sie Go.

   b. Wählen Sie Mit Server verbinden aus.

   c. Geben Sie `vnc://localhost:5900` in das Feld Serveradresse ein.

8. Stellen Sie im macOS-Fenster eine Verbindung zur Remote-Sitzung der Apple-Silicon-Mac-Instance als `aws-managed-user` mit dem Passwort her, das Sie in Schritt 3 erstellt haben.

> **Note**
>
> Wenn Sie aufgefordert werden, sich mit Ihrer Apple ID anzumelden, wählen Sie Später einrichten.

9. Greifen Sie mit einer der folgenden Optionen auf das Amazon EBS Volume zu.

   a. Für macOS Ventura oder höher: Öffnen Sie die Systemeinstellungen, wählen Sie im linken Bereich Allgemein und dann unten rechts im Bereich Startup-Diskette aus.

   b. Für macOS Monterey oder darunter: Öffnen Sie die Systempräferenzen, wählen Sie Startup-Diskette und entsperren Sie den Bereich dann mit dem Schlosssymbol unten links im Fenster.

> **Note**
>
> Wenn Sie bis zum Neustart zur Eingabe eines Administrator-Passworts aufgefordert werden, verwenden Sie das Passwort, das Sie oben für `aws-managed-user` festgelegt haben. Dieses Passwort kann sich von dem unterscheiden, das Sie für `ec2-user` oder für das Standard-Administratorkonto in Ihrer Instance festgelegt haben. Die folgenden Anweisungen geben an, wann das Administratorkennwort Ihrer Instance verwendet werden soll.

10. Wählen Sie das Amazon EBS-Volume aus (das Volume, das InternalDiskim Fenster Startdiskette nicht benannt ist) und wählen Sie Restart.

> **Note**
>
> Wenn Sie mehrere startfähige Amazon-EBS-Volumes an Ihre Apple-Silicon-Mac-Instance angefügt haben, achten Sie darauf, für jedes Volume einen eindeutigen Namen zu verwenden.

11. Bestätigen Sie den Neustart und wählen Sie dann Benutzer autorisieren, wenn Sie dazu aufgefordert werden.

12. Vergewissern Sie sich, dass im Bereich Benutzer auf diesem Volume autorisieren der Administratorbenutzer (standardmäßig `ec2-user`) ausgewählt ist, und wählen Sie dann Autorisieren aus.

13. Geben Sie das `ec2-user`-Passwort ein, das Sie in Schritt 3 des vorherigen Verfahrens erstellt haben, und wählen Sie dann Weiter aus.
14. Geben Sie das Passwort für den speziellen Administratorbenutzer (`aws-managed-user`) ein, wenn Sie dazu aufgefordert werden.
15. Verbinden Sie sich von Ihrem lokalen Computer aus über das Terminal erneut mit Ihrer Instance über SSH mit dem Benutzernamen `ec2-user`.

    > **Tipp zur Problembehebung**
    >
    > Wenn Sie die Warnung `WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!` erhalten, führen Sie den folgenden Befehl aus und stellen Sie mithilfe von SSH erneut eine Verbindung zu Ihrer Instance her.
    >
    > ```
    > rm ~/.ssh/known_hosts
    > ```

16. Verwenden Sie die Befehle unter Software auf x86-Mac-Instances aktualisieren, um das Softwareupdate durchzuführen.

Erhöhen Sie die Größe eines EBS-Volumes auf Ihrer Mac-Instance

Sie können die Größe Ihrer Amazon EBS-Volumes auf Ihrer Mac-Instance erhöhen. Weitere Informationen finden Sie unter Amazon EBS Elastic Volumes im Amazon EBS-Benutzerhandbuch.

Nachdem Sie die Größe des Volumes erhöht haben, müssen Sie die Größe Ihres APFS-Containers wie folgt erhöhen.

So stellen Sie mehr Speicherplatz zur Verfügung:

1. Stellen Sie fest, ob ein Neustart erforderlich ist. Wenn Sie ein bestehendes EBS-Volume an eine laufende Mac-Instance anschließen, müssen Sie die Instance neu starten, um die neue Größe verfügbar zu machen. Wenn während des Startzeitraums eine Änderung am Speicherplatz vorgenommen wurde, ist kein Neustart erforderlich.

   Anzeigen der aktuellen Datenträgergröße:

   ```
   [ec2-user ~]$  diskutil list external physical
   /dev/disk0 (external, physical):
      #:                       TYPE NAME                    SIZE       IDENTIFIER
   ```

```
   0:                 GUID_partition_scheme            *322.1 GB     disk0
   1:                 EFI EFI                           209.7 MB     disk0s1
   2:                 Apple_APFS Container disk2        321.9 GB     disk0s2
```

2. Kopieren Sie den folgenden Befehl und fügen Sie ihn ein.

```
[ec2-user ~]$ PDISK=$(diskutil list physical external | head -n1 | cut -d" " -f1)
APFSCONT=$(diskutil list physical external | grep "Apple_APFS" | tr -s " " | cut -
d" " -f8)
yes | sudo diskutil repairDisk $PDISK
```

3. Kopieren Sie den folgenden Befehl und fügen Sie ihn ein.

```
[ec2-user ~]$ sudo diskutil apfs resizeContainer $APFSCONT 0
```

Stoppen und beenden Sie Ihre Mac-Instance

Wenn Sie eine Mac-Instance anhalten, bleibt die Instance etwa 15 Minuten im `stopping`-Status, bevor sie in den `stopped`-Status eintritt.

Wenn Sie eine Mac-Instance anhalten oder beenden, führt Amazon EC2 einen Scrubbing-Workflow auf dem zugrunde liegenden Dedicated Host durch, um das interne SSD zu löschen, die persistenten NVRAM-Variablen zu löschen und auf die neueste Gerätefirmware zu aktualisieren. Dadurch wird sichergestellt, dass Mac-Instances die gleiche Sicherheit und denselben Datenschutz bieten wie andere EC2 Nitro-Instances. Außerdem können Sie damit die neuesten macOS-AMIs ausführen. Während des Scrubbing-Workflows geht der Dedicated Host vorübergehend in den Schwebezustand über. Bei x86-Mac-Instances kann es bis zu 50 Minuten dauern, bis der Scrubbing-Workflow abgeschlossen ist. Bei Apple-Silicon-Mac-Instances kann es bis zu 110 Minuten dauern, bis der Scrubbing-Workflow abgeschlossen ist. Wenn die Gerätefirmware aktualisiert werden muss, kann es bei x86-Mac-Instances außerdem bis zu drei Stunden dauern, bis der Scrubbing-Workflow abgeschlossen ist.

Sie können die angehaltene Mac-Instance nicht starten oder eine neue Mac-Instance starten, bis der Scrubbing-Workflow abgeschlossen ist. An diesem Punkt wechselt Dedicated Host in den `available`-Status.

Die Erfassung und Abrechnung wird angehalten, wenn der Dedicated Host in den `pending`-Status wechselt. Die Dauer des Scrubbing-Workflows wird Ihnen nicht in Rechnung gestellt.

Geben Sie die Dedicated Host für Ihre Mac-Instance frei

Wenn Sie mit Ihrer Mac-Instance fertig sind, können Sie Dedicated Host freigeben. Bevor Sie den Dedicated Host freigeben können, müssen Sie die Mac-Instance anhalten oder beenden. Sie können den Host erst freigeben, wenn der Zuweisungszeitraum das 24-Stunden-Minimum überschreitet.

So veröffentlichen Sie das Dedicated Host

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Markieren Sie die Instance und wählen Sie Instance state (Instance-Status) und wählen Sie dann entweder Stop instance (Instance anhalten) oder Terminate Instance (Instance beenden).
4. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
5. Wählen Sie Dedicated Host aus und wählen Sie Actions (Aktionen), Release host (Host veröffentlichen).
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Release (Veröffentlichen).

Finden Sie unterstützte macOS-Versionen für Ihren Amazon EC2 Mac Dedicated Host

Sie können sich die neuesten macOS-Versionen ansehen, die von Ihrem Amazon EC2 Mac Dedicated Host unterstützt werden. Mit dieser Funktion können Sie überprüfen, ob Ihr Dedicated Host Instance-Starts mit Ihren bevorzugten macOS-Versionen unterstützen kann.

Für jede macOS-Version ist eine minimale Firmware-Version auf dem zugrunde liegenden Apple Mac erforderlich, um erfolgreich zu booten. Die Apple Mac-Firmware-Version kann veraltet sein, wenn ein zugewiesener Mac Dedicated Host über einen längeren Zeitraum inaktiv war oder wenn auf ihm eine lang laufende Instanz installiert ist.

Um die Unterstützung für die neuesten macOS-Versionen sicherzustellen, können Sie Instances auf Ihrem zugewiesenen Mac Dedicated Host beenden oder beenden. Dadurch wird der Host-Scrubbing-Workflow ausgelöst und die Firmware auf dem zugrunde liegenden Apple Mac aktualisiert, sodass sie die neuesten macOS-Versionen unterstützt. Ein Dedicated Host mit einer lang laufenden Instance wird automatisch aktualisiert, wenn Sie eine laufende Instance beenden oder beenden.

Weitere Informationen zum Scrubbing-Workflow finden Sie unterStoppen und beenden Sie Ihre Mac-Instance.

Weitere Informationen zum Starten von Mac-Instances finden Sie unterStarten einer Mac-Instance.

Sie können Informationen zu den neuesten macOS-Versionen, die auf Ihrem zugewiesenen Dedicated Host unterstützt werden, mithilfe der Amazon EC2 EC2-Konsole oder der AWS CLI anzeigen.

Console

Um Firmware-Informationen für Dedicated Hosts mithilfe der Konsole anzuzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Auf der Detailseite zu Dedicated Hosts finden Sie unter Letzte unterstützte macOS-Versionen die neuesten macOS-Versionen, die der Host unterstützen kann.

AWS CLI

Um Firmware-Informationen für Dedicated Hosts anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den `describe-mac-hosts`Befehl und `region` ersetzen Sie ihn durch den entsprechenden AWS-Region.

```
$ aws ec2 describe-mac-hosts --region us-east-1
  {
      "MacHosts": [
          {
              "HostId": "h-07879acf49EXAMPLE",
              "MacOSLatestSupportedVersions": [
                  "14.3",
                  "13.6.4",
                  "12.7.3"
              ]
          }
      ]
  }
```

So abonnieren Sie macOS-AMI-Benachrichtigungen

Um benachrichtigt zu werden, wenn neue AMIs veröffentlicht werden oder wenn bridgeOS aktualisiert wurde, abonnieren Sie Benachrichtigungen über Amazon SNS.

Weitere Informationen zu EC2-macOS-AMIs finden Sie unterVersionshinweise zu Amazon EC2 macOS AMIs.

So abonnieren Sie macOS-AMI-Benachrichtigungen

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region verwenden, da die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region erstellt wurden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription die folgenden Schritte aus:

   a. Kopieren und fügen Sie als Topic ARN einen der folgenden Amazon-Ressourcennamen (ARNs) hinzu:

      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-macos-ami-updates`**
      - **`arn:aws:sns:us-east-1:898855652048:amazon-ec2-bridgeos-updates`**

   b. Wählen Sie für Protocol eine der folgenden Optionen aus:

      - E-Mail:

        Geben Sie unter Endpoint eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen. Nachdem Sie Ihr Abonnement erstellt haben, erhalten Sie eine Bestätigungs-Nachricht mit der Betreffzeile `AWS Notification - Subscription Confirmation`. Öffnen Sie die E-Mail und wählen Sie Confirm subscription aus, um Ihr Abonnement abzuschließen.

      - SMS:

        Geben Sie unter Endpunkt eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.

      - AWS Lambda, Amazon SQS, Amazon Data Firehose (Benachrichtigungen werden im JSON-Format geliefert):

        Geben Sie für Endpunkt den ARN für die Lambda-Funktion, die SQS-Warteschlange oder den Firehose-Stream ein, den Sie zum Empfangen der Benachrichtigungen verwenden können.

c. Wählen Sie Create subscription (Abonnement erstellen) aus.

Jedes Mal wenn neue macOS-AMIs veröffentlicht werden, senden wir Benachrichtigungen an die Abonnenten des Themas `amazon-ec2-macos-ami-updates`. Immer wenn bridgeOS aktualisiert wird, senden wir Benachrichtigungen an die Abonnenten des `amazon-ec2-bridgeos-updates`-Themas. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

So melden Sie sich von den macOS-AMI-Benachrichtigungen ab

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region verwenden, da die SNS-Benachrichtigungen in dieser Region erstellt wurden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie die Abonnements aus und wählen Sie anschließend Actions und Delete Subscriptions. Klicken Sie zum Bestätigen auf Delete.

Versionshinweise zu Amazon EC2 macOS AMIs

Die folgenden Informationen enthalten Details zu den Paketen, die standardmäßig in den EC2 macOS-AMIs enthalten sind, und fassen die Änderungen für jede EC2 macOS-AMI-Version zusammen.

Informationen zum Abonnieren von macOS AMI-Benachrichtigungen finden Sie unterSo abonnieren Sie macOS-AMI-Benachrichtigungen.

In Amazon EC2 macOS-AMIs enthaltene Standardpakete

In der folgenden Tabelle werden Pakete beschrieben, die standardmäßig in den EC2-macOS-AMIs enthalten sind.

Pakete	Versionshinweise
EC2macOS Init	https://github.com/aws/ec2-macos-init/tags
EC2macOS Utilities	https://github.com/aws/ec2-macos-utils/tags

Pakete	Versionshinweise
AmazonSSM-Agent	https://github.com/aws/amazon-ssm-agent/releases
AWS Command Line Interface (AWS CLI) Ausführung 2	https://raw.githubusercontent.com/aws/aws-cli/v2/CHANGELOG.rst
Befehlszeilen-Tools für Xcode	https://developer.apple.com/documentation/xcode-release-notes
Homebrew	https://github.com/Homebrew/brew/releases
EC2 Instance Connect	https://github.com/aws/aws-ec2-instance-connect-config/releases
Safari	https://developer.apple.com/documentation/safari-release-notes

Amazon EC2 macOS AMI-Aktualisierungen

In der folgenden Tabelle werden die Änderungen beschrieben, die in den EC2 macOS AMI-Versionen enthalten sind. Beachten Sie, dass einige Änderungen für alle EC2-macOS-AMIs gelten, während andere nur für eine Teilmenge dieser AMIs gelten.

EC2 macOS AMI-Aktualisierungen

Veröffentlichung	Änderungen
2024.06.07	Alle AMIs • Homebrew wurde auf 4.3.1-1 aktualisiert • `aws-cli`Auf 2.15.56 aktualisiert • Auf 3.3.380.0-1 aktualisiert `amazon-ssm-agent` Veröffentlichung von macOS Sonoma 14.5 (alle Mac-Instanzen) • Sicherheitsinhalt von macOS Sonoma 14.5

Veröffentlichung	Änderungen

	Veröffentlichung von macOS Ventura 13.6.7 (alle Mac-Instanzen)
	• Sicherheitsinhalt von macOS Ventura 13.6.7
	• Safari wurde auf 17.5 aktualisiert
	  • Sicherheitsinhalt von Safari 17.5
	
	Veröffentlichung von macOS Monterey 12.7.5 (alle Mac-Instanzen)
	• Sicherheitsinhalt von macOS Monterey 12.7.5
	• Safari wurde auf 17.5 aktualisiert
	  • Sicherheitsinhalt von Safari 17.5

2024.04.12	Alle AMIs
	• Homebrew wurde auf 4.2.16-1 aktualisiert
	• `aws-cli`Auf 2.15.36 aktualisiert
	
	Veröffentlichung von macOS Sonoma 14.4.1 (alle Mac-Instanzen)
	• Sicherheitsinhalt von macOS Sonoma 14.4.1
	
	Veröffentlichung von macOS Ventura 13.6.6 (alle Mac-Instanzen)
	• Sicherheitsinhalt von macOS Ventura 13.6.6
	• Safari wurde auf 17.4.1 aktualisiert
	  • Sicherheitsinhalt von Safari 17.4.1
	
	Für macOS Monterey (alle Mac-Instanzen)
	• Safari wurde auf 17.4.1 aktualisiert
	  • Sicherheitsinhalt von Safari 17.4.1

Verwenden von Amazon EBS-optimierten Instances

Eine Amazon EBS-optimierte Instance nutzt einen optimierten Konfigurations-Stack und bietet zusätzliche dedizierte Kapazität für I/O-Vorgänge in Amazon EBS. Diese Optimierung bietet die beste Leistung für Ihre EBS-Volumes, indem Konflikte zwischen I/O-Vorgängen in Amazon EBS und anderem Datenverkehr von Ihrer Instance minimiert werden.

EBS-optimierte Instances bieten eine dedizierte Bandbreite für Amazon EBS. Wenn sie einer EBS-optimierten Instance zugeordnet sind, sind Allzweck-SSD (`gp2` und `gp3`)-Volumes darauf ausgelegt, mindestens 90 % ihrer bereitgestellten IOPS-Leistung zu 99 % der Zeit in einem bestimmten Jahr bereitzustellen, und bereitgestellte IOPS-SSD (`io1` und `io2`)-Volumes sind darauf ausgelegt, mindestens 90 % ihrer bereitgestellten IOPS-Leistung zu 99,9 % der Zeit in einem Jahr bereitzustellen. Sowohl durchsatzoptimierte HDD (`st1`) als auch Cold-HDD (`sc1`) liefern mindestens 90 % ihrer erwarteten Durchsatzleistung in 99 % der Zeit in einem bestimmten Jahr. Davon abweichende Zeiträume sind ziemlich gleichmäßig verteilt, sodass 99 % des erwarteten Gesamtdurchsatzes pro Stunde erreicht werden. Weitere Informationen finden Sie unter Amazon EBS-Volumetypen im Amazon EBS-Benutzerhandbuch.

> **Important**
>
> Die EBS-Leistung einer Instance wird durch die Leistungsgrenzen der Instance oder die aggregierte Leistung der angefügten Volumes begrenzt, je nachdem, welcher Wert kleiner ist. Um die maximale EBS-Leistung zu erreichen, muss eine Instance über angefügte Volumes verfügen, die zusammen eine Leistung bereitstellen, die der maximalen Leistung der Instance entspricht oder darüber liegt. Um beispielsweise `80,000` IOPS für `r6i.16xlarge` zu erreichen, müssen für die Instance mindestens `5` `gp3` Volumes mit jeweils `16,000` IOPS bereitgestellt werden (`5` Volumes x `16,000` IOPS = `80,000` IOPS).

Inhalt

Unterstützte Instance-Typen

Die folgenden Tabellen zeigen, welche Instance-Typen die EBS-Optimierung unterstützen. Sie enthalten die dedizierte Bandbreite zu Amazon EBS, den typischen maximalen kombinierten Durchsatz, der über diese Verbindung für einen Streaming-Lese-Workload und eine I/O-Größe von 128 KiB erreicht werden kann, sowie die maximale IOPS-Anzahl, die von der Instance unterstützt werden kann, wenn Sie eine I/O-Größe von 16 KiB verwenden.

Entscheiden Sie sich für eine EBS-optimierte Instance, die dedizierteren Amazon EBS-Durchsatz bietet, als Ihre Anwendung benötigt; andernfalls kann die Verbindung zwischen Amazon EBS und Amazon EC2 zu einem Leistungsengpass werden.

Inhalt

Standardmäßig EBS-optimiert

In den folgenden Tabellen sind die Instance-Typen aufgeführt, die die EBS-Optimierung unterstützen. Die EBS-Optimierung ist standardmäßig aktiviert. Die EBS-Optimierung muss nicht aktiviert werden, und ihre Deaktivierung hat keinerlei Auswirkungen.

> **Note**
>
> Sie können diese Informationen auch programmatisch mit dem anzeigen. AWS CLI Weitere Informationen finden Sie unter Anzeigen von Instance-Typen, die EBS-Optimierung unterstützen.

Themen

Allgemeine Zwecke

Important

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
a1.medium [1]	300	3500	37,50	437,50	2500	20000
a1.large [1]	525	3500	65,62	437,50	4000	20000
a1.xlarge [1]	800	3500	100,00	437,50	6 000	20000
a1.2xlarge [1]	1750	3500	218,75	437,50	10000	20000
a1.4xlarge [2]	3500		437,5		20000	
a1.metal [2]	3500		437,5		20000	
m4.large [2]	450		56,25		3600	
m4.xlarge [2]	750		93,75		6 000	
m4.2xlarge [2]	1000		125,0		8000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m4.4xlarge [2]	2000		250,0		16000	
m4.10xlarge [2]	4000		500,0		32000	
m4.16xlarge [2]	10000		1250,0		65000	
m5.large [1]	650	4750	81,25	593,75	3600	18750
m5.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5.4xlarge [2]	4750		593,75		18750	
m5.8xlarge [2]	6800		850,0		30000	
m5.12xlarge [2]	9500		1187,5		40000	
m5.16xlarge [2]	13600		1700,0		60000	
m5.24xlarge [2]	19000		2375,0		80000	
m5.metal [2]	19000		2375,0		80000	
m5a.large [1]	650	2880	81,25	360,00	3600	16000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5a.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
m5a.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
m5a.4xlarge [2]	2880		360,0		16000	
m5a.8xlarge [2]	4750		593,75		20000	
m5a.12xlarge [2]	6780		847,5		30000	
m5a.16xlarge [2]	9500		1187,5		40000	
m5a.24xlarge [2]	13750		1718,75		60000	
m5ad.large [1]	650	2880	81,25	360,00	3600	16000
m5ad.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
m5ad.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
m5ad.4xlarge [2]	2880		360,0		16000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5ad.8xlarge [2]	4750		593,75		20000	
m5ad.12xlarge [2]	6780		847,5		30000	
m5ad.16xlarge [2]	9500		1187,5		40000	
m5ad.24xlarge [2]	13750		1718,75		60000	
m5d.large [1]	650	4750	81,25	593,75	3600	18750
m5d.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5d.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5d.4xlarge [2]	4750		593,75		18750	
m5d.8xlarge [2]	6800		850,0		30000	
m5d.12xlarge [2]	9500		1187,5		40000	
m5d.16xlarge [2]	13600		1700,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5d.24xlarge [2]	19000		2375,0		80000	
m5d.metal [2]	19000		2375,0		80000	
m5dn.large [1]	650	4750	81,25	593,75	3600	18750
m5dn.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5dn.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5dn.4xlarge [2]	4750		593,75		18750	
m5dn.8xlarge [2]	6800		850,0		30000	
m5dn.12xlarge [2]	9500		1187,5		40000	
m5dn.16xlarge [2]	13600		1700,0		60000	
m5dn.24xlarge [2]	19000		2375,0		80000	
m5dn.metal [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5n.large [1]	650	4750	81,25	593,75	3600	18750
m5n.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
m5n.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
m5n.4xlarge [2]	4750		593,75		18750	
m5n.8xlarge [2]	6800		850,0		30000	
m5n.12xlarge [2]	9500		1187,5		40000	
m5n.16xlarge [2]	13600		1700,0		60000	
m5n.24xlarge [2]	19000		2375,0		80000	
m5n.metal [2]	19000		2375,0		80000	
m5zn.large [1]	800	3170	100,00	396,25	3333	13333
m5zn.xlarge [1]	1564	3170	195,50	396,25	6667	13333

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m5zn.2xlarge [2]	3170		396,25		13333	
m5zn.3xlarge [2]	4750		593,75		20000	
m5zn.6xlarge [2]	9500		1187,5		40000	
m5zn.12xlarge [2]	19000		2375,0		80000	
m5zn.metal [2]	19000		2375,0		80000	
m6a.large [1]	650	10000	81,25	1250,00	3600	40000
m6a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6a.8xlarge [2]	10000		1250,0		40000	
m6a.12xlarge [2]	15000		1875,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6a.16xlarge [2]	20000		2500,0		80000	
m6a.24xlarge [2]	30000		3750,0		120000	
m6a.32xlarge [2]	40000		5000,0		160000	
m6a.48xlarge [2]	40000		5000,0		240000	
m6a.metal [2]	40000		5000,0		240000	
m6g.medium [1]	315	4750	39,38	593,75	2500	20000
m6g.large [1]	630	4750	78,75	593,75	3600	20000
m6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
m6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
m6g.4xlarge [2]	4750		593,75		20000	
m6g.8xlarge [2]	9500		1187,5		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6g.12xlarge [2]	14250		1781,25		50000	
m6g.16xlarge [2]	19000		2375,0		80000	
m6g.metal [2]	19000		2375,0		80000	
m6gd.medium [1]	315	4750	39,38	593,75	2500	20000
m6gd.large [1]	630	4750	78,75	593,75	3600	20000
m6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
m6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
m6gd.4xlarge [2]	4750		593,75		20000	
m6gd.8xlarge [2]	9500		1187,5		40000	
m6gd.12xlarge [2]	14250		1781,25		50000	
m6gd.16xlarge [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6gd.metal [2]	19000		2375,0		80000	
m6i.large [1]	650	10000	81,25	1250,00	3600	40000
m6i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6i.8xlarge [2]	10000		1250,0		40000	
m6i.12xlarge [2]	15000		1875,0		60000	
m6i.16xlarge [2]	20000		2500,0		80000	
m6i.24xlarge [2]	30000		3750,0		120000	
m6i.32xlarge [2]	40000		5000,0		160000	
m6i.metal [2]	40000		5000,0		160000	
m6id.large [1]	650	10000	81,25	1250,00	3600	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6id.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m6id.8xlarge [2]	10000		1250,0		40000	
m6id.12xlarge [2]	15000		1875,0		60000	
m6id.16xlarge [2]	20000		2500,0		80000	
m6id.24xlarge [2]	30000		3750,0		120000	
m6id.32xlarge [2]	40000		5000,0		160000	
m6id.metal [2]	40000		5000,0		160000	
m6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
m6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
m6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6idn.8xlarge [2]	25000		312,50		100000	
m6idn.12xlarge [2]	37500		4687,5		150000	
m6idn.16xlarge [2]	50000		6250,0		200000	
m6idn.24xlarge [2]	75000		9375,0		300000	
m6idn.32xlarge [2]	100000		12500,0		400000	
m6idn.metal [2]	100000		12500,0		400000	
m6in.large [1]	1562	25000	195,31	3125,00	6250	100000
m6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
m6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
m6in.8xlarge [2]	25000		312,50		100000	
m6in.12xlarge [2]	37500		4687,5		150000	
m6in.16xlarge [2]	50000		6250,0		200000	
m6in.24xlarge [2]	75000		9375,0		300000	
m6in.32xlarge [2]	100000		12500,0		400000	
m6in.metal [2]	100000		12500,0		400000	
m7a.medium [1]	325	10000	40,62	1250,00	2500	40000
m7a.large [1]	650	10000	81,25	1250,00	3600	40000
m7a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7a.8xlarge [2]	10000		1250,0		40000	
m7a.12xlarge [2]	15000		1875,0		60000	
m7a.16xlarge [2]	20000		2500,0		80000	
m7a.24xlarge [2]	30000		3750,0		120000	
m7a.32xlarge [2]	40000		5000,0		160000	
m7a.48xlarge [2]	40000		5000,0		240000	
m7a.metal-48xl [2]	40000		5000,0		240000	
m7g.medium [1]	315	10000	39,38	1250,00	2500	40000
m7g.large [1]	630	10000	78,75	1250,00	3600	40000
m7g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7g.8xlarge [2]	10000		1250,0		40000	
m7g.12xlarge [2]	15000		1875,0		60000	
m7g.16xlarge [2]	20000		2500,0		80000	
m7g.metal [2]	20000		2500,0		80000	
m7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
m7gd.large [1]	630	10000	78,75	1250,00	3600	40000
m7gd.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7gd.8xlarge [2]	10000		1250,0		40000	
m7gd.12xlarge [2]	15000		1875,0		60000	
m7gd.16xlarge [2]	20000		2500,0		80000	
7 mg. Metall 2	20000		2500,0		80000	
m7i.large [1]	650	10000	81,25	1250,00	3600	40000
m7i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
m7i.8xlarge [2]	10000		1250,0		40000	
m7i.12xlarge [2]	15000		1875,0		60000	
m7i.16xlarge [2]	20000		2500,0		80000	
m7i.24xlarge [2]	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
m7i.48xlarge [2]	40000		5000,0		240000	
m7i.metal-24xl [2]	30000		3750,0		120000	
m7i.metal-48xl [2]	40000		5000,0		240000	
m7i-flex.large [1]	312	10000	39,06	1250,00	2500	40000
m7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
m7i-flex.2xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
m7i-flex.4xlarge [1]	2500	10000	312,50	1250,00	12000	40000
m7i-flex.8xlarge [1]	5000	10000	625,00	1250,00	20000	40000
mac1.metal [2]	14000		1750,0		80000	
mac2.metal [2]	10000		1250,0		55000	
mac2-m2.metal [2]	8000		1000,0		55000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
mac2-m2pro.metal [2]	8000		1000,0		55000	
t3.nano [1]	43	2085	5,38	260,62	250	11800
t3.micro [1]	87	2085	10,88	260,62	500	11800
t3.small [1]	174	2085	21,75	260,62	1000	11800
t3.medium [1]	347	2085	43,38	260,62	2000	11800
t3.large [1]	695	2780	86,88	347,50	4000	15700
t3.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.nano [1]	45	2085	5,62	260,62	250	11800
t3a.micro [1]	90	2085	11,25	260,62	500	11800
t3a.small [1]	175	2085	21,88	260,62	1000	11800
t3a.medium [1]	350	2085	43,75	260,62	2000	11800
t3a.large [1]	695	2780	86,88	347,50	4000	15700
t3a.xlarge [1]	695	2780	86,88	347,50	4000	15700
t3a.2xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.nano [1]	43	2085	5,38	260,62	250	11800

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
t4g.micro [1]	87	2085	10,88	260,62	500	11800
t4g.small [1]	174	2085	21,75	260,62	1000	11800
t4g.medium [1]	347	2085	43,38	260,62	2000	11800
t4g.large [1]	695	2780	86,88	347,50	4000	15700
t4g.xlarge [1]	695	2780	86,88	347,50	4000	15700
t4g.2xlarge [1]	695	2780	86,88	347,50	4000	15700

Für Datenverarbeitung optimiert

> **Important**
>
> [1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.
>
> [2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c4.large [2]	500		62,5		4000	
c4.xlarge [2]	750		93,75		6 000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c4.2xlarge [2]	1000		125,0		8000	
c4.4xlarge [2]	2000		250,0		16000	
c4.8xlarge [2]	4000		500,0		32000	
c5.large [1]	650	4750	81,25	593,75	4000	20000
c5.xlarge [1]	1150	4750	143,75	593,75	6 000	20000
c5.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5.4xlarge [2]	4750		593,75		20000	
c5.9xlarge [2]	9500		1187,5		40000	
c5.12xlarge [2]	9500		1187,5		40000	
c5.18xlarge [2]	19000		2375,0		80000	
c5.24xlarge [2]	19000		2375,0		80000	
c5.metal [2]	19000		2375,0		80000	
c5a.large [1]	200	3170	25,00	396,25	800	13300

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c5a.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5a.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5a.4xlarge [1]	1580	3170	197,50	396,25	6600	13300
c5a.8xlarge [2]	3170		396,25		13300	
c5a.12xlarge [2]	4750		593,75		20000	
c5a.16xlarge [2]	6300		787,5		26700	
c5a.24xlarge [2]	9500		1187,5		40000	
c5ad.large [1]	200	3170	25,00	396,25	800	13300
c5ad.xlarge [1]	400	3170	50,00	396,25	1600	13300
c5ad.2xlarge [1]	800	3170	100,00	396,25	3200	13300
c5ad.4xlarge [1]	1580	3170	197,50	396,25	6600	13300

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c5ad.8xlarge [2]	3170		396,25		13300	
c5ad.12xlarge [2]	4750		593,75		20000	
c5ad.16xlarge [2]	6300		787,5		26700	
c5ad.24xlarge [2]	9500		1187,5		40000	
c5d.large [1]	650	4750	81,25	593,75	4000	20000
c5d.xlarge [1]	1150	4750	143,75	593,75	6 000	20000
c5d.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5d.4xlarge [2]	4750		593,75		20000	
c5d.9xlarge [2]	9500		1187,5		40000	
c5d.12xlarge [2]	9500		1187,5		40000	
c5d.18xlarge [2]	19000		2375,0		80000	
c5d.24xlarge [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c5d.metal [2]	19000		2375,0		80000	
c5n.large [1]	650	4750	81,25	593,75	4000	20000
c5n.xlarge [1]	1150	4750	143,75	593,75	6 000	20000
c5n.2xlarge [1]	2300	4750	287,50	593,75	10000	20000
c5n.4xlarge [2]	4750		593,75		20000	
c5n.9xlarge [2]	9500		1187,5		40000	
c5n.18xlarge [2]	19000		2375,0		80000	
c5n.metal [2]	19000		2375,0		80000	
c6a.large [1]	650	10000	81,25	1250,00	3600	40000
c6a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6a.8xlarge [2]	10000		1250,0		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6a.12xlarge [2]	15000		1875,0		60000	
c6a.16xlarge [2]	20000		2500,0		80000	
c6a.24xlarge [2]	30000		3750,0		120000	
c6a.32xlarge [2]	40000		5000,0		160000	
c6a.48xlarge [2]	40000		5000,0		240000	
c6a.metal [2]	40000		5000,0		240000	
c6g.medium [1]	315	4750	39,38	593,75	2500	20000
c6g.large [1]	630	4750	78,75	593,75	3600	20000
c6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
c6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
c6g.4xlarge [2]	4750		593,75		20000	
c6g.8xlarge [2]	9500		1187,5		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6g.12xlarge [2]	14250		1781,25		50000	
c6g.16xlarge [2]	19000		2375,0		80000	
c6g.metal [2]	19000		2375,0		80000	
c6gd.medium [1]	315	4750	39,38	593,75	2500	20000
c6gd.large [1]	630	4750	78,75	593,75	3600	20000
c6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
c6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
c6gd.4xlarge [2]	4750		593,75		20000	
c6gd.8xlarge [2]	9500		1187,5		40000	
c6gd.12xlarge [2]	14250		1781,25		50000	
c6gd.16xlarge [2]	19000		2375,0		80000	
c6gd.metal [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6gn.medium [1]	760	9500	95,00	1187,50	2500	40000
c6gn.large [1]	1235	9500	154,38	1187,50	5000	40000
c6gn.xlarge [1]	2375	9500	296,88	1187,50	10000	40000
c6gn.2xlarge [1]	4750	9500	593,75	1187,50	20000	40000
c6gn.4xlarge [2]	9500		1187,5		40000	
c6gn.8xlarge [2]	19000		2375,0		80000	
c6gn.12xlarge [2]	28500		3562,5		120000	
c6gn.16xlarge [2]	38000		4750,0		160000	
c6i.large [1]	650	10000	81,25	1250,00	3600	40000
c6i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6i.8xlarge [2]	10000		1250,0		40000	
c6i.12xlarge [2]	15000		1875,0		60000	
c6i.16xlarge [2]	20000		2500,0		80000	
c6i.24xlarge [2]	30000		3750,0		120000	
c6i.32xlarge [2]	40000		5000,0		160000	
c6i.metal [2]	40000		5000,0		160000	
c6id.large [1]	650	10000	81,25	1250,00	3600	40000
c6id.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c6id.8xlarge [2]	10000		1250,0		40000	
c6id.12xlarge [2]	15000		1875,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6id.16xlarge [2]	20000		2500,0		80000	
c6id.24xlarge [2]	30000		3750,0		120000	
c6id.32xlarge [2]	40000		5000,0		160000	
c6id.metal [2]	40000		5000,0		160000	
c6in.large [1]	1562	25000	195,31	3125,00	6250	100000
c6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
c6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
c6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
c6in.8xlarge [2]	25000		312,50		100000	
c6in.12xlarge [2]	37500		4687,5		150000	
c6in.16xlarge [2]	50000		6250,0		200000	
c6in.24xlarge [2]	75000		9375,0		300000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c6in.32xlarge [2]	100000		12500,0		400000	
c6in.metal [2]	100000		12500,0		400000	
c7a.medium [1]	325	10000	40,62	1250,00	2500	40000
c7a.large [1]	650	10000	81,25	1250,00	3600	40000
c7a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7a.8xlarge [2]	10000		1250,0		40000	
c7a.12xlarge [2]	15000		1875,0		60000	
c7a.16xlarge [2]	20000		2500,0		80000	
c7a.24xlarge [2]	30000		3750,0		120000	
c7a.32xlarge [2]	40000		5000,0		160000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7a.48xlarge [2]	40000		5000,0		240000	
c7a.metal-48xl [2]	40000		5000,0		240000	
c7g.medium [1]	315	10000	39,38	1250,00	2500	40000
c7g.large [1]	630	10000	78,75	1250,00	3600	40000
c7g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7g.8xlarge [2]	10000		1250,0		40000	
c7g.12xlarge [2]	15000		1875,0		60000	
c7g.16xlarge [2]	20000		2500,0		80000	
c7g.metal [2]	20000		2500,0		80000	
c7gd.medium [1]	315	10000	39,38	1250,00	2500	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7gd.large [1]	630	10000	78,75	1250,00	3600	40000
c7gd.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7gd.8xlarge [2]	10000		1250,0		40000	
c7gd.12xlarge [2]	15000		1875,0		60000	
c7gd.16xlarge [2]	20000		2500,0		80000	
c7gd.metall 2	20000		2500,0		80000	
c7gn.medium [1]	521	10000	65,12	1250,00	2083	40000
c7gn.large [1]	1042	10000	130,25	1250,00	4167	40000
c7gn.xlarge [1]	2083	10000	260,38	1250,00	8333	40000
c7gn.2xlarge [1]	4167	10000	520,88	1250,00	16667	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7gn.4xlarge [1]	833	10000	1041,62	1250,00	33333	40000
c7gn.8xlarge [1]	16667	20000	2083,38	2500,00	66667	80000
c7gn.12xlarge [1]	25000	30000	3125,00	3750,00	100000	120000
c7gn.16xlarge [1]	33333	40000	4166,62	5000,00	133333	160000
C7GN. Metall 1	33333	40000	4166,62	5000,00	133333	160000
c7i.large [1]	650	10000	81,25	1250,00	3600	40000
c7i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
c7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
c7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
c7i.8xlarge [2]	10000		1250,0		40000	
c7i.12xlarge [2]	15000		1875,0		60000	
c7i.16xlarge [2]	20000		2500,0		80000	
c7i.24xlarge [2]	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c7i.48xlarge [2]	40000		5000,0		240000	
c7i.metal-24xl [2]	30000		3750,0		120000	
c7i.metal-48xl [2]	40000		5000,0		240000	
c7i-flex.groß [1]	312	10000	39,06	1250,00	2500	40000
c7i-flex.xlarge [1]	625	10000	78,12	1250,00	3600	40000
c7i-flex.2xgroß [1]	1250	10000	156,25	1250,00	6 000	40000
c7i-flex.4x groß [1]	2500	10000	312,50	1250,00	12000	40000
c7i-flex.8xgroß [1]	5000	10000	625,00	1250,00	20000	40000

RAM-optimiert

Important

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r4.large [2]	425		53.125		3000	
r4.xlarge [2]	850		106,25		6 000	
r4.2xlarge [2]	1700		212,5		12000	
r4.4xlarge [2]	3500		437,5		18750	
r4.8xlarge [2]	7000		875,0		37500	
r4.16xlarge [2]	14000		1750,0		75000	
r5.large [1]	650	4750	81,25	593,75	3600	18750
r5.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5.4xlarge [2]	4750		593,75		18750	
r5.8xlarge [2]	6800		850,0		30000	
r5.12xlarge [2]	9500		1187,5		40000	
r5.16xlarge [2]	13600		1700,0		60000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5.24xlarge [2]	19000		2375,0		80000	
r5.metal [2]	19000		2375,0		80000	
r5a.large [1]	650	2880	81,25	360,00	3600	16000
r5a.xlarge [1]	1085	2880	135,62	360,00	6 000	16000
r5a.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
r5a.4xlarge [2]	2880		360,0		16000	
r5a.8xlarge [2]	4750		593,75		20000	
r5a.12xlarge [2]	6780		847,5		30000	
r5a.16xlarge [2]	9500		1187,5		40000	
r5a.24xlarge [2]	13570		1696,25		60000	
r5ad.large [1]	650	2880	81,25	360,00	3600	16000
r5ad.xlarge [1]	1085	2880	135,62	360,00	6 000	16000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5ad.2xlarge [1]	1580	2880	197,50	360,00	8333	16000
r5ad.4xlarge [2]	2880		360,0		16000	
r5ad.8xlarge [2]	4750		593,75		20000	
r5ad.12xlarge [2]	6780		847,5		30000	
r5ad.16xlarge [2]	9500		1187,5		40000	
r5ad.24xlarge [2]	13570		1696,25		60000	
r5b.large [1]	1250	10000	156,25	1250,00	5417	43333
r5b.xlarge [1]	2500	10000	312,50	1250,00	10833	43333
r5b.2xlarge [1]	5000	10000	625,00	1250,00	21667	43333
r5b.4xlarge [2]	10000		1250,0		43333	
r5b.8xlarge [2]	20000		2500,0		86667	
r5b.12xlarge [2]	30000		3750,0		130000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5b.16xlarge [2]	40000		5000,0		173333	
r5b.24xlarge [2]	60000		7500,0		260000	
r5b.metal [2]	60000		7500,0		260000	
r5d.large [1]	650	4750	81,25	593,75	3600	18750
r5d.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5d.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5d.4xlarge [2]	4750		593,75		18750	
r5d.8xlarge [2]	6800		850,0		30000	
r5d.12xlarge [2]	9500		1187,5		40000	
r5d.16xlarge [2]	13600		1700,0		60000	
r5d.24xlarge [2]	19000		2375,0		80000	
r5d.metal [2]	19000		2375,0		80000	
r5dn.large [1]	650	4750	81,25	593,75	3600	18750

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5dn.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5dn.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5dn.4xlarge [2]	4750		593,75		18750	
r5dn.8xlarge [2]	6800		850,0		30000	
r5dn.12xlarge [2]	9500		1187,5		40000	
r5dn.16xlarge [2]	13600		1700,0		60000	
r5dn.24xlarge [2]	19000		2375,0		80000	
r5dn.metal [2]	19000		2375,0		80000	
r5n.large [1]	650	4750	81,25	593,75	3600	18750
r5n.xlarge [1]	1150	4750	143,75	593,75	6 000	18750
r5n.2xlarge [1]	2300	4750	287,50	593,75	12000	18750
r5n.4xlarge [2]	4750		593,75		18750	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r5n.8xlarge [2]	6800		850,0		30000	
r5n.12xlarge [2]	9500		1187,5		40000	
r5n.16xlarge [2]	13600		1700,0		60000	
r5n.24xlarge [2]	19000		2375,0		80000	
r5n.metal [2]	19000		2375,0		80000	
r6a.large [1]	650	10000	81,25	1250,00	3600	40000
r6a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r6a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6a.8xlarge [2]	10000		1250,0		40000	
r6a.12xlarge [2]	15000		1875,0		60000	
r6a.16xlarge [2]	20000		2500,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6a.24xlarge [2]	30000		3750,0		120000	
r6a.32xlarge [2]	40000		5000,0		160000	
r6a.48xlarge [2]	40000		5000,0		240000	
r6a.metal [2]	40000		5000,0		240000	
r6g.medium [1]	315	4750	39,38	593,75	2500	20000
r6g.large [1]	630	4750	78,75	593,75	3600	20000
r6g.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
r6g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
r6g.4xlarge [2]	4750		593,75		20000	
r6g.8xlarge [2]	9500		1187,5		40000	
r6g.12xlarge [2]	14250		1781,25		50000	
r6g.16xlarge [2]	19000		2375,0		80000	
r6g.metal [2]	19000		2375,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6gd.medium [1]	315	4750	39,38	593,75	2500	20000
r6gd.large [1]	630	4750	78,75	593,75	3600	20000
r6gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
r6gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
r6gd.4xlarge [2]	4750		593,75		20000	
r6gd.8xlarge [2]	9500		1187,5		40000	
r6gd.12xlarge [2]	14250		1781,25		50000	
r6gd.16xlarge [2]	19000		2375,0		80000	
r6gd.metal [2]	19000		2375,0		80000	
r6i.large [1]	650	10000	81,25	1250,00	3600	40000
r6i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r6i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6i.8xlarge [2]	10000		1250,0		40000	
r6i.12xlarge [2]	15000		1875,0		60000	
r6i.16xlarge [2]	20000		2500,0		80000	
r6i.24xlarge [2]	30000		3750,0		120000	
r6i.32xlarge [2]	40000		5000,0		160000	
r6i.metal [2]	40000		5000,0		160000	
r6idn.large [1]	1562	25000	195,31	3125,00	6250	100000
r6idn.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6idn.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6idn.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6idn.8xlarge [2]	25000		312,50		100000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6idn.12xlarge [2]	37500		4687,5		150000	
r6idn.16xlarge [2]	50000		6250,0		200000	
r6idn.24xlarge [2]	75000		9375,0		300000	
r6idn.32xlarge [2]	100000		12500,0		400000	
r6idn.metal [2]	100000		12500,0		400000	
r6in.large [1]	1562	25000	195,31	3125,00	6250	100000
r6in.xlarge [1]	3125	25000	390,62	3125,00	12500	100000
r6in.2xlarge [1]	6250	25000	781,25	3125,00	25000	100000
r6in.4xlarge [1]	12500	25000	1562,50	3125,00	50000	100000
r6in.8xlarge [2]	25000		312,50		100000	
r6in.12xlarge [2]	37500		4687,5		150000	
r6in.16xlarge [2]	50000		6250,0		200000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r6in.24xlarge [2]	75000		9375,0		300000	
r6in.32xlarge [2]	100000		12500,0		400000	
r6in.metal [2]	100000		12500,0		400000	
r6id.large [1]	650	10000	81,25	1250,00	3600	40000
r6id.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r6id.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r6id.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r6id.8xlarge [2]	10000		1250,0		40000	
r6id.12xlarge [2]	15000		1875,0		60000	
r6id.16xlarge [2]	20000		2500,0		80000	
r6id.24xlarge [2]	30000		3750,0		120000	
r6id.32xlarge [2]	40000		5000,0		160000	
r6id.metal [2]	40000		5000,0		160000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7a.medium [1]	325	10000	40,62	1250,00	2500	40000
r7a.large [1]	650	10000	81,25	1250,00	3600	40000
r7a.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r7a.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7a.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7a.8xlarge [2]	10000		1250,0		40000	
r7a.12xlarge [2]	15000		1875,0		60000	
r7a.16xlarge [2]	20000		2500,0		80000	
r7a.24xlarge [2]	30000		3750,0		120000	
r7a.32xlarge [2]	40000		5000,0		160000	
r7a.48xlarge [2]	40000		5000,0		240000	
r7a.metal-48xl [2]	40000		5000,0		240000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7g.medium [1]	315	10000	39,38	1250,00	2500	40000
r7g.large [1]	630	10000	78,75	1250,00	3600	40000
r7g.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r7g.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7g.8xlarge [2]	10000		1250,0		40000	
r7g.12xlarge [2]	15000		1875,0		60000	
r7g.16xlarge [2]	20000		2500,0		80000	
r7g.metal [2]	20000		2500,0		80000	
r7gd.medium [1]	315	10000	39,38	1250,00	2500	40000
r7gd.large [1]	630	10000	78,75	1250,00	3600	40000
r7gd.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7gd.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7gd.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7gd.8xlarge [2]	10000		1250,0		40000	
r7gd.12xlarge [2]	15000		1875,0		60000	
r7gd.16xlarge [2]	20000		2500,0		80000	
r7gd.metall 2	20000		2500,0		80000	
r7i.large [1]	650	10000	81,25	1250,00	3600	40000
r7i.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
r7i.2xlarge [1]	2500	10000	312,50	1250,00	12000	40000
r7i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7i.8xlarge [2]	10000		1250,0		40000	
r7i.12xlarge [2]	15000		1875,0		60000	
r7i.16xlarge [2]	20000		2500,0		80000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7i.24xlarge [2]	30000		3750,0		120000	
r7i.48xlarge [2]	40000		5000,0		240000	
r7i.metal-24xl [2]	30000		3750,0		120000	
r7i.metal-48xl [2]	40000		5000,0		240000	
r7iz.large [1]	792	10000	99,00	1250,00	3600	40000
r7iz.xlarge [1]	1584	10000	198,00	1250,00	6667	40000
r7iz.2xlarge [1]	3168	10000	396,00	1250,00	13333	40000
r7iz.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
r7iz.8xlarge [2]	10000		1250,0		40000	
r7iz.12xlarge [2]	19000		2375,0		76000	
r7iz.16xlarge [2]	20000		2500,0		80000	
r7iz.32xlarge [2]	40000		5000,0		160000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r7iz.metal-16xl [2]	20000		2500,0		80000	
r7iz.metal-32xl [2]	40000		5000,0		160000	
u-3tb1.56xlarge [2]	19000		2375,0		80000	
u-6tb1.56xlarge [2]	38000		4750,0		160000	
u-6tb1.112xlarge [2]	38000		4750,0		160000	
u-6tb1.metal [2]	38000		4750,0		160000	
u-9tb1.112xlarge [2]	38000		4750,0		160000	
u-9tb1.metal [2]	38000		4750,0		160000	
u-12tb1.112xlarge [2]	38000		4750,0		160000	
u-12tb1.metal [2]	38000		4750,0		160000	
u-18tb1.112xlarge [2]	38000		4750,0		160000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
u-18tb1.metal [2]	38000		4750,0		160000	
u-24tb1.112xlarge [2]	38000		4750,0		160000	
u-24tb1.metal [2]	38000		4750,0		160000	
u7i-12 tb.224x groß 2	60000		7500,0		420000	
U7in, 16 TB. 224x, groß 2	100000		12500,0		420000	
U7 in, 24 TB. 224x, groß 2	100000		12500,0		420000	
u7in-32 TB. 224x groß 2	100000		12500,0		420000	
x1.16xlarge [2]	7000		875,0		40000	
x1.32xlarge [2]	14000		1750,0		80000	
x2gd.medium [1]	315	4750	39,38	593,75	2500	20000
x2gd.large [1]	630	4750	78,75	593,75	3600	20000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
x2gd.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
x2gd.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
x2gd.4xlarge [2]	4750		593,75		20000	
x2gd.8xlarge [2]	9500		1187,5		40000	
x2gd.12xlarge [2]	14250		1781,25		60000	
x2gd.16xlarge [2]	19000		2375,0		80000	
x2gd.metal [2]	19000		2375,0		80000	
x2idn.16xlarge [2]	40000		5000,0		173333	
x2idn.24xlarge [2]	60000		7500,0		260000	
x2idn.32xlarge [2]	80000		10000,0		260000	
x2idn.metal [2]	80000		10000,0		260000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
x2iedn.xlarge [1]	2500	20000	312,50	2500,00	8125	65000
x2iedn.2xlarge [1]	5000	20000	625,00	2500,00	16250	65000
x2iedn.4xlarge [1]	10000	20000	1250,00	2500,00	32500	65000
x2iedn.8xlarge [2]	20000		2500,0		65000	
x2iedn.16xlarge [2]	40000		5000,0		130000	
x2iedn.24xlarge [2]	60000		7500,0		195000	
x2iedn.32xlarge [2]	80000		10000,0		260000	
x2iedn.metal [2]	80000		10000,0		260000	
x2iezn.2xlarge [2]	3170		396,25		13333	
x2iezn.4xlarge [2]	4750		593,75		20000	
x2iezn.6xlarge [2]	9500		1187,5		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
x2iezn.8xlarge [2]	12000		1500,0		55000	
x2iezn.12xlarge [2]	19000		2375,0		80000	
x2iezn.metal [2]	19000		2375,0		80000	
x1e.xlarge [2]	500		62,5		3700	
x1e.2xlarge [2]	1000		125,0		7400	
x1e.4xlarge [2]	1750		218,75		10000	
x1e.8xlarge [2]	3500		437,5		20000	
x1e.16xlarge [2]	7000		875,0		40000	
x1e.32xlarge [2]	14000		1750,0		80000	
z1d.large [1]	800	3170	100,00	396,25	3333	13333
z1d.xlarge [1]	1580	3170	197,50	396,25	6667	13333
z1d.2xlarge [2]	3170		396,25		13333	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
z1d.3xlarge [2]	4750		593,75		20000	
z1d.6xlarge [2]	9500		1187,5		40000	
z1d.12xlarge [2]	19000		2375,0		80000	
z1d.metal [2]	19000		2375,0		80000	

Speicheroptimiert

> **Important**
>
> [1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.
>
> [2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
d2.xlarge [2]	750		93,75		6 000	
d2.2xlarge [2]	1000		125,0		8000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
d2.4xlarge [2]	2000		250,0		16000	
d2.8xlarge [2]	4000		500,0		32000	
d3.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3.4xlarge [2]	2800		350,0		15000	
d3.8xlarge [2]	5000		625,0		30000	
d3en.xlarge [1]	850	2800	106,25	350,00	5000	15000
d3en.2xlarge [1]	1700	2800	212,50	350,00	10000	15000
d3en.4xlarge [2]	2800		350,0		15000	
d3en.6xlarge [2]	4000		500,0		25000	
d3en.8xlarge [2]	5000		625,0		30000	
d3en.12xlarge [2]	7000		875,0		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
h1.2xlarge [2]	1750		218,75		12000	
h1.4xlarge [2]	3500		437,5		20000	
h1.8xlarge [2]	7000		875,0		40000	
h1.16xlarge [2]	14000		1750,0		80000	
i3.large [2]	425		53.125		3000	
i3.xlarge [2]	850		106,25		6 000	
i3.2xlarge [2]	1700		212,5		12000	
i3.4xlarge [2]	3500		437,5		16000	
i3.8xlarge [2]	7000		875,0		32500	
i3.16xlarge [2]	14000		1750,0		65000	
i3.metal [2]	19000		2375,0		80000	
i3en.large [1]	576	4750	72,10	593,75	3000	20000
i3en.xlarge [1]	1153	4750	144,20	593,75	6 000	20000
i3en.2xlarge [1]	2307	4750	288,39	593,75	12000	20000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
i3en.3xlarge [1]	3800	4750	475,00	593,75	15000	20000
i3en.6xlarge [2]	4750		593,75		20000	
i3en.12xlarge [2]	9500		1187,5		40000	
i3en.24xlarge [2]	19000		2375,0		80000	
i3en.metal [2]	19000		2375,0		80000	
i4g.large [1]	625	10000	78,12	1250,00	2500	40000
i4g.xlarge [1]	1250	10000	156,25	1250,00	5000	40000
i4g.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i4g.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4g.8xlarge [2]	10000		1250,0		40000	
i4g.16xlarge [2]	20000		2500,0		80000	
i4i.large [1]	625	10000	78,12	1250,00	2500	40000
i4i.xlarge [1]	1250	10000	156,25	1250,00	5000	40000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
i4i.2xlarge [1]	2500	10000	312,50	1250,00	10000	40000
i4i.4xlarge [1]	5000	10000	625,00	1250,00	20000	40000
i4i.8xlarge [2]	10000		1250,0		40000	
i4i.12xlarge [2]	15000		1875,0		60000	
i4i.16xlarge [2]	20000		2500,0		80000	
i4i.24xlarge [2]	30000		3750,0		120000	
i4i.32xlarge [2]	40000		5000,0		160000	
i4i.metal [2]	40000		5000,0		160000	
im4gn.large [1]	1250	10000	156,25	1250,00	5000	40000
im4gn.xlarge [1]	2500	10000	312,50	1250,00	10000	40000
im4gn.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
im4gn.4xlarge [2]	10000		1250,0		40000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
im4gn.8xlarge [2]	20000		2500,0		80000	
im4gn.16xlarge [2]	40000		5000,0		160000	
is4gen.medium [1]	625	10000	78,12	1250,00	2500	40000
is4gen.large [1]	1250	10000	156,25	1250,00	5000	40000
is4gen.xlarge [1]	2500	10000	312,50	1250,00	10000	40000
is4gen.2xlarge [1]	5000	10000	625,00	1250,00	20000	40000
is4gen.4xlarge [2]	10000		1250,0		40000	
is4gen.8xlarge [2]	20000		2500,0		80000	

Beschleunigtes Computing

Important

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
dl1.24xlarge [2]	19000		2375,0		80000	
dl2q.24xlarge [2]	19000		2375,0		80000	
f1.2xlarge [2]	1700		212,5		12000	
f1.4xlarge [2]	3500		437,5		44000	
f1.16xlarge [2]	14000		1750,0		75000	
g3.4xlarge [2]	3500		437,5		20000	
g3.8xlarge [2]	7000		875,0		40000	
g3.16xlarge [2]	14000		1750,0		80000	
g4ad.xlarge [1]	400	3170	50,00	396,25	1700	13333
g4ad.2xlarge [1]	800	3170	100,00	396,25	3400	13333
g4ad.4xlarge [1]	1580	3170	197,50	396,25	6700	13333
g4ad.8xlarge [2]	3170		396,25		13333	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
g4ad.16xlarge [2]	6300		787,5		26667	
g4dn.xlarge [1]	950	3500	118,75	437,50	3000	20000
g4dn.2xlarge [1]	1150	3500	143,75	437,50	6 000	20000
g4dn.4xlarge [2]	4750		593,75		20000	
g4dn.8xlarge [2]	9500		1187,5		40000	
g4dn.12xlarge [2]	9500		1187,5		40000	
g4dn.16xlarge [2]	9500		1187,5		40000	
g4dn.metal [2]	19000		2375,0		80000	
g5.xlarge [1]	700	3500	87,50	437,50	3000	15000
g5.2xlarge [1]	850	3500	106,25	437,50	3500	15000
g5.4xlarge [2]	4750		593,75		20000	
g5.8xlarge [2]	16000		2000,0		65000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
g5.12xlarge [2]	16000		2000,0		65000	
g5.16xlarge [2]	16000		2000,0		65000	
g5.24xlarge [2]	19000		2375,0		80000	
g5.48xlarge [2]	19000		2375,0		80000	
g5g.xlarge [1]	1188	4750	148,50	593,75	6 000	20000
g5g.2xlarge [1]	2375	4750	296,88	593,75	12000	20000
g5g.4xlarge [2]	4750		593,75		20000	
g5g.8xlarge [2]	9500		1187,5		40000	
g5g.16xlarge [2]	19000		2375,0		80000	
g5g.metal [2]	19000		2375,0		80000	
g6.x groß 1	1000	5000	125,00	625,00	4000	20000
g 6.2 x groß 1	2000	5000	250,00	625,00	8000	20000
g 6.4 x groß 2	8000		1000,0		32000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
g 6,8 x groß 2	16000		2000,0		64000	
g 6.12 x groß 2	20000		2500,0		80000	
g 6.16 x groß 2	20000		2500,0		80000	
g 6,24 x groß 2	30000		3750,0		120000	
g 6,48 x groß 2	60000		7500,0		240000	
gr 6,4 x groß 2	8000		1000,0		32000	
gr 6,8 x groß 2	16000		2000,0		64000	
inf1.xlarge [1]	1190	4750	148,75	593,75	4000	20000
inf1.2xlarge [1]	1190	4750	148,75	593,75	6 000	20000
inf1.6xlarge [2]	4750		593,75		20000	
inf1.24xlarge [2]	19000		2375,0		80000	
inf2.xlarge [1]	1250	10000	156,25	1250,00	6 000	40000
inf2.8xlarge [2]	10000		1250,0		40000	
inf2.24xlarge [2]	30000		3750,0		120000	

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
inf2.48xlarge [2]	60000		7500,0		240000	
p2.xlarge [2]	750		93,75		6 000	
p2.8xlarge [2]	5000		625,0		32500	
p2.16xlarge [2]	10000		1250,0		65000	
p3.2xlarge [2]	1750		218,75		10000	
p3.8xlarge [2]	7000		875,0		40000	
p3.16xlarge [2]	14000		1750,0		80000	
p3dn.24xlarge [2]	19000		2375,0		80000	
p4d.24xlarge [2]	19000		2375,0		80000	
p4de.24xlarge [2]	19000		2375,0		80000	
p5.48xlarge [2]	80000		10000,0		260000	
trn1.2xlarge [1]	5000	20000	625,00	2500,00	16250	65000

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
trn1.32xlarge [2]	80000		10000,0		260000	
trn1n.32xlarge [2]	80000		10000,0		260000	
vt1.3xlarge [1]	2375	4750	296,88	593,75	10000	20000
vt1.6xlarge [2]	4750		593,75		20000	
vt1.24xlarge [2]	19000		2375,0		80000	

Datenverarbeitung in Hochleistung

Important

[1] Diese Instances können mindestens einmal alle 24 Stunden für 30 Minuten die maximale Leistung erbringen, danach fallen sie auf ihre Basisleistung zurück.

[2] Diese Instances können ihre angegebene Leistung auf unbestimmte Zeit aufrechterhalten. Wenn Ihre Workload länger als 30 Minuten anhaltende maximale Leistung erfordert, verwenden Sie eine dieser Instances.

Instance-Größe	Baseline-Bandbreite (Mbit/s)	Maximale Bandbreite (Mbit/s)	Baseline-Durchsatz (MB/s, 128 KiB I/O)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Baseline-IOPS (16 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
hpc6a.48xlarge [1]	87	2085	10,88	260,62	500	11000
hpc6id.32xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.12xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.24xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.48xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7a.96xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.4xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.8xlarge [1]	87	2085	10,88	260,62	500	11000
hpc7g.16xlarge [1]	87	2085	10,88	260,62	500	11000

EBS-Optimierung unterstützt

In der folgenden Tabelle sind die Instance-Typen aufgeführt, die die EBS-Optimierung unterstützen (die EBS-Optimierung ist standardmäßig nicht aktiviert). Sie können die EBS-Optimierung aktivieren, wenn Sie diese Instances starten oder nachdem sie ausgeführt werden. Für Instances muss die EBS-Optimierung aktiviert sein, um die beschriebene Leistungsstufe zu erreichen. Wenn Sie die

EBS-Optimierung für eine Instance aktivieren, die nicht standardmäßig EBS-optimiert ist, wird für die dedizierte Kapazität eine zusätzliche, geringe Gebühr auf Stundenbasis berechnet. Informationen zu Preisen finden Sie unter „EBS-optimierte Instances“ auf der Seite Amazon EC2-Preise, -On-Demand-Preise.

> **Note**
>
> Sie können diese Informationen auch programmatisch mit dem anzeigen. AWS CLI Weitere Informationen finden Sie unter Anzeigen von Instance-Typen, die EBS-Optimierung unterstützen.

Instance-Größe	Maximale Bandbreite (Mbit/s)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
c1.xlarge	1000	125.0	8000
c3.xlarge	500	62,5	4000
c3.2xlarge	1000	125,0	8000
c3.4xlarge	2000	250,0	16000
i2.xlarge	500	62,5	4000
i2.2xlarge	1000	125,0	8000
i2.4xlarge	2000	250,0	16000
m1.large	500	62,5	4000
m1.xlarge	1000	125,0	8000
m2.2xlarge	500	62,5	4000
m2.4xlarge	1000	125,0	8000
m3.xlarge	500	62,5	4000
m3.2xlarge	1000	125,0	8000

Instance-Größe	Maximale Bandbreite (Mbit/s)	Maximaler Durchsatz (MB/s, 128 KiB I/O)	Maximale IOPS-Anzahl (16 KiB I/O)
r3.xlarge	500	62,5	4000
r3.2xlarge	1000	125,0	8000
r3.4xlarge	2000	250,0	16000

Die Instances `i2.8xlarge`, `c3.8xlarge` und `r3.8xlarge` haben keine dedizierte EBS-Bandbreite und bieten daher keine EBS-Optimierung. In diesen Instances wird der Netzwerkdatenverkehr zusammen mit dem Amazon EBS-Datenverkehr durch dieselbe 10-Gigabit-Netzwerkschnittstelle geleitet.

Erzielen maximaler Leistung

Mithilfe der Metriken `EBSIOBalance%` und `EBSByteBalance%` können Sie leichter ermitteln, ob Ihre Instances korrekt dimensioniert sind. Sie können diese Messwerte in der CloudWatch Konsole anzeigen und einen Alarm einrichten, der auf der Grundlage eines von Ihnen angegebenen Schwellenwerts ausgelöst wird. Diese Metriken werden als Prozentsatz angezeigt. Instances mit einem dauerhaft niedrigen Saldoprozentsatz sind Kandidaten für eine Vergrößerung. Instances, bei denen der Saldoprozentsatz nie unter 100 % fällt, sind Kandidaten für eine Verkleinerung. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.

Die High Memory-Instances sind so konzipiert, dass große In-Memory-Datenbanken, einschließlich Produktionsbereitstellungen der SAP HANA-In-Memory-Datenbank in der Cloud, ausgeführt werden. Um die EBS-Leistung zu maximieren, verwenden Sie High Memory-Instances mit einer geraden Anzahl von `io1`- oder `io2`-Volumes mit identischer bereitgestellter Leistung. Verwenden Sie beispielsweise für hohe IOPS-Workloads vier `io1`- oder `io2`-Volumes mit 40 000 bereitgestellten IOPS, um die maximal 160 000 Instance-IOPS zu erhalten. In ähnlicher Weise verwenden Sie bei Workloads mit hohem Durchsatz sechs `io1`- oder `io2`-Volumes mit 48 000 bereitgestellten IOPS, um den maximalen Durchsatz von 4 750 MB/s zu erzielen. Weitere Empfehlungen finden Sie unter Speicherkonfiguration für SAP HANA.

Überlegungen

- Die Instances G4dn, I3en, M5a, M5ad, R5a, R5ad, T3, T3a und Z1d, die nach dem 26. Februar 2020 gestartet wurden, bieten die maximale Leistung, die in der obigen Tabelle aufgeführt ist. Um

die maximale Leistung einer Instance zu erhalten, die vor dem 26. Februar 2020 gestartet wurde, beenden und starten Sie sie.

- Die Instances C5, C5d, C5n, M5, M5d, M5n, M5dn, R5, R5d, R5n, R5dn und P3dn, die nach dem 3. Dezember 2019 gestartet wurden, bieten die maximale Leistung, die in der obigen Tabelle aufgeführt ist. Um die maximale Leistung einer Instance zu erhalten, die vor dem 3. Dezember 2019 gestartet wurde, beenden und starten Sie sie.
- Die Instances `u-6tb1.metal`, `u-9tb1.metal` und `u-12tb1.metal`, die nach dem 12. März 2020 gestartet wurden, bieten die Leistung in der obigen Tabelle. Instances dieser Typen, die vor dem 12. März 2020 gestartet wurden, bieten möglicherweise eine geringere Leistung. Um die maximale Leistung einer Instance zu erhalten, die vor dem 12. März 2020 gestartet wurde, wenden Sie sich an Ihr Kontoteam, um die Instance ohne zusätzliche Kosten zu aktualisieren.

Anzeigen von Instance-Typen, die EBS-Optimierung unterstützen

Sie können den verwenden AWS CLI , um die Instance-Typen in der aktuellen Region anzuzeigen, die die EBS-Optimierung unterstützen.

So zeigen Sie die Instance-Typen an, die EBS-Optimierung unterstützen und diese standardmäßig aktiviert haben:

Verwenden Sie den folgenden describe-instance-types-Befehl. Wenn Sie diesen Befehl an einer Windows-Befehlszeile ausführen, ersetzen Sie die\ line-Fortsetzungszeichen durch das Zeichen ^.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=default --output=table
```

Beispielausgabe für `eu-west-1`:

```
-------------------------------------------------------------------------
|                          DescribeInstanceTypes                        |
+-------------------+---------------------+-----------+-----------------------+
|   InstanceType    | MaxBandwidth(Mb/s)  |  MaxIOPS  |  MaxThroughput(MB/s)  |
+-------------------+---------------------+-----------+-----------------------+
|  m5dn.8xlarge     |  6800               |  30000    |  850.0                |
|  m6gd.xlarge      |  4750               |  20000    |  593.75               |
```

```
|  c4.4xlarge       |  2000               |  16000    |  250.0                |
|  r4.16xlarge      |  14000              |  75000    |  1750.0               |
|  m5ad.large       |  2880               |  16000    |  360.0                |
...
```

So zeigen Sie die Instance-Typen an, die EBS-Optimierung unterstützen, diese jedoch nicht standardmäßig aktiviert haben:

Verwenden Sie den folgenden describe-instance-types-Befehl.

```
aws ec2 describe-instance-types \
--query 'InstanceTypes[].{InstanceType:InstanceType,"MaxBandwidth(Mb/
s)":EbsInfo.EbsOptimizedInfo.MaximumBandwidthInMbps,MaxIOPS:EbsInfo.EbsOptimizedInfo.MaximumIop
s)":EbsInfo.EbsOptimizedInfo.MaximumThroughputInMBps}' \
--filters Name=ebs-info.ebs-optimized-support,Values=supported --output=table
```

Beispielausgabe für `eu-west-1`:

```
-------------------------------------------------------------------------
|                        DescribeInstanceTypes                          |
+--------------+----------------------+----------+-----------------------+
| InstanceType | MaxBandwidth(Mb/s)   | MaxIOPS  |  MaxThroughput(MB/s)  |
+--------------+----------------------+----------+-----------------------+
|  i2.2xlarge  |  1000                |  8000    |  125.0                |
|  m2.4xlarge  |  1000                |  8000    |  125.0                |
|  m2.2xlarge  |  500                 |  4000    |  62.5                 |
|  c1.xlarge   |  1000                |  8000    |  125.0                |
|  i2.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.xlarge   |  500                 |  4000    |  62.5                 |
|  m1.xlarge   |  1000                |  8000    |  125.0                |
|  r3.4xlarge  |  2000                |  16000   |  250.0                |
|  r3.2xlarge  |  1000                |  8000    |  125.0                |
|  c3.xlarge   |  500                 |  4000    |  62.5                 |
|  m3.2xlarge  |  1000                |  8000    |  125.0                |
|  r3.xlarge   |  500                 |  4000    |  62.5                 |
|  i2.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.4xlarge  |  2000                |  16000   |  250.0                |
|  c3.2xlarge  |  1000                |  8000    |  125.0                |
|  m1.large    |  500                 |  4000    |  62.5                 |
+--------------+----------------------+----------+-----------------------+
```

Aktivieren der EBS-Optimierung beim Start

Sie können die Optimierung für eine Instance aktivieren, indem Sie das Attribut für die EBS-Optimierung entsprechend setzen.

So aktivieren Sie die Amazon EBS-Optimierung beim Starten einer Instance über die Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance aus.
3. Wählen Sie unter Step 1: Choose an Amazon Machine Image (AMI) (Schritt 1: Auswählen eines Amazon Machine Images (AMI)) ein AMI aus.
4. Wählen Sie unter Step 2: Choose an Instance Type (Schritt 2: Auswählen eines Instance-Typs) einen Instance-Typ aus, der die Amazon EBS-Optimierung unterstützt.
5. Füllen Sie unter Step 3: Configure Instance Details (Schritt 3: Konfigurieren der Instance-Details) die Felder aus, die Sie benötigen, und wählen Sie die Option Launch as EBS-optimized instance (Als EBS-optimierte Instance starten). Wenn der Instance-Typ, den Sie im letzten Schritt ausgewählt haben, die Amazon EBS-Optimierung nicht unterstützt, wird diese Option nicht angezeigt. Wenn der ausgewählte Instance-Typ standardmäßig Amazon EBS-optimiert ist, ist diese Option bereits ausgewählt und Sie können Sie nicht deaktivieren.
6. Befolgen Sie die Anweisungen, um den Assistenten zu beenden und Ihre Instance zu starten.

So aktivieren Sie die EBS-Optimierung beim Starten einer Instance über die Befehlszeile

Sie können einen der folgenden Befehle mit der entsprechenden Option verwenden. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- run-instances mit `--ebs-optimized` (AWS CLI)
- New-EC2Instancemit `-EbsOptimized` (AWS Tools for Windows PowerShell)

Aktivieren der EBS-Optimierung für eine vorhandene Instance

Sie können die Optimierung für eine vorhandene Instance aktivieren oder deaktivieren, indem Sie das Instance-Attribut für die Amazon EBS-Optimierung entsprechend ändern. Wenn die Instance ausgeführt wird, müssen Sie sie zuerst stoppen.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

So aktivieren Sie die EBS-Optimierung für eine vorhandene Instance über die Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Wählen Sie zum Anhalten der Instance Aktionen, Instance-Status, Instance anhalten aus. Das Anhalten der Instance kann einige Minuten dauern.
4. Während die Instance noch ausgewählt ist, wählen Sie Aktionen, Instance-Einstellungen, Instance-Typ ändern aus.
5. Führen Sie für Instance-Typ ändern einen der folgenden Schritte aus:
   - Wenn der Typ Ihrer Instance standardmäßig Amazon EBS-optimiert ist, ist die Option EBS-optimized (EBS-optimiert) bereits ausgewählt, und Sie können Sie nicht ändern. Sie können Cancel (Abbrechen) wählen, da die Amazon EBS-Optimierung bereits für die Instance aktiviert ist.
   - Wenn der Instance-Typ Ihrer Instance die Amazon EBS-Optimierung unterstützt, wählen Sie die Option EBS-optimiert aus und klicken Sie anschließend auf Übernehmen.
   - Wenn der Instance-Typ Ihrer Instance die Amazon EBS-Optimierung nicht unterstützt, können Sie die Option EBS-optimized (EBS-optimiert) nicht auswählen. Sie können unter Instance-Typ einen Instance-Typ auswählen, der die Amazon EBS-Optimierung unterstützt; wählen Sie die Option EBS-optimized aus und klicken Sie anschließend auf Übernehmen.
6. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

So aktivieren Sie die EBS-Optimierung für eine vorhandene Instance über die Befehlszeile

1. Wenn die Instance ausgeführt wird, verwenden Sie einen der folgenden Befehle, um sie zu stoppen:
   - stop-instances (AWS CLI)
   - Stop-EC2Instance (AWS Tools for Windows PowerShell)

2. Um die EBS-Optimierung zu aktivieren, verwenden Sie einen der folgenden Befehle mit der entsprechenden Option:

   - modify-instance-attribute mit `--ebs-optimized` (AWS CLI)
   - Edit-EC2InstanceAttributemit `-EbsOptimized` (AWS Tools for Windows PowerShell)

Instance-Kaufoptionen

Amazon EC2 bietet die folgenden Kaufoptionen, um Ihnen die Möglichkeit zu bieten, Ihre Kosten basierend auf Ihren Anforderungen zu optimieren.

- On-Demand Instances: Sie bezahlen nach Sekunde für die gestarteten Instances.
- Savings Plans: Reduzieren Sie die Amazon EC2-Kosten, indem Sie sich auf eine konsistente Nutzung (in USD/h) für eine Laufzeit von ein bis drei Jahren festlegen.
- Reserved Instances: Reduzieren Sie die Amazon EC2-Kosten, indem Sie sich auf eine konsistente Instance-Konfiguration (einschließlich Instance-Typ und Region) für eine Laufzeit von ein oder drei Jahren festlegen.
- Spot Instances: Sie können ungenutzte EC2-Instances anfordern, wodurch sich die Amazon EC2-Kosten erheblich verringern lassen.
- Dedicated Hosts: Sie zahlen für einen Host, der ausschließlich für Ihre Instances reserviert ist, und stellen eigene Softwarelizenzen pro Socket, Kern oder VM bereit, um Kosten zu sparen.
- Dedicated Instances: Stundenweise Abrechnung für Instances, die auf Single–Tenant-Hardware ausgeführt werden.
- Kapazitätsreservierungen — Reservieren Sie Kapazität für Ihre EC2-Instances in einer bestimmten Availability Zone.

Wenn Sie sich nicht auf eine bestimmte Instance-Konfiguration festlegen können, sich aber auf einen Nutzungsbetrag festlegen können, erwerben Sie Savings Plans, um Ihre On-Demand-Instance-Kosten zu senken.Wenn Sie eine Kapazitätsreservierung benötigen, kaufen Sie Reserved Instances oder Kapazitätsreservierungen für eine bestimmte Availability Zone. Mithilfe von Kapazitätsblöcken kann ein Cluster von GPU-Instances reserviert werden. Spot-Instances sind eine kostengünstige Wahl, sofern Sie bei der Ausführung Ihrer Anwendungen zeitlich flexibel sind und Unterbrechungen verschmerzen können. Dedicated Hosts oder Dedicated Instances können Sie bei der Einhaltung von Compliance-Anforderungen unterstützen und Kosten senken, indem sie Ihre vorhandenen

servergebundenen Software-Lizenzen verwenden. Weitere Informationen finden Sie unter Amazon EC2 – Preise.

Weitere Informationen zu Savings Plans finden Sie im Savings Plans User Guide.

Inhalt

Festlegen des Instance-Lebenszyklus

Der Lebenszyklus einer Instance beginnt, wenn sie gestartet wird, und endet, wenn sie beendet wird. Die Kaufoption, die Sie wählen, wirkt sich auf den Lebenszyklus der Instance aus. Beispielsweise wird eine On-Demand-Instance ausgeführt, wenn Sie sie starten, und endet, wenn Sie sie beenden. Eine Spot-Instance wird so lange ausgeführt, bis ihre Kapazität verfügbar ist und ihr Höchstpreis den Spot-Preis übersteigt.

Verwenden Sie eine der folgenden Methoden, um den Lebenszyklus einer Instance zu bestimmen.

Festlegen des Instance-Lebenszyklus mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Suchen Sie auf der Registerkarte Details unter Instance-Details nach Lebenszyklus. Wenn der Wert `spot` ist, ist die Instance eine Spot-Instance. Wenn der Wert `normal` ist, ist die Instance eine On-Demand-Instance oder eine Reserved Instance.
5. Suchen Sie auf der Registerkarte Details unter Host und Platzierungsgruppe die nach Tenancy. Wenn der Wert `host` ist, wird die Instance auf einem Dedicated Host ausgeführt. Wenn der Wert `dedicated` ist, ist die Instance eine Dedicated Instance.

Um den Instanzlebenszyklus mit dem zu ermitteln AWS CLI

Verwenden Sie den folgenden describe-instances-Befehl:

```
aws ec2 describe-instances --instance-ids i-1234567890abcdef0
```

Wenn die Instance auf einer Dedicated Host ausgeführt wird, enthält die Ausgabe die folgenden Informationen:

```
"Tenancy": "host"
```

Wenn die Instance eine Dedicated Instance ist, enthält die Ausgabe die folgenden Informationen:

```
"Tenancy": "dedicated"
```

Wenn die Instance eine Spot-Instance ist, enthält die Ausgabe die folgenden Informationen:

```
"InstanceLifecycle": "spot"
```

Andernfalls enthält die Ausgabe nicht `InstanceLifecycle`.

On-Demand Instances

Mit On-Demand-Instances zahlen Sie für Rechenkapazität nach der Sekunde ohne langfristige Verpflichtungen. Sie haben vollständige Kontrolle über den Lebenszyklus der Instance. Sie entscheiden, wann sie aufgerufen, angehalten, in den Ruhezustand versetzt, neu gestartet oder beendet werden soll.

Mit dem Erwerb von On-Demand-Instances sind keine langfristigen Verpflichtungen verbunden. Sie bezahlen nur für die Sekunden, in denen sich Ihre On-Demand-Instances im Status `running` befinden, mit einem Minimum von 60 Sekunden. Der Preis pro Sekunde für eine laufende On-Demand-Instance ist festgelegt und auf der Seite Preise zu Amazon EC2, On-Demand-Preisseite aufgelistet.

Wir empfehlen, für Anwendungen mit kurzfristigen, unregelmäßigen Workloads, die nicht unterbrochen werden können, On-Demand-Instances zu verwenden.

Verwenden Sie für signifikante Einsparungen im Vergleich zu On-Demand-Instances AWS Savings Plans, Spot-Instances oder Reserved Instances.

Inhalt

Kontingente für On-Demand-Instances

Es gibt Kontingente für die Anzahl der laufenden On-Demand-Instances AWS-Konto pro Region. Kontingente für On-Demand-Instances werden in Bezug auf die Anzahl der virtuellen Recheneinheiten (vCPUs) verwaltet, die Ihre laufenden On-Demand-Instances verwenden (unabhängig vom Instance-Typ). Jeder Kontingenttyp gibt die maximale Anzahl von vCPUs für eine oder mehrere Instance-Familien an.

Ihr Konto umfasst die folgenden Kontingente für On-Demand-Instances. Kontingente gelten nur für laufende Instances. Wenn Ihre Instance ausstehend, gestoppt, gestoppt oder im Ruhezustand ist, wird sie nicht auf Ihre Kontingente angerechnet.

Name	Standard	Anpassbar
Ausführen von On-Demand-DL-Instances	0	Ja
Ausführen von On-Demand-F-Instances	0	Ja
Ausführen von On-Demand-G- und VT-Instances	0	Ja
Ausführen von On-Demand-HPC-Instances	0	Ja
Ausführen von On-Demand-High–Memory-Instances	0	Ja
Ausführen von On-Demand-Inf-Instances	0	Ja
Ausführen von On-Demand-P-Instances	0	Ja
On-Demand-Ausführung von Standard-Instances (A, C, D, H, I, M, R, T, Z)	5	Ja
Ausführen von On-Demand-Trn-Instances	0	Ja

Name	Standard	Anpassbar
Ausführen von On-Demand-X-Instances	0	Ja

Informationen zu den verschiedenen Instance-Familien, Generationen und Größen finden Sie im Amazon EC2 Instance Types Guide.

Sie können jede Kombination von Instance-Typen starten, die Ihre jeweiligen Anwendungen erfüllen, sofern die Anzahl der vCPUs Ihr Kontokontingent nicht überschreitet. Beispiel: Bei einem Standard-Instance-Kontingent von 256 vCPUs könnten Sie 32 `m5.2xlarge`-Instances (32 x 8 vCPUs) oder 16 `c5.4xlarge`-Instances (16 x 16 vCPUs) starten. Weitere Informationen finden Sie unter EC2-On-Demand-Instance-Limits.

Aufgaben

- Überwachen von Kontingenten für On-Demand-Instances und der Nutzung
- Anfordern einer Kontingenterhöhung

Überwachen von Kontingenten für On-Demand-Instances und der Nutzung

Sie können Ihre Kontingent für On-Demand-Instances für die einzelnen Regionen mit den folgenden Methoden anzeigen und verwalten.

Anzeigen Ihrer aktuellen Kontingente mit der Service-Quotas-Konsole

1. Öffnen Sie die Service Quotas Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Wählen Sie auf der Navigationsleiste eine Region aus.
3. Geben Sie im Filterfeld den Wert **`On-Demand`** ein.
4. In der Spalte Angewandter Kontingentwert wird die maximale Anzahl der vCPUs für jeden Kontingenttyp der On-Demand-Instance für Ihr Konto angezeigt.

Um Ihre aktuellen Kontingente mit der AWS Trusted Advisor Konsole einzusehen

Öffnen Sie die Seite mit den Dienstbeschränkungen in der AWS Trusted Advisor Konsole.

Um CloudWatch Alarme zu konfigurieren

Mit der Integration von Amazon CloudWatch Metrics können Sie Ihre EC2-Nutzung anhand Ihrer Kontingente überwachen. Sie können auch Alarme konfigurieren, um vor beinahe erreichten Kontingenten zu warnen. Weitere Informationen finden Sie unter Service Quotas und CloudWatch Amazon-Alarme im Service Quotas Quotas-Benutzerhandbuch.

Anfordern einer Kontingenterhöhung

Auch wenn Amazon EC2 Ihre Kontingente für On-Demand-Instances automatisch basierend auf Ihrer Nutzung erhöht, können Sie bei Bedarf eine Kontingenterhöhung anfordern. Wenn Sie beispielsweise mehr Instances starten möchten, als Ihr aktuelles Kontingent zulässt, können Sie mithilfe der Service-Quotas-Konsole wie in Amazon-EC2-Service Quotas beschrieben eine Kontingenterhöhung beantragen.

Preise für On-Demand-Instances anfordern

Sie können die Price List Service API oder die AWS Price List API verwenden, um die Preise von On-Demand-Instances abzufragen. Weitere Informationen finden Sie unter Verwenden der AWS Preislisten-API im AWS Billing Benutzerhandbuch.

Reserved Instances

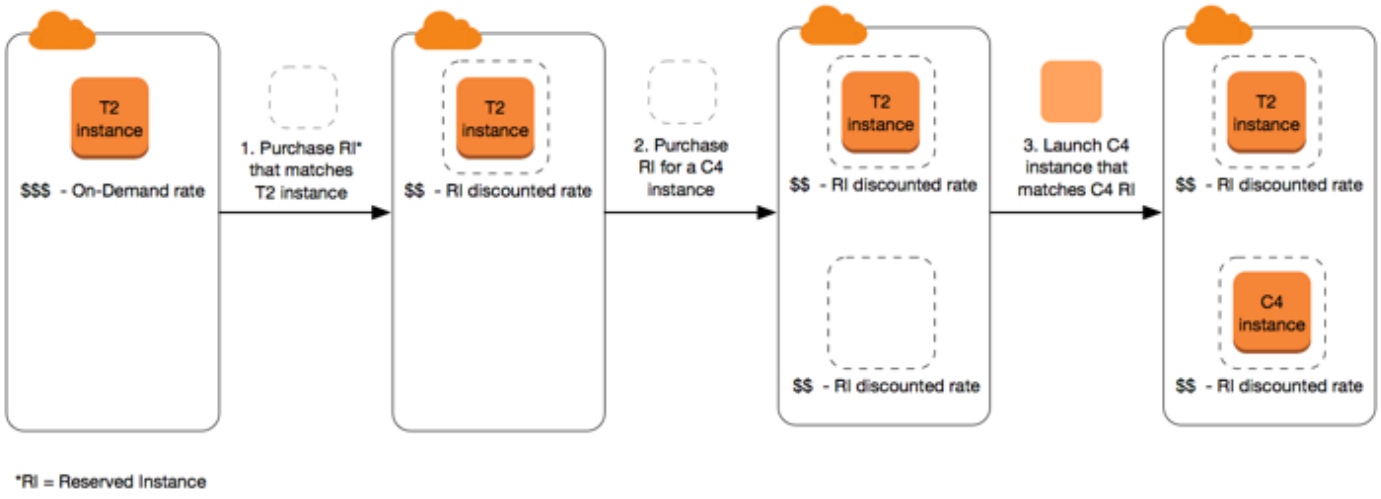
> **Important**
>
> Wir empfehlen Savings Plans gegenüber Reserved Instances. Sparpläne sind die einfachste und flexibelste Möglichkeit, Geld bei Ihren AWS Rechenkosten zu sparen und bieten niedrigere Preise (bis zu 72% Rabatt auf On-Demand-Preise), genau wie Reserved Instances. Savings Plans unterscheiden sich jedoch von Reserved Instances. Bei Reserved Instances verpflichten Sie sich zu einer bestimmten Instance-Konfiguration, wohingegen Sie mit Savings Plans die Flexibilität haben, die Instance-Konfigurationen zu verwenden, die Ihren Anforderungen am besten entsprechen. Um Savings Plans nutzen zu können, verpflichten Sie sich zu einem gleichbleibenden Nutzungsbetrag, gemessen in USD pro Stunde. Weitere Informationen finden Sie im AWS Benutzerhandbuch zu Savings Plans.

Reserved Instances bieten Ihnen deutlich reduzierte Amazon EC2-Kosten im Vergleich zu den Preisen für On-Demand-Instances. Bei Reserved-Instances handelt es sich nicht um physische Instances, sondern um einen Fakturierungsrabatt für die Nutzung gewisser On-Demand-Instances in Ihrem Konto. Diese On-Demand-Instances müssen verschiedenen Attributen wie Instance-Typ und Region entsprechen, um vom Fakturierungsrabatt zu profitieren.

Themen für Reserved Instances

Reserved Instance-Übersicht

Das folgende Diagramm zeigt eine grundlegende Übersicht zum Kauf und zur Nutzung von Reserved Instances.



In diesem Szenario verfügen Sie über eine aktive On-Demand-Instance (T2) in Ihrem Konto. Für diese zahlen Sie zurzeit die On-Demand-Tarife. Sie erwerben eine den Attributen Ihrer aktiven Instance entsprechende Reserved Instance und erhalten einen sofortigen Preisvorteil. Als Nächstes erwerben Sie eine Reserved Instance für eine C4-Instance. In Ihrem Konto sind keine aktiven

Instances vorhanden, die den Attributen dieser Reserved Instance entsprechen. Als Letztes starten Sie eine Instance, die den Attributen der C4-Reserved Instance entspricht, und Sie erhalten einen sofortigen Preisvorteil.

Schlüsselvariablen zur Bestimmung der Reserved Instance-Preise

Die Reserved Instance-Preise werden anhand der folgenden Schlüsselvariablen bestimmt.

Instance-Attribute

Eine Reserved Instance hat vier Instance-Attribute, von denen ihr Preis abhängig ist.

- Instance-Typ: Beispielsweise `m4.large`. Dieser besteht aus der Instance-Familie (z. B. `m4`) und der Instance-Größe (z. B. `large`).
- Region: Die Region, in der das Reserved Instance gekauft wird.
- Tenancy: Ob die Instance auf gemeinsam genutzter Hardware (Standard) oder auf Single–Tenant-Hardware (dediziert) ausgeführt wird. Weitere Informationen finden Sie unter Dedicated Instances.
- Plattform: Das Betriebssystem (z. B. Windows oder Linux/Unix). Weitere Informationen finden Sie unter Wählen einer Plattform.

Dauerhafte Verpflichtung

Sie können eine Reserved Instance für eine ein- oder dreijährige Laufzeit erwerben, wobei für die dreijährige Laufzeitverpflichtung ein größerer Rabatt angeboten wird.

- Ein Jahr: Ein Jahr wird als 31536000 Sekunden (365 Tage) definiert.
- Drei Jahre: Drei Jahre werden als 94608000 Sekunden (1095 Tage) definiert.

Reserved Instances werden nicht automatisch verlängert. Wenn sie auslaufen, können Sie ohne jegliche Unterbrechung die EC2-Instance weiter nutzen. In diesem Fall werden jedoch die On-Demand-Tarife berechnet. Wenn die Reserved Instances für die T2- und C4-Instances im Beispiel oben auslaufen, zahlen Sie bis zur Beendigung der Instances oder dem Kauf neuer Reserved Instances mit den passenden Instance-Attributen wieder die On-Demand-Tarife.

> **Important**
>
> Der Kauf einer Reserved Instance kann nicht storniert werden. Sollten sich Ihre Anforderungen ändern, können Sie Ihre Reserved Instance jedoch möglicherweise ändern, austauschen oder verkaufen.

Zahlungsoptionen

Für Reserved Instances stehen folgende Zahlungsoptionen zur Verfügung:

- Komplette Vorauszahlung: Die gesamte Zahlung wird zum Anfang der Laufzeit durchgeführt. Es entstehen keine weiteren Kosten und es werden für die gesamte Laufzeit keine weiteren Stundensätze berechnet (unabhängig von den genutzten Stunden).
- Teilweise Vorauszahlung: Ein Teil der Kosten muss im Voraus bezahlt werden und die restlichen Stunden während der Laufzeit werden zu einem ermäßigten Stundensatz abgerechnet (unabhängig von der Nutzung der Reserved Instance).
- Keine Vorauszahlung: Sie zahlen einen ermäßigten Stundensatz für jede Stunde im Rahmen der Laufzeit (unabhängig davon, ob die Reserved Instance genutzt wird). Es ist keine Vorauszahlung erforderlich.

> **Note**
>
> Reserved Instances ohne Vorauszahlung arbeiten mit einer vertraglichen Verpflichtung zur monatlichen Zahlung über die gesamte Laufzeit hinweg. Aus diesem Grund benötigen Sie einen positiven Abrechnungsverlauf, bevor Sie Reserved Instances ohne Vorauszahlung erwerben können.

Im Allgemeinen sparen Sie durch eine größere Vorauszahlung für Reserved Instances mehr Geld. Im Reserved Instance Marketplace werden Reserved Instances von Drittanbietern zu günstigeren Preisen und mit kürzeren Laufzeiten angeboten. Weitere Informationen finden Sie unter Verkaufen im Reserved Instance Marketplace.

Angebotsklasse

Wenn sich Ihre Anforderungen ändern, können Sie Ihre Reserved Instance jedoch ändern oder austauschen (je nach Angebotsklasse).

- Standard: Diese Klasse bietet den signifikantesten Rabatt, kann aber nur geändert werden. Standard Reserved Instances kann nicht ausgetauscht werden.
- Convertible: Diese Klasse bietet einen geringeren Rabatt als Standard-Reserved Instances, kann aber gegen eine andere Convertible Reserved Instance mit anderen Instance-Attributen ausgetauscht werden. Convertible Reserved Instances können auch geändert werden.

Weitere Informationen finden Sie unter Reserved Instances-Typen (Angebotsklassen).

> **Important**
>
> Der Kauf einer Reserved Instance kann nicht storniert werden. Sollten sich Ihre Anforderungen ändern, können Sie Ihre Reserved Instance jedoch möglicherweise ändern, austauschen oder verkaufen.

Weitere Informationen finden Sie auf der Seite Preise für Amazon EC2 Reserved Instances.

Regionale und zonengebundene Reserved Instances (Umfang)

Bei dem Erwerb einer Reserved Instance legen Sie den Geltungsbereich der Reserved Instance fest. Der Umfang ist entweder regional oder zonengebunden.

- Regional: Wenn Sie eine Reserved Instance für eine Region erwerben, wird sie als regionale Reserved Instance bezeichnet.
- Zonengebunden: Wenn Sie eine Reserved Instance für eine bestimmte Availability Zone erwerben, wird sie als zonengebundene Reserved Instance bezeichnet.

Der Umfang hat keinen Einfluss auf den Preis. Sie zahlen den gleichen Preis für regionale oder zonengebundene Reserved Instance. Weitere Informationen zu Preisen Reserved Instance erhalten Sie unter Schlüsselvariablen zur Bestimmung der Reserved Instance-Preise und Preise für Amazon-EC2-Reserved-Instances.

Weitere Informationen darüber, wie Sie den Geltungsbereich einer Reserved Instance festlegen können, finden Sie unter RI-Attribute, insbesondere unter dem Aufzählungspunkt Availability Zone.

Unterschiede zwischen regionalen und zonengebundenen Reserved Instances

Die folgende Tabelle hebt einige der wichtigsten Unterschiede zwischen regionalen Reserved Instances und zonengebundenen Reserved Instances hervor:

	Regionsgebundene Reserved Instances	Zonengebundene Reserved Instances
Fähigkeit zum Reservieren von Kapazität	Ein regionaler Reserved Instance reserviert keine Kapazität.	Ein zonaler Reserved Instance reserviert Kapazität in der angegebenen Availability Zone.
Flexibilität bezüglich der Availability Zone	Der Reserved Instance-Rabatt gilt für die Instance-Nutzung in jeder Availability Zone in der angegebenen Region.	Keine Flexibilität bezüglich der Availability Zone – Der Reserved Instance-Rabatt gilt nur für die Instance-Nutzung in der angegebenen Availability Zone.
Flexibilität bezüglich der Instance-Größe	Der Reserved Instance-Rabatt gilt unabhängig von der Größe für die Instance-Nutzung in der Instance-Familie. Wird nur für Reserved Instances der Amazon Linux/ Unix-Plattform mit Standard-Tenancy unterstützt. Weitere Informationen finden Sie unter Flexibilität bezüglich der Instance-Größe anhängig vom Normalisierungsfaktor.	Keine Flexibilität bezüglich der Instance-Größe – Der Reserved Instance-Rabatt gilt nur für die Instance-Nutzung für die angegebene Kombinati on aus Instance-Typ und -Größe.
Einen Kauf in die Warteschl ange stellen	Sie können Käufe für regionale Reserved Instances in Warteschlange stellen	Sie können Käufe für zonengebundene Reserved Instances nicht in Warteschl ange stellen.

Weitere Informationen und Beispiele finden Sie unter So werden Reserved Instances angewendet.

Reserved Instances-Typen (Angebotsklassen)

Die Angebotsklasse von Reserved Instance ist entweder Standard oder Convertible. Ein Standard-Reserved-Instance bietet einen größeren Rabatt als ein Convertible-Reserved-Instance, aber Sie können keinen Standard-Reserved-Instance umtauschen. Sie können Convertible-Reserved Instances wechseln. Sie können Standard- und Convertible-Reserved Instances ändern.

Die Konfiguration eines Reserved Instance umfasst einen einzelnen Instance-Typ, eine Plattform, einen Umfang und eine Tenancy über eine Laufzeit. Wenn sich Ihre Anforderungen ändern, können Sie Ihre Reserved Instance jedoch ändern oder austauschen.

Unterschiede zwischen Standard- und Convertible-Reserved Instances

Die folgenden Unterschiede gelten zwischen den Standard- und Convertible-Reserved Instances.

	Standard-Reserved Instance	Convertible Reserved Instance
Ändern von Reserved Instances	Einige Attribute können geändert werden. Weitere Informationen finden Sie unter Ändern von Reserved Instances.	Einige Attribute können geändert werden. Weitere Informationen finden Sie unter Ändern von Reserved Instances.
Reserved Instances auswechseln	Kann nicht ausgetauscht werden.	Kann während der Laufzeit gegen eine andere Convertible Reserved Instance mit neuen Attributen inkl. Instance-Familie, Instance-Typ, Plattform, Umfang und Tenancy ausgetauscht werden. Weitere Informationen finden Sie unter Austausch en von Convertible Reserved Instances.
Verkaufen im Reserved Instance Marketplace	Kann im Reserved Instance Marketplace verkauft werden.	Kann nicht im Reserved Instance Marketplace verkauft werden.

	Standard-Reserved Instance	Convertible Reserved Instance
Einkaufen im Reserved Instance Marketplace	Kann im Reserved Instance Marketplace gekauft werden.	Kann nicht im Reserved Instance Marketplace gekauft werden.

So werden Reserved Instances angewendet

Reserved Instances sind keine physischen Instances, sondern ein Abrechnungsrabatt, der auf die laufenden On-Demand-Instances in Ihrem Konto angewendet wird. Die On-Demand-Instances müssen bestimmten Spezifikationen der Reserved Instances entsprechen, damit der Abrechnungsrabatt angewendet werden kann.

Wenn Sie eine Reserved Instance erwerben und bereits über eine laufende On-Demand-Instance verfügen, die den Spezifikationen der Reserved Instance entspricht, wird der Abrechnungsrabatt sofort und automatisch angewendet. Sie müssen Ihre Instances nicht neu starten. Wenn Sie über keine berechtigte On-Demand-Instance verfügen, starten Sie eine On-Demand-Instance mit denselben Spezifikationen wie Ihre Reserved Instance. Weitere Informationen finden Sie unter Nutzen Ihres Reserved Instances.

Die Angebotsklasse (Standard oder Convertible) der Reserved Instance hat keinen Einfluss darauf, wie der Abrechnungsrabatt angewendet wird.

Themen

So werden zonengebundene Reserved Instances angewendet

Eine Reserved Instance, die gekauft wird, um Kapazität in einer bestimmten Availability Zone zu reservieren, wird als zonengebundene Reserved Instance bezeichnet.

- Der Reserved-Instance-Rabatt gilt für die übereinstimmende Instance-Nutzung in dieser Availability Zone.

- Die Attribute (Tenancy, Plattform, Availability Zone, Instance-Typ und Instance-Größe) der aktiven Instances müssen denen der Reserved Instances entsprechen.

Wenn Sie beispielsweise zwei `c4.xlarge` Standard-Tenancy Linux/Unix Standard Reserved Instances in der Availability Zone „us-east-1a“ erwerben, kann der Reserved-Instance-Rabatt auf bis zu zwei aktive `c4.xlarge` Standard-Tenancy Linux/Unix-Instances in der Availability Zone „us-east-1a“ angewendet werden.

So werden regionale Reserved Instances angewendet

Eine für eine Region erworbene Reserved Instance wird als regionale Reserved Instance bezeichnet und bietet Flexibilität in Bezug auf die Instance-Größe und Availability Zone.

- Der Reserved Instance-Rabatt gilt für die Instance-Nutzung in jeder Availability Zone in dieser Region.
- Der Reserved-Instance-Rabatt gilt für die Instance-Nutzung innerhalb der Instance-Familie, unabhängig von der Größe – dies wird als Instance-Größenflexibilität bezeichnet.

Flexibilität bezüglich der Instance-Größe

Bei flexibler Instance-Größe gilt der Rabatt für Reserved Instances für die Nutzung von Instances, die dieselbe Familie, Generation und dasselbe Attribut haben. Die Reserved Instance wird basierend auf dem Normalisierungsfaktor innerhalb der Instance-Familie von der kleinsten bis hin zur größten Instance-Größe angewendet. Ein Beispiel für die Anwendung des Reserved-Instance-Rabatts finden Sie unter Szenario 2: Reserved Instances in einem einzigen Konto unter Anwendung des Normalisierungsfaktors.

Einschränkungen

- Unterstützt: Die Flexibilität der Instance-Größe wird nur für regionale Reserved Instances unterstützt.
- Nicht unterstützt: Die Flexibilität der Instance-Größe wird für die folgenden Reserved Instances nicht unterstützt:
  - Reserved Instances, die für eine bestimmte Availability Zone erworben werden (zonengebundene Reserved Instances)
  - Reservierte Instances für G4ad-, G4dn-, G5-, G5g-, Inf1- und Inf2-Instances

- Reserved Instances für Windows Server, Windows Server mit SQL Standard, Windows Server mit SQL Server Enterprise, Windows Server mit SQL Server Web, RHEL und SUSE Linux Enterprise Server
- Reserved Instances mit Dedicated Tenancy

Flexibilität bezüglich der Instance-Größe anhängig vom Normalisierungsfaktor

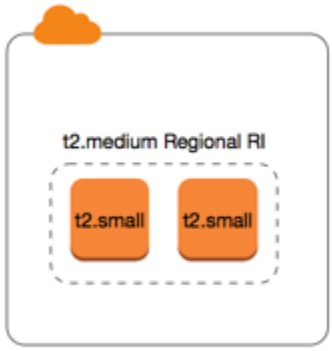
Die flexible Instance-Größe wird durch den Normalisierungsfaktor der Instance-Größe bestimmt. Der Rabatt gilt für aktive Instances derselben Instance-Familie Typs in jeder Availability Zone der Region entweder vollständig oder teilweise. Dies hängt von der Instance-Größe der Reservierung ab. Nur die Attribute Instance-Familie, Tenancy und Plattform müssen übereinstimmen.

In der folgenden Tabelle sind die unterschiedlichen Größen innerhalb einer Instance-Familie und der entsprechende Normalisierungsfaktor aufgeführt. Diese Maßeinheit wird zur Anwendung des Rabatts für Reserved Instances auf die normalisierte Nutzung des Instance-Familie genutzt.

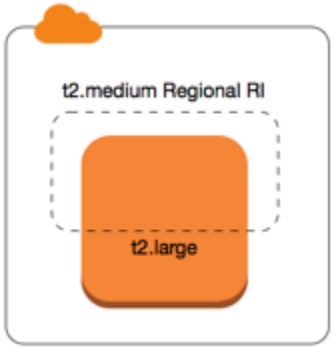
Instance-Größe	Normalisierungsfaktor
nano	0,25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64

Instance-Größe	Normalisierungsfaktor
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Eine `t2.medium`-Instance hat beispielsweise einen Normalisierungsfaktor von 2. Wenn Sie eine `t2.medium` Standard-Tenancy Amazon Linux/Unix Reserved Instance in US East (N. Virginia) erwerben, und in der Region über zwei aktive `t2.small` Instances in Ihrem Konto verfügen, wird der Rabatt voll auf beide Instances angewendet.



Wenn Sie über eine `t2.large`-Instance in der Region USA Ost (Nord-Virginia) in Ihrem Konto verfügen, wird der Rabatt zu 50 % auf die Nutzung der Instance angewendet.



Der Normalisierungsfaktor wird auch angewendet, wenn Sie Reserved Instances ändern. Weitere Informationen finden Sie unter Ändern von Reserved Instances.

Normalisierungsfaktor für Bare Metal-Instances

Flexibilität bezüglich der Instance-Größe gilt auch für Bare Metal-Instances in der Instance-Familie. Bei regionalen Amazon Linux/Unix-Reserved Instances mit geteilter Tenancy für Bare Metal-Instances können Sie von den Reserved Instance-Einsparungen in derselben Instance-Familie profitieren. Dies gilt auch umgekehrt. Bei regionalen Amazon Linux/Unix-Reserved Instances mit geteilter Tenancy für Instances in derselben Familie wie eine Bare Metal-Instance können Sie von den Reserved Instance-Einsparungen für die Bare Metal-Instance profitieren.

Die `metal`-Instance-Größe besitzt keinen einzigen Normalisierungsfaktor. Eine Bare Metal-Instance hat den gleichen Normalisierungsfaktor wie die entsprechende virtualisierte Instance-Größe innerhalb derselben Instance-Familie. Beispielsweise hat eine `i3.metal`-Instance den gleichen Normalisierungsfaktor wie eine `i3.16xlarge`-Instance.

Instance-Größe	Normalisierungsfaktor
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128
`c5n.metal`	144

Instance-Größe	Normalisierungsfaktor
c5.metal | c5d.metal | i3en.metal | m5.metal | m5d.metal | m5dn.metal | m5n.metal | r5.metal | r5b.metal | r5d.metal | r5dn.metal | r5n.metal	192
c6i.metal | c6id.metal | m6i.metal | m6id.metal | r6d.metal | r6id.metal	256
u-*.metal	896

Beispiel: Eine i3.metal-Instance hat beispielsweise einen Normalisierungsfaktor von 128. Wenn Sie eine i3.metal-Reserved Instance der Amazon Linux/Unix-Plattform mit Standard-Tenancy in der Region US East (N. Virginia) erwerben, kann der Rabatt wie folgt angewendet werden:

- Wenn Sie in Ihrem Konto in dieser Region über eine aktive i3.16xlarge-Instance verfügen, wird der Rabatt voll auf die i3.16xlarge-Instance (i3.16xlarge-Normalisierungsfaktor = 128) angewendet.
- Oder wenn Sie in Ihrem Konto in dieser Region über zwei aktive i3.8xlarge-Instances verfügen, wird der Rabatt voll auf beide i3.8xlarge-Instances (i3.8xlarge-Normalisierungsfaktor = 64) angewendet.
- Oder wenn Sie in Ihrem Konto in dieser Region über vier aktive i3.4xlarge-Instances verfügen, wird der Rabatt voll auf alle vier i3.4xlarge-Instances (i3.4xlarge-Normalisierungsfaktor = 32) angewendet.

Dies gilt auch umgekehrt. Wenn Sie z. B. zwei i3.8xlarge-Reserved Instances auf der Amazon Linux/Unix-Plattform mit Standard-Tenancy in der Region US East (N. Virginia) erwerben und bereits über eine aktive i3.metal-Instance in dieser Region verfügen, wird der Rabatt voll auf die i3.metal-Instance angewendet.

Beispiele zur Anwendung von Reserved Instances

Die folgenden Szenarien decken die Anwendungsmöglichkeiten von Reserved Instances ab.

- Szenario 1: Reserved Instances in einem einzigen Konto

Szenario 1: Reserved Instances in einem einzigen Konto

Sie führen die folgenden On-Demand-Instances in Konto A aus:

- 4 x `m3.large` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a
- 2 x `m4.xlarge` Amazon Linux, Standard-Tenancy-Instances in Availability Zone us-east-1b
- 1 x `c4.xlarge` Amazon Linux, Standard-Tenancy-Instances in Availability Zone us-east-1c

Sie erwerben die folgenden Reserved Instances in Konto A:

- 4 x `m3.large` Linux, Standard-Tenancy Reserved Instances in Availability Zone us-east-1a (Kapazität ist reserviert)
- 4 x `m4.large` Amazon Linux, Standard-Tenancy Reserved Instances in der Region us-east-1
- 1 x `c4.large` Amazon Linux, Standard-Tenancy Reserved Instances in der Region us-east-1

Die Reserved Instance-Rabatte werden folgendermaßen angewendet:

- Da die Attribute (Instance-Größe, Region, Plattform, Tenancy) übereinstimmen, werden der Rabatt und die Kapazitätsreservierung der vier `m3.large` Zonen-Reserved Instances für die vier `m3.large` Instances genutzt.
- Die regionalen `m4.large` Reserved Instances bieten eine Flexibilität für die Availability Zone und die Instance-Größe. Sie sind regionale Amazon Linux Reserved Instances mit Standard-Tenancy.

  Eine `m4.large` entspricht 4 normalisierten Einheiten/Stunde.

  Sie haben vier regionale `m4.large` Reserved Instances erworben. Insgesamt entsprechen diese 16 normalisierten Einheiten/Stunde (4x4). Konto A verfügt über zwei aktive `m4.xlarge` Instances. Dies entspricht 16 normalisierten Einheiten/Stunde (2x8). In diesem Fall sorgen die vier regionalen `m4.large`-Reserved-Instances für den vollständigen Rabatt für die Nutzung der zwei `m4.xlarge`-Instances.

- Die regionale `c4.large` Reserved Instance in us-east-1 bietet eine Flexibilität für die Availability Zone und die Instance-Größe, denn sie ist eine regionale Amazon Linux Reserved Instance mit Standard-Tenancy und wird auf die `c4.xlarge` Instance angewendet. Eine `c4.large` Instance entspricht 4 normalisierten Einheiten/Stunde und eine `c4.xlarge` entspricht 8 normalisierten Einheiten/Stunde.

  In diesem Fall wird die regionale `c4.large` Reserved Instance teilweise auf die `c4.xlarge`-Nutzung angewendet. Dies liegt daran, dass die `c4.large` Reserved Instance der Nutzung von 4 normalisierten Einheiten/Stunde entspricht, die `c4.xlarge` Instance jedoch 8 normalisierte Einheiten/Stunde erfordert. Aus diesem Grund wird der Rabatt durch die `c4.large` Reserved Instance nur zu 50 % auf die `c4.xlarge`-Nutzung angewendet. Die verbleibende `c4.xlarge`-Nutzung wird über den On-Demand-Tarif abgerechnet.

Szenario 2: Reserved Instances in einem einzigen Konto unter Anwendung des Normalisierungsfaktors

Sie führen die folgenden On-Demand-Instances in Konto A aus:

- 2 x `m3.xlarge` Amazon Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a
- 2 x `m3.large` Amazon Linux, Standard-Tenancy-Instances in Availability Zone us-east-1b

Sie erwerben die folgende Reserved Instance in Konto A:

- 1 x `m3.2xlarge` Amazon Linux, Standard-Tenancy-Reserved-Instance in der Region us-east-1

Die Reserved Instance-Rabatte werden folgendermaßen angewendet:

- Die `m3.2xlarge` regionale Reserved Instance in us-east-1 bietet Flexibilität in Bezug auf die Availability Zone und die Instance-Größe, denn es handelt sich um eine regionale Amazon-Linux-Reserved-Instance mit Standard-Tenancy. Sie wird zunächst auf die `m3.large`-Instances und dann auf die `m3.xlarge`-Instances angewendet, da die Anwendung innerhalb der Instance-Familie basierend auf dem Normalisierungsfaktor von der kleinsten bis zur größten Instance-Größe erfolgt.

  Eine `m3.large`-Instance entspricht 4 normalisierten Einheiten/Stunde.

  Eine `m3.xlarge`-Instance entspricht 8 normalisierten Einheiten/Stunde.

Eine `m3.2xlarge`-Instance entspricht 16 normalisierten Einheiten/Stunde.

Der Rabatt wird wie folgt angewendet:

Die `m3.2xlarge` regionale Reserved Instance bietet den vollständigen Rabatt für 2 x `m3.large` Nutzung, da diese beiden Instances zusammen 8 normalisierten Einheiten/Stunde entsprechen. Damit verbleiben 8 normalisierte Einheiten/Stunde, die auf die `m3.xlarge`-Instances angewendet werden.

Mit den verbleibenden 8 normalisierten Einheiten/Stunde wendet die `m3.2xlarge` regionale Reserved Instance den vollständigen Rabatt auf 1 x `m3.xlarge` Nutzung an, da jede `m3.xlarge` Instance 8 normalisierten Einheiten/Stunde entspricht. Die verbleibende `m3.xlarge`-Nutzung wird über den On-Demand-Tarif abgerechnet.

Szenario 3: Regionale Reserved Instances in verknüpften Konten

Reserved Instances werden zuerst auf die Nutzung im erwerbenden Konto angewendet. Danach folgt die qualifizierte Nutzung in anderen Konten der Organisation. Weitere Informationen finden Sie unter Reserved Instances- und konsolidierte Fakturierung. Bei regionalen Reserved Instances, die Größenflexibilität für Instances anbieten, wird der Vorteil innerhalb der Instance-Familie von der kleinsten bis hin zur größten Instance-Größe angewendet.

Sie führen die folgenden On-Demand-Instances in Konto A (das erwerbende Konto) aus:

- 2 x `m4.xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a
- 1 x `m4.2xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1b
- 2 x `c4.xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a
- 1 x `c4.2xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1b

Ein weiterer Kunde führt die folgenden On-Demand-Instances in Konto B— (ein verknüpftes Konto) aus:

- 2 x `m4.xlarge` Linux, Standard-Tenancy-Instances in Availability Zone us-east-1a

Sie erwerben die folgenden regionalen Reserved Instances in Konto A:

- 4 x `m4.xlarge` Linux, Standard-Tenancy Reserved Instances in der Region us-east-1

- 2 x `c4.xlarge` Linux, Standard-Tenancy Reserved Instances in der Region us-east-1

Die regionalen Reserved Instance-Rabatte werden folgendermaßen angewendet:

- Der Rabatt der vier `m4.xlarge`-Reserved Instances wird von den beiden `m4.xlarge`-Instances und der einzelnen `m4.2xlarge`-Instance in Konto A (dem erwerbenden Konto) genutzt. Alle drei Instance entsprechen den Attributen (Instance-Familie, Region, Plattform, Tenancy). Der Rabatt wird zuerst auf die Instances im erwerbenden Konto (Konto A) angewendet, obwohl Konto B (verknüpftes Konto) über zwei `m4.xlarge` verfügt, dem den Reserved Instances ebenfalls entsprechen. Es wird keine Kapazitätsreservierung geboten, da es sich bei den Reserved Instances um regionale Reserved Instances handelt.
- Der Rabatt auf die zwei `c4.xlarge` Reserved Instances wird auf die zwei `c4.xlarge` Instances angewendet, da ihre Instance-Größe kleiner als die der `c4.2xlarge` Instance ist. Es wird keine Kapazitätsreservierung geboten, da es sich bei den Reserved Instances um regionale Reserved Instances handelt.

Szenario 4: Zonenbasierte Reserved Instances in einem verknüpften Konto

Reserved Instances im Besitz eines Kontos werden grundsätzlich erst auf die Nutzung in diesem Konto angewendet. Wenn es qualifizierende und nicht genutzte Reserved Instances für eine bestimmte Availability Zone (zonenbasierte Reserved Instances) in anderen Konten in der Organisation gibt, werden diese vor den regionalen Reserved Instances im Besitz des Kontos auf das Konto angewendet. Dies geschieht, um eine maximale Nutzung der Reserved Instances und somit eine geringere Rechnung zu gewährleisten. Zu Fakturierungszwecken werden alle Konten in der Organisation wie ein einziges Konto behandelt. Das folgende Beispiel veranschaulicht dies.

Sie führen die folgenden On-Demand-Instance in Konto A (das erwerbende Konto) aus:

- 1 x `m4.xlarge` Linux, Standard-Tenancy-Instance in Availability Zone us-east-1a

Ein Kunde führt die folgende On-Demand-Instance im verknüpften Konto B aus:

- 1 x `m4.xlarge` Linux, Standard-Tenancy-Instance in Availability Zone us-east-1b

Sie erwerben die folgenden regionalen Reserved Instances in Konto A:

- 1 x `m4.xlarge` Linux, Standard-Tenancy Reserved Instance in der Region us-east-1

Ein Kunde erwirbt die folgenden zonenbezogenen Reserved Instances im verknüpften Konto C:

- 1 x `m4.xlarge` Linux, Standard-Tenancy-Reserved Instances in Availability Zone us-east-1a

Die Reserved Instance-Rabatte werden folgendermaßen angewendet:

- Der Rabatt der zonenbezogenen `m4.xlarge` Reserved Instances im Besitz von Konto C wird auf die `m4.xlarge`-Nutzung in Konto A angewendet.
- Der Rabatt der regionalen `m4.xlarge` Reserved Instances im Besitz von Konto A wird auf die `m4.xlarge`-Nutzung in Konto B angewendet.
- Wenn die regionale Reserved Instance im Besitz von Konto A zuerst auf die Nutzung in Konto A angewendet wurde, bleibt die zonenbezogene Reserved Instance im Besitz von Konto C ungenutzt und die Nutzung in Konto B wird zum On-Demand-Tarif abgerechnet.

Weitere Informationen finden Sie unter der Reserved Instances im Billing and Cost Management Report.

> **Note**
>
> Zonal Reserved Instances reservieren Kapazität nur für das Besitzerkonto und können nicht für andere AWS-Konten freigegeben werden. Wenn Sie Kapazität mit anderen teilen müssen, verwenden Sie. AWS-KontenOn-Demand Capacity Reservations

Nutzen Ihres Reserved Instances

Reserved Instances werden bei übereinstimmenden Spezifikationen automatisch auf aktive On-Demand-Instances angewendet. Wenn Sie über keine On-Demand-Instances mit passenden Spezifikationen Ihrer Reserved Instance verfügen, bleibt die Reserved Instance bis zum Start einer Instance mit den erforderlichen Spezifikationen ungenutzt.

Wenn Sie eine On-Demand-Instance starten, um den Abrechnungsrabatt einer Reserved Instance zu nutzen, stellen Sie sicher, dass Sie bei der Konfiguration Ihrer On-Demand-Instance die folgenden Informationen angeben:

Plattform

Sie müssen ein Amazon Machine Image (AMI) angeben, das der Plattform (Produktbeschreibung) der Reserved Instance entspricht. Wenn Sie beispielsweise `Linux/UNIX` für Ihre Reserved Instance angegeben haben, können Sie eine Instance von einem Amazon Linux AMI oder einem Ubuntu AMI starten.

Instance-Typ

Wenn Sie eine zonengebundene Reserved Instance erworben haben, müssen Sie denselben Instance-Typ wie Ihre Reserved Instance angeben; zum Beispiel `t3.large`. Weitere Informationen finden Sie unter So werden zonengebundene Reserved Instances angewendet.

Wenn Sie eine regionale Reserved Instance erworben haben, müssen Sie einen Instance-Typ aus derselben Instance-Familie wie der Instance-Typ Ihrer Reserved Instance angeben. Wenn Sie beispielsweise `t3.xlarge` für Ihre Reserved Instance angegeben haben, müssen Sie Ihre Instance aus der T3-Familie starten, können aber eine beliebige Größe angeben, beispielsweise `t3.medium`. Weitere Informationen finden Sie unter So werden regionale Reserved Instances angewendet.

Availability Zone

Wenn Sie eine zonengebundene Reserved Instance für eine bestimmte Availability Zone erworben haben, müssen Sie die Instance in derselben Availability Zone starten.

Wenn Sie eine regionale Reserved Instance erworben haben, können Sie die Instance in jeder Availability Zone in der Region starten, die Sie für die Reserved Instance angegeben haben.

Tenancy

Die Tenancy (`dedicated` oder `shared`) der Instance muss mit der Tenancy Ihrer Reserved Instance übereinstimmen. Weitere Informationen finden Sie unter Dedicated Instances.

Beispiele zur Anwendung von Reserved Instances auf aktive On-Demand-Instances finden Sie unter So werden Reserved Instances angewendet. Weitere Informationen finden Sie unter Warum werden meine Amazon EC2 Reserved Instances nicht wie erwartet auf meine AWS Abrechnung angerechnet?

Sie können verschiedene Methoden verwenden, um die On-Demand-Instances zu starten, die Ihren Reserved-Instance-Rabatt verwenden. Weitere Informationen zu den verschiedenen Startmethoden finden Sie unter Starten Ihrer Instance. Sie können auch Amazon EC2 Auto Scaling verwenden, um

eine Instance zu starten. Weitere Informationen hierzu finden Sie unter Amazon EC2 Auto Scaling-Benutzerhandbuch.

So wird abgerechnet

Alle Reserved Instances bieten im Vergleich mit den Preisen für On-Demand-Instances einen Rabatt. Mit Reserved Instances zahlen Sie für die gesamte Laufzeit statt für die tatsächliche Nutzung. Je nach der für die Reserved Instance festgelegten Zahlungsoption bezahlen Sie die Reserved Instance im Voraus, teilweise im Voraus oder monatlich.

Wenn Reserved Instances ausläuft, zahlen Sie On-Demand-Tarife für eine Nutzung der EC2-Instance. Sie können eine Reserved Instance bis zu drei Jahre im Voraus für den Kauf in die Warteschlange einstellen. So können Sie sicherstellen, dass jederzeit die erforderlichen Kapazitäten verfügbar sind. Weitere Informationen finden Sie unter Einstellen des Kaufs in die Warteschlange.

Das AWS kostenlose Kontingent ist für neue AWS Konten verfügbar. Wenn Sie das kostenlose Kontingent für AWS zur Ausführung von Amazon-EC2-Instances nutzen und eine Reserved Instance erwerben, erfolgt die Abrechnung nach den Standard-Preisrichtlinien. Weitere Informationen finden Sie unter Kostenloses Kontingent für AWS.

Inhalt

Nutzungsabrechnung

Während der gewählten Laufzeit werden Reserved Instances jeweils zur vollen Stunde abgerechnet – unabhängig davon, ob eine Instance ausgeführt wird. Eine volle Stunde wird als vierundzwanzigster Teil des Zeitraums von Mitternacht bis Mitternacht definiert; 1:00:00 bis 1:59:59 Uhr ist beispielsweise eine volle Stunde. Weitere Informationen zum Instance-Status finden Sie unter Instance-Lebenszyklus.

Ein Reserved Instance-Abrechnungsvorteil wird auf eine laufende Instance auf Sekundenbasis angewendet. Sekundengenaue Abrechnung ist für Instances verfügbar, die eine Open-Source-Linux-Distribution verwenden, wie z. B. Amazon Linux und Ubuntu. Stundengenaue Abrechnung wird für

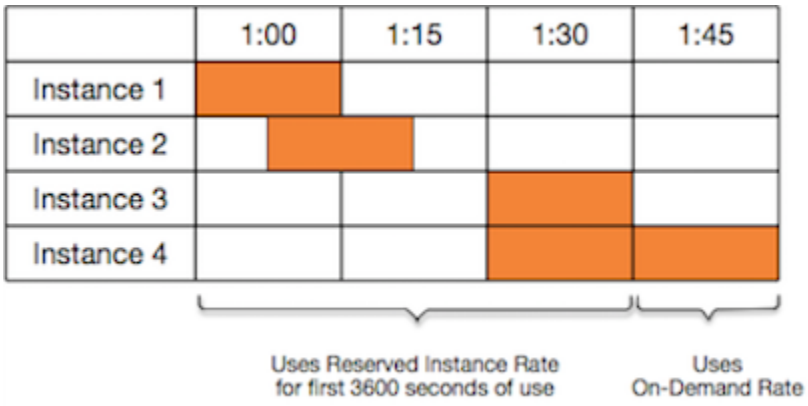
kommerzielle Linux-Distributionen, wie z. B. Red Hat Enterprise Linux und SUSE Linux Enterprise Server, verwendet.

Ein Reserved Instance-Rabatte wird nur auf eine Instance-Stunde pro voller Stunde bis zu maximal 3600 Sekunden (eine Stunde) angewendet. Sie können mehrere Instances gleichzeitig ausführen, aber Sie können nur den Vorteil des Reserved Instance-Rabatts für insgesamt 3600 Sekunden auf Stundenbasis beanspruchen. Die Instance-Nutzung, die 3600 Sekunden auf Stundenbasis überschreitet, wird nach dem Bedarfssatz berechnet.

Wenn Sie beispielsweise eine `m4.xlarge` Reserved Instance kaufen und gleichzeitig vier `m4.xlarge`-Instances gleichzeitig eine Stunde lang ausführen, wird eine Instance pro Stunde der Reserved Instance-Nutzung und die anderen drei Instances werden für drei Stunden nach bedarfsgesteuerter Nutzung berechnet.

Wenn Sie jedoch eine `m4.xlarge` Reserved Instance kaufen und vier `m4.xlarge`-Instances 15 Minuten (900 Sekunden) lang jeweils innerhalb derselben Stunde ausführen, beträgt die gesamte Laufzeit für die Instance eine Stunde, was zu einer Stunde der Reserved Instance-Nutzung und 0 Stunden der bedarfsgesteuerten Nutzung führt.

Wenn mehrere geeignete Instances gleichzeitig laufen, wird der Rechnungsrabatt für Reserved Instance auf alle Instances gleichzeitig bis zu maximal 3600 Sekunden auf einer Stundenbasis angewendet; danach gelten bedarfsorientierte Sätze.



Cost Explorer auf der Billing and Cost Management-Konsole bietet Ihnen die Möglichkeit, die Einsparungen gegen laufende On-Demand-Instances zu analysieren. Die Reserved Instances FAQ enthält ein Beispiel zu einer Listenwertberechnung.

Wenn Sie Ihr AWS Konto schließen, wird die On-Demand-Abrechnung für Ihre Ressourcen eingestellt. Wenn Sie jedoch in Ihrem Konto über Reserved Instances verfügen, erhalten Sie bis zu deren Auslaufen auch weiterhin eine Rechnung.

Anzeigen Ihrer Rechnung

Die Tarife und Gebühren für Ihr Konto können Sie über die Seite AWS Billing and Cost Management in der Konsole anzeigen.

- Das Dashboard zeigt eine Ausgabenzusammenfassung für Ihr Konto an.
- Erweitern Sie auf der Seite Bills (Rechnungen) unter Details den Abschnitt Elastic Compute Cloud und die Region, um Fakturierungsdaten zu Ihren Reserved Instances abzurufen.

Sie können die Gebühren online anzeigen oder eine CSV-Datei herunterladen.

Sie können die Auslastung Ihrer Reserved Instance auch mithilfe des AWS Kosten- und Nutzungsberichts verfolgen. Weitere Informationen finden Sie in Reserved Instances unter „Kosten- und Nutzungsbericht“ im Benutzerhandbuch für AWS Billing Billing and Cost Management.

Reserved Instances- und konsolidierte Fakturierung

Die Preisvorteile von Reserved Instances werden geteilt, wenn das kaufende Konto Teil eines Satzes von Konten ist, die unter einem einzigen, konsolidierten Zahlerkonto abgerechnet werden. Der Instance-Nutzung für alle Mitgliedskonten wird jeden Monat im Zahlerkonto zusammengefasst. Dies ist in der Regel für Unternehmen nützlich, in denen es verschiedene Funktionsteams oder -gruppen gibt. Zur Berechnung der Abrechnung wird die normale Logik für Reserved Instances angewendet. Weitere Informationen finden Sie unter Konsolidierte Fakturierung im AWS Organizations.

Wenn Sie das Konto schließen, das die Reserved Instance erworben hat, wird das Konto des Zahlers für die Reserved Instance belastet, bis die Reserved Instance abläuft. Das geschlossene Konto wird nach 90 Tagen endgültig gelöscht, und die Mitgliedskonten profitieren nicht mehr von dem Reserved-Instance-Abrechnungsrabatt.

> **Note**
>
> Zonal Reserved Instances reservieren Kapazität nur für das Besitzerkonto und können nicht für andere AWS-Konten freigegeben werden. Wenn Sie Kapazität mit anderen teilen müssen AWS-Konten, verwenden SieOn-Demand Capacity Reservations.

Reserved Instance-Rabatt-Preisstufen

Wenn Ihr Konto für eine Rabattpreisstufe qualifiziert ist, erhält es beim Kauf von Reserved Instances innerhalb der Stufe ab dem Kaufzeitpunkt die Rabatte automatisch für Vorabzahlungen und Nutzungsgebühren für die Instance. Um für einen Rabatt qualifiziert zu sein, muss der Listenwert Ihrer Reserved Instances in der Region bei mindestens 500 000 USD liegen.

Es gelten die folgenden Regeln:

- Die Preisstufen und die entsprechenden Rabatte gelten nur für Käufe von Amazon EC2 Standard Reserved Instances.
- Die Preisstufen gelten nicht für Reserved Instancess für Windows mit SQL Server Standard oder SQL Server Web und SQL Server Enterprise.
- Die Preisstufen gelten nicht für Reserved Instancess für Linux mit SQL Server Standard oder SQL Server Web und SQL Server Enterprise.
- Preisstaffelrabatte gelten nur für Käufe von AWS. Sie gelten nicht für Käufe von Reserved Instances bei Drittanbietern.
- Die Rabattpreisstufen gelten im Moment nicht für Convertible Reserved Instance-Käufe.

Themen

Berechnen der Reserved Instance-Preisrabatte

Sie können die Preisstufe für Ihr Konto berechnen, indem Sie den Listenwert Ihrer gesamten Reserved Instances in einer Region berechnen. Multiplizieren Sie den stündlichen, regelmäßigen

Preis für jede Reservierung mit den gesamten Stundenzahl für die Laufzeit verbleibenden Stunden und addieren Sie dann den Vorauszahlungspreis ohne Rabatt (der sogenannte Festpreis) zum Zeitpunkt des Kaufs. Da der Listenwert auf den Preisen ohne Rabatt (öffentlich) basiert, ändert er sich durch Ihre Qualifizierung für einen Volumenrabatt oder bei einer Preissenkung nach dem Kauf Ihrer Reserved Instances nicht.

```
List value = fixed price + (undiscounted recurring hourly price * hours in term)
```

Nehmen wir beispielsweise für eine 1-jährige Teilvorauszahlung `t2.small` Reserved Instance den Anzahlungspreis von 60,00 USD und einen Stundensatz von 0,007 USD an. Dies ergibt einen Listenwert von 121,32 $.

```
121.32 = 60.00 + (0.007 * 8760)
```

New console

So zeigen Sie die Festpreise für Reserved Instances mithilfe der Amazon EC2-Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Um die Spalte „Vorauszahlung“ anzuzeigen, wählen Sie „Einstellungen“ (⚙) in der oberen rechten Ecke aus, aktivieren Sie „Vorauszahlung“ und wählen Sie „Bestätigen“.

Old console

So zeigen Sie die Festpreise für Reserved Instances mithilfe der Amazon EC2-Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Um die Spalte „Vorauszahlung“ anzuzeigen, wählen Sie „Einstellungen“ (⚙) in der oberen rechten Ecke aus, wählen Sie „Vorauszahlung“ und dann „Schließen“.

So zeigen Sie die Festpreise für Reserved Instances mithilfe der Befehlszeile an

- describe-reserved-instances (AWS CLI)

- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)
- DescribeReservedInstanzen (Amazon EC2 EC2-API)

Kaufen mit einer Rabattstufe

Wenn Sie Reserved Instances erwerben, wendet Amazon EC2 automatisch alle Rabatte auf Ihre Käufe in einer Rabattpreisstufe an. Sie müssen nichts anders machen. Sie können die Reserved Instances ganz normal über die Amazon EC2-Tools kaufen. Weitere Informationen finden Sie unter Kaufen von Reserved Instances.

Nachdem der Listenwert Ihrer aktiven Reserved Instances in einer Region den Wert für eine Rabattpreisstufe erreicht, werden alle weiteren Käufe von Reserved Instances in dieser Region zum Rabatttarif berechnet. Wenn Sie mit einem einzelnen Kauf von Reserved Instances in einer Region den Wert für eine Rabattpreisstufe erreichen, wird der Teil des Kaufes, der über dem Grenzwert liegt, zum Rabatttarif berechnet. Weitere Informationen über die im Rahmen des Kaufprozesses erstellten temporären Reserved Instances-IDs finden Sie unter Überschreiten von Preisstufen.

Wenn Ihr Listenwert unter den Wert für die Rabattpreisstufe fällt (beispielsweise, wenn einige Ihrer Reserved Instances auslaufen), werden alle weiteren Käufe von Reserved Instances in dieser Region nicht mehr zum Rabatttarif berechnet. Sie erhalten jedoch für alle ursprünglich zur Rabattpreisstufe erworbenen Reserved Instances weiterhin den Rabatt.

Beim Kauf von Reserved Instances gilt eines von vier möglichen Szenarien:

- Kein Rabatt – Ihr Kauf innerhalb einer Region liegt weiterhin unter dem Rabattgrenzwert.
- Teilweiser Rabatt – Ihr Kauf innerhalb einer Region überschreitet den Rabattgrenzwert für die erste Rabattstufe. Auf eine oder mehrere Reservierungen wird kein Rabatt angewendet. Auf die restlichen Reservierungen wird der Rabatt angewendet.
- Voller Rabatt – Ihr kompletter Kauf innerhalb einer Region fällt in eine Rabattstufe und der entsprechende Rabatt wird angewendet.
- Zwei Rabatttarife – Ihr Kauf innerhalb einer Region überschreitet den Rabattgrenzwert für eine höhere Rabattstufe. Ihnen werden zwei verschiedene Tarife berechnet: Auf eine oder mehrere Reservierungen wird der geringere Rabatt angewendet. Auf die restlichen Reservierungen wird der Rabatt der höheren Rabattstufe angewendet.

Überschreiten von Preisstufen

Wenn Ihr Kauf eine Rabattpreisstufe überschreitet, werden mehrere Einträge für diesen Kauf angezeigt: Ein Eintrag für den Kauf zum regulären Preis und ein weiterer für den Teil des Kaufes, der mit dem entsprechenden Rabatt berechnet wird.

Der Reserved Instance-Service generiert mehrere Reserved Instance-IDs, da Ihr Kauf auch Teile mit und ohne Rabatt umfasst. Es gibt eine ID für jeden Reservierungssatz in einer Stufe. Die vom CLI-Befehl oder durch die API-Aktion zurückgegebene ID unterscheidet sich daher von der tatsächlichen ID der neuen Reserved Instances.

Konsolidierte Fakturierung für Preisstufen

Ein Konto für die konsolidierte Fakturierung fasst den Listenwert von Mitgliedskonten innerhalb einer Region zusammen. Wenn der Listenwert aller aktiven Reserved Instances für das konsolidierte Fakturierungskonto eine Rabattpreisstufe erreicht, werden ab diesem Zeitpunkt alle Reserved Instances-Käufe durch jedes Mitglied des konsolidierten Abrechnungskontos zum Rabatttarif berechnet (solange der Listenwert für das konsolidierte Konto über dem Rabattpreisstufengrenzwert bleibt). Weitere Informationen finden Sie unter Reserved Instances- und konsolidierte Fakturierung.

Kaufen von Reserved Instances

Um eine Reserved Instance zu kaufen, suchen Sie nach Reserved Instance-Angeboten von Drittanbietern AWS und passen Sie Ihre Suchparameter an, bis Sie genau das gefunden haben, wonach Sie suchen.

Wenn Sie nach Angeboten für Reserved Instances suchen, erhalten Sie eine Information zu den Kosten der gefundenen Angebote. Wenn Sie mit dem Kauf fortfahren, AWS wird automatisch ein Limitpreis auf den Kaufpreis festgelegt. Die Gesamtkosten Ihrer Reserved Instances liegen auf keinen Fall über dem angebotenen Preis.

Wenn der Preis aus irgendwelchen Gründen steigt oder sich verändert, wird der Kauf nicht abgeschlossen. Wenn Sie die Reserved Instance eines Drittanbieters auf dem EC2 Reserved Instance Marketplace kaufen und es Angebote gibt, die Ihrer Wahl ähneln, aber zu einem niedrigeren Vorabpreis angeboten werden, werden Ihnen die Angebote zum niedrigeren Vorabpreis AWS verkauft.

Bevor Sie Ihren Kauf bestätigen, sollten Sie sich die Details zu der Reserved Instance ansehen. Stellen Sie sicher, dass alle Parameter korrekt sind. Nachdem Sie eine Reserved Instance gekauft haben (entweder von einem Drittanbieter im Reserved Instance Marketplace oder von AWS), können Sie Ihren Kauf nicht mehr stornieren.

Um Reserved Instances zu erwerben und zu ändern, stellen Sie sicher, dass Ihr Benutzer über die entsprechenden Berechtigungen verfügt, z. B. die Fähigkeit, Availability Zones zu beschreiben. Informationen finden Sie unter the section called “Arbeiten mit Reserved Instances” (API) oder the section called “Arbeiten mit Reserved Instances” (Konsole).

Themen

Wählen einer Plattform

Amazon EC2 unterstützt die folgenden Plattformen für Reserved Instances:

- Linux/Unix
- Linux mit SQL Server-Standard
- Linux mit SQL Server Web
- Linux mit SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- Red Hat Enterprise Linux mit HA
- Windows
- Windows mit SQL Server-Standard
- Windows mit SQL Server Web
- Windows mit SQL Server Enterprise

Wenn Sie ein Reserved Instance kaufen, müssen Sie ein Angebot für eine Plattform wählen, die das Betriebssystem für Ihre Instance darstellt.

Linux-Instances

- Für SUSE Linux- und RHEL-Verteilungen müssen Sie Angebote für diese spezifischen Plattformen wählen, d. h. für die SUSE Linux- oder Red Hat Enterprise Linux-Plattformen.
- Bei allen anderen Linux-Distributionen (einschließlich Ubuntu) wählen Sie ein Angebot für die Linux/UNIX-Plattform.
- Wenn Sie bereits ein RHEL-Abonnement besitzen, müssen Sie ein Angebot für die Linux/UNIX-Plattform auswählen und nicht für die Red Hat Enterprise Linux-Plattform.

Windows-Instances

- Bei Windows mit SQL Standard, Windows mit SQL Server Enterprise und Windows mit SQL Server Web müssen Sie Angebote für diese speziellen Plattformen auswählen.
- Bei allen anderen Windows-Versionen wählen Sie ein Angebot für die Windows-Plattform.

> **Note**
>
> Ubuntu Pro ist nicht als Reserved Instance verfügbar. Wenn Sie im Vergleich zu den Preisen für On-Demand-Instances erhebliche Einsparungen erzielen möchten, empfiehlt es sich, Ubuntu Pro mit Savings Plans zu verwenden. Weitere Informationen finden Sie im Benutzerhandbuch zu Savings Plans.

> **Important**
>
> Wenn Sie vorhaben, eine Reserved Instance zu erwerben, um sie auf eine On-Demand-Instance anzuwenden, die von einem AWS Marketplace -AMI gestartet wurde, prüfen Sie zuerst das Feld `PlatformDetails` des AMI. Das Feld `PlatformDetails` zeigt, welches Reserved Instance zu erwerben ist. Die Plattformdetails des AMIs müssen mit der Plattform des Reserved Instance übereinstimmen, andernfalls wird das Reserved Instance nicht auf das On-Demand-Instance angewendet. Informationen darüber, wie die Plattformdetails des AMIs angezeigt werden können, finden Sie unter Verstehen von AMI-Fakturierungsdaten.

Einstellen des Kaufs in die Warteschlange

Wenn Sie eine Reserved Instance kaufen, wird der Kauf normalerweise sofort ausgeführt. Sie können einen Kauf aber auch für ein künftiges Ausführungsdatum (samt Zeit) in die Warteschlange einstellen. Sie können beispielsweise einen Kauf für den Zeitpunkt in die Warteschlange einstellen, an dem eine vorhandene Reserved Instance abläuft. So können Sie sicherstellen, dass jederzeit die erforderlichen Kapazitäten verfügbar sind.

Sie können Käufe regionaler Reserved Instances in die Warteschlange einstellen, nicht aber die Käufe für zonengebundene Reserved Instances oder Reserved Instances anderer Verkäufer. Sie können einen Kauf bis zu drei Jahre im Voraus in die Warteschlange einstellen. Zum geplanten Zeitpunkt wird der Kauf unter Verwendung der Standard-Zahlungsweise ausgeführt. Nachdem die Zahlung abgewickelt wurde, wird der Bonus zugewiesen.

Sie können in die Warteschlange eingestellte Käufe in der Amazon EC2-Konsole anzeigen. Der Status der in die Warteschlange eingestellten Käufe lautet queued (In Warteschlange). Sie können einen in die Warteschleife eingestellten Kauf jederzeit stornieren, bevor der Kaufzeitpunkt erreicht ist. Details hierzu finden Sie unter Stornieren eines in die Warteschlange eingestellten Kaufs.

Kaufen von Standard-Reserved Instances

Sie können Standard-Reserved Instances in einer bestimmten Availability Zone kaufen und so eine Kapazitätsreservierung erhalten. Alternativ können Sie auf die Kapazitätsreservierung verzichten und eine regionale Standard-Reserved Instance kaufen.

New console

So kaufen Sie Standard-Reserved Instances über die Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances (Reservierte Instances) und dann Purchase Reserved Instances (Reserved Instances kaufen) aus.
3. Wählen Sie für Offering class (Angebotsklasse) Standard aus, um Standard-Reserved Instances anzuzeigen.
4. Aktivieren Sie auf der Kaufseite in der rechten oberen Ecke Only show offerings that reserve capacity. Wenn Sie diese Einstellung aktivieren, wird das Feld Availability Zone angezeigt.

   Um ein regionales Reserved Instance zu kaufen, deaktivieren Sie diese Einstellung. Wenn Sie diese Einstellung deaktivieren, verschwindet das Feld Availability Zone .

5. Wählen Sie bei Bedarf andere Konfigurationen aus und wählen Sie dann Search aus.
6. Geben Sie für jede Reserved Instance, die Sie kaufen möchten, die gewünschte Menge ein und wählen Sie Add to Cart (In den Einkaufswagen) aus.

   Suchen Sie in der Spalte Seller nach 3rd party, um eine Standard-Reserved-Instance im Reserved Instance Marketplace zu erwerben. Die Spalte Term zeigt Nicht-Standard-Laufzeiten an. Weitere Informationen finden Sie unter Einkaufen im Reserved Instance-Marketplace.
7. Wählen Sie Reserved InstancesView Cart (Warenkorb anzeigen) aus, um eine Zusammenfassung der ausgewählten anzuzeigen.
8. Wenn für Order On (Bestellen am) der Wert Now (Jetzt) eingestellt ist, wird der Kauf sofort ausgeführt, nachdem Sie Order all (Alle bestellen) ausgewählt haben. Um einen Kauf in die Warteschlange einzustellen, wählen Sie Now (Jetzt) und dann ein Datum aus. Sie können für jedes entsprechende Angebot im Warenkorb ein anderes Datum auswählen. Der Kauf wird am ausgewählten Datum bis 00:00 Uhr UTC in die Warteschlange gestellt.
9. Wählen Sie Order all (Alle bestellen) aus, um den Kauf abzuschließen.

   Wenn es zum Zeitpunkt der Bestellung Angebote gibt, die Ihrer Wahl ähneln, aber zu einem niedrigeren Preis angeboten werden, AWS verkauft Ihnen diese Angebote zu einem niedrigeren Preis.
10. Klicken Sie auf Close.

    Der Status Ihrer Bestellung wird in der Spalte State (Status) angezeigt. Wenn Ihre Bestellung abgeschlossen ist, ändert sich der State-Wert von `Payment-pending` auf `Active`. Wenn die Reserved Instance den Status `Active` hat, kann sie verwendet werden.

> **Note**
>
> Wenn der Status auf lautet`Retired`, haben Sie Ihre Zahlung AWS möglicherweise nicht erhalten.

Old console

So kaufen Sie Standard-Reserved Instances über die Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Reserved Instances (Reservierte Instances) und dann Purchase Reserved Instances (Reserved Instances kaufen) aus.
3. Wählen Sie für Offering Class (Angebotsklasse) Standard aus, um Standard-Reserved Instances anzuzeigen.
4. Wählen Sie auf der Kaufseite in der rechten oberen Ecke Only show offerings that reserve capacity aus. Lassen Sie das Kontrollkästchen deaktiviert, um eine regionale Reserved Instance zu erwerben.
5. Wählen Sie bei Bedarf andere Konfigurationen aus und wählen Sie Search aus.

   Suchen Sie in der Spalte Seller nach 3rd Party, um eine Standard-Reserved-Instance im Reserved Instance Marketplace zu erwerben. Die Spalte Term zeigt Nicht-Standard-Laufzeiten an.
6. Geben Sie für jede Reserved Instance, die Sie kaufen möchten, die Menge ein und wählen Sie Add to Cart (In den Einkaufswagen) aus.
7. Wählen Sie Reserved InstancesView Cart (Warenkorb anzeigen) aus, um eine Zusammenfassung der ausgewählten anzuzeigen.
8. Wenn für Order On (Bestellen am) der Wert Now (Jetzt) eingestellt ist, wird der Kauf sofort ausgeführt. Um einen Kauf in die Warteschlange einzustellen, wählen Sie Now (Jetzt) und dann ein Datum aus. Sie können für jedes entsprechende Angebot im Warenkorb ein anderes Datum auswählen. Der Kauf wird am ausgewählten Datum bis 00:00 Uhr UTC in die Warteschlange gestellt.
9. Wählen Sie Order (Bestellen) aus, um den Kauf abzuschließen.

   Wenn es zum Zeitpunkt der Bestellung Angebote gibt, die Ihrer Wahl ähneln, aber zu einem niedrigeren Preis angeboten werden, AWS verkauft Ihnen diese Angebote zu einem niedrigeren Preis.
10. Klicken Sie auf Close.

    Der Status Ihrer Bestellung wird in der Spalte State (Status) angezeigt. Wenn Ihre Bestellung abgeschlossen ist, ändert sich der State-Wert von `payment-pending` auf `active`. Wenn die Reserved Instance den Status `active` hat, kann sie verwendet werden.

> **Note**
>
> Wenn der Status auf lautet`retired`, haben Sie Ihre Zahlung AWS möglicherweise nicht erhalten.

Um eine Standard Reserved Instance mit dem zu kaufen AWS CLI

1. Suchen Sie mit dem Befehl describe-reserved-instances-offerings nach verfügbaren Reserved Instances. Geben Sie für den Parameter `standard` den Wert `--offering-class` an, um nur Standard-Reserved Instances zurückzugeben. Sie können zusätzliche Parameter anwenden, um Ihre Ergebnisse einzuschränken. So suchen Sie beispielsweise eine regionale `t2.large` Reserved Instance mit einem Standard-Tenancy für `Linux/UNIX` und einer Laufzeit von nur einem Jahr:

   ```
   aws ec2 describe-reserved-instances-offerings \
       --instance-type t2.large \
       --offering-class standard \
       --product-description "Linux/UNIX" \
       --instance-tenancy default \
       --filters Name=duration,Values=31536000 Name=scope,Values=Region
   ```

   Um Reserved Instances nur im Reserved Instance Marketplace zu suchen, verwenden Sie den `marketplace`-Filter und geben in der Anforderung keine Laufzeit an (die Laufzeit kann kürzer als ein oder drei Jahre sein).

   ```
   aws ec2 describe-reserved-instances-offerings \
       --instance-type t2.large \
       --offering-class standard \
       --product-description "Linux/UNIX" \
       --instance-tenancy default \
       --filters Name=marketplace,Values=true
   ```

   Wenn Sie eine zu Ihren Anforderungen passende Reserved Instance finden, notieren Sie sich die Angebots-ID. Beispiel:

   ```
   "ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
   ```

2. Verwenden Sie den Befehl purchase-reserved-instances-offering, um die Reserved Instance zu kaufen. Sie müssen die Reserved Instance-Angebots-ID aus dem vorherigen Schritt und die Anzahl der Instances für die Reservierung angeben.

```
aws ec2 purchase-reserved-instances-offering \
    --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
    --instance-count 1
```

   Normalerweise wird der Kauf sofort ausgeführt. Sie können den Kauf aber in die Warteschlange einstellen, indem Sie dem vorherigen Aufruf den folgenden Parameter hinzufügen.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Verwenden Sie den Befehl describe-reserved-instances, um den Status Ihrer Reserved Instance abzurufen.

```
aws ec2 describe-reserved-instances
```

Verwenden Sie alternativ die folgenden AWS Tools for Windows PowerShell Befehle:

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Nach Abschluss des Kaufs wird der Bonus sofort zugewiesen, sofern Sie bereits eine Instance ausführen, die den Spezifikationen der Reserved Instance entspricht. Sie müssen Ihre Instances nicht neu starten. Wenn Sie über keine passende Instance verfügen, starten Sie eine Instance mit denselben Kriterien, die Sie für die Reserved Instance angegeben haben. Weitere Informationen finden Sie unter Nutzen Ihres Reserved Instances.

Beispiele zur Anwendung von Reserved Instances auf aktive Instances finden Sie unter So werden Reserved Instances angewendet.

Kaufen von Convertible Reserved Instances

Sie können Convertible Reserved Instances in einer bestimmten Availability Zone kaufen und so eine Kapazitätsreservierung erhalten. Alternativ können Sie auf die Kapazitätsreservierung verzichten und eine regionale Convertible Reserved Instance kaufen.

New console

So kaufen Sie Convertible Reserved Instances über die Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances und dann Purchase Reserved Instances (Reserved Instances kaufen) aus.
3. Wählen Sie für Offering class (Angebotsklasse) Convertible aus, um Convertible Reserved Instances anzuzeigen.
4. Aktivieren Sie auf der Kaufseite in der rechten oberen Ecke Only show offerings that reserve capacity. Wenn Sie diese Einstellung aktivieren, wird das Feld Availability Zone angezeigt.

   Um ein regionales Reserved Instance zu kaufen, deaktivieren Sie diese Einstellung. Wenn Sie diese Einstellung deaktivieren, verschwindet das Feld Availability Zone .
5. Wählen Sie bei Bedarf andere Konfigurationen aus und wählen Sie Search aus.
6. Geben Sie für jede Convertible Reserved Instance, die Sie kaufen möchten, die Menge ein und wählen Sie Add to cart (In den Einkaufswagen) aus.
7. Wählen Sie View Cart (Warenkorb anzeigen) aus, um eine Zusammenfassung der Auswahl anzuzeigen.
8. Wenn für Order On (Bestellen am) der Wert Now (Jetzt) eingestellt ist, wird der Kauf sofort ausgeführt, nachdem Sie Order all (Alle bestellen) ausgewählt haben. Um einen Kauf in die Warteschlange einzustellen, wählen Sie Now (Jetzt) und dann ein Datum aus. Sie können für jedes entsprechende Angebot im Warenkorb ein anderes Datum auswählen. Der Kauf wird am ausgewählten Datum bis 00:00 Uhr UTC in die Warteschlange gestellt.
9. Wählen Sie Order all (Alle bestellen) aus, um den Kauf abzuschließen.

   Wenn es zum Zeitpunkt der Bestellung Angebote gibt, die Ihrer Auswahl ähneln, aber zu einem niedrigeren Preis angeboten werden, AWS verkauft Ihnen diese Angebote zu einem niedrigeren Preis.
10. Klicken Sie auf Close.

    Der Status Ihrer Bestellung wird in der Spalte State (Status) angezeigt. Wenn Ihre Bestellung abgeschlossen ist, ändert sich der State-Wert von `Payment-pending` auf `Active`. Wenn die Reserved Instance den Status `Active` hat, kann sie verwendet werden.

> **Note**
>
> Wenn der Status auf lautet`Retired`, haben Sie Ihre Zahlung AWS möglicherweise nicht erhalten.

Old console

So kaufen Sie Convertible Reserved Instances über die Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances und dann Purchase Reserved Instances (Reserved Instances kaufen) aus.
3. Wählen Sie für Offering Class (Angebotsklasse) Convertible aus, um Convertible Reserved Instances anzuzeigen.
4. Wählen Sie auf der Kaufseite in der rechten oberen Ecke Only show offerings that reserve capacity aus. Lassen Sie das Kontrollkästchen deaktiviert, um eine regionale Reserved Instance zu erwerben.
5. Wählen Sie bei Bedarf andere Konfigurationen aus und wählen Sie Search aus.
6. Geben Sie für jede Convertible Reserved Instance, die Sie kaufen möchten, die Menge ein und wählen Sie Add to Cart (In den Einkaufswagen) aus.
7. Wählen Sie View Cart (Warenkorb anzeigen) aus, um eine Zusammenfassung der Auswahl anzuzeigen.
8. Wenn für Order On (Bestellen am) der Wert Now (Jetzt) eingestellt ist, wird der Kauf sofort ausgeführt. Um einen Kauf in die Warteschlange einzustellen, wählen Sie Now (Jetzt) und dann ein Datum aus. Sie können für jedes entsprechende Angebot im Warenkorb ein anderes Datum auswählen. Der Kauf wird am ausgewählten Datum bis 00:00 Uhr UTC in die Warteschlange gestellt.
9. Wählen Sie Order (Bestellen) aus, um den Kauf abzuschließen.

   Wenn es zum Zeitpunkt der Bestellung Angebote gibt, die Ihrer Wahl ähneln, aber zu einem niedrigeren Preis angeboten werden, AWS verkauft Ihnen diese Angebote zu einem niedrigeren Preis.
10. Klicken Sie auf Close.

Der Status Ihrer Bestellung wird in der Spalte State (Status) angezeigt. Wenn Ihre Bestellung abgeschlossen ist, ändert sich der State-Wert von `payment-pending` auf `active`. Wenn die Reserved Instance den Status `active` hat, kann sie verwendet werden.

> **Note**
>
> Wenn der Status auf lautet`retired`, haben Sie Ihre Zahlung AWS möglicherweise nicht erhalten.

Um eine Convertible Reserved Instance mit dem zu kaufen AWS CLI

1. Suchen Sie mit dem Befehl describe-reserved-instances-offerings nach verfügbaren Reserved Instances. Geben Sie für den Parameter `convertible` den Wert `--offering-class` an, um nur Convertible Reserved Instances zurückzugeben. Sie können weitere Parameter nutzen, um die Ergebnisse einzugrenzen. So suchen Sie beispielsweise eine regionale `t2.large` Reserved Instance mit einem Standard-Tenancy für `Linux/UNIX`:

   ```
   aws ec2 describe-reserved-instances-offerings \
       --instance-type t2.large \
       --offering-class convertible \
       --product-description "Linux/UNIX" \
       --instance-tenancy default \
       --filters Name=scope,Values=Region
   ```

   Wenn Sie eine zu Ihren Anforderungen passende Reserved Instance finden, notieren Sie sich die Angebots-ID. Beispiel:

   ```
   "ReservedInstancesOfferingId": "bec624df-a8cc-4aad-a72f-4f8abc34caf2"
   ```

2. Verwenden Sie den Befehl purchase-reserved-instances-offering, um die Reserved Instance zu kaufen. Sie müssen die Reserved Instance-Angebots-ID aus dem vorherigen Schritt und die Anzahl der Instances für die Reservierung angeben.

   ```
   aws ec2 purchase-reserved-instances-offering \
       --reserved-instances-offering-id bec624df-a8cc-4aad-a72f-4f8abc34caf2 \
       --instance-count 1
   ```

Normalerweise wird der Kauf sofort ausgeführt. Sie können den Kauf aber in die Warteschlange einstellen, indem Sie dem vorherigen Aufruf den folgenden Parameter hinzufügen.

```
--purchase-time "2020-12-01T00:00:00Z"
```

3. Verwenden Sie den Befehl describe-reserved-instances, um den Status Ihrer Reserved Instance abzurufen.

```
aws ec2 describe-reserved-instances
```

Verwenden Sie alternativ die folgenden AWS Tools for Windows PowerShell Befehle:

- Get-EC2ReservedInstancesOffering
- New-EC2ReservedInstance
- Get-EC2ReservedInstance

Wenn Sie bereits über eine aktive Instance verfügen, die mit den Spezifikationen der Reserved Instance übereinstimmt, wird der Rabatt sofort angewendet. Sie müssen Ihre Instances nicht neu starten. Wenn Sie über keine passende Instance verfügen, starten Sie eine Instance mit denselben Kriterien, die Sie für die Reserved Instance angegeben haben. Weitere Informationen finden Sie unter Nutzen Ihres Reserved Instances.

Beispiele zur Anwendung von Reserved Instances auf aktive Instances finden Sie unter So werden Reserved Instances angewendet.

Einkaufen im Reserved Instance-Marketplace

Sie können Reserved Instances von Drittanbietern kaufen, die über Reserved Instances vom Reserved Instance Marketplace verfügen, die sie nicht mehr brauchen. Sie können mithilfe der Amazon EC2-Konsole oder einem Befehlszeilen-Tool kaufen. Der Vorgang ähnelt dem Kauf von Reserved Instances bei AWS. Weitere Informationen finden Sie unter Kaufen von Standard-Reserved Instances.

Es gibt einige Unterschiede zwischen Reserved Instances, die im Reserved Instance Marketplace gekauft wurden, und Reserved Instances, die direkt gekauft wurden bei AWS:

- Laufzeit: Von Drittanbietern erworbene Reserved Instances bieten nicht mehr die volle Standardlaufzeit. Die vollständigen Standardbedingungen haben eine AWS Laufzeit von einem oder drei Jahren.
- Vorauszahlungspreis: Reserved Instances von Drittanbietern können zu abweichenden Vorauszahlungspreisen verkauft werden. Die Nutzungs- oder wiederkehrenden Gebühren bleiben dieselben wie die Gebühren, die beim ursprünglichen Kauf der Reserved Instances festgelegt wurden AWS.
- Typen von Reserved Instances: Nur Amazon EC2 Standard-Reserved-Instances können über den Reserved Instance Marketplace erworben werden. Convertible Reserved Instances, Amazon RDS und Amazon ElastiCache Reserved Instances können nicht auf dem Reserved Instance Marketplace erworben werden.

Dem Verkäufer werden grundlegende Informationen zu Ihnen mitgeteilt (z. B. die Postleitzahl und das Land).

Mit diesen Informationen kann der Verkäufer möglicherweise anfallenden Transaktionssteuern (z. B. Mehrwertsteuer) bestimmen. Sie werden als Auszahlungsbericht bereitgestellt. In seltenen Fällen müssen Sie dem Verkäufer AWS möglicherweise Ihre E-Mail-Adresse mitteilen, damit er Sie bei Fragen im Zusammenhang mit dem Verkauf (z. B. Steuerfragen) kontaktieren kann.

Teilt aus ähnlichen Gründen AWS den Namen der juristischen Person des Verkäufers auf der Kaufrechnung des Käufers mit. Wenn Sie aus steuerlichen oder anderen Gründen weitere Informationen zum Verkäufer benötigen, kontaktieren Sie bitte den AWS Support.

Anzeigen Ihrer Reserved Instances

Sie können erworbenen Reserved Instances über die Amazon EC2-Konsole oder ein Befehlszeilen-Tool anzeigen.

So zeigen Sie Ihre Reserved Instances in der Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Ihre in die Warteschlange eingestellten, aktiven und abgelaufenen Reserved Instances werden angezeigt. Die Spalte Status zeigt den Status an.
4. Wenn Sie ein Verkäufer im Reserved Instance Marketplace sind, zeigt die Registerkarte My Listings den Status einer Reservierung im Reserved Instance Marketplace an. Weitere Informationen finden Sie unter Reserved Instance-Angebotsstatus.

So zeigen Sie Ihre Reserved Instances mit dem Befehlszeilenclient an

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance(Tools für Windows PowerShell)

Stornieren eines in die Warteschlange eingestellten Kaufs

Sie können einen Kauf bis zu drei Jahre im Voraus in die Warteschlange einstellen. Sie können einen in die Warteschleife eingestellten Kauf jederzeit stornieren, bevor der Kaufzeitpunkt erreicht ist.

New console

So stornieren Sie einen in die Warteschlange eingestellten Kauf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie mindestens eine Reserved Instances aus.
4. Wählen Sie Actions (Aktionen), Delete Queued Reserved Instances (In die Warteschlange eingestellte reservierte Instances löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen) und dann Close (Schließen) aus.

Old console

So stornieren Sie einen in die Warteschlange eingestellten Kauf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie mindestens eine Reserved Instances aus.
4. Wählen Sie Actions (Aktionen), Delete Queued Reserved Instances (In die Warteschlange eingestellte reservierte Instances löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Yes, Delete.

So stornieren Sie einen Einkauf in der Warteschlange über die Befehlszeile:

- delete-queued-reserved-instances (AWS CLI)

- Remove-EC2QueuedReservedInstance(Tools für Windows PowerShell)

Erneuern eines Reserved Instance

Sie können einen Reserved Instance verlängern, bevor er abläuft. Beim Erneuern einesReserved Instance wird der Kauf eines Reserved Instance mit der gleichen Konfiguration in die Warteschlange gesetzt, bis der aktuelle Reserved Instance abläuft.

New console

So verlängern Sie einen Reserved Instance mit einem in die Warteschlange gesetzten Einkauf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie die zu erneuernde Reserved Instance aus.
4. Wählen Sie Actions (Aktionen), Renew Reserved Instances (Reserved Instances erneuern).
5. Um die Bestellung abzuschließen, wählen Sie Order all (Alle bestellen) und dann Close (Schließen) aus.

Old console

So verlängern Sie einen Reserved Instance mit einem in die Warteschlange gesetzten Einkauf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie die zu erneuernde Reserved Instance aus.
4. Wählen Sie Actions (Aktionen), Renew Reserved Instances (Reserved Instances erneuern).
5. Wählen Sie Order (Bestellen) aus, um den Kauf abzuschließen.

Verkaufen im Reserved Instance Marketplace

Der Reserved Instance Marketplace ist eine Plattform, die den Verkauf von ungenutzten Standard Reserved Instances von Drittanbietern und AWS Kunden unterstützt, die sich in Laufzeiten und Preisoptionen unterscheiden. Möglicherweise möchten Sie Reserved Instances verkaufen, nachdem Sie Instances in eine neue AWS Region verschoben, zu einem neuen Instance-Typ gewechselt

haben, Projekte vor Ablauf der Laufzeit beendet haben, wenn sich Ihre Geschäftsanforderungen ändern oder wenn Sie nicht benötigte Kapazität haben.

Sobald Sie Ihre Reserved Instances im Reserved Instances Marketplace anbieten, sind diese für mögliche Kunden sichtbar. Alle Reserved Instances werden nach deren verbleibender Laufzeit und dem Stundenpreis gruppiert.

Um der Anfrage eines Käufers nachzukommen, die Reserved Instance eines Drittanbieters über den EC2 Reserved Instance Marketplace zu erwerben, wird AWS zunächst die Reserved Instance mit dem niedrigsten Vorabpreis in der angegebenen Gruppierung verkauft. AWS Verkauft dann die Reserved Instance mit dem nächstniedrigsten Preis, bis die gesamte Bestellung des Käufers erfüllt ist. AWS verarbeitet dann die Transaktionen und überträgt das Eigentum an den Reserved Instances auf den Käufer.

Die Reserved Instance bleibt bis zum Verkauf in Ihrem Besitz. Nach dem Verkauf geben Sie die Kapazitätsreservierungen und die regelmäßigen Rabatte ab. Wenn Sie Ihre Instance weiterhin nutzen, AWS berechnet Ihnen der On-Demand-Preis ab dem Zeitpunkt, an dem Ihre Reserved Instance verkauft wurde.

Wenn Sie nicht genutzte Reserved Instances im Reserved Instance Marketplace verkaufen möchten, müssen Sie bestimmte Kriterien erfüllen.

Weitere Informationen zum Kauf von Reserved Instances im Reserved Instance Marketplace finden Sie im Einkaufen im Reserved Instance-Marketplace.

Inhalt

Beschränkungen und Einschränkungen

Bevor Sie Ihre nicht genutzten Reservierungen verkaufen können, müssen sich als Verkäufer im Reserved Instance Marketplace registrieren. Weitere Informationen finden Sie unter Registrieren als Verkäufer.

Beim Verkauf von Reserved Instances gelten die folgenden Begrenzungen und Einschränkungen:

- Es können nur regionale und zonale Amazon EC2 Standard Reserved Instances über den Reserved-Instance-Marketplace verkauft werden.
- Amazon EC2 Convertible Reserved Instances können nicht über den Reserved-Instance-Marketplace verkauft werden.
- Reserved Instances für andere AWS Dienste wie Amazon RDS und Amazon ElastiCache können nicht im Reserved Instance Marketplace verkauft werden.
- Die verbleibende Laufzeit der Standard-Reserved Instance muss mindestens einen Monat betragen.
- Sie können keine Standard-Reserved Instance in einer Region verkaufen, die standardmäßig deaktiviert ist.
- Der Mindestpreis im Reserved Instance Marketplace beträgt 0,00 USD.
- Sie können Reserved Instances vom Typ „No Upfront“ (Keine Vorauszahlung), „Partial Upfront“ (Teilweise Vorauszahlung) oder „All Upfront“ (Komplette Vorauszahlung) im Reserved Instance Marketplace verkaufen, sofern sie seit mindestens 30 Tagen in Ihrem Konto aktiv sind. Wenn es eine Vorauszahlung für eine Reserved Instance gibt, kann diese erst dann verkauft werden, wenn AWS die Vorauszahlung erhalten hat.
- Sie können Ihr Angebot im Reserved Instance Marketplace nicht direkt bearbeiten. Sie können jedoch das Angebot stornieren und dann ein neues Angebot mit neuen Parametern erstellen. Weitere Informationen finden Sie unter Preis festsetzen von Reserved Instances. Sie können Ihre Reserved Instances außerdem vor dem Verkaufsangebot ändern. Weitere Informationen finden Sie unter Ändern von Reserved Instances.
- AWS erhebt eine Servicegebühr in Höhe von 12 Prozent des gesamten Vorauspreises für jede Standard Reserved Instance, die Sie auf dem Reserved Instance Marketplace verkaufen. Der Vorauszahlungspreis ist der Preis, der dem Verkäufer für die Standard-Reserved Instance berechnet wird.
- Wenn Sie sich als Verkäufer registrieren, muss die von Ihnen angegebene Bank eine US-Adresse aufweisen. Weitere Informationen finden Sie unter Zusätzliche Anforderungen für Verkäufer für kostenpflichtige Produkte im AWS Marketplace -Verkäuferhandbuch.

- Kunden von Amazon Web Services India Private Limited (AWS Indien) können Reserved Instances nicht im Reserved Instance Marketplace verkaufen, selbst wenn sie über ein US-Bankkonto verfügen. Weitere Informationen finden Sie unter Was sind die Unterschiede zwischen Konten AWS-Konten und Konten AWS in Indien?

Registrieren als Verkäufer

> **Note**
>
> Nur Root-Benutzer des AWS-Kontos sie können ein Konto als Verkäufer registrieren.

Für den Verkauf auf dem Reserved Instance Marketplace müssen Sie sich zuerst als Verkäufer registrieren. Während der Registrierung müssen Sie folgende Informationen angeben:

- Bankinformationen — Sie AWS benötigen Ihre Bankdaten, um Gelder auszahlen zu können, die beim Verkauf Ihrer Reservierungen eingezogen wurden. Die angegebene Bank muss über eine US-Anschrift verfügen. Weitere Informationen finden Sie unter Bankkonto für Auszahlung.
- Tax information (Steuerinformationen) — Alle Verkäufer sind verpflichtet, ein Interview zu den Steuerinformationen durchzuführen, um die erforderlichen steuerlichen Meldepflichten zu ermitteln. Weitere Informationen finden Sie unter Steuerinformationen.

Nachdem Sie AWS Ihre vollständige Verkäuferregistrierung erhalten haben, erhalten Sie eine E-Mail, die Ihre Registrierung bestätigt und Sie darüber informiert, dass Sie mit dem Verkauf auf dem Reserved Instance Marketplace beginnen können.

Bankkonto für Auszahlung

AWS Sie benötigen Ihre Bankdaten, um die beim Verkauf Ihrer Reserved Instance gesammelten Gelder auszahlen zu können. Die angegebene Bank muss über eine US-Anschrift verfügen. Weitere Informationen finden Sie unter Zusätzliche Anforderungen für Verkäufer für kostenpflichtige Produkte im AWS Marketplace -Verkäuferhandbuch.

So registrieren Sie ein Standardbankkonto für Auszahlungen

1. Öffnen Sie die Seite Reserved Instance Marketplace Seller Registration und melden Sie sich mit Ihren AWS -Anmeldeinformationen an.
2. Geben Sie auf der Seite Manage Bank Account die folgenden Informationen zur Bank an:

- Name des Bankkontoinhabers
- Bankleitzahl
- Kontonummer
- Kontotyp

> **Note**
>
> Wenn Sie ein Unternehmenskonto verwenden, müssen Sie die Informationen zum Bankkonto per Fax senden(+1 206-765-3424).

Nach der Registrierung wird das angegebene Bankkonto als Standardkonto mit ausstehender Verifizierung durch die Bank eingerichtet. Die Verifizierung eines neuen Bankkontos kann bis zu zwei Wochen dauern. Während dieser Zeit können Sie keine Auszahlungen erhalten. Bei einem bereits etablierten Konto dauert es normalerweise ca. zwei Tage, bis die Auszahlung abgeschlossen ist.

So ändern Sie das Standardbankkonto für Auszahlungen

1. Öffnen Sie die Seite Reserved Instance Marketplace Seller Registration und melden Sie sich mit dem Konto an, das Sie bei der Registrierung verwendet haben.
2. Fügen Sie auf der Seite Manage Bank Account ein neues Bankkonto hinzu oder bearbeiten Sie das Standardbankkonto.

Steuerinformationen

Ihr Verkauf von Reserved Instances kann transaktionsbasierten Steuern unterliegen (z. B. Mehrwertsteuer). Sie sollten gemeinsam mit der Steuer-, Rechts-, Buchhaltungs- oder Finanzabteilung Ihres Unternehmens prüfen, ob Transaktionssteuern anfallen. Sie sind für die Erfassung und die Zahlung von entsprechenden Steuern an die jeweilige Behörde verantwortlich.

Im Rahmen des Registrierungsprozesses für Verkäufer müssen Sie im Seller Registration Portal ein Steuer-Interview durchführen. In dem Interview werden Ihre Steuerinformationen erfasst und ein IRS-Formular W-9, W-8BEN oder W-8BEN-E ausgefüllt, das verwendet wird, um alle erforderlichen steuerlichen Meldepflichten zu ermitteln.

Die im Rahmen des Steuer-Interviews anzugebenden Steuerinformationen hängen ggf. davon ab, ob Sie als Privatperson oder als Unternehmen tätig sind und ob Sie oder Ihr Unternehmen eine US-amerikanische oder nicht-amerikanische natürliche oder juristische Person sind. Berücksichtigen Sie beim Ausfüllen des Steuer-Interviews Folgendes:

- Die von bereitgestellten Informationen AWS, einschließlich der Informationen in diesem Thema, stellen keine Steuer-, Rechts- oder sonstige professionelle Beratung dar. Um die möglicherweise für Ihr Unternehmen geltenden Anforderungen für das IRS-Reporting zu ermitteln und bei weiteren Fragen, sprechen Sie bitte Ihren Steuerberater, Rechtsberater oder Unternehmensberater an.
- Beantworten Sie alle Fragen und geben Sie alle angeforderten Informationen ein, um die IRS-Reporting-Anforderungen möglichst vollständig zu erfüllen.
- Überprüfen Sie Ihre Antworten. Vermeiden Sie Tippfehler oder fehlerhafte Steueridentifikationsnummern. Diese können dazu führen, dass das Steuerformular ungültig ist.

Basierend auf Ihren Antworten auf Steuerbenachrichtigungen und IRS-Meldeschwellen reicht Amazon ggf. das Formular 1099-K ein. Amazon sendet eine Kopie Ihres 1099-K-Formulars am oder vor dem 31. Januar des Jahres, das auf das Jahr folgt, in dem Ihr Steuerkonto die Schwellenwerte erreicht. Wenn Ihr Konto den Grenzwert im Jahr 2018 erreicht, wird Ihr Formular 1099-K beispielsweise am oder vor dem 31. Januar 2019 verschickt.

Weitere Informationen zu den IRS-Anforderungen und dem Formular 1099-K finden Sie auf der IRS-Website.

Preis festsetzen von Reserved Instances

Wenn Sie die Gebühr für Ihre Reserved Instances festlegen, beachten Sie Folgendes:

- Vorabgebühr – Die Vorabgebühr ist die einzige Gebühr, die Sie für von Ihnen verkaufte Reserved Instances festlegen können. Die Vorabgebühr ist die einmalige Gebühr, die der Käufer beim Kauf einer Reserved Instance bezahlt.

  Da der Wert von Reserved Instances im Laufe der Zeit abnimmt, AWS kann standardmäßig festgelegt werden, dass die Preise von Monat zu Monat in gleichen Schritten sinken. Sie können jedoch entsprechend dem Verkaufszeitpunkt Ihrer Reservierung abweichende Preise im Voraus festlegen. Wenn Ihre Reserved Instance beispielsweise noch über eine verbleibende Laufzeit von neun Monaten verfügt, können Sie den akzeptablen Betrag für einen Kauf dieser Reserved Instance innerhalb der verbleibenden neun Monate festlegen. Sie können einen anderen Preis für fünf verbleibende Monate und einen weiteren Preis für einen verbleibenden Monat festlegen.

Der Mindestpreis im Reserved Instance Marketplace beträgt 0,00 USD.

- Limits – Die folgenden Limits für den Verkauf von Reserved Instances gelten für die Lebensdauer Ihres AWS-Konto. Sie sind keine jährlichen Limits.
  - Sie können bis zu 50 000 USD in Reserved Instances verkaufen.
  - Sie können bis zu 5 000 Reserved Instances verkaufen.

  Diese Grenzwerte können in der Regel nicht erhöht werden, werden aber auf Anfrage case-by-case individuell bewertet. Um eine Limit-Erhöhung zu beantragen, füllen Sie das Formular Service-Limit-Erhöhung aus. Wählen Sie für Limit-Typ die Option EC2-Reserved-Instances aus.
- Kann nicht bearbeitet werden – Sie können Ihr Angebot nicht direkt bearbeiten. Sie können jedoch das Angebot stornieren und dann ein neues Angebot mit neuen Parametern erstellen.
- Kann storniert werden – Sie können ein Angebot jederzeit stornieren (solange es den Status `active` aufweist). Sie können das Angebot nicht stornieren, wenn es bereits einem Verkauf zugeordnet oder für diesen verarbeitet wird. Wenn einige Instances aus Ihrem Angebot zugeordnet sind, und Sie das Angebot stornieren, werden nur die noch nicht zugeordneten Instances aus dem Angebot entfernt.

Auflisten Ihrer Reserved Instances

Als registrierter Verkäufer können Sie eine oder mehrere Reserved Instances. Sie können entweder alle über ein Angebot verkaufen oder diese in Teilen verkaufen. Des Weiteren können Sie Reserved Instances in jeder Konfiguration aus Instance-Typ, Plattform und Umfang anbieten.

Die Konsole ermittelt einen vorgeschlagenen Preis. Sie überprüft, ob Angebote entsprechend Ihrer Reserved Instance vorliegen, und gibt das Angebot mit dem niedrigsten Preis zurück. Andernfalls berechnet sie einen vorgeschlagenen Preis anhand der Kosten der Reserved Instance für die verbleibende Zeit. Wenn der berechnete Preis unter 1,01 USD liegt, beträgt der vorgeschlagene Preis 1,01 USD.

Sie können Ihr Angebot stornieren. Wurde ein Angebot bereits verkauft, so gilt die Stornierung nicht für den bereits verkauften Teil. Nur noch nicht verkaufte Teile des Angebotes werden aus dem Reserved Instance Marketplace entfernt.

Um eine Reserved Instance im Reserved Instance Marketplace aufzulisten, verwenden Sie den AWS Management Console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie das aufzulistende Reserved Instances aus, und wählen Sie Actions (Aktionen), Sell Reserved Instances (Verkaufen).
4. Wählen Sie auf der Seite Configure Your Reserved Instances Listing in den entsprechenden Spalten die Anzahl der zu verkaufenden Instances sowie den Vorauszahlungspreis für die verbleibende Laufzeit aus. Sehen Sie sich über den Pfeil neben der Spalte Months Remaining die Wertveränderung Ihrer Reservierung an.
5. Wenn Sie ein fortgeschrittener Benutzer sind und die Preisgestaltung anpassen möchten, können Sie unterschiedliche Werte für die nachfolgenden Monate eingeben. Wählen Sie Reset aus, um die standardmäßige, lineare Preisreduzierung wiederherzustellen.
6. Wählen Sie Continue aus, sobald Sie mit der Konfiguration fertig sind.
7. Bestätigen Sie die Details Ihres Angebotes auf der Seite Confirm Your Reserved Instances Listing. Wählen Sie List Reserved Instance aus, sobald alles korrekt ist.

So zeigen Sie Ihre Angebote in der Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie das Reserved Instance aus, das Sie aufgelistet haben, und wählen Sie die Registerkarte My Listings (Meine Auflistungen) am unteren Rand der Seite.

Um Reserved Instances auf dem Reserved Instance Marketplace zu verwalten, verwenden Sie AWS CLI

1. Rufen Sie über den Befehl Reserved Instancesdescribe-reserved-instances eine Liste Ihrer ab.
2. Notieren Sie sich die ID der Reserved Instance für das Angebot und rufen Sie Sell Reserved Instances auf. Sie müssen die ID der Reserved Instance, die Anzahl der Instances und den Preisplan angeben.
3. Verwenden Sie den Befehl describe-reserved-instances-listings, um Ihr Angebot anzuzeigen.
4. Verwenden Sie den Befehl cancel-reserved-instances-listings, um Ihr Angebot zu stornieren.

Reserved Instance-Angebotsstatus

Listing State (Angebotsstatus) auf der Registerkarte My Listings (Meine Angebote) der Reserved Instances-Seite zeigt den Status Ihrer aktuellen Angebote an:

Die in Listing State angezeigten Informationen stellen den Status Ihres Angebots im Reserved Instance Marketplace dar. Er unterscheidet sich im Status in der Spalte State auf der Seite Reserved Instances. Diese State-Information bezieht sich auf Ihre Reservierung.

- Active — Das Angebot steht zum Kauf zur Verfügung.
- Cancelled: Das Angebot wurde storniert und steht nicht im Reserved Instance Marketplace zum Kauf zur Verfügung.
- Closed — Die Reserved Instance wird nicht angeboten. Eine Reserved Instance kann `closed` sein, da der Verkauf des Angebots abgeschlossen ist.

Lebenszyklus eines Angebots

Wenn alle Instances in Ihrem Angebot zugeordnet und verkauft sind, zeigt die Registerkarte My Listings in Total instance count die gleiche Anzahl wie in Sold an. Es sind keine Instances mit dem Status Available mehr für Ihr Angebot vorhanden. Sein Status lautet `closed`.

Wenn nur ein Teil Ihres Angebots verkauft ist, werden die Reserved Instances in der Liste AWS ausgemustert und die Anzahl der Reserved Instances wird entsprechend den verbleibenden Reserved Instances berechnet. Die Angebots-ID und das entsprechende Angebot bleiben mit weniger zu verkaufenden Reservierungen weiterhin aktiv.

Alle weiteren Verkäufe von Reserved Instances in diesem Angebot werden genauso verarbeitet. Wenn alle Reserved Instances im Angebot verkauft sind, AWS markiert das Angebot als`closed`.

Sie erstellen beispielsweise ein Angebot wie Reserved Instances listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample mit einer Angebotsmenge von 5.

Die Registerkarte My Listings auf der Konsolenseite Reserved Instance zeigt das Angebot folgendermaßen an:

Reserved Instance listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 0
- Available = 5
- Status = active

Ein Käufer kauft zwei der Reservierungen. Es verbleiben also drei zu verkaufende Reservierungen. Da es sich um einen teilweisen Verkauf handelt, erstellt AWS eine neue Reservierung mit der Anzahl drei für die verbleibenden Reservierungen.

So sieht Ihr Angebot auf der Registerkarte My Listings aus:

Reserved Instance listing ID 5ec28771-05ff-4b9b-aa31-9e57dexample

- Total reservation count = 5
- Sold = 2
- Available = 3
- Status = active

Sie können Ihr Angebot stornieren. Wurde ein Angebot bereits verkauft, so gilt die Stornierung nicht für den bereits verkauften Teil. Nur noch nicht verkaufte Teile des Angebotes werden aus dem Reserved Instance Marketplace entfernt.

Nach dem Verkauf Ihrer Reserved Instance

Wenn Ihre Reserved Instance verkauft ist AWS , erhalten Sie eine E-Mail-Benachrichtigung. Sie erhalten für jeden Tag mit einer beliebigen Aktivität eine E-Mail-Benachrichtigung zu allen Aktivitäten des Tages. Zu den Aktivitäten kann gehören, wenn Sie ein Angebot erstellen oder verkaufen oder wann Geld AWS auf Ihr Konto überwiesen wird.

So verfolgen Sie den Status einer Reserved Instance-Auflistung in der Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsseite Reserved Instances aus.
3. Wählen Sie die Registerkarte My Listings (Meine Auflistungen).

   Die Registerkarte My Listings enthält den Listing State-Wert. Sie enthält außerdem Informationen zur Laufzeit, zum Angebotspreis und eine Zusammenfassung zur Menge der im Angebot verfügbaren, ausstehenden, verkauften und stornierten Instances.

Sie können außerdem den Befehle describe-reserved-instances-listings mit dem passenden Filter nutzen, um Informationen zu Ihren Angeboten abzurufen.

Auszahlung

Sobald Geld vom Käufer AWS eingegangen ist, wird eine Nachricht an die E-Mail-Adresse des registrierten Eigentümerkontos für die verkaufte Reserved Instance gesendet.

AWS sendet eine ACH-Überweisung (Automated Clearing House) auf das von Ihnen angegebene Bankkonto. Dieser Transfer findet normalerweise zwischen einem und drei Tagen nach dem Verkauf Ihrer Reserved Instance statt. Die Auszahlung findet einmal pro Tag statt. Sie erhalten eine E-Mail mit einem Auszahlungsbericht, nachdem die Mittel freigegeben wurden. Berücksichtigen Sie, dass Sie erst dann eine Auszahlung erhalten können, wenn AWS eine Verifizierung von Ihrer Bank erhalten hat. Dieser Vorgang kann bis zu zwei Wochen dauern.

Die verkaufte Reserved Instance wird auch weiterhin in der Beschreibung Ihrer Reserved Instances angezeigt.

Sie erhalten eine Barauszahlung für Ihre Reserved Instances per Banküberweisung direkt auf Ihr Bankkonto. AWS erhebt eine Servicegebühr in Höhe von 12 Prozent des gesamten Vorauspreises für jede Reserved Instance, die Sie im Reserved Instance Marketplace verkaufen.

Weitergabe von Informationen an den Käufer

Wenn Sie auf dem Reserved Instance Marketplace verkaufen, AWS teilt gemäß den US-Vorschriften den offiziellen Namen Ihres Unternehmens auf dem Kontoauszug des Käufers mit. Wenn der Käufer anruft, AWS Support weil er Sie wegen einer Rechnung oder aus einem anderen steuerlichen Grund kontaktieren muss, müssen Sie dem Käufer AWS möglicherweise Ihre E-Mail-Adresse mitteilen, damit der Käufer Sie direkt kontaktieren kann.

Aus denselben Gründen erhalten die Verkäufer über den Auszahlungsbericht die Postleitzahl und das Land des Käufers. Als Verkäufer benötigen Sie diese Informationen möglicherweise für die anfallenden Transaktionssteuern (z. B. Mehrwertsteuer).

AWS kann keine Steuerberatung anbieten, aber wenn Ihr Steuerspezialist feststellt, dass Sie spezielle zusätzliche Informationen benötigen, wenden Sie sich an. AWS Support

Ändern von Reserved Instances

Wenn sich Ihre Anforderungen ändern, können Sie Ihre Standard- oder Convertible Reserved Instances ändern. So profitieren Sie auch weiterhin von den Rabatten. Sie können Attribute wie die Availability Zone, die Instance-Größe (innerhalb derselben Instance-Familie und -Generation) und den Umfang Ihrer Reserved Instance ändern.

> **Note**
>
> Sie können auch eine Convertible Reserved Instance gegen eine andere Convertible Reserved Instance mit einer anderen Konfiguration austauschen. Weitere Informationen finden Sie unter Austauschen von Convertible Reserved Instances.

Sie können Ihre kompletten Reserved Instances oder einen Teil ändern. Sie können Ihre ursprünglichen Reserved Instances in zwei oder mehr neue Reserved Instances aufteilen. Wenn Sie beispielsweise über eine Reservierung für 10 Instances in `us-east-1a` verfügen und Sie 5 Instances in `us-east-1b` verschieben möchten, führt die Änderungsanforderung zu zwei neuen Reservierungen: Eine für 5 Instances in `us-east-1a`, und eine für 5 Instances in `us-east-1b`.

Sie können außerdem zwei oder mehr Reserved Instances in einer einzige Reserved Instance zusammenführen. Wenn Sie beispielsweise vier `t2.small` Reserved Instances mit jeweils einer Instance haben, können Sie diese in einer `t2.large` Reserved Instance zusammenführen. Weitere Informationen finden Sie unter Support für das Ändern von Instance-Größen.

Nach der Änderung wird der Rabatt für die Reserved Instances nur auf Instances mit den neuen Parametern angewendet. Wenn Sie beispielsweise die Availability Zone einer Reservierung ändern, werden die Kapazitätsreservierung und die Preisvorteile automatisch auf die Instance-Nutzung in der neuen Availability Zone angewendet. Solange keine anderen gültigen Reservierungen in Ihrem Konto vorhanden sind, werden Instances, die nicht mehr mit den neuen Parametern übereinstimmen, über den On-Demand-Tarif abgerechnet.

Wenn Ihre Änderungsanforderung erfolgreich ist:

- Die geänderte Reservierung gilt sofort. Die Preisvorteile werden eine Stunde nach Ihrer Änderungsanforderungen auf die neuen Instances angewendet. Wenn Sie beispielsweise Ihre Reservierung um 21:15 Uhr erfolgreich ändern, wird der Preisvorteil um 21:00 Uhr auf Ihre neue Instance übertragen. Sie können das Datum des Inkrafttretens der abgeänderten Reserved Instances mithilfe des Befehls describe-reserved-instances abrufen.
- Die ursprüngliche Reservierung wird zurückgezogen. Ihr Enddatum entspricht dem Startdatum der neuen Reservierung. Das Enddatum der neuen Reservierung entspricht dem Enddatum der ursprünglichen Reserved Instance. Wenn Sie eine dreijährige Reservierung mit einer verbleibenden Laufzeit von 16 Monaten ändern, hat die resultierende, geänderte Reservierung eine Laufzeit von 16 Monaten. Das Enddatum entspricht dem der ursprünglichen Reservierung.

- Die geänderte Reservierung zeigt einen Festpreis von 0 USD statt des Festpreises der ursprünglichen Reservierung an.
- Der Festpreis der geänderten Reservierung wirkt sich nicht auf die Rabattstufenpreisberechnungen für Ihr Konto aus. Diese basieren auf dem Festpreis der ursprünglichen Reservierung.

Wenn Ihre Änderungsanforderung fehlschlägt, verbleiben Ihre Reserved Instances in der ursprünglichen Konfiguration. Sie stehen direkt für eine weitere Änderungsanforderung zur Verfügung.

Es gibt keine Gebühr für die Änderung. Sie erhalten keine neuen Rechnungen.

Sie können Ihre Reservierungen beliebig oft ändern. Sie können jedoch nach der Übermittlung keine ausstehenden Änderungsanforderungen ändern oder diese stornieren. Nach der erfolgreichen Durchführung der Änderungen. So können sie die Änderungen bei Bedarf rückgängig machen.

Inhalt

Anforderungen und Einschränkungen für Änderungen

Sie können diese Attribute wie folgt ändern.

Änderbares Attribut	Unterstützte Plattformen	Einschränkungen und Überlegungen
Ändern der Availability Zones innerhalb einer Region	Linux und Windows	-
Ändern des Umfangs von einer Availability Zone auf eine Region und entgegengesetzt	Linux und Windows	Eine zonale Reserved Instance ist auf eine Availability Zone ausgerichtet und reserviert die Kapazität in

Änderbares Attribut	Unterstützte Plattformen	Einschränkungen und Überlegungen
		dieser Availability Zone. Wenn Sie den Umfang von einer Availability Zone auf eine Region ändern (mit anderen Worten, von zonal zu regional) , verlieren Sie den Vorteil der Kapazitätsreservierung. Eine regionale Reserved Instance ist auf eine Region ausgerichtet. Der Reserved-Instance-Rabatt gilt für die Instance-Nutzung in jeder Availability Zone in dieser Region. Darüber hinaus gilt der Reserved-Instance-Rabatt auf die Instance-Nutzung in allen Größen in der ausgewähl ten Instance-Familie. Wenn Sie den Umfang von einer Region auf eine Availability Zone ändern (mit anderen Worten, von regional zu zonal), verlieren Sie die Flexibilität für die Availability Zone und die Instance-Größe (falls zutreffend). Weitere Informationen finden Sie unter So werden Reserved Instances angewendet.

Änderbares Attribut	Unterstützte Plattformen	Einschränkungen und Überlegungen
Ändern der Instance-Größe innerhalb desselben Instance-Familie und -Generation	Nur Linux/UNIX Die Flexibilität der Instance-Größe ist für Reserved Instances auf den anderen Plattformen nicht verfügbar, darunter fallen Linux mit SQL Server Standard, Linux mit SQL Server Web, Linux mit SQL Server Enterprise, Red Hat Enterprise Linux, SUSE Linux, Windows, Windows mit SQL Standard, Windows mit SQL Server Enterprise und Windows mit SQL Server Web.	Die Reservierung muss die Standard-Tenancy verwenden . Einige Instance-Familien werden nicht unterstützt, da keine anderen Größen verfügbar sind. Weitere Informationen finden Sie unter Support für das Ändern von Instance-Größen.

Voraussetzungen

Amazon EC2 verarbeitet Ihre Änderungsanforderungen, sofern eine ausreichende Kapazität für Ihre neue Konfiguration zur Verfügung steht (falls zutreffend). Außerdem müssen die folgenden Bedingungen zutreffen:

- Die Reserved Instance kann nicht vor dem Kauf oder beim Kauf geändert werden.
- Die Reserved Instance muss aktiv sein.
- Es dürfen keine Änderungsanforderungen ausstehen.
- Die Reserved Instance ist nicht im Reserved Instance Marketplace aufgelistet.
- Der Ressourcenbedarf der Instance-Größe der Origianlreservierung und der neuen Konfiguration müssen übereinstimmen. Weitere Informationen finden Sie unter Support für das Ändern von Instance-Größen.
- Die Original-Reserved Instances müssen entweder Standard-Reserved Instances oder Convertible Reserved Instances, aber nicht eine Kombination aus beiden sein.

- Die Original-Reserved Instances müssen in derselben Stunde ablaufen, wenn es sich um Standard-Reserved Instances handelt.
- Die Reserved Instance ist keine G4-, G4ad-, G4dn-, G5-, G5g-, Inf1- oder Inf2-Instance.

Support für das Ändern von Instance-Größen

Sie können die Instance-Größe einer Reserved Instance ändern, wenn die folgenden Anforderungen erfüllt sind.

Voraussetzungen

- Die Plattform ist Linux/UNIX.
- Sie müssen eine andere Instance-Größe in derselben Instance-Familie (gekennzeichnet durch einen Buchstaben, z. B. T) und Generation (gekennzeichnet durch eine Zahl, z. B. 2) auswählen.

  Sie können beispielsweise eine Reserved Instance von `t2.small` auf `t2.large` ändern, da beide zur gleichen T2-Familie und -Generation gehören. Sie können eine Reserved Instance jedoch nicht von T2 auf M2 oder von T2 auf T3 ändern, da in diesen beiden Beispielen die Ziel-Instance-Familie und -Generation nicht mit der ursprünglichen Reserved Instance identisch sind.
- Sie können die Instance Größe von Reserved Instances für die folgenden Instances nicht ändern, da jede der folgenden Instances nur über eine Größe verfügt:
  - `t1.micro`
- Sie können die Instance-Größe von Reserved Instances für die folgenden Kombinationen aus Instance-Familie, Generation und Attribut nicht ändern:
  - G4ad
  - G4dn
  - G5
  - G5g
  - Inf1
  - Inf2
- Das Original und die neue Reserved Instance müssen denselben Ressourcenbedarf für die Instance-Größe aufweisen.

Inhalt

- Normalisierungsfaktoren für Bare Metal-Instances

Ressourcenbedarf für die Instance-Größe

Jede Reserved Instance hat einen Ressourcenbedarf für die Instance-Größe. Dieser wird über den Normalisierungsfaktor der Instance-Größe und die Anzahl der Instances in der Reservierung bestimmt. Wenn Sie die Instance-Größen in einer Reserved Instance ändern, muss der Ressourcenbedarf der neuen Konfiguration mit dem der ursprünglichen Konfiguration übereinstimmen. Andernfalls wird die Änderungsanforderung nicht verarbeitet.

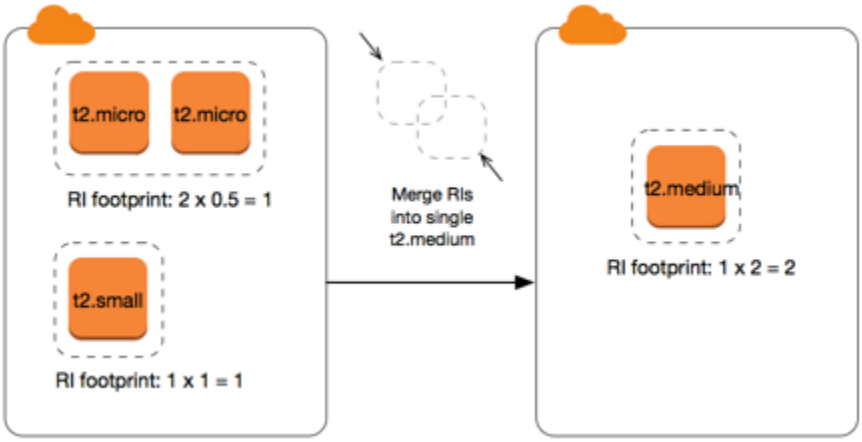
Um den Ressourcenbedarf für die Instance-Größe einer Reserved Instance zu berechnen, multiplizieren Sie die Anzahl der Instances mit dem Normalisierungsfaktor. In der Amazon EC2-Konsole wird der Normalisierungsfaktor in Einheiten gemessen. In der folgenden Tabelle wird der Normalisierungsfaktor für die Instance-Größen in einer Instance-Familie beschrieben. `t2.medium` hat beispielsweise einen Normalisierungsfaktor von 2. Daher hat eine Reservierung für vier `t2.medium`-Instances einen Ressourcenbedarf von 8 Einheiten.

Instance-Größe	Normalisierungsfaktor
nano	0,25
micro	0.5
small	1
medium	2
large	4
xlarge	8
2xlarge	16
3xlarge	24
4xlarge	32
6xlarge	48
8xlarge	64

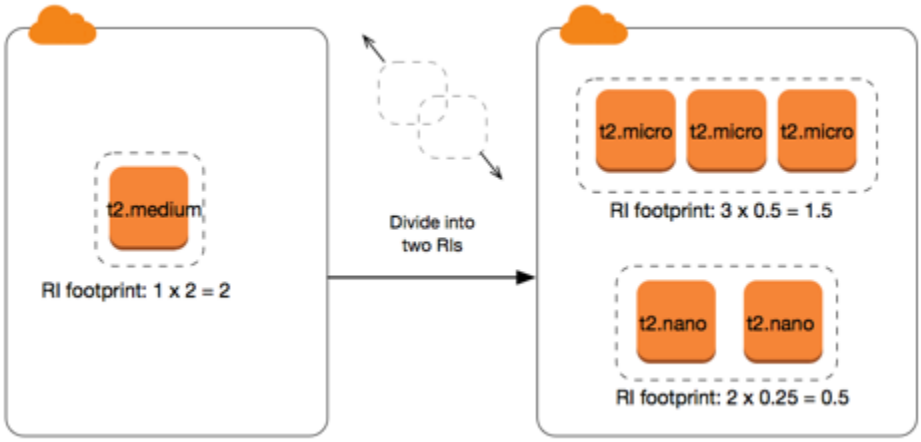
Instance-Größe	Normalisierungsfaktor
9xlarge	72
10xlarge	80
12xlarge	96
16xlarge	128
18xlarge	144
24xlarge	192
32xlarge	256
48xlarge	384
56xlarge	448
112xlarge	896

Sie können Ihre Reservierungen unterschiedlichen Instance-Größen in derselben Instance-Familie zuweisen, sofern der Ressourcenbedarf für die Instance-Größe Ihrer Reservierung gleichbleibt. Beispielsweise können Sie eine Reservierung für eine `t2.large`-Instance (1 @ 4 Einheiten) in vier `t2.small`-Instances (4 @ 1 Einheit) unterteilen. Ebenso können Sie eine Reservierung für vier `t2.small`-Instances in einer `t2.large`-Instance kombinieren. Sie können Ihre Reservierung für zwei `t2.small`-Instances jedoch nicht in eine `t2.large`-Instance ändern, da der Ressourcenbedarf der neuen Reservierung (4 Einheiten) größer ist als der Ressourcenbedarf der Originalreservierung (2 Einheiten).

Im folgenden Beispiel haben Sie eine Reservierung mit zwei `t2.micro`-Instances (1 Einheit) und eine Reservierung mit einer `t2.small`-Instance (1 Einheit). Wenn Sie beide Reservierungen mit einer einzigen Reservierung mit einer `t2.medium`-Instance (2 Einheiten) zusammenführen, entspricht der Ressourcenbedarf der neuen Reservierung dem Ressourcenbedarf der kombinierten Reservierungen.



Sie können außerdem eine Reservierung in zwei oder mehr Reservierungen aufteilen. Im folgenden Beispiel haben Sie eine Reservierung mit einer `t2.medium`-Instance (2 Einheiten). Sie können die Reservierung in zwei Reservierungen unterteilen, eine mit zwei `t2.nano`-Instances (0,5 Einheiten) und die andere mit drei `t2.micro`-Instances (1,5 Einheiten).



Normalisierungsfaktoren für Bare Metal-Instances

Sie können eine Reservierung mit `metal`-Instances ändern, die andere Größen innerhalb derselben Instance-Familie verwenden. Ebenso können Sie eine Reservierung mit anderen Instances als Bare Metal-Instances ändern, indem Sie die `metal`-Größe innerhalb derselben Instance-Familie verwenden. Im Allgemeinen hat eine Bare Metal-Instance dieselbe Größe wie die größte verfügbare Instance-Größe innerhalb derselben Instance-Familie. Beispielsweise hat eine `i3.metal`-Instance die gleiche Größe wie eine `i3.16xlarge`-Instance, sodass sie denselben Normalisierungsfaktor haben.

In der folgenden Tabelle wird der Normalisierungsfaktor für die Bare Metal-Instance-Größen in den Instance-Familien mit Bare Metal-Instances beschrieben. Der Normalisierungsfaktor für `metal`-Instances hängt im Gegensatz zu den anderen Instance-Größen von der Instance-Familie ab.

Instance-Größe	Normalisierungsfaktor
`a1.metal`	32
`m5zn.metal` | `x2iezn.metal` `z1d.metal`	96
`c6g.metal` | `c6gd.metal` | `i3.metal` | `m6g.metal` | `m6gd.metal` | `r6g.metal` | `r6gd.metal` | `x2gd.metal`	128
`c5n.metal`	144
`c5.metal` | `c5d.metal` | `i3en.metal` | `m5.metal` | `m5d.metal` | `m5dn.metal` | `m5n.metal` | `r5.metal` | `r5b.metal` | `r5d.metal` | `r5dn.metal` | `r5n.metal`	192
`c6i.metal` | `c6id.metal` | `m6i.metal` | `m6id.metal` | `r6d.metal` | `r6id.metal`	256
`u-*.metal`	896

Beispiel: Eine `i3.metal`-Instance hat beispielsweise einen Normalisierungsfaktor von 128. Wenn Sie eine `i3.metal`-Reserved Instance der Amazon Linux/Unix-Plattform mit Standard-Tenancy erwerben, können Sie die Reservierung wie folgt aufteilen:

- Da eine `i3.16xlarge`-Instance dieselbe Größe wie eine `i3.metal`-Instance hat, ist ihr Normalisierungsfaktor 128 (128/1). Die Reservierung für eine `i3.metal`-Instance kann in eine `i3.16xlarge`-Instance geändert werden.
- Da eine `i3.8xlarge`-Instance halb so groß wie eine `i3.metal`-Instance ist, ist ihr Normalisierungsfaktor 64 (128/2). Die Reservierung für eine `i3.metal`-Instance kann in zwei `i3.8xlarge`-Instances aufgeteilt werden.
- Da eine `i3.4xlarge`-Instance ein Viertel der Größe einer `i3.metal`-Instance ist, ist ihr Normalisierungsfaktor 32 (128/4). Die Reservierung für eine `i3.metal`-Instance kann in vier `i3.4xlarge`-Instances aufgeteilt werden.

Senden von Änderungsanforderungen

Bevor Sie Ihre Reserved Instances ändern, stellen Sie sicher, dass Sie die geltenden Einschränkungen gelesen haben. Bevor Sie die Instance-Größe ändern, berechnen Sie die gesamte Instance-Größe der ursprünglichen Reservierungen, die Sie ändern möchten, und stellen Sie sicher, dass sie mit der gesamten Instance-Größe Ihrer neuen Konfigurationen übereinstimmt.

New console

Um Ihre Reserved Instances zu ändern, verwenden Sie AWS Management Console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Seite Reserved Instances eine oder mehrere zu ändernde Reserved Instances aus und wählen Sie dann Actions (Aktionen), Modify Reserved Instances (Reserved Instances ändern) aus.

   > **Note**
   >
   > Wenn Ihre Reserved Instances nicht im aktiven Status sind oder nicht geändert werden können, ist Modify Reserved Instances (&ris; ändern) deaktiviert.

3. Der erste Eintrag in der Änderungstabelle zeigt die Attribute der gewählten Reserved Instances sowie mindestens eine Zielkonfiguration an. Die Spalte Units zeigt den Gesamtressourcenbedarf für die Instance-Größe an. Wählen Sie Add für jede neue Konfiguration aus. Ändern Sie die Attribute der einzelnen Konfigurationen nach Ihren Anforderungen.

   - Scope (Bereich): Wählen Sie aus, ob die Konfiguration für eine Availability Zone oder die gesamte Region angewendet wird.
   - Availability Zone: Wählen Sie die erforderliche Availability Zone aus. Nicht für regionale Reserved Instances anwendbar.
   - Instance-Typ: Wählen Sie den erforderlichen Instance-Typ aus. Die kombinierten Konfigurationen müssen dem Ressourcenbedarf für die Instance-Größe Ihrer ursprünglichen Konfigurationen entsprechen.
   - Count (Anzahl): Geben Sie die Anzahl der Instances an. Um die Reserved Instances in mehrere Konfigurationen aufzuteilen, reduzieren Sie die Anzahl, wählen Sie Add (Hinzufügen) aus und geben Sie eine Anzahl für die zusätzliche Konfiguration an. Wenn Sie beispielsweise über eine einzelne Konfiguration mit einer Anzahl von 10

verfügen, können Sie deren Anzahl auf 6 ändern und eine Konfiguration mit einer Anzahl von 4 hinzufügen. Durch diesen Vorgang wird die ursprüngliche Reserved Instance zurückgezogen, nachdem die neuen Reserved Instances aktiviert wurden.

4. Klicken Sie auf Continue.
5. Um Ihre Änderung zu bestätigen, wenn Sie die Angabe Ihrer Zielkonfigurationen abgeschlossen haben, wählen Sie Submit Modifications aus.
6. Sie können den Status Ihrer Änderungsanforderung über die Spalte State (Status) auf der Reserved Instances-Seite ablesen. Die folgenden Zustände sind möglich.

   - active (Aktiv) (ausstehende Änderung) – Übergangsstatus für Original-Reserved Instances
   - retired (Veraltet) (ausstehende Änderung) – Übergangsstatus für Original-Reserved Instances, während neue Reserved Instances erstellt werden.
   - veraltet: Reserved Instances erfolgreich geändert und ersetzt
   - aktiv — Einer der Folgenden:
     - Neue Reserved Instances durch eine erfolgreiche Änderungsanforderung erstellt.
     - Ursprüngliche Reserved Instances nach einer fehlgeschlagenen Änderungsanforderung

Old console

Um Ihre Reserved Instances zu ändern, verwenden Sie AWS Management Console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Seite Reserved Instances eine oder mehrere zu ändernde Reserved Instances aus und wählen Sie dann Actions (Aktionen), Modify Reserved Instances (Reserved Instances ändern) aus.

   > **Note**
   >
   > Wenn Ihre Reserved Instances nicht im aktiven Status sind oder nicht geändert werden können, ist Modify Reserved Instances (&ris; ändern) deaktiviert.

3. Der erste Eintrag in der Änderungstabelle zeigt die Attribute der gewählten Reserved Instances sowie mindestens eine Zielkonfiguration an. Die Spalte Units zeigt den Gesamtressourcenbedarf für die Instance-Größe an. Wählen Sie Add für jede neue Konfiguration aus. Ändern Sie die Attribute der einzelnen Konfigurationen nach Ihren Anforderungen und wählen Sie dann Continue (Fortfahren) aus:

- Scope (Bereich): Wählen Sie aus, ob die Konfiguration für eine Availability Zone oder die gesamte Region angewendet wird.
- Availability Zone: Wählen Sie die erforderliche Availability Zone aus. Nicht für regionale Reserved Instances anwendbar.
- Instance-Typ: Wählen Sie den erforderlichen Instance-Typ aus. Die kombinierten Konfigurationen müssen dem Ressourcenbedarf für die Instance-Größe Ihrer ursprünglichen Konfigurationen entsprechen.
- Count (Anzahl): Geben Sie die Anzahl der Instances an. Um die Reserved Instances in mehrere Konfigurationen aufzuteilen, reduzieren Sie die Anzahl, wählen Sie Add (Hinzufügen) aus und geben Sie eine Anzahl für die zusätzliche Konfiguration an. Wenn Sie beispielsweise über eine einzelne Konfiguration mit einer Anzahl von 10 verfügen, können Sie deren Anzahl auf 6 ändern und eine Konfiguration mit einer Anzahl von 4 hinzufügen. Durch diesen Vorgang wird die ursprüngliche Reserved Instance zurückgezogen, nachdem die neuen Reserved Instances aktiviert wurden.

4. Um Ihre Änderung zu bestätigen, wenn Sie die Angabe Ihrer Zielkonfigurationen abgeschlossen haben, wählen Sie Submit Modifications aus.
5. Sie können den Status Ihrer Änderungsanforderung über die Spalte State (Status) auf der Reserved Instances-Seite ablesen. Die folgenden Zustände sind möglich.

   - active (Aktiv) (ausstehende Änderung) – Übergangsstatus für Original-Reserved Instances
   - retired (Veraltet) (ausstehende Änderung) – Übergangsstatus für Original-Reserved Instances, während neue Reserved Instances erstellt werden.
   - veraltet: Reserved Instances erfolgreich geändert und ersetzt
   - aktiv — Einer der Folgenden:
     - Neue Reserved Instances durch eine erfolgreiche Änderungsanforderung erstellt.
     - Ursprüngliche Reserved Instances nach einer fehlgeschlagenen Änderungsanforderung

So zeigen Sie Ihre Reserved Instances mit dem Befehlszeilenclient an

1. Zum Ändern Ihrer Reserved Instances können Sie einen der folgenden Befehle nutzen:
   - modify-reserved-instances (AWS CLI)
   - Edit-EC2ReservedInstance (AWS Tools for Windows PowerShell)
2. Zum Abrufen des Status der Änderungsanforderung (`processing`, `fulfilled` oder `failed`) können Sie einen der folgenden Befehle nutzen:

- describe-reserved-instances-modifications (AWS CLI)
- Get-EC2ReservedInstancesModification (AWS Tools for Windows PowerShell)

Fehlerbehebung bei Änderungsanforderungen

Wenn die angeforderten Zielkonfigurationseinstellungen eindeutig waren, erhalten Sie eine Nachricht zur Verarbeitung Ihrer Anforderung. Zu diesem Zeitpunkt hat Amazon EC2 nur festgestellt, dass die Parameter Ihrer Änderungsanforderung gültig sind. Ihre Änderungsanforderung kann trotzdem während der Verarbeitung aufgrund einer unzureichenden Kapazität fehlschlagen.

In einigen Situationen erhalten Sie möglicherweise eine Nachricht, die eine unvollständige oder fehlgeschlagene Änderungsanforderung anzeigt. Nutzen Sie die Informationen aus diesen Nachrichten als Startpunkt für eine neue Änderungsanforderung. Stellen Sie vor dem Senden der Anforderung sicher, dass Sie die anwendbaren Einschränkungen gelesen haben.

Nicht alle ausgewählten Reserved Instances können für die Änderung verarbeitet werden

Amazon EC2 ermittelt die nicht änderbaren Reserved Instances und führt diese auf. Wenn Sie eine entsprechende Nachricht erhalten, wechseln Sie zur Seite Reserved Instances in der Amazon EC2-Konsole und überprüfen Sie die Informationen für die Reserved Instances.

Fehler bei der Verarbeitung Ihrer Änderungsanforderung

Sie haben eine oder mehrere Reserved Instances für eine Änderung gesendet. Es konnten jedoch nicht alle Anforderungen verarbeitet werden. Abhängig von der Anzahl der zu ändernden Reservierungen können Sie unterschiedliche Versionen der entsprechenden Nachricht erhalten.

Amazon EC2 zeigt die Gründe für die Nicht-Verarbeitung Ihrer Anforderung an. Sie können beispielsweise die gleiche Zielkonfiguration —(eine Kombination aus Availability Zone und Plattform) — für eine oder mehrere Untergruppen der zu ändernden Reserved Instances angegeben haben. Versuchen Sie, die Änderungsanforderung erneut zu senden. Stellen Sie jedoch sicher, dass die Instance-Details der Reservierung übereinstimmen. Stellen Sie außerdem sicher, dass die Zielkonfigurationen für alle zu ändernden Untergruppen einheitlich sind.

Austauschen von Convertible Reserved Instances

Sie können auch eine oder mehrere Convertible Reserved Instances gegen eine andere Convertible Reserved Instance mit einer anderen Konfiguration (einschließlich Instance-Familie, Betriebssystem und Tenancy) austauschen. Es gibt keine Begrenzungen für die Anzahl der Austauschvorgänge.

Die neue Convertible Reserved Instance muss jedoch einen identischen oder höheren Wert als die auszutauschenden originalen Convertible Reserved Instances haben.

Wenn Sie Ihre Convertible Reserved Instance austauschen, wird die Anzahl der Instances für Ihre aktuelle Reservierung gegen die Anzahl der Instances ausgetauscht, die einen identischen oder höheren Wert für die Konfiguration der neuen Convertible Reserved Instance abdeckt. Amazon EC2 berechnet die Anzahl der Reserved Instances, die Sie als Ergebnis des Austauschs erhalten können.

Sie können Standard-Reserved Instances nicht austauschen, aber Sie können sie ändern. Weitere Informationen finden Sie unter Ändern von Reserved Instances.

Inhalt

Anforderungen für den Austausch von Convertible Reserved Instances

Amazon EC2 verarbeitet Ihre Austauschanforderung, sofern die folgenden Bedingungen erfüllt sind. Ihr Convertible Reserved Instance muss folgende Eigenschaften erfüllen:

- Aktiv
- Keine ausstehende vorherige Änderungsanforderung
- Es müssen noch mindestens 24 Stunden bis zum Ablauf verbleiben.

Die folgenden Regeln gelten:

- Convertible Reserved Instances können nur gegen andere Convertible Reserved Instances ausgetauscht werden, die derzeit von AWS angeboten werden.
- Convertible Reserved Instances sind einer bestimmten Region zugeordnet, die für die Dauer der Reservierung festgelegt ist. Sie können eine Convertible Reserved Instance nicht gegen eine Convertible Reserved Instance in einer anderen Region eintauschen.
- Sie können eine oder mehrere Convertible Reserved Instances jeweils nur durch eine neue Convertible Reserved Instance ersetzen.

- Um einen Teil einer Convertible Reserved Instance auszutauschen, können Sie sie in zwei oder mehrere Reservierungen ändern und dann eine oder mehrere der Reservierungen gegen eine neue Convertible Reserved Instance tauschen. Weitere Informationen finden Sie unter Austauschen eines Teils einer Convertible Reserved Instance. Weitere Informationen zum Anpassen Ihrer Reserved Instances finden Sie unter Ändern von Reserved Instances.
- Alle Convertible Reserved Instances mit Vorauszahlung können gegen Convertible Reserved Instances mit teilweiser Vorauszahlung getauscht werden und umgekehrt.

> **Note**
>
> Liegt der für den Austausch erforderliche Gesamtvorauszahlungsbetrag (Anpassungskosten) unter 0,00 USD, stellt Ihnen AWS automatisch eine Anzahl von Instances in der Convertible Reserved Instance zur Verfügung. Dadurch wird sichergestellt, dass die Anpassungskosten 0,00 USD oder mehr betragen.

> **Note**
>
> Wenn der Gesamtwert (Vorabpreis + Stundenpreis x Anzahl der verbleibenden Stunden) der neuen Convertible Reserved Instance unter dem Gesamtwert der ausgetauschten Convertible Reserved Instance liegt, erhalten Sie AWS automatisch eine Anzahl von Instances in der Convertible Reserved Instance, die sicherstellt, dass der Gesamtwert dem der ausgetauschten Convertible Reserved Instance entspricht oder höher ist.

- Um von besseren Preisen zu profitieren, können Sie eine Convertible Reserved Instance ohne Vorauszahlung gegen eine Convertible Reserved Instance mit vollständiger Vorauszahlung oder eine &cri; mit teilweiser Vorauszahlung tauschen.
- Sie können keine Convertible Reserved Instances mit vollständiger Vorauszahlung oder mit teilweiser Vorauszahlung gegen Convertible Reserved Instances ohne Vorauszahlung tauschen.
- Sie können eine Convertible Reserved Instance ohne Vorauszahlung gegen eine andere Convertible Reserved Instance ohne Vorauszahlung nur dann eintauschen, wenn der Stundenpreis der neuen Convertible Reserved Instance gleich oder höher liegt als der Stundenpreis der getauschten Convertible Reserved Instance.

> **Note**
>
> Wenn der Gesamtwert (Stundenpreis x Anzahl der verbleibenden Stunden) der neuen Convertible Reserved Instance unter dem Gesamtwert der ausgetauschten Convertible Reserved Instance liegt, erhalten Sie AWS automatisch eine Anzahl von Instances in der Convertible Reserved Instance, die sicherstellt, dass der Gesamtwert dem der ausgetauschten Convertible Reserved Instance entspricht oder höher ist.

- Wenn Sie mehrere Convertible Reserved Instances mit verschiedenen Ablaufdaten austauschen, entspricht das Ablaufdatum der neuen Convertible Reserved Instance dem Datum, das am weitesten in der Zukunft liegt.
- Wenn Sie eine einzelne Convertible Reserved Instance austauschen, muss sie dieselbe Laufzeit (1 oder 3 Jahre) wie die neue Convertible Reserved Instance. Wenn Sie mehrere Convertible Reserved Instances mit verschiedenen Laufzeiten mischen, hat die neue Convertible Reserved Instance eine Laufzeit von 3 Jahren. Weitere Informationen finden Sie unter Mischen von Convertible Reserved Instances.
- Wenn Amazon EC2 eine Convertible Reserved Instance austauscht, wird die zugehörige Reservierung zurückgezogen und das Enddatum der neuen Reservierung übertragen. Nach dem Umtausch legt Amazon EC2 sowohl das Enddatum für die alte Reservierung als auch das Startdatum für die neue Reservierung fest, das dem Datum des Umtausches entspricht. Wenn Sie beispielsweise eine dreijährige Reservierung austauschen, deren Laufzeit noch 16 Monate beträgt, ist die Reservierung eine 16-monatige Reservierung mit demselben Enddatum wie die Reservierung der von Ihnen ausgetauschten Convertible Reserved Instance.

Berechnen der Convertible Reserved Instances-Austausche

Das Wechseln von Convertible Reserved Instances ist kostenfrei. Es fallen jedoch möglicherweise Anpassungskosten an. Hierbei handelt es sich um anteilige Kosten für den Unterschied zwischen den vorher vorhandenen Convertible Reserved Instances und den neuen Convertible Reserved Instances, die Sie im Zuge des Austauschs erhalten.

Jede Convertible Reserved Instance hat eine Liste mit Werten. Der Listenwert wird mit dem Listenwert der Convertible Reserved Instances vergleichen, die Sie anfordern. So wird festgestellt, wie viele Instance-Reservierungen Sie aus dem Austausch erhalten können.

Beispiel: Sie haben eine Convertible Reserved Instance mit einem Listenwert von 1 x 35 USD, die Sie gegen einen neuen Instance-Typ mit einem Listenwert von 10 USD austauschen möchten.

```
$35/$10 = 3.5
```

Sie können Ihre Convertible Reserved Instance gegen eine 10-USD-Convertible Reserved Instances tauschen. Sie können keine halben Reservierungen erwerben. Daher müssen Sie für den restlichen Teil eine zusätzliche Convertible Reserved Instance erwerben:

```
3.5 = 3 whole Convertible Reserved Instances + 1 additional Convertible Reserved
 Instance
```

Die vierte Convertible Reserved Instance hat dasselbe Enddatum wie die anderen drei. Wenn Sie Convertible Reserved Instances mit teilweiser oder vollständiger Vorauszahlung austauschen, zahlen Sie die Anpassungskosten für die vierte Reservierung. Die verbleibenden Vorauszahlungskosten Ihrer Convertible Reserved Instances betragen 500 USD. Die neue Reservierung würde normalerweise auf Umlagebasis 600 USD kosten. Ihnen werden 100 USD berechnet.

```
$600 prorated upfront cost of new reservations - $500 remaining upfront cost of old
 reservations = $100 difference
```

Mischen von Convertible Reserved Instances

Wenn Sie zwei oder mehr Convertible Reserved Instances zusammenführen, muss die Laufzeit der neuen Convertible Reserved Instance mit der Laufzeit der alten Convertible Reserved Instances oder mit der längsten Laufzeit der Convertible Reserved Instances übereinstimmen. Das Ablaufdatum der neuen Convertible Reserved Instance entspricht dem Ablaufdatum, das am weitesten in der Zukunft liegt.

Angenommen, es gibt die folgenden Convertible Reserved Instances in Ihrem Konto:

Reserved Instance ID	Begriff	Ablaufdatum
aaaa1111	1 Jahr	31.12.2018
bbbb2222	1 Jahr	31.07.2018
cccc3333	3 Jahre	30.06.2018
dddd4444	3 Jahre	31.12.2019

- Sie können `aaaa1111` und `bbbb2222` mischen und sie gegen eine neue 1-Jahres-Convertible Reserved Instance tauschen. Sie können sie nicht gegen eine 3-Jahres-Convertible Reserved Instance tauschen. Das Ablaufdatum der neuen Convertible Reserved Instance ist der 31.12.2018.
- Sie können `bbbb2222` und `cccc3333` mischen und sie gegen eine neue 3-Jahres-Convertible Reserved Instance tauschen. Sie können sie nicht gegen eine 1-Jahres-Convertible Reserved Instance tauschen. Das Ablaufdatum der neuen Convertible Reserved Instance ist der 31.07.2018.
- Sie können `cccc3333` und `dddd4444` mischen und sie gegen eine neue 3-Jahres-Convertible Reserved Instance tauschen. Sie können sie nicht gegen eine 1-Jahres-Convertible Reserved Instance tauschen. Das Ablaufdatum der neuen Convertible Reserved Instance ist der 31.12.2019.

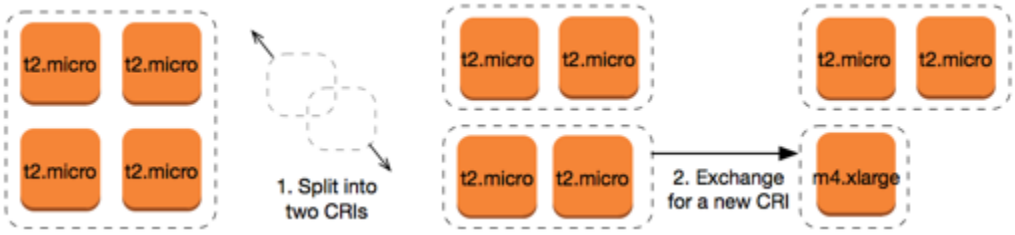
Austauschen eines Teils einer Convertible Reserved Instance

Sie können den Änderungsprozess zum Aufteilen Ihrer Convertible Reserved Instance in kleinere Reservierungen nutzen und dann eine oder mehrere Reservierungen gegen eine neue Convertible Reserved Instance tauschen. Die folgenden Beispiele veranschaulichen die entsprechende Vorgehensweise.

Example Beispiel: Convertible Reserved Instance mit mehreren Instances

In diesem Beispiel haben Sie eine `t2.micro` Convertible Reserved Instance mit vier Instances in der Reservierung. So wechseln Sie zwei `t2.micro` Instances gegen eine `m4.xlarge` Instance:

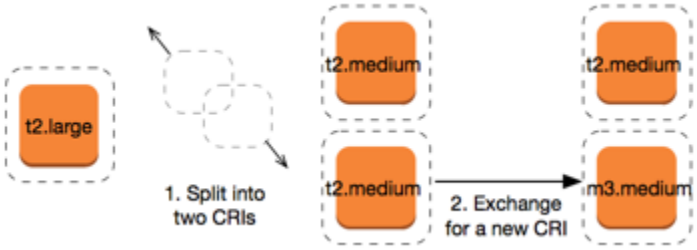
1. Ändern Sie die `t2.micro` Convertible Reserved Instance, indem Sie sie in zwei `t2.micro` Convertible Reserved Instances mit jeweils zwei Instances aufteilen.
2. Wechseln Sie eine der neuen `t2.micro` Convertible Reserved Instances gegen eine `m4.xlarge` Convertible Reserved Instance.



Example Beispiel: Convertible Reserved Instance mit einer einigen Instance

In diesem Beispiel haben Sie eine `t2.large` Convertible Reserved Instance. So ändern Sie sie in eine kleinere `t2.medium` Instance und eine `m3.medium` Instance:

1. Ändern Sie die `t2.large` Convertible Reserved Instance, indem Sie sie in zwei `t2.medium` Convertible Reserved Instances aufteilen. Eine einzelne `t2.large` Instance hat einen genau so großen Instance-Footprint wie zwei `t2.medium` Instances.
2. Wechseln Sie eine der neuen `t2.medium` Convertible Reserved Instances gegen eine `m3.medium` Convertible Reserved Instance.



Weitere Informationen finden Sie unter Support für das Ändern von Instance-Größen und Senden von Austauschanforderungen.

Senden von Austauschanforderungen

Sie können Ihre Convertible Reserved Instances über die Amazon EC2-Konsole oder ein Befehlszeilen-Tool austauschen.

Austauschen einer Convertible Reserved Instance mithilfe der Konsole

Sie können nach Convertible Reserved Instances-Angeboten suchen und unter diesen Ihre neue Konfiguration auswählen.

New console

So tauschen Sie Convertible Reserved Instances mithilfe der Amazon EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Reserved Instances aus, wählen Sie die Convertible Reserved Instances für den Austausch aus und wählen Sie Actions (Aktionen), Exchange Reserved Instance (&ri; tauschen) aus.
3. Wählen Sie die Attribute für die gewünschte Konfiguration aus und wählen Sie Find offering (Angebot finden) aus.

4. Wählen Sie ein neues Convertible Reserved Instance aus. Am unteren Bildschirmrand können Sie die Anzahl von Reserved Instances anzeigen, die Sie für den Austausch erhalten, sowie alle zusätzlichen Kosten.
5. Wenn Sie eine zu Ihren Anforderungen passende Convertible Reserved Instance ausgewählt haben, wählen Sie Review (Überprüfen) aus.
6. Wählen Sie Exchange (Austauschen) und dann Close (Beenden).

Old console

So tauschen Sie Convertible Reserved Instances mithilfe der Amazon EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Reserved Instances aus, wählen Sie die Convertible Reserved Instances für den Austausch aus und wählen Sie Actions (Aktionen), Exchange Reserved Instance (&ri; tauschen) aus.
3. Wählen Sie die Attribute für die gewünschte Konfiguration aus und wählen Sie Find Offering (Angebot finden) aus.
4. Wählen Sie ein neues Convertible Reserved Instance aus. Die Spalte Instance Count (Instance-Anzahl) zeigt die Anzahl der Reserved Instances an, die Sie im Austausch erhalten. Wenn Sie eine zu Ihren Anforderungen passende Convertible Reserved Instance ausgewählt haben, wählen Sie Exchange aus.

Die ausgetauschten Reserved Instances werden zurückgezogen. Die neuen Reserved Instances werden in der Amazon EC2-Konsole angezeigt. Dieser Vorgang kann einige Minuten dauern.

Austauschen einer Convertible Reserved Instance mithilfe der Befehlszeilen-Schnittstelle

Um eine Convertible Reserved Instance auszutauschen, müssen Sie zuerst eine zu Ihren Anforderungen passende neue Convertible Reserved Instance finden:

- describe-reserved-instances-offerings (AWS CLI)
- Get-EC2ReservedInstancesOffering(Tools für Windows PowerShell)

Holen Sie sich ein Angebot für den Austausch. Dieses enthält die Anzahl der Reserved Instances aus dem Austausch und die Anpassungskosten für den Austausch:

- get-reserved-instances-exchange-quote (AWS CLI)

- GetEC2- ReservedInstances ExchangeQuote (Tools für Windows) PowerShell

Führen Sie dann den Austausch durch:

- accept-reserved-instances-exchange-quote (AWS CLI)
- Confirm-EC2ReservedInstancesExchangeQuote(Tools für Windows) PowerShell

Kontingente für Reserved Instances

Sie können jeden Monat neue Reserved Instances erwerben. Die Anzahl der neuen Reserved Instances, die Sie jeden Monat erwerben können, richtet sich nach Ihrem monatlichen Kontingent. Es lautet wie folgt:

Quota-Beschreibung	Standardkontingent
Neue regionsgebundene Reserved Instances	20 pro Region und Monat
Neue zonengebundene Reserved Instances	20 pro Availability Zone und Monat

In einer Region mit drei Availability Zones beträgt das Standardkontingent beispielsweise 80 neue Reserved Instances pro Monat. Es wird wie folgt berechnet:

- 20 regionsgebundene Reserved Instances für die Region
- Plus 60 zonengebundene Reserved Instances (20 für jede der drei Availability Zones)

Instanzen im `running` Bundesstaat werden auf Ihr Kontingent angerechnet. Instances in den `hibernated` Bundesstaaten`pending`, `stopping``stopped`, und werden nicht auf Ihr Kontingent angerechnet.

Gesamtzahl der erworbenen Reserved Instances anzeigen

Die Anzahl der Reserved Instances, die Sie erwerben, wird durch das Konsolenfeld Instance count (Instance-Anzahl) oder den `InstanceCount`-Parameter (AWS CLI) angezeigt. Wenn Sie neue Reserved Instances erwerben, wird das Kontingent an der Gesamtzahl der Instances gemessen. Wenn Sie z. B. eine einzelne Reserved-Instance-Konfiguration mit einer Instance-Anzahl von 10 erwerben, wird der Kauf als 10 und nicht als 1 auf Ihr Kontingent angerechnet.

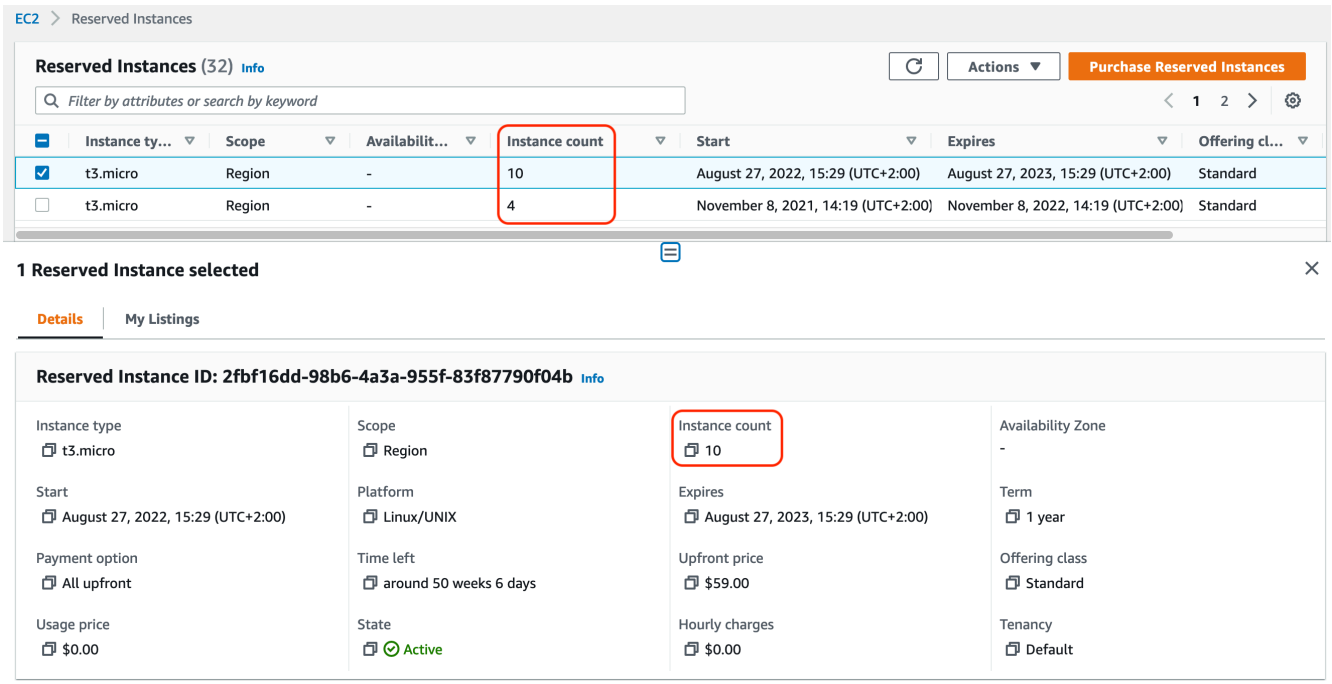
Sie können anzeigen, wie viele Reserved Instances Sie erworben haben, indem Sie Amazon EC2 oder die AWS CLI verwenden.

Console

So zeigen Sie die Gesamtzahl der erworbenen Reserved Instances an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Reserved Instances aus.
3. Wählen Sie eine Reserved-Instance-Konfiguration aus der Tabelle aus und markieren Sie das Feld Instance count (Instance-Anzahl).

   Im folgenden Screenshot stellt die ausgewählte Zeile eine einzelne Reserved-Instance-Konfiguration für einen `t3.micro`-Instance-Typ dar. Die Spalte Instance count (Instance-Anzahl) in der Tabellenansicht und das Feld Instance count (Instance-Anzahl) in der Detailansicht (im Screenshot dargestellt) zeigen an, dass es 10 Reserved Instances für diese Konfiguration gibt.



AWS CLI

So zeigen Sie die Gesamtzahl der erworbenen Reserved Instances an

Verwenden Sie den CLI-Befehl describe-reserved-instances und geben Sie die ID der Reserved-Instance-Konfiguration an.

```
aws ec2 describe-reserved-instances \
    --reserved-instances-ids 2fbf16dd-98b6-4a3a-955f-83f87790f04b \
    --output table
```

Beispielausgabe – Das Feld `InstanceCount` zeigt an, dass es 10 Reserved Instances für diese Konfiguration gibt.

```
-------------------------------------------------------------------
|                    DescribeReservedInstances                    |
+-----------------------------------------------------------------+
||                       ReservedInstances                       ||
|+----------------------+----------------------------------------+|
||  CurrencyCode        |  USD                                   ||
||  Duration            |  31536000                              ||
||  End                 |  2023-08-27T13:29:44+00:00             ||
||  FixedPrice          |  59.0                                  ||
||  InstanceCount       |  10                                    ||
||  InstanceTenancy     |  default                               ||
||  InstanceType        |  t3.micro                              ||
||  OfferingClass       |  standard                              ||
||  OfferingType        |  All Upfront                           ||
||  ProductDescription  |  Linux/UNIX                            ||
||  ReservedInstancesId |  2fbf16dd-98b6-4a3a-955f-83f87790f04b  ||
||  Scope               |  Region                                ||
||  Start               |  2022-08-27T13:29:45.938000+00:00      ||
||  State               |  active                                ||
||  UsagePrice          |  0.0                                   ||
|+----------------------+----------------------------------------+|
|||                     RecurringCharges                        |||
||+---------------------------------+--------------------------+||
|||  Amount                         |  0.0                     |||
|||  Frequency                      |  Hourly                  |||
||+---------------------------------+--------------------------+||
```

Überlegungen

Eine regionale Reserved Instance gewährt einen Rabatt auf eine laufende On-Demand-Instance. Das Standard-On-Demand-Instance-Limit ist 20. Sie können Ihr laufendes On-Demand-Instance-Limit

nicht überschreiten, indem Sie die regionale Reserved Instances kaufen. Wenn Sie beispielsweise bereits 20 laufende On-Demand-Instances haben und 20 regionale Reserved Instances kaufen, werden die 20 regionalen Reserved Instances verwendet, um einen Rabatt auf die 20 laufenden On-Demand-Instances anzuwenden. Wenn Sie mehr regionale Reserved Instances kaufen, können Sie nicht mehr Instances starten, weil Sie Ihr On-Demand-Instance-Limit erreicht haben.

Bevor Sie Reserved Instances regional kaufen, stellen Sie sicher, dass Ihr On-Demand-Instance-Limit der Anzahl der regionalen Reserved Instances entspricht oder diese überschreitet, die Sie nutzen möchten. Stellen Sie bei Bedarf sicher, dass Sie eine Erhöhung Ihres On-Demand-Instance-Limits beantragen, bevor Sie mehr regionale Reserved Instances kaufen.

Eine zonengebundene Reserved Instance – eine Reserved Instance, die für eine bestimmte Availability Zone gekauft wird – bietet sowohl eine Kapazitätsreservierung als auch einen Rabatt. Sie können Ihr laufendes On-Demand-Instance-Limit um überschreiten, indem Sie Zone Reserved Instances kaufen. Wenn Sie zum Beispiel bereits 20 laufende On-Demand-Instances haben und 20 Zonen Reserved Instances kaufen, können Sie weitere 20 On-Demand-Instances starten, die den Spezifikationen Ihrer Zonen Reserved Instances entsprechen, was Ihnen insgesamt 40 laufende Instances gibt.

Anzeigen Ihrer Reserved-Instance-Kontingente und Anfordern einer Kontingenterhöhung

Die Amazon-EC2-Konsole stellt Informationen zum Kontingent bereit. Sie können auch eine Kontingenterhöhung anfordern. Weitere Informationen finden Sie unter Anzeigen Ihrer aktuellen Kontingente und Beantragen einer Erhöhung.

Spot-Instances

Eine Spot-Instance ist eine Instance, die freie EC2-Kapazität nutzt, die für weniger als den On-Demand-Preis verfügbar ist. Da Sie mit Spot-Instances ungenutzte EC2-Instances mit hohen Rabatten anfordern können, können Sie Ihre Amazon EC2 Kosten deutlich senken. Der Stundenpreis für eine Spot-Instance wird als Spot-Preis bezeichnet. Der Spot-Preis aller Instance-Typen in allen Availability Zones wird von Amazon EC2 festgelegt und abhängig vom langfristigen Angebot an und der langfristigen Nachfrage nach Spot-Instances schrittweise angepasst. Ihre Spot Instance läuft, wann immer Kapazität verfügbar ist.

Spot-Instances sind eine kostengünstige Wahl, sofern Sie bei der Ausführung Ihrer Anwendungen zeitlich flexibel sind und Unterbrechungen verschmerzen können. Spot-Instances sind z. B. für Datenanalysen, Batch-Verarbeitungsaufträge, die Hintergrundverarbeitung und optionale Aufgaben geeignet. Weitere Informationen finden Sie unter Amazon-EC2-Spot-Instances.

Einen Vergleich der verschiedenen Kaufoptionen für EC2-Instances finden Sie unter Instance-Kaufoptionen.

Topics

Konzepte

Bevor Sie mit Spot Instances arbeiten, sollten Sie mit den folgenden Konzepten vertraut sein:

- Spot-Kapazitätspool: Ein Satz nicht verwendeter EC2-Instances mit demselben Instance-Typ (z. B. `m5.large`) sowie derselben Availability Zone.
- Spot-Preis: Der aktuelle Preis einer Spot-Instance pro Stunde.
- Spot-Instance-Anforderung: Fordert eine Spot-Instance an. Wenn Kapazität verfügbar ist, erfüllt Amazon EC2 Ihre Anforderung. Eine Spot-Instance-Anforderung erfolgt entweder einmalig oder persistent. Amazon EC2 sendet eine persistente Spot-Instance-Anforderung automatisch erneut, wenn die mit der Spot-Instance-Anforderung verknüpfte Spot Instance beendet wurde.

- Neuausgleichsempfehlung für die EC2-Instance – Amazon EC2 sendet ein Signal zur Neuausgleichsempfehlung für die Instance, um Sie zu benachrichtigen, dass für eine Spot Instance ein erhöhtes Unterbrechungsrisiko besteht. Dieses Signal bietet Ihnen die Möglichkeit, Ihre Workloads proaktiv auf bestehende oder neue Spot Instances zu verteilen, ohne auf die zweiminütige Ankündigung einer Spot-Instance-Unterbrechung warten zu müssen.
- Spot-Instance-Unterbrechung – Amazon EC2 hält Ihre Spot Instance an, beendet sie oder versetzt sie in den Ruhezustand, wenn Amazon EC2 die Kapazität zurück benötigt. Amazon EC2 stellt eine Spot-Instance-Unterbrechungsbenachrichtigung bereit, was der Instance eine zweiminütige Warnung gibt, bevor sie unterbrochen wird.

Hauptunterschiede zwischen Spot-Instances und On-Demand-Instances

In der folgenden Tabelle sind die wichtigsten Unterschiede zwischen Spot Instances und On-Demand-Instances aufgeführt.

	Spot Instances	On-Demand Instances
Startzeit	Kann nur dann sofort gestartet werden, wenn die Spot-Instance-Anforderung aktiv ist und Kapazität vorhanden ist.	Kann nur dann sofort gestartet werden, wenn Sie eine manuelle Startanforderung stellen und Kapazität zur Verfügung steht.
Verfügbare Kapazität	Wenn keine Kapazität verfügbar ist, löst die Spot-Instance-Anforderung automatisch die Startanforderung aus, bis die Kapazität verfügbar ist.	Wenn bei einer Startanforderung keine Kapazität verfügbar ist, erhalten Sie einen Fehler wegen unzureichender Kapazität (ICE).
Stundenpreis	Der stündliche Preis für Spot Instances variiert je nach langfristigem Angebot und Nachfrage.	Der Stundenpreis für On-Demand-Instances ist statisch.
Neuausgleichsempfehlung	Das Signal, das Amazon EC2 für eine laufende Spot-Instance ausgibt, wenn die Instance ein erhöhtes Unterbrechungsrisiko hat.	Sie bestimmen, wann ein On-Demand-Instance unterbrochen (gestoppt, in den Ruhezustand versetzt oder beendet) wird.

	Spot Instances	On-Demand Instances
Instance-Unterbrechung	Sie können eine Amazon EBS-gestützte Spot-Instance beenden und starten. Darüber hinaus kann Amazon EC2 eine einzelne Spot Instance unterbrechen, wenn keine Kapazität mehr verfügbar ist.	Sie bestimmen, wann ein On-Demand-Instance unterbrochen (gestoppt, in den Ruhezustand versetzt oder beendet) wird.

Erste Schritte

Als Erstes müssen Sie sich für die Nutzung von Amazon EC2 einrichten. Erfahrungen beim Starten von On-Demand-Instances können für das Starten von Spot-Instances ebenfalls nützlich sein.

Spot-Grundlagen

- Funktionsweise von Spot-Instances

Arbeiten mit Spot-Instances

- Erstellt eine Spot-Instance-Anforderung
- Anfordern von Anforderungsstatusinformationen
- Spot-Instance-Unterbrechungen

Zugehörige Services

Sie können Spot-Instances direkt über Amazon EC2 bereitstellen. Sie können Spot-Instances auch unter Verwendung anderer Services in AWS bereitstellen. Weitere Informationen finden Sie in der folgenden Dokumentation.

Amazon EC2 Auto Scaling und Spot-Instances

> Sie können Startvorlagen oder -konfigurationen erstellen, damit Amazon EC2 Auto Scaling Spot Instances launchen kann. Weitere Informationen finden Sie unter Anfordern von Spot-Instances für fehlertolerante und flexible Anwendungen und Auto Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen im Amazon EC2 Auto Scaling-Benutzerhandbuch.

Amazon EMR und Spot-Instances

In bestimmten Szenarien kann es hilfreich sein, Spot-Instances in einem Amazon EMR-Cluster auszuführen. Weitere Informationen finden Sie unter Spot-Instances und Wann sollten Sie Spot-Instances verwenden? in Management Guide für Amazon EMR.

AWS CloudFormation Vorlagen

AWS CloudFormation ermöglicht es Ihnen, mithilfe einer Vorlage im JSON-Format eine Sammlung von AWS Ressourcen zu erstellen und zu verwalten. Weitere Informationen finden Sie unter EC2 Spot Instance Updates — Auto Scaling and CloudFormation Integration.

AWS SDK for Java

Sie können die Programmiersprache Java zum Verwalten Ihrer Spot-Instances verwenden. Weitere Informationen finden Sie unter Anleitung: Amazon-EC2-Spot-Instances und Anleitung: Erweiterte Verwaltung von Amazon-EC2-Spot-Anforderungen.

AWS SDK for .NET

Sie können die Programmierumgebung .NET zum Verwalten Ihrer Spot-Instances verwenden. Weitere Informationen finden Sie unter Anleitung: Amazon-EC2-Spot-Instances.

Preise und Einsparungen

Sie zahlen für Spot-Instances den Spot-Preis, der von Amazon EC2 festgelegt und basierend auf dem langfristigen Angebot und der langfristigen Nachfrage nach Spot-Instances schrittweise angepasst wird. Ihre Spot Instances laufen so lange, bis Sie sie beenden, keine Kapazität mehr verfügbar ist oder Ihre Amazon-EC2-Auto-Scaling-Gruppe sie während der Abskalierung beendet.

Wenn Sie oder Amazon EC2 eine ausgeführte Spot-Instance unterbrechen, werden Ihnen die genutzten Sekunden oder die volle Stunde berechnet. Möglicherweise wird Ihnen aber auch nichts berechnet, je nach Betriebssystem, das Sie verwendet haben und das die Spot-Instance unterbrach. Weitere Informationen finden Sie unter Fakturierung für unterbrochene Spot-Instances.

Spot-Instances sind nicht durch Savings Plans abgedeckt. Wenn Sie einen Savings Plan haben, bietet dieser keine zusätzlichen Einsparungen zusätzlich zu den Einsparungen, die Sie bereits durch die Nutzung von Spot-Instances erzielen. Darüber hinaus gelten für Ihre Ausgaben für Spot-Instances nicht die Verpflichtungen in Ihren Compute Savings Plans.

Anzeigen von Preisen

Den aktuellen (alle fünf Minuten aktualisierten) niedrigsten Spot-Preis pro AWS-Region Instance-Typ finden Sie auf der Preisseite für Amazon EC2 Spot-Instances.

Zum Anzeigen des Spot-Preis-Verlaufs für die letzten drei Monate können Sie die Amazon EC2-Konsole oder den Befehl describe-spot-price-history (AWS CLI) verwenden. Weitere Informationen finden Sie unter Spot-Instance-Preisverlauf.

Wir ordnen Availability Zones unabhängig voneinander den jeweiligen AWS-Konto Codes zu. Aus diesem Grund können Sie für denselben Availability-Zone-Code (beispielsweise `us-west-2a`) für verschiedene Konten verschiedene Ergebnisse erhalten.

Anzeigen der Einsparungen

Sie können die Einsparungen anzeigen, die durch die Verwendung von Spot-Instances für eine einzelne Spot-Flotte oder für alle Spot-Instances erzielt wurden. Sie können die Einsparungen der letzten Stunde oder der letzten drei Tag)e sowie die durchschnittlichen Kosten pro vCPU-Stunde und pro Speicher(GiB)-Stunde einsehen. Die Einsparungen werden geschätzt und können von den tatsächlichen Einsparungen abweichen, da sie die Abrechnungsanpassungen für Ihre Nutzung nicht enthalten. Weitere Informationen zur Anzeige von Einsparungsinformationen finden Sie unter Einsparungen durch den Spot-Instances-Einkauf.

Anzeigen der Abrechnung

Ihre Rechnung enthält Einzelheiten zu Ihrer Servicenutzung. Weitere Informationen finden Sie unter Anzeigen Ihrer Rechnung im AWS Billing -Benutzerhandbuch.

Bewährte Methoden für EC2 Spot

Amazon EC2-Spot-Instances sind zusätzliche EC2-Rechenkapazitäten AWS Cloud , die Ihnen im Vergleich zu On-Demand-Preisen mit Einsparungen von bis zu 90% zur Verfügung stehen. Der einzige Unterschied zwischen On-Demand-Instances und Spot-Instances ist, dass Spot-Instances von Amazon EC2 unterbrochen werden kann, mit zwei Minuten Benachrichtigung, wenn Amazon EC2 die Kapazität zurück benötigt.

Spot-Instances werden für zustandslose, fehlertolerante, flexible Anwendungen empfohlen. Spot-Instances eignen sich beispielsweise gut für Big Data, containerisierte Workloads, CI/CD, zustandslose Webserver, High Performance Computing (HPC) und Rendering-Workloads.

Während des Ausführens sind Spot-Instances genau gleich wie On-Demand-Instances. Spot garantiert jedoch nicht, dass Sie Ihre ausgeführten Instances lange genug halten können, um Ihre Workloads abzuschließen. Spot garantiert auch nicht, dass Sie die sofortige Verfügbarkeit der von Ihnen gesuchten Instances erhalten können oder dass Sie immer die von Ihnen angeforderte Gesamtkapazität erhalten können. Darüber hinaus können sich Spot-Instance-Unterbrechungen und Spot-Instance-Kapazitäten im Laufe der Zeit ändern, da die Spot-Instance-Verfügbarkeit je nach Angebot und Nachfrage variiert und die Performance in der Vergangenheit keine Garantie für zukünftige Ergebnisse darstellt.

Spot-Instances sind nicht für Workloads geeignet, die unflexibel, statusbehaftet, fehlerintolerant oder eng zwischen Instance-Knoten verbunden sind. Wir empfehlen Spot-Instances nicht für Workloads, die gelegentliche Perioden nicht tolerieren, in denen die gesamte Zielkapazität nicht vollständig verfügbar ist. Die Einhaltung der Best Practices von Spot, um flexibel in Bezug auf Instance-Typen und Availability Zones zu sein, bietet zwar die beste Chance auf Hochverfügbarkeit, es gibt jedoch keine Garantie dafür, dass Kapazität verfügbar ist, da eine steigende Nachfrage nach On-Demand-Instances die Workloads auf Spot-Instances stören kann.

Wir raten dringend davon ab, Spot-Instances für diese Workloads zu verwenden oder zu versuchen, ein Failover auf On-Demand-Instances durchzuführen, um Unterbrechungen oder Phasen der Nichtverfügbarkeit zu bewältigen. Ein Failover auf On-Demand-Instances kann versehentlich zu Unterbrechungen Ihrer anderen Spot-Instances führen. Wenn Spot-Instances für eine Kombination aus Instance-Typ und Availability Zone unterbrochen werden, kann es für Sie außerdem schwierig werden, On-Demand-Instances mit derselben Kombination zu erhalten.

Unabhängig davon, ob Sie ein erfahrener Spot-Benutzer oder neu bei Spot-Instances sind: Wenn Sie derzeit Probleme mit Spot-Instance-Unterbrechungen oder Spot-Instance-Verfügbarkeit haben, empfehlen wir Ihnen, diese bewährten Methoden zu befolgen, um die beste Erfahrung mit dem Spot-Service zu erzielen.

Bewährte Methoden für Spot

- Vorbereiten einzelner Instances auf Unterbrechungen
- Flexibel sein bei Instance-Typen und Availability Zones
- Verwenden von EC2-Auto-Scaling-Gruppen oder EC2-Spot-Flotte zum Verwalten Ihrer Kapazität
- Nutzen der preis- und kapazitätsoptimierten Zuweisungsstrategie
- Verwenden Sie integrierte AWS Dienste, um Ihre Spot-Instances zu verwalten
- Was ist die beste Spot-Request-Methode?

Vorbereiten einzelner Instances auf Unterbrechungen

Der beste Weg, um Spot-Instance-Unterbrechungen ordnungsgemäß zu handhaben, besteht darin, Ihre Anwendung so zu konzipieren, dass sie eine Fehlertoleranz aufweist. Um dies zu erreichen, können Sie die Empfehlungen zum Neuausgleich von EC2-Instances und Spot-Instance-Unterbrechungsbenachrichtigungen nutzen.

Eine EC2-Instance-Ausgleichsempfehlung ist ein Signal, das Sie benachrichtigt, wenn eine Spot Instance einem erhöhten Risiko einer Unterbrechung ausgesetzt ist. Das Signal gibt Ihnen die Möglichkeit, die Spot-Instance vor der zweiminütigen Spot-Instance-Unterbrechungsbenachrichtigung proaktiv zu verwalten. Sie können entscheiden, Ihr Workload auf neue oder bestehende Spot-Instances auszugleichen, die nicht einem erhöhten Risiko einer Unterbrechung ausgesetzt sind. Wir haben es Ihnen leicht gemacht, dieses Signal zu nutzen, indem wir das Feature Kapazitätsausgleich in Auto-Scaling-Gruppen und EC2-Flotte verwenden.

Eine Benachrichtigung über die Unterbrechung der Spot-Instance ist eine Warnung, die zwei Minuten vor der Unterbrechung einer Spot-Instance durch Amazon EC2 ausgegeben wird. Wenn Ihre Workload „zeitlich flexibel“ ist, können Sie Ihre Spot-Instances so konfigurieren, dass sie bei einer Unterbrechung angehalten oder in den Ruhezustand versetzt werden, anstatt beendet zu werden. Amazon EC2 hält Ihre Spot-Instances bei einer Unterbrechung automatisch an oder versetzt sie in den Ruhezustand und nimmt die Ausführung der Instances automatisch wieder auf, wenn wir über verfügbare Kapazität verfügen.

Wir empfehlen Ihnen, in Amazon eine Regel zu erstellen EventBridge, die die Empfehlungen zur Neuverteilung und die Unterbrechungsbenachrichtigungen erfasst und dann einen Checkpoint für den Fortschritt Ihrer Arbeitslast auslöst oder die Unterbrechung ordnungsgemäß behandelt. Weitere Informationen finden Sie unter Überwachen von Signalen für Neuausgleichsempfehlungen. Ein detailliertes Beispiel, das Sie durch das Erstellen und Verwenden von Ereignisregeln führt, finden Sie unter Taking AdvanTage of Amazon EC2 Spot Instance Interruption Notices.

Weitere Informationen finden Sie unter Empfehlung zum Neuausgleich einer EC2-Instance und Spot-Instance-Unterbrechungen.

Flexibel sein bei Instance-Typen und Availability Zones

Ein Spot-Kapazitätspool ist ein Satz nicht verwendeter EC2-Instances mit demselben Instance-Typ (z. B. `m5.large`) sowie derselben Availability Zone (z. B. us-east-1a). Sie sollten flexibel darin sein, welche Instance-Typen Sie anfordern und in welchen Availability Zones Sie Ihren Workload bereitstellen können. Dies gibt Spot eine bessere Chance, die erforderliche Menge an

Rechenkapazität zu finden und zuzuweisen. Fragen Sie zum Beispiel nicht nur nach `c5.large`, wenn Sie bereit wären, Larges aus den Familien c4, m5 und m4 zu verwenden.

Je nach Ihren spezifischen Anforderungen können Sie auswerten, über welche Instance-Typen hinweg Sie flexibel sein können, um Ihre Computing-Anforderungen zu erfüllen. Wenn ein Workload vertikal skaliert werden kann, sollten Sie größere Instance-Typen (mehr vCPUs und Arbeitsspeicher) in Ihre Anforderungen aufnehmen. Wenn Sie nur horizontal skalieren können, sollten Sie Instance-Typen älterer Generation einbeziehen, da sie von On-Demand-Kunden weniger gefragt sind.

Eine gute Faustregel besteht darin, für jeden Workload über mindestens 10 Instance-Typen hinweg flexibel zu sein. Stellen Sie außerdem sicher, dass alle Availability Zones für die Verwendung in Ihrer VPC konfiguriert und für Ihren Workload ausgewählt sind.

Verwenden von EC2-Auto-Scaling-Gruppen oder EC2-Spot-Flotte zum Verwalten Ihrer Kapazität

Mit Spot können Sie in Bezug auf die Gesamtkapazität denken – in Einheiten, die vCPUs, Arbeitsspeicher, Speicher oder Netzwerkdurchsatz umfassen – anstatt in Bezug auf einzelne Instances zu denken. Mit Auto-Scaling-Gruppen und EC2-Flotte können Sie eine Zielkapazität starten und verwalten und Ressourcen, die unterbrochene oder manuell abgebrochene Ressourcen ersetzen, automatisch anfordern. Wenn Sie eine Auto-Scaling-Gruppe oder eine EC2-Flotte konfigurieren, müssen Sie nur die Instance-Typen und die Zielkapazität entsprechend Ihren Anwendungsanforderungen angeben. Weitere Informationen finden Sie unter Auto Scaling-Gruppen im Amazon EC2 Auto Scaling-Benutzerhandbuch und Erstellen einer EC2-Flotte in diesem Benutzerhandbuch.

Nutzen der preis- und kapazitätsoptimierten Zuweisungsstrategie

Zuweisungsstrategien in Auto Scaling-Gruppen helfen Ihnen, Ihre Zielkapazität bereitzustellen, ohne manuell nach den Spot-Kapazitätspools mit Reservekapazität suchen zu müssen. Es wird empfohlen, die `price-capacity-optimized`-Strategie zu verwenden, da diese Strategie automatisch Instances aus den am häufigsten verfügbaren Spot-Kapazitätspools bereitstellt, die außerdem den niedrigstmöglichen Preis bieten. Sie können auch die `price-capacity-optimized`-Zuweisungsstrategie in einer EC2-Flotte nutzen. Da Ihre Spot-Instance-Kapazität aus Pools mit optimaler Kapazität bezogen wird, verringert dies die Möglichkeit, dass Ihre Spot-Instances zurückgewonnen werden. Weitere Informationen zu Zuweisungsstrategien finden Sie unter Spot-Instances im Amazon EC2 Auto Scaling-Benutzerhandbuch und Wenn Workloads mit hohen Unterbrechungskosten verbunden sind in diesem Benutzerhandbuch.

Verwenden Sie integrierte AWS Dienste, um Ihre Spot-Instances zu verwalten

Andere AWS Dienste lassen sich in Spot integrieren, um die gesamten Rechenkosten zu senken, ohne dass die einzelnen Instances oder Flotten verwaltet werden müssen. Wir empfehlen Ihnen, die folgenden Lösungen für Ihre jeweiligen Workloads in Betracht zu ziehen: Amazon EMR, Amazon Elastic Container Service AWS Batch, Amazon Elastic Kubernetes Service SageMaker, AWS Elastic Beanstalk Amazon und Amazon. GameLift Weitere Informationen zu bewährten Methoden für Spot mit diesen Services finden Sie auf der Amazon-EC2-Spot-Instances-Workshop-Website.

Was ist die beste Spot-Request-Methode?

Bestimmen Sie anhand der folgenden Tabelle, welche API für die Anforderung von Spot-Instances verwendet werden soll.

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
CreateAutoScalingGroup	• Sie benötigen mehrere Instances mit einer einzigen Konfiguration oder einer gemischten Konfiguration. • Sie möchten das Lebenszyklusmanagement mit einer konfigurierbaren API automatisieren.	Erstellen Sie eine Auto-Scaling-Gruppe, die den Lebenszyklus Ihrer Instances verwaltet und gleichzeitig die gewünschte Anzahl von Instances beibehält. Unterstützt die horizontale Skalierung (Hinzufügen weiterer Instances) zwischen festgelegten Mindest- und Maximalgrenzen.	Ja
CreateFleet	• Sie benötigen mehrere Instances mit einer einzigen	Erstellen Sie eine Flotte von On-Demand-Instances und Spot-Instances	Ja – im `instant`-Modus, wenn Sie das Auto Scaling nicht benötigen

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
	Konfiguration oder einer gemischten Konfiguration. • Sie möchten Ihren Instance-Lebenszyklus selbst verwalten. • Wenn Sie kein Auto Scaling benötigen, empfehlen wir eine Flotte des Typs `instant`.	in einer einzigen Anforderung mit mehreren Startspezifikationen, die sich in Bezug auf Instance-Typ, AMIdie Availability Zone oder Subnetz unterscheiden. Die Spot-Instance-Zuweisungsstrategie ist standardmäßig auf `lowest-price` pro Einheit eingestellt, aber Sie können die Einstellung auf `price-capacity-optimized` , `capacity-optimized` oder `diversified` ändern.	

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
RunInstances	• Sie verwenden die RunInstances API bereits zum Starten von On-Demand -Instances und möchten einfach zum Starten von Spot-Instances wechseln, indem Sie einen einzelnen Parameter ändern. • Sie benötigen nicht mehrere Instances mit verschiedenen Instance-Typen.	Starten Sie eine bestimmte Anzahl von Instances mit einem AMI- und einem Instance-Typ.	Nein — weil gemischte Instance-Typen in einer einzigen Anfrage RunInstances nicht zulässig sind

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
RequestSpotFlotte	• Wir raten dringend davon ab, die RequestSpotFleet API zu verwenden, da es sich um eine veraltete API ohne geplante Investitionen handelt. • Wenn Sie den Lebenszyklus Ihrer Instance verwalten möchten, verwenden Sie die CreateFleet API. • Wenn Sie Ihren Instanzlebenszyklus nicht verwalten möchten, verwenden Sie die CreateAutoScalingGroup API.	NICHT VERWENDEN. RequestSpotFleet ist eine veraltete API ohne geplante Investitionen.	Nein

API	Wann sollte dies verwendet werden?	Anwendungsfall	Soll ich diese API verwenden?
RequestSpotInstanzen	• Wir raten dringend davon ab, die RequestSpotInstances API zu verwenden, da es sich um eine veraltete API ohne geplante Investitionen handelt.	NICHT VERWENDEN. RequestSpotInstances ist eine veraltete API ohne geplante Investitionen.	Nein

Funktionsweise von Spot-Instances

Um eine Spot-Instance zu starten, erstellen Sie entweder eineSpot-Instance-Anforderung oder Amazon EC2 erstellt in Ihrem Namen eine Spot-Instance-Anforderung. Die Spot-Instance wird gestartet, wenn die Spot-Instance-Anforderung erfüllt ist.

Sie können eine Spot-Instance mit mehreren verschiedenen Services starten. Weitere Informationen finden Sie unter Erste Schritte mit Amazon-EC2-Spot-Instances. In diesem Benutzerhandbuch beschreiben wir die folgenden Möglichkeiten zum Starten einer Spot-Instance mit EC2:

- Sie können eine Spot-Instance-Anfrage erstellen, indem Sie den Launch-Instance-Assistenten in der Amazon EC2 EC2-Konsole oder den Befehl run-instances AWS CLI verwenden. Weitere Informationen finden Sie unter Erstellt eine Spot-Instance-Anforderung.
- Sie können eine EC2-Flotte erstellen, in der Sie die gewünschte Anzahl von Spot-Instances angeben. Amazon EC2 erstellt in Ihrem Namen eine Spot-Instance-Anforderung für jede Spot-Instance, die in der EC2-Flotte angegeben ist. Weitere Informationen finden Sie unter Erstellen einer EC2-Flotte.
- Sie können eine Spot-Flotten-Anforderung erstellen, in der Sie die gewünschte Anzahl von Spot-Instances angeben. Amazon EC2 erstellt in Ihrem Namen eine Spot-Instance-Anforderung für jede Spot-Instance, die in der Spot-Flotten-Anforderung angegeben ist. Weitere Informationen finden Sie unter Erstellen eine Spot-Flotten-Anforderung.

Ihre Spot Instance wird gestartet, wenn Kapazität verfügbar ist.

Ihre Spot-Instance wird ausgeführt, bis Sie sie anhalten oder beenden oder bis sie von Amazon EC2 unterbrochen wird (bezeichnet als Spot-Instance-Unterbrechung).

Wenn Sie Spot-Instances verwenden, müssen Sie auf Unterbrechungen vorbereitet sein. Amazon EC2 kann Ihre Spot Instance unterbrechen, wenn die Nachfrage nach Spot Instances steigt oder wenn das Angebot an Spot Instances sinkt. Wenn Amazon EC2 eine Spot-Instance unterbricht, wird eine Benachrichtigung über die Unterbrechung der Spot-Instance bereitgestellt. Dadurch erhält die Instance zwei Minuten, bevor sie von Amazon EC2 unterbrochen wird, eine Warnmeldung. Sie können für Spot-Instances keinen Beendigungsschutz aktivieren. Weitere Informationen finden Sie unter Spot-Instance-Unterbrechungen.

Sie können eine Amazon EBS-gestützte Spot-Instance anhalten, starten, neu starten oder beenden. Der Spot-Dienst kann eine Spot-Instance anhalten, beenden oder in den Ruhezustand versetzen, wenn er sie unterbricht.

Inhalt

Starten Sie Spot-Instances in einer Startgruppe

Legen Sie eine Startgruppe in Ihrer Spot-Instance-Anforderung fest, sodass Amazon EC2 einen Satz von Spot-Instances nur dann startet, wenn alle gestartet werden können. Wenn der Spot-Service eine der Instances einer Startgruppe beenden muss, muss er sie alle beenden. Wenn Sie jedoch eine oder mehrere Instances in einer Startgruppe selbst beenden, beendet Amazon EC2 die übrigen Instances in der Startgruppe nicht.

Auch wenn diese Option nützlich sein kann, kann sich durch das Hinzufügen dieser Bedingung die Chance verringern, dass Ihre Spot-Instance-Anforderung erfüllt wird, und die Chance erhöhen, dass Ihre Spot-Instances beendet werden. Ihre Startgruppe umfasst beispielsweise Instances in mehreren Availability Zones. Wenn die Kapazität in einer dieser Availability Zones abnimmt und nicht mehr verfügbar ist, beendet Amazon EC2 alle Instances für die Startgruppe.

Wenn Sie eine weitere erfolgreiche Spot-Instance-Anforderung erstellen, die dieselbe (vorhandene) Startgruppe wie eine zuvor erfolgreiche Anforderung festlegt, werden die neuen Instances zu der

Startgruppe hinzugefügt. Wenn eine Instance in dieser Startgruppe beendet wird, werden folglich alle Instances in der Startgruppe beendet; dies umfasst alle Instances, die durch die erste und zweite Anforderung gestartet wurden.

Starten von Spot-Instances in einer Availability-Zone-Gruppe

Geben Sie in Ihrer Spot-Instance-Anforderung eine Availability-Zone-Gruppe an, um Amazon EC2 anzuweisen, eine Reihe von Spot Instances in derselben Availability Zone zu starten. Amazon EC2 muss nicht alle Instances in einer Availability Zone-Gruppe gleichzeitig unterbrechen. Wenn Amazon EC2 eine der Instances in einer Gruppe von Availability Zones unterbrechen muss, bleiben die anderen aktiv.

Auch wenn diese Option sehr nützlich sein kann, können durch das Hinzufügen dieser Bedingung die Chancen sinken, dass Ihre Spot-Instance-Anforderung erfüllt wird.

Wenn Sie eine Gruppe von Availability Zones angeben, in der Spot-Instance-Anforderung jedoch keine Availability Zone angeben, hängt das Ergebnis vom angegebenen Netzwerk ab.

Standard-VPC

Amazon EC2 verwendet die Availability Zone für das angegebene Subnetz. Wenn Sie kein Subnetz angeben, wählt es eine Availability Zone und sein Standard-Subnetz aus – dies ist jedoch nicht unbedingt die günstigste Zone. Wenn Sie das Standard-Subnetz für eine Availability Zone gelöscht haben, müssen Sie ein anderes Subnetz angeben.

Nicht standardmäßige VPC

Amazon EC2 verwendet die Availability Zone für das angegebene Subnetz.

Starten von Spot-Instances in einer VPC

Sie geben ein Subnetz für Ihre Spot-Instances genau so an, wie Sie ein Subnetz für Ihre On-Demand-Instances angeben.

- [Standard-VPC] Wenn Ihre Spot-Instance in einer bestimmten kostengünstigen Availability Zone gestartet werden soll, müssen Sie das entsprechende Subnetz in Ihrer Spot-Instance-Anforderung angeben. Wenn Sie kein Subnetz angeben, wählt Amazon EC2 eines für Sie aus. Die Availability Zone für dieses Subnetz weist möglicherweise jedoch nicht den niedrigsten Spot-Preis auf.
- [Nicht standardmäßige VPC] Sie müssen das Subnetz für Ihre Spot-Instance angeben.

Spot-Instance-Preisverlauf

Die Preise für Spot-Instances werden von Amazon EC2 festgelegt und ändern sich schrittweise entsprechend der langfristigen Trends beim Angebot von und der Nachfrage nach Spot-Instance-Kapazitäten.

Wenn Ihre Spot-Anforderung erfüllt ist, starten Ihre Spot Instances zum aktuellen Spot-Preis, der den On-Demand-Preis nicht übersteigt. Sie können den Spot-Preisverlauf für die letzten 90 Tage gefiltert nach Instance-Typ, Betriebssystem und Availability Zone anzeigen.

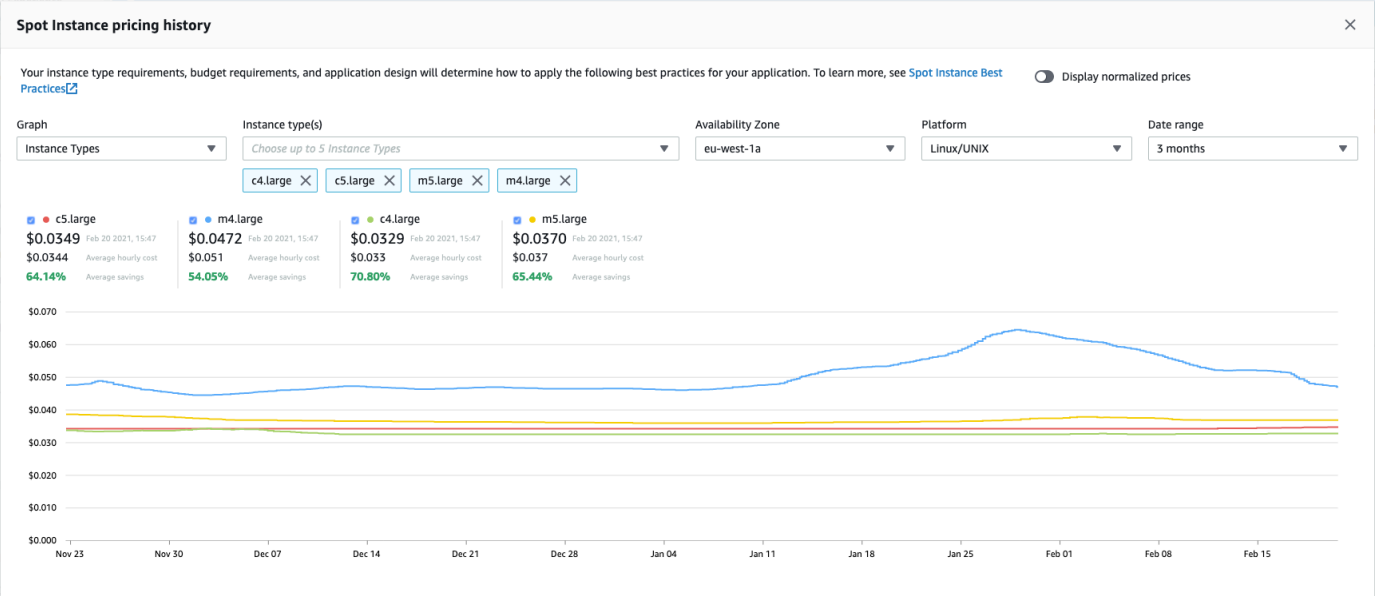
Anzeigen der aktuellen Spot-Preise

Die aktuellen Spot-Instance-Preise finden Sie im Abschnitt Preise für Amazon-EC2-Spot-Instances.

Um den Spot-Preisverlauf über die Konsole einzusehen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Pricing History (Preisverlauf) aus.
4. Vergleichen Sie für Graph (Diagramm) den Preisverlauf nach Availability Zones oder nach Instance-Typen.
   - Wenn Sie Availability Zones auswählen, wählen Sie anschließend Instance type (Instance-Typ), Betriebssystem (Platform) und Date range (Datumsbereich) aus, für die Sie den Preisverlauf anzeigen möchten.
   - Wenn Sie Instance Types (Instance-Typen) auswählen, wählen Sie anschließend bis zu fünf Instance type(s) (Instance-Typ(en)), Availability Zone, Betriebssystem (Platform) und Date range (Datumsbereich) aus, für die Sie den Preisverlauf anzeigen möchten.

   Der folgende Screenshot zeigt einen Preisvergleich für verschiedene Instance-Typen.



5. Bewegen Sie den Mauszeiger über das Diagramm, um die Preise zu bestimmten Zeiten im ausgewählten Datumsbereich anzuzeigen. Die Preise werden in den Informationsblöcken über dem Diagramm angezeigt. Der in der obersten Reihe angezeigte Preis zeigt den Preis an einem bestimmten Datum an. Der in der zweiten Zeile angezeigte Preis zeigt den Durchschnittspreis für den ausgewählten Datumsbereich.
6. Um den Preis pro vCPU anzuzeigen, schalten Sie Normalisierte Preise anzeigen ein. Um den Preis für den Instance-Typ anzuzeigen, deaktivieren Sie Normalisierte Preise anzeigen.

So zeigen Sie den Spot-Preisverlauf mithilfe der Befehlszeile an

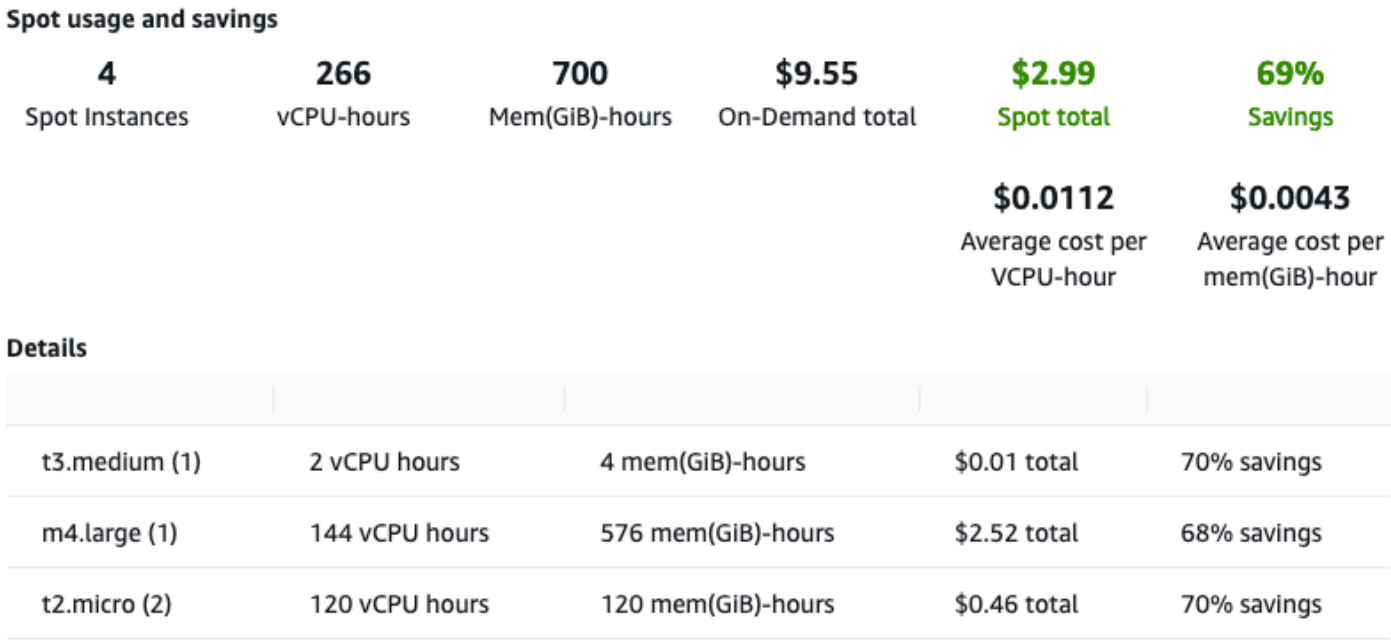
Verwenden Sie einen der folgenden Befehle. Weitere Informationen finden Sie unter Zugriff auf Amazon EC2.

- describe-spot-price-history (AWS CLI)
- Get-EC2SpotPriceHistory (AWS Tools for Windows PowerShell)

Einsparungen durch den Spot-Instances-Einkauf

Sie können die Nutzungs- und Einsparinformationen für Spot-Instances auf Flottenebene oder für alle laufenden Spot-Instances anzeigen. Auf der Ebene der einzelnen Flotten umfassen die Nutzungs- und Einsparungsinformationen alle Instances, die von der Flotte gestartet und beendet werden. Sie können diese Informationen aus der letzten Stunde oder den letzten drei Tagen anzeigen.

Der folgende Screenshot aus dem Abschnitt Einsparungen zeigt die Spot-Nutzungs- und Einsparungsinformationen für eine Spot-Flotte.



Sie können die folgenden Nutzungs- und Einsparungsinformationen anzeigen:

- Spot-Instances: Die Anzahl der Spot-Instances, die von der Spot-Flotte gestartet und beendet wurden. Wenn Sie die Einsparungsübersicht anzeigen, stellt die Zahl alle Ihre laufenden Spot-Instances dar.
- vCPU-hours (vCPU-Stunden) – Die Anzahl der vCPU-Stunden, die über alle Spot-Instances für den ausgewählten Zeitraum hinweg verbraucht werden.
- Mem(GiB)-hours (Mem(GiB)-Stunden) – Die Anzahl der GiB-Stunden, die über alle Spot-Instances für den ausgewählten Zeitraum hinweg verbraucht werden.
- On-Demand total (On-Demand gesamt) – Der Gesamtbetrag, den Sie für den ausgewählten Zeitraum bezahlt hätten, wenn Sie diese Instances mit On-Demand-Instances gestartet hätten.
- Spot total (Spot gesamt) – Der zu zahlende Gesamtbetrag für den gewählten Zeitraum.
- Savings (Einsparungen) – Der Prozentsatz, den Sie sparen, indem Sie den On-Demand-Preis nicht zahlen.
- Average cost per vCPU-hour (Durchschnittskosten pro vCPU-Stunde) – Die durchschnittlichen Kosten pro Stunde für die Nutzung der vCPUs über alle Spot-Instances für den ausgewählten

Zeitraum, berechnet wie folgt: Durchschnittskosten pro vCPU-Stunde = Spot gesamt / vCPU-Stunden.

- Durchschnittliche Kosten pro Mem-Stunde (GiB) — Die durchschnittlichen stündlichen Kosten für die GiBs Nutzung aller Spot-Instances für den ausgewählten Zeitraum, berechnet wie folgt: Durchschnittliche Kosten pro Mem-Stunde (GiB) = Spot-Gesamtwert/Mem (GiB) -Stunden.
- Details-Tabelle: Die verschiedenen Instance-Typen (die Anzahl der Instances pro Instance-Typ steht in Klammern), die die Spot-Flotte bilden. Wenn Sie die Einsparungsübersicht anzeigen, umfassen diese Ihre gesamten laufenden Spot-Instances.

Die Einsparungsinformationen können nur über die Amazon EC2-Konsole angezeigt werden.

So zeigen Sie die Einsparungsinformationen für eine Spot-Flotte mithilfe der Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie die ID einer Spot-Flotten-Anfrage aus und scrollen Sie zum Abschnitt Einsparungen.

   Aktivieren Sie alternativ das Kontrollkästchen neben der Spot-Flottenanforderungs-ID und wählen Sie die Registerkarte Einsparungen.
4. Standardmäßig werden auf der Seite Nutzungs- und Einsparungsinformationen für die letzten drei Tage angezeigt. Sie können last hour (letzte Stunde) oder last three days (letzten drei Tage) auswählen. Für Spot-Flotten, die vor weniger als einer Stunde gestartet wurden, zeigt die Seite die geschätzten Einsparungen für diese Stunde an.

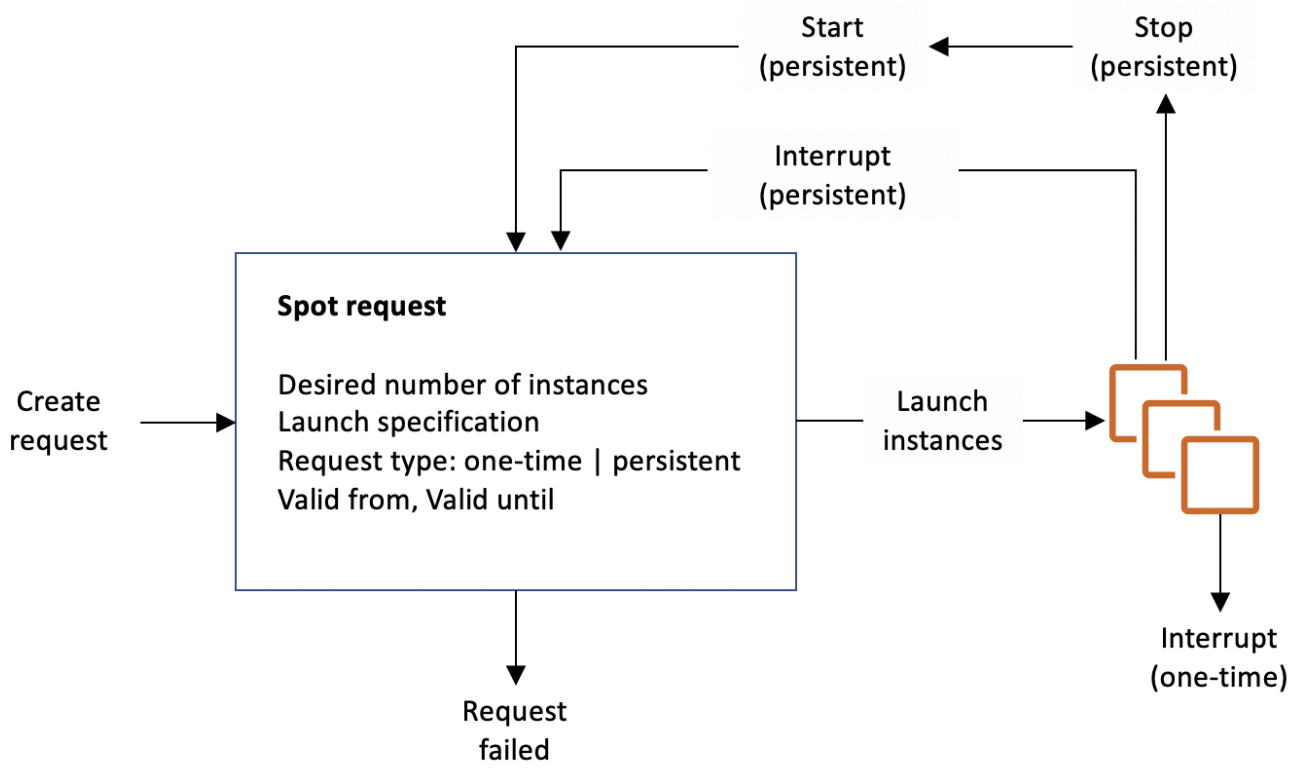
Um die Sparinformationen für alle laufenden Spot-Instances mithilfe der Konsole anzuzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Savings Summary (Einsparungsübersicht) aus.

Arbeiten mit Spot-Instances

Um Spot Instances zu verwenden, erstellen Sie eine Spot-Instance-Anforderung, die die gewünschte Anzahl von Instances, den Instance-Typ und die Availability Zone enthält. Wenn Kapazität verfügbar ist, erfüllt Amazon EC2 Ihre Anforderung sofort. Andernfalls wartet Amazon EC2, bis Ihre Anforderung erfüllt werden kann oder bis Sie die Anforderung abbrechen.

In der folgenden Abbildung ist die Arbeitsweise von Spot-Instance-Anforderungen dargestellt. Der Anforderungstyp (einmalig oder persistent) bestimmt, ob die Anforderung erneut geöffnet wird, wenn Amazon EC2 eine Spot-Instance unterbricht oder Sie eine Spot-Instance anhalten. Wenn die Anforderung persistent ist, wird sie nach der Unterbrechung Ihrer Spot-Instance erneut geöffnet. Wenn die Anforderung persistent ist und Sie die Spot-Instance anhalten, wird die Anforderung erst geöffnet, nachdem Sie die Spot-Instance gestartet haben.



Inhalt

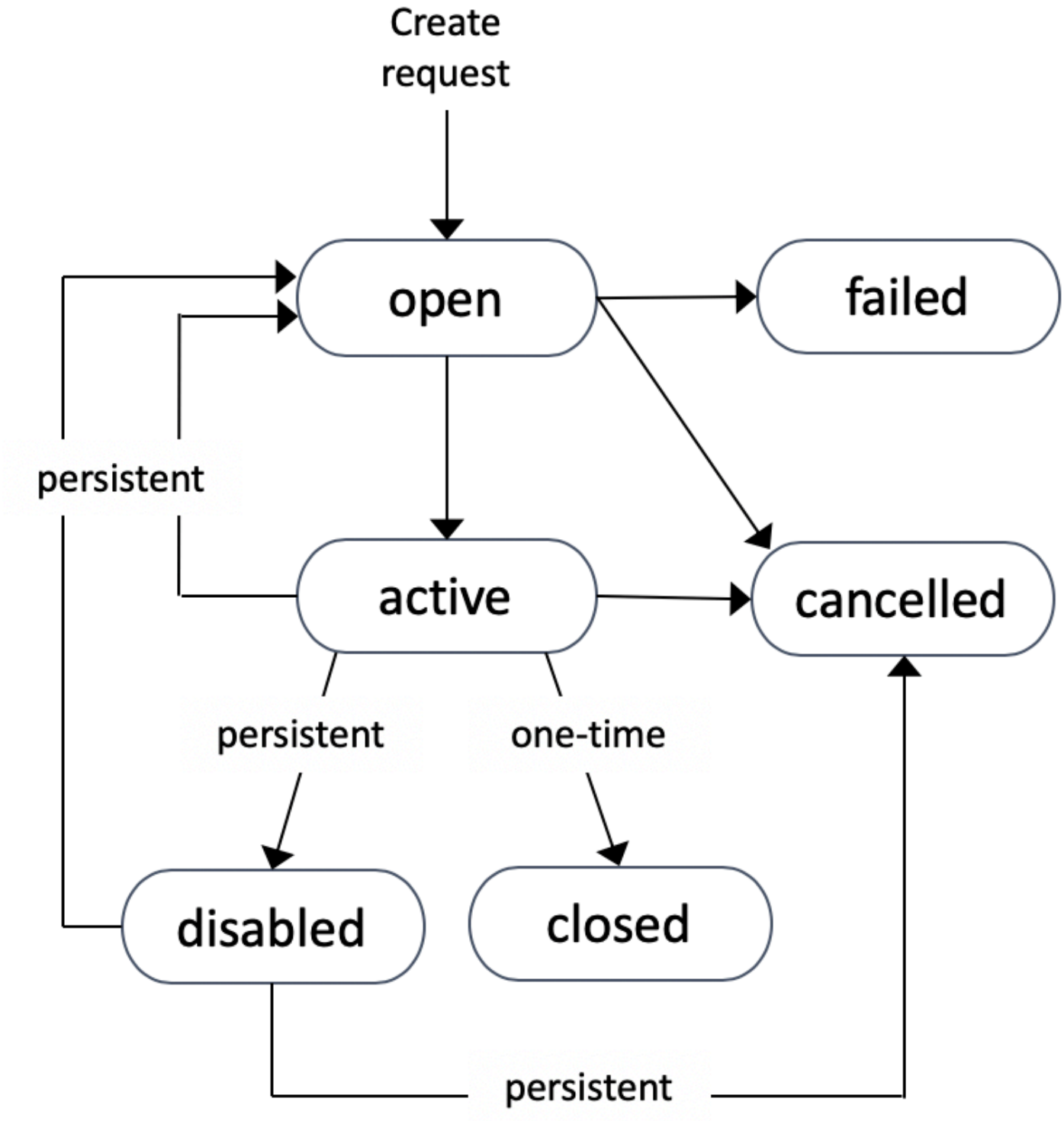
- Starten einer Spot-Instance
- Beenden einer Spot-Instance
- Beispiel-Startspezifikationen für Spot-Instance-Anforderung

Zustand von Spot-Instance-Anforderungen

Eine Spot-Instance-Anforderung kann die folgenden Zustände aufweisen:

- `open`: Die Anforderung wartet darauf, erfüllt zu werden.
- `active`: Die Anforderung wurde erfüllt und ist mit einer Spot-Instance verknüpft.
- `failed`: Die Anforderung weist einen oder mehrere fehlerhafte Parameter auf.
- `closed`: Die Spot-Instance wurde unterbrochen oder beendet.
- `disabled`: Sie haben die Spot-Instance gestoppt.
- `cancelled`: Sie haben die Anforderung storniert oder die Anforderung ist abgelaufen.

Die folgende Abbildung stellt die Übergänge zwischen den Anforderungszuständen dar. Beachten Sie, dass die Übergänge vom Anforderungstyp (einmalig oder persistent) abhängen.



Eine einmalige Spot-Instance-Anforderung bleibt so lange aktiv, bis Amazon EC2 die Spot-Instance startet, die Anforderung abläuft oder Sie die Anforderung abbrechen. Wenn keine Kapazität verfügbar ist, wird Ihre Spot Instance beendet und die Spot-Instance-Anforderung geschlossen.

Eine persistente Spot-Instance-Anforderung bleibt so lange aktiv, bis sie abläuft oder abgebrochen wird, selbst wenn die Anforderung erfüllt wird. Wenn keine Kapazität verfügbar ist, wird Ihre Spot Instance unterbrochen. Nach einer Unterbrechung Ihrer Instance wird die Spot Instance gestartet, wenn sie angehalten wurde oder wieder aufgenommen, wenn sie sich im Ruhezustand befindet. Sie können eine Spot Instance anhalten und erneut starten, wenn die Kapazität verfügbar ist. Wenn die Spot-Instance beendet wird (unabhängig davon, ob die Spot-Instance angehalten ist oder läuft), wird die Spot-Instance-Anforderung erneut geöffnet und Amazon EC2 startet eine neue Spot-Instance. Weitere Informationen finden Sie unter Anhalten einer Spot-Instance, Starten einer Spot-Instance und Beenden einer Spot-Instance.

Sie können den Status Ihrer Spot-Instance-Anforderungen sowie den Status der gestarteten Spot-Instances über den Status nachverfolgen. Weitere Informationen finden Sie unter Spot-Anforderungsstatus.

Angeben einer Tenancy für Ihre Spot-Instances

Spot-Instances können auf Single-Tenant-Hardware ausgeführt werden. Dedizierte Spot-Instances sind physisch von Instances isoliert, die zu anderen AWS Konten gehören. Weitere Informationen finden Sie unter Dedicated Instances und auf der Produktseite Amazon EC2 – Dedicated Instances.

Führen Sie einen der folgenden Schritte aus, um eine Dedicated-Spot-Instance auszuführen:

- Geben Sie beim Erstellen der Spot-Instance-Anforderung eine `dedicated`-Tenancy an. Weitere Informationen finden Sie unter Erstellt eine Spot-Instance-Anforderung.
- Fordern Sie eine Spot-Instance in einer VPC mit einer `dedicated`-Instance-Tenancy an. Weitere Informationen finden Sie unter Erstellen einer VPC mit einer Dedicated-Instance-Tenancy. Sie können keine Spot-Instances mit der Tenancy `default` anfordern, wenn Sie diese in einer VPC mit der Instance-Tenancy `dedicated` anfordern.

Alle Instance-Familien unterstützen Dedicated Spot-Instances außer T-Instances. Für jede unterstützte Instance-Familie unterstützt nur die größte Instance-Größe oder Metallgröße Dedicated Spot-Instances.

Serviceverknüpfte Rolle für Spot-Instance-Anforderungen

Amazon EC2 nutzt serviceverknüpfte Rollen für die Berechtigungen, die für den Aufruf anderer AWS -Services in Ihrem Namen benötigt werden. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit einem AWS Service verknüpft ist. Mit Diensten verknüpfte Rollen bieten eine sichere Möglichkeit, Berechtigungen an AWS Dienste zu delegieren, da nur der verknüpfte Dienst

eine dienstbezogene Rolle übernehmen kann. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im IAM-Benutzerhandbuch.

Amazon EC2 verwendet die angegebene serviceverknüpfte Rolle AWSServiceRoleForEC2Spot, um Spot-Instances in Ihrem Namen zu starten und zu verwalten.

Berechtigungen vonAWSServiceRoleForEC2Spot

Amazon EC2 verwendet AWSServiceRoleForEC2Spot, um die folgenden Aktionen durchzuführen:

- `ec2:DescribeInstances`: Spot-Instances beschreiben
- `ec2:StopInstances`: Spot-Instances stoppen
- `ec2:StartInstances`: Spot-Instances starten

Erstellen der serviceverknüpften Rolle

Größtenteils müssen Sie die serviceverknüpfte Rolle nicht manuell erstellen. Amazon EC2 erstellt die AWSServiceRoleForEC2Spotserviceverknüpfte Rolle, wenn Sie zum ersten Mal eine Spot-Instance über die Konsole anfordern.

Wenn Sie vor Oktober 2017, als Amazon EC2 begann, diese serviceverknüpfte Rolle zu unterstützen, eine aktive Spot-Instance-Anfrage hatten, hat Amazon EC2 die AWSServiceRoleForEC2SpotRolle in Ihrem Konto erstellt. AWS Weitere Informationen finden Sie unter In meinem Konto wird eine neue Rolle angezeigt im IAM-Benutzerhandbuch.

Wenn Sie die AWS CLI oder eine API verwenden, um eine Spot-Instance anzufordern, müssen Sie zunächst sicherstellen, dass diese Rolle existiert.

So erstellen Sie eine AWSServiceRoleForEC2Spot mithilfe der Konsole:

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rolle) aus.
3. Wählen Sie Create role (Rolle erstellen) aus.
4. Wählen Sie auf der Seite Select type of trusted entity (Auswahl des Typs der vertrauenswürdigen Entität) nacheinander EC2, EC2 - Spot Instances (EC2 – Spot-Instances) und Next: Permissions (Weiter: Berechtigungen) aus.
5. Klicken Sie auf der nächsten Seite auf Next: Review (Nächster Schritt: Prüfen).
6. Wählen Sie auf der Seite Review (Prüfen) Create role (Rolle erstellen) aus.

Um AWSServiceRoleForEC2Spotmit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-service-linked-role wie folgt.

```
aws iam create-service-linked-role --aws-service-name spot.amazonaws.com
```

Wenn Sie Spot-Instances nicht mehr verwenden müssen, empfehlen wir Ihnen, die AWSServiceRoleForEC2SpotRolle zu löschen. Wenn diese Rolle in Ihrem Konto gelöscht wurde, erstellt Amazon EC2 die Rolle erneut, sobald Sie Spot-Instances anfordern.

Gewähren von Zugriff auf von Kunden verwaltete Schlüssel zur Verwendung mit verschlüsselten AMIs und EBS-Snapshots

Wenn Sie ein verschlüsseltes AMI oder einen verschlüsselten Amazon EBS-Snapshot für Ihre Spot-Instances angeben und einen vom Kunden verwalteten Schlüssel für die Verschlüsselung verwenden, müssen Sie der AWSServiceRoleForEC2SpotRolle die Berechtigung zur Verwendung des vom Kunden verwalteten Schlüssels erteilen, damit Amazon EC2 Spot-Instances in Ihrem Namen starten kann. Dazu müssen Sie dem vom Kunden verwalteten Schlüssel eine Erteilung hinzufügen, wie im Folgenden gezeigt:

Bei der Einrichtung von Berechtigungen ist die Erteilung von Berechtigung eine Alternative zu Schüsselrichtlinien. Weitere Informationen finden Sie unter Verwenden von Erteilungen und Verwenden von Schlüsselrichtlinien in AWS KMS im Developer-Handbuch für AWS Key Management Service .

So gewähren Sie der Rolle AWSServiceRoleForEC2Spot-Berechtigungen zum Verwenden des vom Kunden verwalteten Schlüssels:

- Verwenden Sie den Befehl create-grant, um dem vom Kunden verwalteten Schlüssel einen Grant hinzuzufügen und den Principal (die mit dem AWSServiceRoleForEC2SpotService verknüpfte Rolle) anzugeben, dem die Berechtigung zur Ausführung der durch die Gewährung erlaubten Operationen erteilt wird. Der vom Kunden verwaltete Schlüssel wird durch den `key-id`-Parameter und den ARN des vom Kunden verwalteten Schlüssels angegeben. Der Principal wird durch den `grantee-principal` Parameter und den ARN der AWSServiceRoleForEC2Spotdienstverknüpften Rolle angegeben.

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
  ```

```
    --grantee-principal arn:aws:iam::111122223333:role/aws-service-role/
spot.amazonaws.com/AWSServiceRoleForEC2Spot \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Erstellt eine Spot-Instance-Anforderung

Sie können den Launch-Instance-Assistenten in der Amazon EC2 EC2-Konsole oder den AWS CLI Befehl run-instances verwenden, um eine Spot-Instance auf die gleiche Weise anzufordern, wie Sie eine On-Demand-Instance starten können. Diese Methode wird nur aus folgenden Gründen empfohlen:

- Sie verwenden bereits den Launch Instance Wizard oder den run-instances-Befehl, um On-Demand-Instances zu launchen, und Sie möchten einfach zum Launchen von Spot Instances wechseln, indem Sie einen einzelnen Parameter ändern.
- Sie benötigen nicht mehrere Instances mit verschiedenen Instance-Typen.

Diese Methode wird im Allgemeinen nicht zum Launchen von Spot Instances empfohlen, da Sie nicht mehrere Instance-Typen angeben können und Spot Instances und On-Demand-Instances nicht in derselben Anforderung launchen können. Für die bevorzugten Methoden zum Starten von Spot Instances, darunter das Starten einer Flotte einschließlich Spot Instances und On-Demand-Instances mit mehreren Instance-Typen finden Sie unter Was ist die beste Spot-Request-Methode?

Wenn Sie mehrere Spot-Instances gleichzeitig anfordern, erstellt Amazon EC2 separate Spot-Instance-Anforderungen, sodass Sie den Status der einzelnen Anforderungen separat nachverfolgen können. Weitere Informationen zum Nachverfolgen von Spot-Instance-Anforderungen finden Sie unter Spot-Anforderungsstatus.

New console

So erstellen Sie eine Spot-Instance-Anforderung mit dem Launch Instance Wizard

Die Schritte 1 bis 9 sind die gleichen Schritte, die Sie zum Launchen einer On-Demand-Instance verwenden würden. In Schritt 10 konfigurieren Sie die Spot-Instance-Anforderung.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste oben auf dem Bildschirm eine Region aus.

3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.
4. (Optional) Unter Name and Tags (Name und Tags) können Sie Ihre Instance benennen und die Spot-Instance-Anforderung, die Instance, die Volumes und die elastischen Grafiken markieren. Informationen zu Tags siehe Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

   a. Geben Sie unter Name einen beschreibenden Namen für Ihre Instance ein.

      Der Instance-Name ist ein Tag, wobei der Schlüssel Name ist und es sich bei dem Wert um den von Ihnen angegebenen Namen handelt. Wenn Sie keinen Namen angeben, kann die Instance anhand der ID identifiziert werden, die beim Starten der Instance automatisch generiert wird.

   b. Um die Spot-Instance-Anforderung, die Instance, die Volumes und die elastischen Grafiken zu markieren, wählen Sie Add additional tags (Zusätzliche Tags hinzufügen) aus. Klicken Sie auf Tag hinzufügen, geben Sie dann einen Schlüssel und einen Wert ein und wählen Sie den Ressourcentyp aus, den Sie markieren möchten. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.
5. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) das Betriebssystem (OS) für Ihre Instance aus und wählen Sie dann eine AMI aus. Weitere Informationen finden Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image).
6. Wählen Sie unter Instance type (Instance-Typ) den Instance-Typ aus, der Ihren Anforderungen für die Hardware-Konfiguration und Größe Ihrer Instance entspricht. Weitere Informationen finden Sie unter Instance-Typ.
7. Wählen Sie unter Key pair (login) (Schlüsselpaar (Login) ein vorhandenes Schlüsselpaar aus oder wählen Sie Create new key pair (Neues Schlüsselpaar erstellen), um ein neues zu erstellen. Weitere Informationen finden Sie unter Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances.

> **Important**
>
> Wenn Sie die Option Proceed without key pair (Not recommended) (Ohne Schlüsselpaar fortfahren (Nicht empfohlen)) auswählen, können Sie keine Verbindung zur Instance herstellen, es sei denn, Sie wählen ein AMI aus, das entsprechend konfiguriert ist, um Benutzern eine andere Anmeldemöglichkeit zu erlauben.

8. Verwenden Sie unter Network settings (Netzwerkeinstellungen) die Standardeinstellungen oder wählen Sie Edit (Bearbeiten), um die Netzwerkeinstellungen nach Bedarf zu konfigurieren.

   Sicherheitsgruppen sind Teil der Netzwerkeinstellungen und definieren Firewall-Regeln für Ihre Instance. Diese Regeln legen fest, welcher eingehende Netzwerkverkehr an Ihre Instance übertragen wird.

   Weitere Informationen finden Sie unter Network settings (Netzwerkeinstellungen).

9. Die von Ihnen ausgewählte AMI beinhaltet ein oder mehrere Speicher-Volumes, einschließlich eines Root-Gerät-Volumes. Unter Configure Storage (Speicher konfigurieren) können Sie zusätzliche Volumes angeben, die der Instance angefügt werden, indem Sie Add New Volume (Neues Volume hinzufügen) auswählen. Weitere Informationen finden Sie unter Speicher konfigurieren.

10. Unter Advanced details (Erweiterte Details) konfigurieren Sie die Spot-Instance-Anforderung wie folgt:

    a. Unter Purchasing option (Kaufoption) wählen Sie das Kontrollkästchen Request Spot Instances (Spot Instances anfordern).

    b. Sie können entweder die Standardkonfiguration für die Spot-Instance-Anforderung beibehalten oder Customize (Anpassen) rechts auswählen, um benutzerdefinierte Einstellungen für Ihre Spot-Instance-Anfrage festzulegen.

       Wenn Sie Customize (Anpassen) wählen, werden die folgenden Felder angezeigt.

       i. Maximum price (Maximaler Preis): Sie können Spot Instances zum Spot-Preis anfordern, der auf den On-Demand-Preis begrenzt ist oder den Höchstbetrag angeben, den Sie zu zahlen bereit sind.

          > **Warning**
          >
          > Wenn Sie einen Höchstpreis angeben, werden Ihre Instances häufiger unterbrochen, als wenn Sie No maximum price (Kein Höchstpreis) auswählen.

- No maximum price (Kein maximaler Preis): Ihre Spot Instance wird zum aktuellen Spot-Preis gestartet. Der Preis wird niemals den On-Demand-Preis überschreiten. (Empfohlen)
- Set your maximum price (per instance/hour) (Festlegen Ihres Höchstpreises (pro Instance/Stunde)): Sie können den Höchstbetrag angeben, den Sie zahlen möchten.
  - Wenn Sie einen Höchstpreis angeben, der unter dem aktuellen Spot-Preis liegt, wird Ihre Spot Instance nicht gestartet.
  - Wenn Sie einen Höchstpreis angeben, der über dem aktuellen Spot-Preis liegt, wird Ihre Spot Instance zum aktuellen Spot-Preis gelauncht und berechnet. Wenn Ihre Spot Instance ausgeführt wird und der Spot-Preis über Ihren Höchstpreis steigt, unterbricht Amazon EC2 Ihre Spot Instance.
  - Unabhängig vom Höchstpreis, den Sie angeben, wird Ihnen immer der aktuelle Spot-Preis in Rechnung gestellt.

  Informationen zu den Entwicklungen der Spot-Preise finden Sie unter Spot-Instance-Preisverlauf.

ii. Request type (Typ der Anforderung): Der von Ihnen gewählte Spot-Instance-Anforderungstyp bestimmt, was passiert, wenn Ihre Spot Instance unterbrochen wird.

- One-time (Einmalig): Amazon EC2 stellt eine einmalige Anfrage für Ihre Spot Instance. Wenn Ihre Spot Instance unterbrochen wird, wird die Anforderung nicht erneut gesendet.
- Persistent request (Persistente Anforderung): Amazon EC2 stellt eine dauerhafte Anfrage für Ihre Spot Instance. Wenn Ihre Spot Instance unterbrochen wird, wird sie erneut übermittelt, um die unterbrochene Spot Instance aufzufüllen.

Wenn Sie keinen Wert angeben, handelt es sich standardmäßig um eine einmalige Anforderung.

iii. Valid to (Gültig bis): Das Ablaufdatum einer persistenten Spot-Instance-Anforderung.

Dieses Feld wird für einmalige Anforderungen nicht unterstützt. Eine one-time-Anfrage bleibt so lange aktiv, bis alle Instances startet, die Anfrage abläuft oder Sie die Anfrage abbrechen.

- No request expiry date (Kein Ablaufdatum der Anforderung): Die Anforderung bleibt so lange aktiv, bis Sie sie abbrechen.
- Set your request expiry date (Festlegen eines Ablaufdatums für die Anforderung): Die dauerhafte Anforderung bleibt bis zu dem von Ihnen angegebenen Datum oder bis zum Abbruch aktiv.

iv. Interruption behavior (Verhalten bei Unterbrechungen): Das von Ihnen gewählte Verhalten bestimmt, was passiert, wenn eine Spot Instance unterbrochen wird.

- Gültige Werte für persistente Anforderungen sind Stop (Anhalten) und Hibernate (Ruhezustand). Wenn eine Instance angehalten wird, fallen Gebühren für EBS-Volume-Speicher an.

> **Note**
>
> Spot Instances nutzen jetzt die gleiche Ruhezustandsfunktion wie On-Demand-Instances. Um den Ruhezustand zu aktivieren, können Sie entweder hier Ruhezustand auswählen oder Aktivieren aus dem Feld Stopp – Ruhezustand auswählen, das weiter unten im Launch Instance Wizard angezeigt wird. Informationen zu den Voraussetzungen für den Ruhezustand finden Sie unter Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance.

- Für einmalige Anforderungen ist nur Terminate (Beenden) gültig.

Wenn Sie keinen Wert angeben, ist der Standard Terminate (Beenden), was für eine dauerhafte Spot-Instance-Anforderung nicht gültig ist. Wenn Sie den Standardwert beibehalten und versuchen, eine dauerhafte Spot-Instance-Anfrage zu starten, wird eine Fehlermeldung angezeigt.

Weitere Informationen finden Sie unter Verhalten von Spot-Instance-Unterbrechungen.

11. Geben Sie im Bereich Summary (Zusammenfassung) für Number of Instances (Anzahl der Instances) die Anzahl der Instances ein, die gelauncht werden sollen.

    > **Note**
    >
    > Amazon EC2 erstellt eine separate Anforderung für jede Spot-Instance.

12. Überprüfen Sie im Übersichts-Bereich die Details Ihrer Instance und nehmen Sie ggf. Änderungen vor. Nachdem Sie Ihre Spot-Instance-Anforderung übermittelt haben, können Sie die Parameter der Anforderung nicht mehr ändern. Sie können direkt zu einem Abschnitt im Launch Instance Wizard navigieren, indem Sie den entsprechenden Link im Übersichts-Bereich auswählen. Weitere Informationen finden Sie unter Übersicht.
13. Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Instance starten aus.

    Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Old console

So erstellen Sie eine Spot-Instance-Anforderung mit dem Launch Instance Wizard

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste oben auf dem Bildschirm eine Region aus.
3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Launch Instance aus.
4. Wählen Sie auf der Seite Choose an Amazon Machine Image (AMI) (AMI auswählen) ein AMI aus. Weitere Informationen finden Sie unter Schritt 1: Auswählen eines Amazon Machine Images (AMI).
5. Wählen Sie auf der Seite Choose an Instance Type (Instance-Typ auswählen) die Hardwarekonfiguration und -größe der zu launchenden Instance und dann Next: Configure Instance Details (Weiter: Instance-Details konfigurieren) aus. Weitere Informationen finden Sie unter Schritt 2: Auswählen eines Instance-Typs.
6. Konfigurieren Sie die Spot-Instance-Anforderung auf der Seite Configure Instance Details (Instance-Details konfigurieren) wie folgt:

    - Number of instances: Geben Sie die Anzahl der Instances ein, die gestartet werden sollen.

> **Note**
>
> Amazon EC2 erstellt eine separate Anforderung für jede Spot-Instance.

- (Optional) Damit sichergestellt wird, dass Sie die richtige Zahl an Instances haben, um den Bedarf Ihre Anwendung zu verarbeiten, können Sie die Option Launch into Auto Scaling Group auswählen, um eine Startkonfiguration und eine Auto Scaling-Gruppe zu erstellen. Auto Scaling skaliert die Anzahl der Instances in der Gruppe entsprechend Ihren Spezifikationen. Weitere Informationen hierzu finden Sie unter Amazon EC2 Auto Scaling-Benutzerhandbuch.
- Purchasing option: Wählen Sie Request Spot instances (Spot-Instances anfordern) aus, um eine Spot-Instance zu starten. Wenn Sie diese Option wählen, werden die folgenden Felder angezeigt.
- Current price (Aktueller Preis): Der aktuelle Spot-Preis in jeder Availability Zone wird für den ausgewählten Instance-Typ angezeigt.
- (Optional) Maximum price (Höchstpreis): Sie können das Feld leer lassen oder den Höchstbetrag angeben, den Sie zu zahlen bereit sind.

> **Warning**
>
> Wenn Sie einen Höchstpreis angeben, werden Ihre Instances häufiger unterbrochen, als wenn Sie das Feld leer lassen.

  - Wenn Sie einen Höchstpreis angeben, der unter dem Spot-Preis liegt, wird Ihre Spot Instance nicht gelauncht.
  - Wenn Sie einen Höchstpreis angeben, der über dem aktuellen Spot-Preis liegt, wird Ihre Spot Instance zum aktuellen Spot-Preis gelauncht und berechnet. Wenn Ihre Spot Instance ausgeführt wird und der Spot-Preis über Ihren Höchstpreis steigt, unterbricht Amazon EC2 Ihre Spot Instance.
  - Unabhängig vom Höchstpreis, den Sie angeben, wird Ihnen immer der aktuelle Spotpreis berechnet.
  - Wenn Sie das Feld leer lassen, zahlen Sie den aktuellen Spot-Preis.
- Persistente Anforderung: Wählen Sie Persistente Anforderung, um die Spot-Instance-Anforderung erneut zu übermitteln, wenn Ihre Spot-Instance unterbrochen wird.

- Unterbrechungsverhalten: Standardmäßig beendet der Spot-Service eine Spot-Instance, wenn sie unterbrochen wird. Wenn Sie Persistente Anforderung auswählen, können Sie angeben, dass der Spot-Service Ihre Spot-Instance beendet oder in den Ruhezustand versetzt, wenn sie unterbrochen wird. Weitere Informationen finden Sie unter Verhalten von Spot-Instance-Unterbrechungen.
- (Optional) Request valid to (Anforderung gültig für): Wählen Sie Edit (Bearbeiten) um anzugeben, wann die Spot-Instance-Anforderung abläuft.

Weitere Informationen zum Konfigurieren von Spot-Instances finden Sie unter Schritt 3: Konfigurieren der Instance-Details.

7. Die von Ihnen ausgewählte AMI beinhaltet ein oder mehrere Speicher-Volumes, einschließlich eines Root-Gerät-Volumes. Auf der Seite Add Storage (Speicher hinzufügen) können Sie durch Auswahl von Add New Volume (Neues Volume hinzufügen) zusätzliche Volumes angeben, die der Instance zugeordnet werden. Weitere Informationen finden Sie unter Schritt 4: Hinzufügen von Speicher.
8. Legen Sie auf der Seite Add Tags die Tags (Markierungen) fest, indem Sie die Schlüssel- und Wert-Kombinationen angeben. Weitere Informationen finden Sie unter Schritt 5: Hinzufügen von Tags (Markierungen).
9. Verwenden Sie auf der Seite Configure Security Group eine Sicherheitsgruppe, um Firewall-Regeln für Ihre Instance zu definieren. Diese Regeln legen fest, welcher eingehende Netzwerkverkehr an Ihre Instance übertragen wird. Der gesamte übrige Datenverkehr wird ignoriert. (Weitere Informationen zu Sicherheitsgruppen finden Sie unter Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances.) Gehen Sie folgendermaßen vor, um eine Sicherheitsgruppe auszuwählen oder zu erstellen. Klicken Sie anschließend auf Review and Launch (Prüfen und Starten). Weitere Informationen finden Sie unter Schritt 6: Konfigurieren einer Sicherheitsgruppe.
10. Prüfen Sie auf der Seite Review Instance Launch die Details Ihrer Instance und nehmen Sie notwendige Änderungen vor, indem Sie den entsprechenden Edit-Link auswählen. Sobald Sie bereit sind, wählen Sie Launch aus. Weitere Informationen finden Sie unter Schritt 7: Prüfen des Instance-Starts und Auswahl des Schlüsselpaars.
11. Im Dialogfeld Select an existing key pair or create a new key pair (Ein bestehendes Schlüsselpaar wählen oder ein neues Schlüsselpaar erstellen) können Sie ein bestehendes Schlüsselpaar wählen oder ein neues erstellen. Wählen Sie beispielsweise Choose an existing key pair (Vorhandenes Schlüsselpaar auswählen) und wählen Sie dann das

Schlüsselpaar aus, das Sie beim Einrichten erstellt haben. Weitere Informationen finden Sie unter Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances.

> **Important**
>
> Wenn Sie die Option Proceed without key pair auswählen, können Sie keine Verbindung zur Instance herstellen, es sei denn, Sie wählen ein AMI aus, das so konfiguriert ist, dass Benutzern eine andere Anmeldemöglichkeit erlaubt ist.

12. Zum Starten Ihrer Instance aktivieren Sie das Bestätigungskontrollkästchen und wählen Sie dann Launch Instances aus.

    Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

AWS CLI

So erstellen Sie eine Spot-Instance-Anforderung mit run-instances

Verwenden Sie den Befehl run-instances und geben Sie die Spot-Instance-Optionen im `--instance-market-options`-Parameter an.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type t2.micro \
    --count 5 \
    --subnet-id subnet-08fc749671b2d077c \
    --key-name MyKeyPair \
    --security-group-ids sg-0b0384b66d7d692f9 \
    --instance-market-options file://spot-options.json
```

Nachfolgend finden Sie die Datenstruktur, die in der JSON-Datei für anzugeben is `--instance-market-options`. Sie können auch `ValidUntil` und `InstanceInterruptionBehavior` angeben. Wenn Sie kein Feld in der Datenstruktur angeben, wird der Standardwert verwendet.

Das folgende Beispiel erstellt eine `persistent`-Anforderung.

```
{
  "MarketType": "spot",
```

```
  "SpotOptions": {
    "SpotInstanceType": "persistent"
  }
}
```

So erstellen Sie eine Spot-Instance-Anforderung mit request-spot-instances

> **Note**
>
> Wir raten dringend davon ab, den request-spot-instances-Befehl zu verwenden, da es sich um eine Legacy-API ohne geplante Investition handelt. Weitere Informationen finden Sie unter Was ist die beste Spot-Request-Methode?

Verwenden Sie den Befehl request-spot-instances, um eine einmalige Anforderung zu erstellen:

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json
```

Verwenden Sie den Befehl request-spot-instances, um eine persistente Anforderung zu erstellen.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "persistent" \
    --launch-specification file://specification.json
```

Beispiel-Startkonfigurationsdateien, die mit diesen Befehlen verwendet werden können, finden Sie unter Beispiel-Startspezifikationen für Spot-Instance-Anforderung. Wenn Sie eine Launch-Spezifikations-Datei in der Spot-Requests-Konsole herunterladen, müssen Sie stattdessen den Befehl request-spot-fleet verwenden (die Konsole erstellt eine Spot-Instance-Anforderung mithilfe einer Spot-Flotte).

Finden Sie Ihre Spot-Instances

Amazon EC2 startet eine Spot Instance, wenn Kapazität verfügbar ist. Eine Spot-Instance wird so lange ausgeführt, bis sie entweder unterbrochen oder von Ihnen beendet wird.

Eine Spot-Instance wird zusammen mit On-Demand-Instances auf der Instance-Seite in der Konsole angezeigt. Gehen Sie wie folgt vor, um Ihre Spot-Instances zu finden.

Console

So finden Sie Ihre Spot-Instances mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Um alle Spot-Instances zu finden, wählen Sie im Suchbereich Instance lifelycle=spot aus.
4. Um zu überprüfen, ob es sich bei einer Instance um eine Spot-Instance handelt, wählen Sie die Instance aus, wählen Sie die Registerkarte Details und überprüfen Sie den Wert von Lifecycle. Der Wert für eine Spot-Instance ist `spot` und der Wert für eine On-Demand-Instance ist`normal`.

AWS CLI

Um Ihre Spot-Instances mit dem zu finden AWS CLI

Verwenden Sie den Befehl describe-instances mit der `--filters` Option.

```
aws ec2 describe-instances \
    --filters "Name=instance-lifecycle,Values=spot"
```

Um festzustellen, ob es sich bei einer Instance um eine Spot-Instance handelt

Verwenden Sie den Befehl describe-instances und verwenden Sie dabei die `--query` Option, um den Lebenszykluswert zu überprüfen.

```
aws ec2 describe-instances \
    --instance-ids i-0123a456700123456 \
    --query "Reservations[*].Instances[*].InstanceLifecycle" \
    --output text
```

Wenn die Ausgabe lautet`spot`, handelt es sich bei der Instance um eine Spot-Instance. Wenn keine Ausgabe erfolgt, handelt es sich bei der Instance um eine On-Demand-Instance.

Gehen Sie wie folgt vor, um die Spot-Instances zu finden, die über eine bestimmte Spot-Instance- oder Spot-Flotte-Anfrage gestartet wurden.

Console

So finden Sie mithilfe der Konsole die Spot-Instances für eine Anfrage

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus. Die Liste enthält sowohl Spot-Instance-Anfragen als auch Spot-Flottenanfragen.
3. Wenn eine Spot-Instance-Anfrage erfüllt wird, ist Capacity die ID der Spot-Instance. Bei einer Spot-Flotte zeigt Kapazität an, wie viel der angeforderten Kapazität erfüllt wurde. Sie können die IDs der Instances in einer Spot-Flotte anzeigen, indem Sie auf den Erweiterungspfeil klicken oder die Flotte und anschließend Instances auswählen.
4. Bei einer Spot-Flotte gibt Capacity an, wie viel der angeforderten Kapazität erfüllt ist. Um die IDs der Instances in einer Spot-Flotte anzuzeigen, wählen Sie die Flotten-ID aus, um die zugehörige Detailseite zu öffnen und den Bereich Instances zu suchen.

AWS CLI

Um die Spot-Instances für eine Anfrage zu finden, verwenden Sie AWS CLI

Verwenden Sie den Befehl describe-spot-instance-requests mit der Option. `--query`

```
aws ec2 describe-spot-instance-requests \
    --query "SpotInstanceRequests[*].{ID:InstanceId}"
```

Das Folgende ist Ausgabebeispiel:

```
[
    {
        "ID": "i-1234567890abcdef0"
    },
    {
        "ID": "i-0598c7d356eba48d7"
    }
]
```

Spot-Instance-Anforderungen markieren

Um die Kategorisierung und Verwaltung Ihrer Spot-Instance-Anforderungen zu vereinfachen, können Sie sie mit benutzerdefinierten Metadaten markieren. Sie können einer Spot-Instance-Anforderung

beim Erstellen oder danach einen Tag (Markierung) zuweisen. Sie können Tags (Markierungen) über die Amazon EC2-Konsole oder ein Befehlszeilen-Tool zuweisen.

Wenn Sie eine Spot-Instance-Anforderung markieren, werden die Instances und Volumes, die von der Spot-Instance-Anforderung gestartet werden, nicht automatisch markiert. Sie müssen die von der Spot-Instance-Anforderungen gestarteten Instances und Volumes explizit markieren. Sie können ein Tag (Markierung) zu einer Spot-Instance und Volumes während des Starts oder danach zuweisen.

Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

Inhalt

Voraussetzungen

Gewähren Sie dem Benutzer die Berechtigung zum Markieren von Ressourcen. Weitere Informationen zu IAM-Richtlinien und Beispielrichtlinien finden Sie unter Beispiel: Markieren von Ressourcen.

Die von Ihnen erstellte IAM-Richtlinie wird anhand der Methode bestimmt, mit der Sie eine Spot-Instance-Anforderung erstellen.

- Wenn Sie den Launch Instance Wizard oder `run-instances` zum Anfordern von Spot-Instances verwenden, finden Sie weitere Informationen unter To grant a user the permission to tag resources when using the launch instance wizard or run-instances.
- Wenn Sie den `request-spot-instances`-Befehl verwenden, um Spot-Instances anzufordern, lesen Sie To grant a user the permission to tag resources when using request-spot-instances.

So gewähren Sie einem Benutzer die Berechtigung, Ressourcen zu markieren, wenn er den Launch Instance Wizard oder zum Ausführen von Instances verwendet

Erstellen Sie eine IAM-Richtlinie, die Folgendes beinhaltet:

- Die Aktion `ec2:RunInstances`. Dadurch wird dem Benutzer die Berechtigung zum Starten einer Instance gewährt.
- Legen Sie für `Resource` die Option `spot-instances-request` fest. Auf diese Weise können Benutzer Spot-Instance-Anforderungen erstellen, die Spot-Instances anfordern.
- Die Aktion `ec2:CreateTags`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen von Tags.
- Legen Sie für `Resource` die Option `*` fest. Auf diese Weise können Benutzer alle Ressourcen markieren, die während des Instance-Starts erstellt werden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowLaunchInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagSpotInstanceRequests",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Wenn Sie die RunInstances Aktion verwenden, um Spot-Instance-Anfragen zu erstellen und die Spot-Instance-Anfragen bei der Erstellung zu taggen, müssen Sie wissen, wie Amazon EC2 die `spot-`

`instances-request` Ressource in der RunInstances Anweisung bewertet, sie wird in der IAM-Richtlinie wie folgt bewertet:

- Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung nicht taggen, bewertet Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung nicht.
- Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung taggen, bewertet Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung.

Daher gelten für die `spot-instances-request`-Ressource die folgenden Regeln für die IAM-Richtlinie:

- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und nicht beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource nicht explizit zulassen. Der Aufruf ist erfolgreich.
- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource in die RunInstances Allow-Anweisung aufnehmen, andernfalls schlägt der Aufruf fehl.
- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource angeben oder einen * Platzhalter in der Allow-Anweisung CreateTags angeben, andernfalls schlägt der Aufruf fehl.

Beispiele für IAM-Richtlinien, einschließlich Richtlinien, die für Spot-Instance-Anforderungen nicht unterstützt werden, finden Sie unter Arbeiten mit Spot-Instances.

So gewähren Sie einem Benutzer die Berechtigung, Ressourcen bei Verwendung von Anfrage-Spot-Instances zu markieren

Erstellen Sie eine IAM-Richtlinie, die Folgendes beinhaltet:

- Die Aktion `ec2:RequestSpotInstances`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen einer Spot-Instance-Anforderung.
- Die Aktion `ec2:CreateTags`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen von Tags.
- Legen Sie für `Resource` die Option `spot-instances-request` fest. Auf diese Weise können Benutzer nur die Spot-Instance-Anforderung markieren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotInstanceRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:RequestSpotInstances",
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-instances-request/*"
}
```

Neue Spot-Instance-Anforderung markieren

Console

So markieren Sie eine neue Spot-Instance-Anforderung mithilfe der Konsole:

1. Folgen Sie dem Verfahren unter Erstellt eine Spot-Instance-Anforderung.
2. Um ein Tags (Markierungen) hinzuzufügen, wählen Sie auf der Seite Add Tags (Tags (Markierungen) hinzufügen) die Option Add Tags (Tags (Markierungen) hinzufügen) und geben Sie den Schlüssel und den Wert für den Tag (Markierung) ein. Wählen Sie für jedes weitere Tags (Markierungen) Add another Tag (Weiteren Tag (Markierungen) hinzufügen) .

   Für jeden Tag (Markierung) können Sie die Spot-Instance-Anforderung, die Spot-Instances und die Volumes mit demselben Tag (Markierung) markieren. Um alle drei zu markieren, stellen Sie sicher, dass Instances , Volumes und Spot-Instance-Anforderungen ausgewählt sind. Wenn Sie nur ein oder zwei mit Tags (Markierungen) markieren möchten, stellen Sie sicher, dass die Ressourcen, die Sie markieren möchten, ausgewählt sind und die anderen Ressourcen gelöscht wurden.
3. Füllen Sie die erforderlichen Felder aus, um eine Spot-Instance-Anforderung zu erstellen, und wählen Sie dann Launch (Starten) aus. Weitere Informationen finden Sie unter Erstellt eine Spot-Instance-Anforderung.

AWS CLI

Um eine neue Spot-Instance-Anfrage zu taggen, verwenden Sie AWS CLI

Um eine Spot-Instance-Anforderung bei der Erstellung zu markieren, konfigurieren Sie die Spot-Instance-Anforderungskonfiguration wie folgt:

- Geben Sie die Tags (Markierungen) für die Spot-Instance-Anforderung mithilfe des Parameters `--tag-specification`an.
- Legen Sie für `ResourceType` die Option `spot-instances-request` fest. Wenn Sie einen anderen Wert angeben, schlägt die Spot-Instance-Anforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

Im folgenden Beispiel wird die Spot-Instance-Anforderung mit zwei Tags (Markierungen) markiert: Key=Environment und Value=Production sowie Key=Cost-Center und Value=123.

```
aws ec2 request-spot-instances \
    --instance-count 5 \
    --type "one-time" \
    --launch-specification file://specification.json \
    --tag-specification 'ResourceType=spot-instances-
request,Tags=[{Key=Environment,Value=Production},{Key=Cost-Center,Value=123}]'
```

So markieren Sie eine vorhandene Spot-Instance-Anforderung:

Console

So markieren Sie eine bestehende Spot-Instance-Anforderung mithilfe der Konsole:

Nachdem Sie eine Spot-Instance-Anforderung erstellt haben, können Sie der Spot-Instance-Anforderung mithilfe der Konsole Tags (Markierungen) hinzufügen.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Instance-Anforderung aus.
4. Wählen Sie die Registerkarte Tags (Markierungen), und wählen Sie Create Tags (Tags (Markierungen) erstellen).

So markieren Sie eine bestehende Spot-Instance-Anforderung mithilfe der Konsole:

Nachdem Ihre Spot-Instance-Anforderung Ihre Spot-Instance gestartet hat, können Sie der Instance mithilfe der Konsole Tags (Markierungen) hinzufügen. Weitere Informationen finden Sie unter Hinzufügen und Löschen von Tags (Markierungen) für einzelne Ressourcen.

AWS CLI

Um eine bestehende Spot-Instance-Anfrage oder Spot-Instance mit dem zu taggen AWS CLI

Verwenden Sie den Befehl create-tags, um vorhandene Ressourcen zu markieren. Im folgenden Beispiel werden die vorhandene Spot-Instance-Anforderung und die Spot-Instance mit Key=purpose und Value=test markiert.

```
aws ec2 create-tags \
    --resources sir-08b93456 i-1234567890abcdef0 \
    --tags Key=purpose,Value=test
```

Anzeigen von Anforderungs-Tags (Markierungen) der Spot-Instance

Console

So sehen Sie eine Spot-Instance-Anforderung mithilfe der Konsole an:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Instance-Anforderung und dann die Registerkarte Tags aus.

AWS CLI

So beschreiben Sie Anforderungs-Tags (Markierungen) der Spot-Instance:

Sie können die Tags einer Spot-Instance-Anfrage anzeigen, indem Sie die Spot-Instance-Anfrage beschreiben. Verwenden Sie den Befehl describe-spot-fleet-requests, um die Konfiguration der angegebenen Spot-Instance-Anforderung anzuzeigen, die alle Tags enthält, die für die Anforderung angegeben wurden.

```
aws ec2 describe-spot-instance-requests \
    --spot-instance-request-ids sir-EXAMPLE1 \
```

```
    --query "SpotInstanceRequests[*].Tags"
```

Es folgt eine Beispielausgabe.

```
[
    [
        {
            "Key": "Environment",
            "Value": "Production"
        },
        {
            "Key": "Department",
            "Value": "101"
        }
    ]
]
```

Stornieren einer Spot-Instance-Anforderung

Wenn Sie Ihre Spot-Instance-Anforderung nicht mehr benötigen, können Sie sie abbrechen. Sie können nur Spot-Instance-Anforderungen stornieren, deren Status `open`, `active` oder `disabled` lautet.

- Ihre Spot-Instance-Anforderung weist den Status `open` auf, wenn sie noch nicht erfüllt wurde und keine Instances gestartet wurden.
- Ihre Spot-Instance-Anforderung weist den Status `active` auf, wenn sie erfüllt wurde und Spot-Instances infolgedessen gestartet wurden.
- Ihre Spot-Instance-Anforderung weist den Status `disabled` auf, wenn Sie die Spot-Instance stoppen.

Wenn der Status Ihrer Spot-Instance-Anforderung `active` ist und eine zugehörige Spot-Instance läuft, wird diese Instance durch das Stornieren der Anforderung nicht beendet. Weitere Informationen zum Beenden von Spot-Instances finden Sie unter Beenden einer Spot-Instance.

Console

Um eine Spot-Instance-Anfrage über die Konsole zu stornieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie die Spot-Instance-Anfrage aus.
4. Wählen Sie Actions (Aktionen), Cancel request (Anforderungen abbrechen).
5. (Optional) Wenn Sie die zugehörigen Spot-Instances nicht mehr benötigen, können Sie diese beenden. Wählen Sie im Dialogfeld Cancel Spot request (Spot-Anforderung abbrechen) die Option Terminate instances (Instances beenden) und klicken Sie dann auf Confirm (Bestätigen).

AWS CLI

Um eine Spot-Instance-Anfrage mit dem zu stornieren AWS CLI

Verwenden Sie den Befehl cancel-spot-instance-requests, um die angegebene Spot-Instance-Anforderung abzubrechen.

```
aws ec2 cancel-spot-instance-requests --spot-instance-request-ids sir-08b93456
```

Anhalten einer Spot-Instance

Wenn Sie die Spot-Instances jetzt nicht benötigen, sie aber später neu starten möchten, ohne die Daten auf dem Amazon EBS-Volume zu verlieren, können Sie sie anhalten. Die Schritte zum Anhalten einer Spot-Instance ähneln den Schritten zum Anhalten einer On-Demand-Instance.

> **Note**
>
> Wenn eine Spot-Instance angehalten wird, können Sie mache Instance-Attribute ändern, aber nicht den Instance-Typ.
> Wir stellen für eine angehaltene Spot-Instance keine abgerechneten Nutzungsgebühren oder Gebühren für die Datenübertragung in Rechnung. Für Speicher für Amazon EBS-Volumes fallen jedoch Gebühren an.

Einschränkungen

- Sie können eine Spot-Instance nur anhalten, wenn die Spot-Instance aus einer `persistent`-Spot-Instance-Anforderung gestartet wurde.

- Sie können eine Spot-Instance nicht anhalten, wenn die zugehörige Spot-Instance-Anforderung abgebrochen wurde. Wenn die Spot-Instance-Anforderung abgebrochen wurde, können Sie nur die Spot-Instance beenden.
- Sie können eine Spot-Instance nicht anhalten, wenn sie Teil einer Flotte, einer Startgruppe oder einer Availability-Zone-Gruppe ist.

Console

Um eine Spot-Instance über die Konsole zu beenden

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Spot-Instance aus. Wenn Sie die Instance-ID der Spot-Instance nicht gespeichert haben, finden Sie weitere Informationen unterthe section called “Finden Sie Ihre Spot-Instances”.
4. Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten).
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus.

AWS CLI

Um eine Spot-Instance mit dem zu beenden AWS CLI

Verwenden Sie den Befehl stop-instances, um Ihre Spot-Instances manuell zu stoppen.

```
aws ec2 stop-instances --instance-ids i-1234567890abcdef0
```

Starten einer Spot-Instance

Sie können eine Spot-Instance starten, die Sie zuvor angehalten haben.

Voraussetzungen

Sie können eine Spot-Instance nur starten, wenn:

- Sie die Spot-Instance manuell angehalten haben.
- Die Spot-Instance eine EBS-gestützte Instance ist.
- Spot-Instance-Kapazität verfügbar ist.

- Der Spot-Preis niedriger ist als Ihr Höchstpreis.

Einschränkungen

- Sie können eine Spot-Instance nicht starten, wenn sie Teil einer Flotte, einer Startgruppe oder einer Availability-Zone-Gruppe ist.

Die Schritte zum Starten einer Spot-Instance ähneln den Schritten zum Starten einer On-Demand-Instance.

Console

Um eine Spot-Instance mit der Konsole zu starten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Spot-Instance aus. Wenn Sie die Instance-ID der Spot-Instance nicht gespeichert haben, finden Sie weitere Informationen unterthe section called “Finden Sie Ihre Spot-Instances”.
4. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

AWS CLI

Um eine Spot-Instance zu starten, ist AWS CLI

Verwenden Sie den Befehl start-instances, um Ihre Spot-Instances manuell zu starten.

```
aws ec2 start-instances --instance-ids i-1234567890abcdef0
```

Beenden einer Spot-Instance

Wenn Sie eine laufende oder angehaltene Spot-Instance beenden, die durch eine persistente Spot-Instance-Anforderung gestartet wurde, geht die Spot-Instance-Anforderung in den Status `open` über, sodass eine neue Spot-Instance gestartet werden kann. Um sicherzustellen, dass keine neue Spot-Instance gestartet wird, müssen Sie zuerst die Spot-Instance-Anforderung stornieren.

Wenn Sie eine `active`-Spot-Instance-Anfrage mit einer laufenden Spot-Instance abbrechen, wird die laufende Spot-Instance nicht automatisch beendet. Sie müssen die Spot-Instance manuell beenden.

Wenn Sie eine `disabled`-Spot-Instance-Anfrage stornieren, die eine gestoppte Spot-Instance enthält, wird die angehaltene Spot-Instance automatisch vom Amazon-EC2-Spot-Service beendet. Es kann eine kurze Verzögerung zwischen dem Abbrechen der Spot-Instance-Anfrage und dem Zeitpunkt geben, an dem der Spot-Service die Spot-Instance beendet.

Weitere Informationen finden Sie unter Stornieren einer Spot-Instance-Anforderung.

Console

So beenden Sie manuell eine Spot-Instance über die Konsole:

1. Stellen Sie vor dem Beenden einer Instance sicher, dass Sie keine Daten verlieren werden, indem Sie sich vergewissern, dass Ihre Amazon EBS-Volumes beim Abschalten nicht gelöscht werden und dass Sie alle Daten kopiert haben, die Sie von Ihren Instance-Speicher-Volumes für persistenten Speicher wie Amazon EBS oder Amazon S3 benötigen.
2. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Instances aus.
4. Wählen Sie die Spot-Instance aus. Wenn Sie die Instance-ID der Spot-Instance nicht gespeichert haben, finden Sie weitere Informationen unterthe section called “Finden Sie Ihre Spot-Instances”.
5. Wählen Sie Instance state (Instance-Status), Terminate instance (Instance beenden).
6. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.

AWS CLI

Um eine Spot-Instance manuell zu beenden, verwenden Sie AWS CLI

Verwenden Sie den Befehl terminate-instances, um Ihre Spot-Instances manuell zu beenden.

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0 i-0598c7d356eba48d7
```

Beispiel-Startspezifikationen für Spot-Instance-Anforderung

Die folgenden Beispiele zeigen Startkonfigurationen, die Sie mit dem Befehl request-spot-instances zum Erstellen einer Spot-Instance-Anforderung verwenden können. Weitere Informationen finden Sie unter Erstellt eine Spot-Instance-Anforderung.

> **Important**
>
> Wir raten dringend davon ab, den request-spot-instances-Befehl zu verwenden, da es sich um eine Legacy-API ohne geplante Investition handelt. Weitere Informationen finden Sie unter Was ist die beste Spot-Request-Methode?

Beispiele

- Beispiel 1: Spot-Instances starten
- Beispiel 2: Starten von Spot-Instances in der angegebenen Availability Zone
- Beispiel 3: Starten von Spot-Instances im angegebenen Subnetz
- Beispiel 4: Starten einer Dedicated-Spot-Instance

Beispiel 1: Spot-Instances starten

Das folgende Beispiel enthält keine Availability Zone oder ein Subnetz. Amazon EC2 wählt eine Availability Zone für Sie aus. Amazon EC2 startet die Instances im Standard-Subnetz der ausgewählten Availability Zone.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Beispiel 2: Starten von Spot-Instances in der angegebenen Availability Zone

Das folgende Beispiel enthält eine Availability Zone. Amazon EC2 startet die Instances im Standard-Subnetz der ausgewählten Availability Zone.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
```

```
  "InstanceType": "m5.medium",
  "Placement": {
    "AvailabilityZone": "us-west-2a"
  },
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Beispiel 3: Starten von Spot-Instances im angegebenen Subnetz

Das folgende Beispiel enthält ein Subnetz. Amazon EC2 startet die Instances im ausgewählten Subnetz. Wenn es sich bei der VPC um eine nicht standardmäßige VPC handelt, erhält die Instance standardmäßig keine öffentliche IPv4-Adresse.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "m5.medium",
  "SubnetId": "subnet-1a2b3c4d",
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Um einer Instance in einer nicht standardmäßigen VPC eine IPv4-Adresse zuzuweisen, geben Sie das Feld `AssociatePublicIpAddress` wie im folgenden Beispiel gezeigt an. Wenn Sie eine Netzwerkschnittstelle angeben, müssen Sie die Subnetz-ID und die Sicherheitsgruppen-ID über die Netzwerkschnittstelle angeben, anstatt die Felder `SubnetId` und `SecurityGroupIds` aus dem vorherigen Codeblock zu verwenden.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "InstanceType": "m5.medium",
  "NetworkInterfaces": [
    {
      "DeviceIndex": 0,
      "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
      "Groups": [ "sg-1a2b3c4d5e6f7g8h9" ],
      "AssociatePublicIpAddress": true
```

```
    }
  ],
  "IamInstanceProfile": {
      "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
  }
}
```

Beispiel 4: Starten einer Dedicated-Spot-Instance

Im folgenden Beispiel wird eine Spot-Instance mit der Tenancy `dedicated` angefordert. Eine Dedicated-Spot-Instance muss in einer VPC gestartet werden.

```
{
  "ImageId": "ami-0abcdef1234567890",
  "KeyName": "my-key-pair",
  "SecurityGroupIds": [ "sg-1a2b3c4d5e6f7g8h9" ],
  "InstanceType": "c5.8xlarge",
  "SubnetId": "subnet-1a2b3c4d5e6f7g8h9",
  "Placement": {
    "Tenancy": "dedicated"
  }
}
```

Spot-Anforderungsstatus

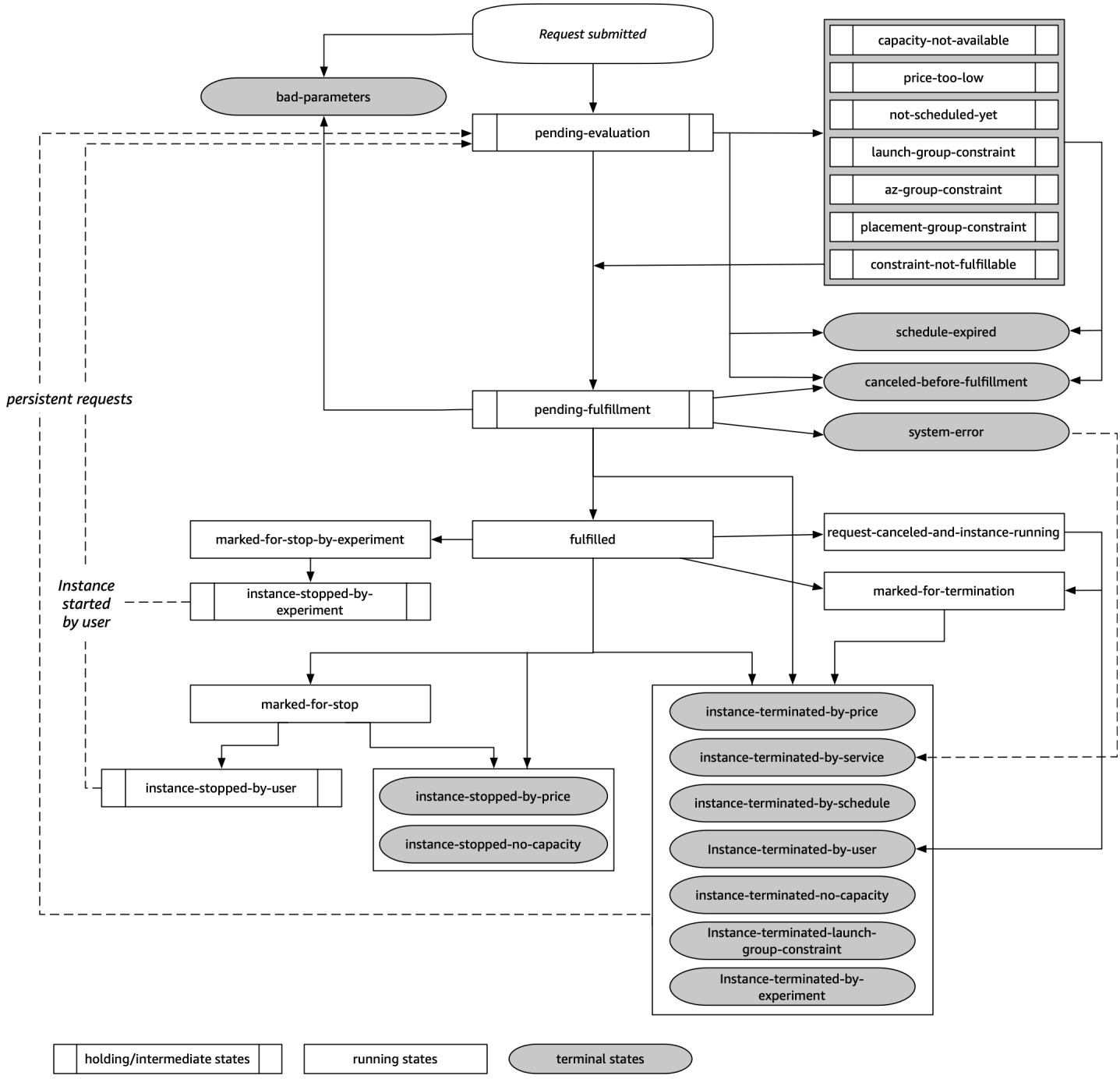
Um Sie bei der Verfolgung Ihrer Spot-Instance-Anforderungen zu unterstützen und Ihre Nutzung von Spot-Instances zu planen, verwenden Sie den Anforderungsstatus von Amazon EC2. Durch den Anforderungsstatus erfahren Sie beispielsweise den Grund dafür, warum Ihre Spot-Anforderung noch nicht erfüllt wurde oder der Anforderungsstatus listet die Bedingungen auf, die verhindern, dass Ihre Spot-Anforderung erfüllt wird.

In jedem Schritt des Prozesses, der auch als Lebenszyklus der Spot-Anforderung bezeichnet wird, legen spezifische Ereignisse sukzessive Anforderungsstatus fest.

Inhalt

Lebenszyklus einer Spot-Anforderung

Das folgende Diagramm zeigt die Pfade, denen Ihre Spot-Anfrage während ihres Lebenszyklus folgen kann, von der Übermittlung bis zur Beendigung. Die einzelnen Schritte werden durch Knoten dargestellt und der Statuscode für die einzelnen Knoten beschreibt den Status der Spot-Anfrage und der Spot-Instance.



Evaluierung ausstehend

Sobald Sie eine Spot-Instance-Anforderung erstellen, wird diese in den Status `pending-evaluation` versetzt – allerdings nur, wenn keine ungültigen Anforderungsparameter vorliegen (`bad-parameters`).

Statuscode	Anforderungsstatus	Instance-Status
`pending-evaluation`	`open`	Nicht zutreffend
`bad-parameters`	`closed`	Nicht zutreffend

Wartestatus

Wenn eine oder mehrere Anforderungsbedingungen gültig sind, jedoch noch nicht erfüllt werden können oder wenn nicht genügend Kapazität vorhanden ist, geht die Anforderung in einem Wartestatus über, bis die Bedingungen erfüllt werden. Die Anforderungsoptionen wirken sich auf die Wahrscheinlichkeit aus, dass die Anforderung erfüllt wird. Wenn beispielsweise keine Kapazität vorhanden ist, bleibt Ihre Anforderung so lange im Wartestatus, bis Kapazität verfügbar ist. Wenn Sie eine Gruppe von Availability Zones angeben, bleibt die Anforderung so lange im Wartestatus, bis die Bedingung der Availability Zone erfüllt wird.

Bei einem Ausfall in einer Availability Zone besteht die Möglichkeit, dass sich dies auf die freie EC2-Kapazität auswirkt, die für Spot-Instance-Anforderungen in anderen Availability Zones verfügbar ist.

Statuscode	Anforderungsstatus	Instance-Status
`capacity-not-available`	`open`	Nicht zutreffend
`price-too-low`	`open`	Nicht zutreffend
`not-scheduled-yet`	`open`	Nicht zutreffend
`launch-group-constraint`	`open`	Nicht zutreffend
`az-group-constraint`	`open`	Nicht zutreffend

Statuscode	Anforderungsstatus	Instance-Status
placement-group-constraint	open	Nicht zutreffend
constraint-not-fulfillable	open	Nicht zutreffend

Evaluierung/Erfüllung ausstehend – Terminal

Ihre Spot-Instance-Anforderung kann den Status `terminal` annehmen, wenn Sie eine Anforderung erstellen, die nur während eines bestimmten Zeitraums gültig ist und dieser Zeitraum abläuft, bevor Ihre Anforderung die Phase der ausstehenden Erfüllung erreicht. Dies kann auch vorkommen, wenn Sie die Anforderung abbrechen oder wenn ein Systemfehler auftritt.

Statuscode	Anforderungsstatus	Instance-Status
schedule-expired	cancelled	Nicht zutreffend
canceled-before-fulfillment [1]	cancelled	Nicht zutreffend
bad-parameters	failed	Nicht zutreffend
system-error	closed	Nicht zutreffend

[1] Wenn Sie die Anforderung abbrechen.

Ausstehende Erfüllung

Wenn die von Ihnen angegebenen Bedingungen (sofern vorhanden) erfüllt werden, geht Ihre Spot-Anforderung in den `pending-fulfillment`-Zustand.

Zu diesem Zeitpunkt wird Amazon EC2 für die Bereitstellung der angeforderten Instances vorbereitet. Wenn der Prozess zu diesem Zeitpunkt beendet wird, liegt dies wahrscheinlich daran, dass er durch

den Benutzer abgebrochen wurde, bevor eine Spot-Instance gestartet wurde. Dies kann auch daran liegen, dass ein unerwarteter Systemfehler aufgetreten ist.

Statuscode	Anforderungsstatus	Instance-Status
`pending-fulfillment`	`open`	Nicht zutreffend

Erfüllt

Wenn alle Spezifikationen für Ihre Spot-Instances erfüllt sind, wird Ihre Spot-Anforderung erfüllt. Amazon EC2 startet die Spot-Instances, was einige Minuten dauern kann. Wenn eine Spot-Instance bei einer Unterbrechung in den Ruhezustand versetzt oder angehalten wird, verbleibt sie in diesem Zustand, bis die Anforderung wieder erfüllt werden kann oder abgebrochen wird.

Statuscode	Anforderungsstatus	Instance-Status
`fulfilled`	`active`	`pending` → `running`
`fulfilled`	`active`	`stopped` → `running`

Wenn Sie eine Spot-Instance stoppen, wird Ihre Spot-Anforderung in den Status `marked-for-stop` oder `instance-stopped-by-user` versetzt, bis die Spot-Instance erneut gestartet werden kann oder die Anforderung storniert wird.

Statuscode	Anforderungsstatus	Instance-Status
`marked-for-stop`	`active`	`stopping`
`instance-stopped-by-user`[1]	`disabled` oder `cancelled` [2]	`stopped`

[1] Eine Spot Instance geht in den `instance-stopped-by-user`-Zustand über, wenn Sie die Instance anhalten oder den Shutdown-Befehl von der Instance aus ausführen. Wenn Sie die Instance angehalten haben, können Sie sie erneut starten. Beim Neustart wird die Spot-Instance-Anforderung

in den Status `pending-evaluation` zurückversetzt und dann startet Amazon EC2 eine neue Spot-Instance, wenn die Beschränkungen erfüllt sind.

² Der Status der Spot-Anforderung lautet `disabled`, wenn Sie die Spot Instance beenden, aber die Anforderung nicht abbrechen. Der Anforderungsstatus lautet `cancelled`, wenn Ihre Spot-Instance gestoppt wird und die Anforderung abläuft.

Erfüllt – Terminal

Ihre Spot Instance laufen weiter, solange die Kapazität für Ihren Instance-Typ verfügbar ist und Sie die Instance nicht beenden. Wenn Amazon EC2 Ihre Spot Instances beenden muss, geht die Spot-Anforderung in einen Terminal-Status über. Eine Anforderung geht auch in den Terminal-Status über, wenn Sie die Spot-Anforderung abbrechen oder die Spot Instances beenden.

Statuscode	Anforderungsstatus	Instance-Status
`request-canceled-and-instance-running`	`cancelled`	`running`
`marked-for-stop`	`active`	`running`
`marked-for-termination`	`active`	`running`
`instance-stopped-by-price`	`disabled`	`stopped`
`instance-stopped-by-user`	`disabled`	`stopped`
`instance-stopped-no-capacity`	`disabled`	`stopped`
`instance-terminated-by-price`	`closed` (einmalig), `open` (persistent)	`terminated`
`instance-terminated-by-schedule`	`closed`	`terminated`

Statuscode	Anforderungsstatus	Instance-Status
`instance-terminated-by-service`	`cancelled`	`terminated`
`instance-terminated-by-user`	`closed` oder `cancelled` [1]	`terminated`
`instance-terminated-no-capacity`	`closed` (einmalig), `open` (persistent)	`running` †
`instance-terminated-no-capacity`	`closed` (einmalig), `open` (persistent)	`terminated`
`instance-terminated-launch-group-constraint`	`closed` (einmalig), `open` (persistent)	`terminated`

[1] Der Anforderungsstatus lautet `closed`, wenn Sie die Instance beenden, die Anforderung jedoch nicht abbrechen. Der Anforderungsstatus lautet `cancelled`, wenn Sie die Instance beenden und die Anforderung abbrechen. Selbst wenn Sie eine Spot-Instance beenden, bevor Sie die zugehörige Anforderung abbrechen, kann es zu einer Verzögerung kommen, bis Amazon EC2 feststellt, dass Ihre Spot-Instance beendet wurde. In diesem Fall kann der Anforderungsstatus entweder `closed` oder `cancelled` lauten.

† Wenn Amazon EC2 eine Spot-Instance unterbricht, weil es die Kapazität wieder benötigt, und die Instance so konfiguriert ist, dass sie bei Unterbrechung beendet wird, wird der Status sofort auf `instance-terminated-no-capacity` gesetzt (wenn er nicht auf `marked-for-termination` eingestellt ist). Die Instance bleibt jedoch 2 Minuten lang im Status `running`, um den 2-Minuten-Zeitraum widerzuspiegeln, in dem die Instance die Unterbrechungsmitteilung für die Spot-Instance erhält. Nach 2 Minuten wird der Instance-Status auf `terminated` festgelegt.

Experimente zur Unterbrechung

Sie können AWS Fault Injection Service damit eine Spot-Instance-Unterbrechung einleiten, sodass Sie testen können, wie die Anwendungen auf Ihren Spot-Instances reagieren. Wenn eine Spot-Instance AWS FIS gestoppt wird, wechselt Ihre Spot-Anfrage in den `marked-for-stop-by-experiment` Status und dann in den `instance-stopped-by-experiment` Status. Wenn

eine Spot-Instance AWS FIS beendet wird, wechselt Ihre Spot-Anfrage in den `instance-terminated-by-experiment` Status. Weitere Informationen finden Sie unter the section called “Eine Unterbrechung einleiten”.

Statuscode	Anforderungsstatus	Instance-Status
`marked-for-stop-by-experiment`	`active`	`running`
`instance-stopped-by-experiment`	`disabled`	`stopped`
`instance-terminated-by-experiment`	`closed`	`terminated`

Persistente Anforderungen

Wenn Ihre Spot-Instances (entweder durch Sie oder durch Amazon EC2) beendet werden und es sich bei der Spot-Anforderung um eine persistente Anforderung handelt, wird diese in den Status `pending-evaluation` zurückversetzt und Amazon EC2 kann eine neue Spot-Instance starten, wenn die Beschränkungen erfüllt sind.

Anfordern von Anforderungsstatusinformationen

Sie können Informationen zum Anforderungsstatus mithilfe des Befehlszeilentools AWS Management Console oder eines Befehlszeilentools abrufen.

Um Informationen zum Anforderungsstatus mithilfe der Konsole abzurufen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Spot-Anforderungen und wählen Sie die Spot-Anforderung aus.
3. Um den Status zu überprüfen, aktivieren Sie auf der Registerkarte Beschreibung das Feld Status.

So rufen Sie Anforderungsstatusinformationen über die Befehlszeile ab

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-spot-instance-requests (AWS CLI)
- Get-EC2SpotInstanceRequest (AWS Tools for Windows PowerShell)

Statuscodes für Spotanforderungen

Spot-Anforderungsstatusinformationen bestehen aus einem Statuscode, der Aktualisierungszeit und einer Statusmeldung. Gemeinsam helfen Ihnen diese Informationen, die Disposition Ihrer Spot-Anforderung zu ermitteln.

Im Folgenden finden Sie die möglichen Spot-Anforderungsstatuscodes:

`az-group-constraint`

Amazon EC2 kann nicht alle angeforderten Instances in derselben Availability Zone starten.

`bad-parameters`

Ein oder mehrere Parameter für Ihre Spot-Anforderung sind nicht gültig (beispielsweise existiert die angegebene AMI nicht). Die Statusmeldung gibt an, welcher Parameter nicht gültig ist.

`canceled-before-fulfillment`

Der Benutzer hat die Spot-Anforderung abgebrochen, bevor sie erfüllt wurde.

`capacity-not-available`

Es ist nicht genügend Kapazität für die angeforderten Instances vorhanden.

`constraint-not-fulfillable`

Die Spot-Anforderung kann nicht erfüllt werden, da eine oder mehrere Bedingungen nicht gültig sind (beispielsweise ist die Availability Zone nicht vorhanden). Die Statusmeldung gibt an, welche Bedingung nicht gültig ist.

`fulfilled`

Die Spot-Anfrage ist `active` und Amazon EC2 startet Ihre Spot-Instances.

`instance-stopped-by-price`

Ihre Instance wurde beendet, da der Spot-Preis Ihren Höchstpreis überschritten hat.

`instance-stopped-by-user`

Ihre Instance wurde angehalten, weil ein Benutzer die Instance angehalten oder den Befehl „shutdown“ von der Instance ausgeführt hat.

`instance-stopped-no-capacity`

Ihre Instance wurde aufgrund von EC2-Kapazitätsmanagement-Anforderungen gestoppt.

`instance-terminated-by-price`

Ihre Instance wurde beendet, da der Spot-Preis Ihren Höchstpreis überschritten hat. Wenn Ihre Anforderung persistent ist, wird der Prozess neu gestartet, sodass die Evaluierung Ihrer Anforderung noch aussteht.

`instance-terminated-by-schedule`

Ihre Spot-Instance wurde am Ende ihrer geplanten Dauer beendet.

`instance-terminated-by-service`

Ihre Instance wurde in einem angehaltenen Zustand beendet.

`instance-terminated-by-user` oder `spot-instance-terminated-by-user`

Sie haben eine Spot-Instance beendet, die bereits erfüllt wurde, deshalb lautet der Anforderungsstatus `closed` (außer bei einer persistenten Anforderung) und der Instance-Status `terminated`.

`instance-terminated-launch-group-constraint`

Eine oder mehrere Instances in Ihrer Startgruppe wurde beendet, sodass die Bedingung für die Startgruppe nicht mehr erfüllt wird.

`instance-terminated-no-capacity`

Ihre Instance wurde aufgrund von standardmäßigen Kapazitätsverwaltungsprozessen beendet.

`launch-group-constraint`

Amazon EC2 kann nicht alle angeforderten Instances gleichzeitig starten. Alle Instances in einer Startgruppe werden zusammen gestartet und beendet.

`limit-exceeded`

Das Limit für die Anzahl an EBS-Volumes oder der Volume-Gesamtspeicher wurde überschritten. Weitere Informationen zu diesen Limits und dazu, wie eine Erhöhung angefordert werden kann, finden Sie unter Amazon-EBS-Limits in der Allgemeine Amazon Web Services-Referenz.

`marked-for-stop`

Die Spot-Instance wird zum Stoppen markiert.

`marked-for-termination`

Die Spot-Instance wird für das Beenden markiert.

`not-scheduled-yet`

Die Spot-Anfrage wird erst zum geplanten Termin ausgewertet.

`pending-evaluation`

Nachdem Sie eine Spot-Instance-Anforderung erstellt haben, wird diese in den Status `pending-evaluation` versetzt, während das System die Parameter Ihrer Anforderung evaluiert.

`pending-fulfillment`

Amazon EC2 versucht, Ihre Spot-Instances bereitzustellen.

`placement-group-constraint`

Die Spot-Anforderung kann noch nicht erfüllt werden, da eine Spot-Instance zu diesem Zeitpunkt nicht der Platzierungsgruppe hinzugefügt werden kann.

`price-too-low`

Die Anforderung kann noch nicht erfüllt werden, da der Höchstpreis den Spot-Preis unterschreitet. In diesem Fall wird keine Instance gestartet und Ihre Anforderung verbleibt im Status `open`.

`request-canceled-and-instance-running`

Sie haben die Spot-Anforderung abgebrochen, die Spot-Instances werden jedoch weiterhin ausgeführt. Die Anforderung weist den Status `cancelled`, die Instances jedoch den Status `running` auf.

`schedule-expired`

Die Spot-Anforderung ist abgelaufen, da sie vor dem angegebenen Datum nicht erfüllt wurde.

`system-error`

Es ist ein unerwarteter Systemfehler aufgetreten. Wenn es sich um ein wiederkehrendes Problem handelt, wenden Sie sich bitte an uns, AWS Support um Unterstützung zu erhalten.

Ereignis zur Erfüllung einer EC2-Spot-Instance-Anforderung

Wenn eine Spot-Instance-Anfrage erfüllt ist, sendet Amazon EC2 ein EC2-Spot-Instance-Request-Erfüllungsereignis an Amazon. EventBridge Sie können eine Regel erstellen, um bei diesem Ereignis jeweils eine Aktion auszuführen, wie z. B. das Aufrufen einer Lambda-Funktion oder das Benachrichtigen eines Amazon-SNS-Themas.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "01234567-1234-0123-1234-012345678901",
    "detail-type": "EC2 Spot Instance Request Fulfillment",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "spot-instance-request-id": "sir-1a2b3c4d",
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Empfehlung zum Neuausgleich einer EC2-Instance

Eine EC2-Instance-Neuausgleichsempfehlung ist ein Signal, das Sie benachrichtigt, wenn eine Spot Instance einem erhöhten Risiko einer Unterbrechung ausgesetzt ist. Das Signal kann früher als die zweiminütige Unterbrechungsbenachrichtigung der Spot-Instance eintreffen, sodass Sie die Möglichkeit haben, die Spot-Instance proaktiv zu verwalten. Sie können entscheiden, Ihr Workload auf neue oder bestehende Spot-Instances auszugleichen, die nicht einem erhöhten Risiko einer Unterbrechung ausgesetzt sind.

Es ist Amazon EC2 nicht immer möglich, das Signal für die Neuausgleichsempfehlung vor der zweiminütigen Spot-Instance-Unterbrechungsbenachrichtigung zu senden. Daher kann das Neuausgleichsempfehlungsignal zusammen mit der zweiminütigen Unterbrechungsbenachrichtigung eingehen.

Empfehlungen zur Neuverteilung werden als EventBridge Ereignis und als Element in den Instance-Metadaten auf der Spot-Instance zur Verfügung gestellt. Ereignisse werden auf bestmögliche Weise ausgegeben.

> **Note**
>
> Neuausgleichsempfehlungen werden nur für Spot-Instances unterstützt, die nach dem 5. November 2020 00:00 UTC gestartet werden.

Themen

Ausgleich von Aktionen, die Sie ergreifen können

Dies sind einige der möglichen Neuausgleichsaktionen, die Sie ergreifen können:

Korrektes Herunterfahren

Wenn Sie das Neuausgleichsempfehlungsignal für eine Spot-Instance erhalten, können Sie Ihre Instance-Abschaltverfahren starten, wozu auch gehören kann, sicherzustellen, dass Prozesse abgeschlossen sind, bevor Sie sie anhalten. Sie können beispielsweise System- oder Anwendungsprotokolle auf Amazon Simple Storage Service (Amazon S3) hochladen, Amazon-SQS-Mitarbeiter herunterfahren oder die Abmeldung vom Domain Name System (DNS) durchführen. Sie können Ihre Arbeit auch im externen Speicher speichern und zu einem späteren Zeitpunkt wieder aufnehmen.

Verhindern, dass neue Arbeit geplant wird

Wenn Sie das Neuausgleichsempfehlungsignal für eine Spot-Instance erhalten, können Sie verhindern, dass neue Arbeiten auf der Instance geplant werden, während Sie die Instance weiterhin verwenden, bis die geplante Arbeit abgeschlossen ist.

Proaktiv neue Ersatz-Instances starten

Sie können Auto-Scaling-Gruppen, EC2-Flottte oder Spot-Flotte konfigurieren, um Ersatz-Spot-Instances automatisch zu starten, wenn ein Neuausgleichsempfehlungsignal ausgegeben wird.

Weitere Informationen finden Sie unter Verwendung von Kapazitätsausgleich zur Bewältigung von Amazon-EC2 Spot-Unterbrechungen im Benutzerhandbuch für Amazon EC2 Auto Scaling und Kapazitätsausgleich für EC2-Flotte und Kapazitätsausgleich für Spot-Flotte in diesem Benutzerhandbuch.

Überwachen von Signalen für Neuausgleichsempfehlungen

Sie können das Signal für die Neuausgleichsempfehlung überwachen, damit Sie bei der Absendung des Signals die im vorherigen Abschnitt angegebenen Aktionen ausführen können. Das Rebalance-Empfehlungssignal wird als Ereignis, das an Amazon gesendet wird EventBridge (früher bekannt als Amazon CloudWatch Events), und als Instance-Metadaten auf der Spot-Instance zur Verfügung gestellt.

Überwachen von Signalen für Neuausgleichsempfehlungen:

- Verwenden Sie Amazon EventBridge
- Verwenden von Instance-Metadaten

Verwenden Sie Amazon EventBridge

Wenn das Rebalance-Empfehlungssignal für eine Spot-Instance ausgegeben wird, wird das Ereignis für das Signal an Amazon EventBridge gesendet. Wenn ein Ereignismuster EventBridge erkannt wird, das einem in einer Regel definierten Muster entspricht, EventBridge ruft es ein oder mehrere in der Regel angegebene Ziel (oder Ziele) auf.

Es folgt ein Beispielereignis für das Neuausgleichsempfehlungssignal.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Instance Rebalance Recommendation",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2:123456789012:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0"
    }
}
```

Die folgenden Felder bilden das in der Regel definierte Ereignismuster:

`"detail-type": "EC2 Instance Rebalance Recommendation"`

Gibt an, dass das Ereignis ein Neuausgleichsempfehlungsereignis ist

`"source": "aws.ec2"`

Gibt an, dass das Ereignis aus Amazon EC2 stammt

Erstellen Sie eine Regel EventBridge

Sie können eine EventBridge Regel schreiben und automatisieren, welche Aktionen ausgeführt werden, wenn das Ereignismuster mit der Regel übereinstimmt.

Im folgenden Beispiel wird eine EventBridge Regel erstellt, nach der jedes Mal, wenn Amazon EC2 ein Empfehlungssignal zur Neuverteilung ausgibt, eine E-Mail, eine Textnachricht oder eine mobile Push-Benachrichtigung sendet. Das Signal wird als `EC2 Instance Rebalance Recommendation`-Ereignis ausgegeben, das die durch die Regel definierte Aktion auslöst.

Bevor Sie die EventBridge Regel erstellen, müssen Sie das Amazon SNS SNS-Thema für die E-Mail, Textnachricht oder mobile Push-Benachrichtigung erstellen.

Um eine EventBridge Regel für ein Remalance-Empfehlungsereignis zu erstellen

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:
   a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

      Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.
   b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird dieses stets an den standardmäßigen Event Bus Ihres Kontos weitergeleitet.
   c. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
   d. Wählen Sie Weiter aus.

4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:

   a. Wählen Sie als Quelle für Ereignisse die Option AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.

   b. Bei Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, um mit dem `EC2 Instance Rebalance Recommendation`-Ereignis übereinzustimmen, und wählen dann Save (Speichern) aus.

      ```
      {
       "source": ["aws.ec2"],
       "detail-type": ["EC2 Instance Rebalance Recommendation"]
      }
      ```

      Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

      i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

         A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

         B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

         C. Wählen Sie für AWS Service EC2 Spot Fleet (EC2-Spot-Flotte) aus.

         D. Wählen Sie als Event type (Ereignistyp) die Option EC2 Instance Rebalance Recommendation (Empfehlung zur Neugewichtung der EC2-Instance).

         E. Um die Vorlage anzupassen, wählen Sie Edit pattern (Muster bearbeiten) und nehmen Sie Ihre Änderungen vor, damit sie dem Beispiel-Ereignismuster entsprechen.

      ii. (Alternativ) So geben Sie ein benutzerdefiniertes Ereignismuster an:

         A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

         B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

   c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.
b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.
c. Wählen Sie für Topic (Thema) ein vorhandenes Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.
d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).
e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.
7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.
b. Wählen Sie Regel erstellen aus.

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

Verwenden von Instance-Metadaten

Die Kategorie der Instance-Metadaten `events/recommendations/rebalance` gibt die ungefähre Zeit in UTC an, zu der das Neuausgleichsempfehlungssignal für eine Spot-Instance ausgegeben wurde.

Wir empfehlen Ihnen, alle 5 Sekunden nach Neuausgleichsempfehlungssignalen zu suchen, damit Sie keine Gelegenheit verpassen, auf den Neuausgleich zu reagieren.

Wenn die Spot-Instance eine Neuausgleichsempfehlung erhält, ist der Zeitpunkt, zu dem das Signal ausgegeben wurde, in den Instance-Metadaten vorhanden. Sie können die Zeit, zu der das Signal gesendet wurde, wie folgt abrufen.

Verwenden Sie den Befehl für Ihr Betriebssystem.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Windows

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/events/recommendations/rebalance
```

Im Folgenden finden Sie eine Beispielausgabe, die die Zeit in UTC angibt, zu der das Neuausgleichsempfehlungssignal für die Spot-Instance ausgegeben wurde.

```
{"noticeTime": "2020-10-27T08:22:00Z"}
```

Wenn das Signal für die Instance nicht ausgegeben wurde, ist `events/recommendations/rebalance` nicht vorhanden und Sie erhalten einen HTTP-404-Fehler, wenn Sie versuchen, sie abzurufen.

Dienste, die das Neuausgleichsempfehlungssignal verwenden

Amazon EC2 Auto Scaling, EC2-Flotte und Spot-Flotte verwenden das Neuausgleichsempfehlungssignal, um es Ihnen zu erleichtern, die Verfügbarkeit von Workloads aufrechtzuerhalten, indem Sie Ihre Flotte proaktiv um eine neue Spot-Instance erweitern, bevor eine laufende Instance eine zweiminütige Spot-Instance-Unterbrechungsbenachrichtigung erhält. Sie können diese Dienste Änderungen überwachen lassen und proaktiv auf Änderungen reagieren lassen, die sich auf die Verfügbarkeit Ihrer Spot-Instances auswirken. Weitere Informationen finden Sie hier:

- Verwendung von Kapazitätsausgleich, um Amazon-EC2-Spot-Unterbrechungen zu bewältigen im Benutzerhandbuch für Amazon EC2 Auto Scaling
- Kapazitätsausgleich im EC2-Flotte-Thema in diesem Benutzerhandbuch
- Kapazitätsausgleich im Thema „Spot-Flotte“ in diesem Benutzerhandbuch

Spot-Instance-Unterbrechungen

Sie können Spot-Instances für steile Rabatte auf Ersatz-EC2-Kapazität starten, solange sie im Austausch dafür zurückgegeben werden, wenn Amazon EC2 die Kapazität wieder benötigt. Wenn Amazon EC2 eine Spot-Instance zurückfordert, wird ein solches Ereignis als Spot-Instance-Unterbrechung bezeichnet.

Wenn Amazon EC2 eine Spot-Instance unterbricht, wird die Instance entweder angehalten, beendet oder in den Ruhezustand versetzt, je nachdem, was Sie bei der Erstellung der Spot-Anforderung festgelegt haben.

Die Nachfrage nach Spot-Instances kann sich von einem Moment zum anderen erheblich unterscheiden, und die Verfügbarkeit von Spot-Instances kann sich abhängig von der Verfügbarkeit ungenutzter EC2-Instances ebenfalls erheblich unterscheiden. Zudem besteht immer die Möglichkeit, dass Ihre Spot-Instance unterbrochen wird.

Eine On-Demand-Instance, die in einer EC2-Flotte oder Spot-Flotte angegeben wurde, kann nicht unterbrochen werden.

Inhalt

Gründe für die Unterbrechung der Spot-Instance

Im Folgenden finden Sie mögliche Gründe dafür, dass Amazon EC2 Ihre Spot-Instances möglicherweise unterbricht:

Kapazität

Amazon EC2 kann Ihre Spot-Instance unterbrechen, wenn sie wieder benötigt wird. EC2 ruft Ihre Instance hauptsächlich zurück, um Kapazität neu zu verwenden, kann dies aber auch aus anderen Gründen wie der Hostwartung oder der Hardwareausfall tun.

Preis

Der Spotpreis ist höher als Ihr Höchstpreis.

Sie können den Höchstpreis in Ihrer Spot-Anforderung angeben. Wenn Sie jedoch einen Höchstpreis angeben, werden Ihre Instances häufiger unterbrochen, als wenn Sie dies nicht tun.

Beschränkungen

Wenn Ihre Spot-Anforderung eine Bedingung enthält, z. B. eine Startgruppe oder eine Gruppe von Availability Zones, werden die Spot-Instances als Gruppe beendet, wenn die Bedingung nicht mehr erfüllt werden kann.

Sie können die historischen Unterbrechungsraten für Ihren Instance-Typ im Spot-Instance-Advisor sehen.

Verhalten von Spot-Instance-Unterbrechungen

Sie können angeben, dass Amazon EC2 eine der folgenden Aktionen ausführen muss, wenn es eine Spot-Instance unterbricht:

- Unterbrochene Spot-Instances anhalten
- Unterbrochene Spot-Instances in den Ruhezustand versetzen
- Unterbrochene Spot-Instances beenden (Das ist das Standardverhalten.)

Festlegen des Unterbrechungsverhaltens

Sie können das Unterbrechungsverhalten angeben, wenn Sie eine Spot-Anforderung erstellen. Wenn Sie kein Unterbrechungsverhalten angeben, werden Spot-Instances standardmäßig von Amazon EC2 beendet, wenn sie unterbrochen werden.

Die Art und Weise, in der Sie das Unterbrechungsverhalten angeben, unterscheidet sich je nach Anforderung der Spot-Instances.

- Wenn Sie Spot Instances mit dem Launch Instance Wizard anfordern, können Sie das Unterbrechungsverhalten wie folgt festlegen: Erweitern Sie im Launch Instance Wizard die Option Erweiterte Details und aktivieren Sie das Kontrollkästchen Spot Instances anfordern. Wählen Sie Anpassen aus. Wählen Sie unter Unterbrechungsverhalten ein Unterbrechungsverhalten aus. Wenn das Unterbrechungsverhalten der Ruhezustand ist, können Sie alternativ Aktivieren für Stopp – Ruhezustand-Verhalten auswählen.
- Wenn Sie Spot Instances mithilfe der CLI run-instances anfordern, können Sie das Unterbrechungsverhalten wie folgt festlegen: Geben Sie in der Konfiguration der Anfrage (`--instance-market-options`) für `InstanceInterruptionBehavior` ein Unterbrechungsverhalten an. Wenn das Unterbrechungsverhalten `hibernate` ist, können Sie den Ruhezustand alternativ mit dem `--hibernation-options Configured=true`-Parameter aktivieren.
- Wenn Sie Spot-Instances in einer Startvorlage konfigurieren, können Sie das Unterbrechungsverhalten wie folgt angeben: Erweitern Sie in der Startvorlage Erweiterte Details und aktivieren Sie das Kontrollkästchen Spot-Instances anfordern. Wählen Sie Anpassen und dann unter Verhalten bei Unterbrechungen ein Unterbrechungsverhalten aus.
- Wenn Sie Spot-Instances mithilfe der Spot-Konsole anfordern, können Sie das Unterbrechungsverhalten wie folgt angeben: Aktivieren Sie das Kontrollkästchen Zielkapazität aufrechterhalten und wählen Sie dann unter Verhalten bei Unterbrechungen ein Unterbrechungsverhalten aus.
- Wenn Sie Spot-Instances in der Anforderungskonfiguration konfigurieren und die CLI create-fleet verwenden, können Sie das Unterbrechungsverhalten wie folgt angeben: Geben Sie für `InstanceInterruptionBehavior` ein Unterbrechungsverhalten an.
- Wenn Sie Spot-Instances in der Anforderungskonfiguration konfigurieren und die CLI request-spot-fleet verwenden, können Sie das Unterbrechungsverhalten wie folgt angeben: Geben Sie für `InstanceInterruptionBehavior` ein Unterbrechungsverhalten an.
- Wenn Sie Spot-Instances mithilfe der request-spot-instances-CLI konfigurieren, können Sie das Unterbrechungsverhalten wie folgt angeben: Geben Sie für `--instance-interruption-behavior` ein Unterbrechungsverhalten an.

> **Note**
>
> Wir raten dringend davon ab, die Befehle request-spot-fleet und „request-spot-instances zum Anfordern von Spot Instances zu verwenden, da es sich um Legacy-APIs ohne geplante Investition handelt. Weitere Informationen finden Sie unter Was ist die beste Spot-Request-Methode?.

Unterbrochene Spot-Instances anhalten

Sie können angeben, dass Amazon EC2 die Spot-Instances beenden soll, wenn diese unterbrochen werden. Weitere Informationen finden Sie unter Festlegen des Unterbrechungsverhaltens.

Überlegungen

- Eine unterbrochene gestoppte Spot-Instance kann nur von Amazon EC2 neu gestartet werden.
- Für eine durch eine `persistent` Spot-Instance-Anforderung gestartete Spot-Instance startet Amazon EC2 die angehaltene Instance neu, wenn die Kapazität in derselben Availability Zone und für denselben Instance-Typ wie die angehaltene Instance verfügbar ist. (Dabei muss dieselbe Startspezifikation verwendet werden.)
- Für Spot-Instances, die von einer EC2-Flotte oder Spot-Flotte des Typs `maintain` gestartet wurden: Nachdem eine Spot-Instance unterbrochen wurde, startet Amazon EC2 eine Ersatz-Instance, um die Zielkapazität aufrechtzuerhalten. Amazon EC2 findet die besten Spot-Kapazitätspools basierend auf der angegebenen Zuweisungsstrategie (`lowestPrice`, `diversified` oder `InstancePoolsToUseCount`). Der Pool mit der früher angehaltenen Instance wird nicht priorisiert. Wenn die Zuweisungsstrategie später zu einem Pool mit der früher angehaltenen Instance führt, startet Amazon EC2 die angehaltene Instance neu, um die Zielkapazität zu erfüllen.

  Ziehen Sie beispielsweise eine Spot-Flotte mit der `lowestPrice`-Zuweisungsstrategie in Betracht. Beim ersten Start erfüllt ein `c3.large`-Pool die `lowestPrice`-Kriterien für die Start-Spezifikation. Wenn die `c3.large`-Instances später unterbrochen sind, hält Amazon EC2 die Instances an und füllt Kapazität aus einem anderen Pool auf, der zur `lowestPrice`-Strategie passt. Dieses Mal ist der Pool ein `c4.large`-Pool und Amazon EC2 startet `c4.large`-Instances, um die Zielkapazität zu erfüllen. Ebenso könnte die Spot-Flotte das nächste Mal in einen `c5.large`-Pool verlegt werden. Bei keinem dieser Übergänge priorisiert Amazon EC2 Pools mit früher angehaltenen Instances. Die Priorisierung erfolgt stattdessen rein auf der angegeben Zuweisungsstrategie. Die `lowestPrice`-Strategie kann zurück zu Pools mit früher gestoppten Instances führen. Wenn

Instances zum Beispiel im `c5.large`-Pool unterbrochen werden und die `lowestPrice`-Strategie zurück zu den `c3.large`- oder `c4.large`-Pools führt, werden die früher gestoppten Instances neu gestartet, um die Zielkapazität zu erfüllen.

- Wenn eine Spot-Instance angehalten wird, können Sie mache Instance-Attribute ändern, aber nicht den Instance-Typ. Wenn Sie ein EBS-Volume trennen oder löschen, wird es nicht neu zugeordnet, wenn die Spot-Instance gestartet wird. Wenn Sie das Root-Volume trennen und Amazon EC2 versucht, die Spot-Instance zu starten, schlägt der Start der Instance fehl und Amazon EC2 beendet die angehaltene Instance.
- Sie können eine Spot-Instance beenden, wenn sie angehalten wird.
- Wenn Sie eine Spot-Instance-Anforderung, eine EC2-Flotte oder eine Spot-Flotte abbrechen, beendet Amazon EC2 alle verknüpften Spot-Instances, die angehalten werden.
- Während eine unterbrochene Spot-Instance angehalten wird, werden nur Gebühren für die EBS-Volumes berechnet, die beibehalten werden. Wenn bei der Verwendung einer EC2-Flotte und Spot-Flotte viele Instances angehalten wurden, können Sie das Limit für die Anzahl der EBS-Volumes in Ihrem Konto überschreiten. Weitere Informationen zur Kostenberechnung, wenn eine Spot-Instance unterbrochen wird, finden Sie unter Fakturierung für unterbrochene Spot-Instances.
- Stellen Sie sicher, dass Sie mit den Auswirkungen des Stoppens einer Instance vertraut sind. Weitere Informationen darüber, was passiert und was Sie tun können, wenn eine Instance angehalten wird, finden Sie unter Unterschiede zwischen Neustart, Anhalten, Ruhezustand und Beenden.

Voraussetzungen

Wenn Sie eine unterbrochene Spot-Instance anhalten möchten, müssen die folgenden Voraussetzungen erfüllt sein:

Art der Spot-Anforderung

Der Anforderungstyp der Spot-Instance muss `persistent` sein. Sie können in der Spot-Instance-Anforderung keine Startgruppe angeben.

Der Anforderungstyp der EC2-Flotte oder Spot-Flotte muss `maintain` sein.

Root-Volume-Typ

Muss ein EBS-Volume sein, kein Instance-Speicher-Volume.

Unterbrochene Spot-Instances in den Ruhezustand versetzen

Sie können angeben, dass Amazon EC2 die Spot-Instances in den Ruhezustand versetzen soll, wenn diese unterbrochen werden. Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand.

Amazon EC2 bietet nun das gleiche Ruhezustandserlebnisfür Spot Instances, die derzeit auch für On-Demand-Instances verfügbar ist. Es bietet eine umfassendere Unterstützung, wobei für den Ruhezustand von Spot Instances jetzt Folgendes unterstützt wird:

- Weitere unterstützte AMIs
- Weitere unterstützte Instance-Familien
- Vom Benutzer initiierter Ruhezustand

Unterbrochene Spot-Instances beenden

Wenn Amazon EC2 eine Spot-Instance unterbricht, beendet es die Instance standardmäßig, es sei denn, Sie legen eine andere Aktion wie Stoppen oder Ruhezustand für den Fall einer Unterbrechung fest. Weitere Informationen finden Sie unter Festlegen des Unterbrechungsverhaltens.

Bereiten Sie sich auf Spot-Instance-Unterbrechungen vor

Die Nachfrage nach Spot-Instances kann sich von einem Moment zum anderen erheblich unterscheiden, und die Verfügbarkeit von Spot-Instances kann sich abhängig von der Verfügbarkeit ungenutzter EC2-Instances ebenfalls erheblich unterscheiden. Zudem besteht immer die Möglichkeit, dass Ihre Spot-Instance unterbrochen wird. Aus diesem Grund müssen Sie sicherstellen, dass Ihre Anwendung auf eine Spot-Instance-Unterbrechung vorbereitet ist.

Wir empfehlen, dass Sie sich an die folgenden bewährten Methoden halten, damit Sie auf eine Unterbrechung der Spot-Instance vorbereitet sind.

- Erstellen Sie Ihre Spot-Anforderung mit einer Auto-Scaling-Gruppe. Wenn Ihre Spot-Instances unterbrochen werden, startet die Auto-Scaling-Gruppe automatisch Ersatz-Instances. Weitere Informationen finden Sie unter Auto-Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen im Amazon EC2 Auto Scaling-Benutzerhandbuch.
- Stellen Sie sicher, dass Ihre Instance einsatzbereit ist, sobald die Anforderung erfüllt ist, indem Sie ein Amazon Machine Image (AMI) verwenden, das die erforderliche Softwarekonfiguration enthält. Sie können auch Benutzerdaten verwenden, um beim Startup Befehle auszuführen.

- Daten auf Instance-Speicher-Volumes gehen verloren, wenn die Instance angehalten oder beendet wird. Sichern Sie alle wichtigen Daten auf Instance-Speicher-Volumes auf einem persistenteren Speicher wie Amazon S3, Amazon EBS oder Amazon DynamoDB.
- Speichern Sie wichtige Daten regelmäßig an einem Ort, der vom Beenden der Spot-Instance nicht betroffen ist. Sie können beispielsweise Amazon S3, Amazon EBS oder DynamoDB verwenden.
- Teilen Sie die Arbeit in kleine Aufgaben auf (mit einer Grid-, Hadoop- oder warteschlangenbasierten Architektur) oder verwenden Sie Prüfpunkte, damit Sie Ihre Arbeit häufig speichern können.
- Amazon EC2 sendet ein Neuausgleichsempfehlungssignal an die Spot-Instance aus, wenn die Instance ein erhöhtes Unterbrechungsrisiko hat. Sie können sich auf die Neuausgleichsempfehlung verlassen, um Spot-Instance-Unterbrechungen proaktiv zu verwalten, ohne auf die zweiminütige Spot-Instance-Unterbrechungsbenachrichtigung warten zu müssen. Weitere Informationen finden Sie unter Empfehlung zum Neuausgleich einer EC2-Instance.
- Verwenden Sie die zweiminütigen Spot-Instance-Unterbrechungsbenachrichtigungen, um den Status Ihrer Spot-Instances zu überwachen. Weitere Informationen finden Sie unter Spot-Instance-Unterbrechungsbenachrichtigungen.
- Obwohl wir bemüht sind, diese Warnmeldungen so schnell wie möglich bereitzustellen, besteht die Möglichkeit, dass Ihre Spot-Instance unterbrochen ist, bevor die Warnmeldungen bereitgestellt werden können. Testen Sie Ihre Anwendung und stellen Sie sicher, dass unerwartete Unterbrechungen von Instances elegant abgewickelt werden, auch wenn Sie die Neuausgleichsempfehlungsignale und Benachrichtigungen über Unterbrechungen durchführen überwachen. Führen Sie hierzu die Anwendung mithilfe einer On-Demand-Instance aus und beenden Sie die On-Demand-Instance anschließend selbst.
- Führen Sie ein Experiment mit kontrollierter Fehlerinjektion durch AWS Fault Injection Service , um zu testen, wie Ihre Anwendung reagiert, wenn Ihre Spot-Instance unterbrochen wird. Weitere Informationen finden Sie im Tutorial: Testen von Spot-Instance-Unterbrechungen mit AWS FIS im AWS Fault Injection Service -Benutzerhandbuch.

Initiieren einer Spot-Instance-Unterbrechung

Sie können eine Spot-Instance-Anforderung in der Amazon-EC2-Konsole auswählen und eine Unterbrechung initiieren, um zu testen, wie die Anwendungen auf Ihren Spot Instances mit Unterbrechungen umgehen. Wenn Sie eine Spot-Instance-Unterbrechung initiieren, werden Sie von Amazon EC2 darüber informiert, dass Ihre Spot Instance in zwei Minuten unterbrochen wird, und nach zwei Minuten wird die Instance unterbrochen.

Der zugrunde liegende Dienst, der die Spot-Instance-Unterbrechung durchführt, ist AWS Fault Injection Service (AWS FIS). Informationen zu finden AWS FIS Sie unter AWS Fault Injection Service.

> **Note**
>
> Verhaltensweisen bei Unterbrechungen sind `terminate`, `stop` und `hibernate`. Wenn Sie das Unterbrechungsverhalten auf `hibernate` einstellen, erfolgt bei Initiierung einer Spot-Instance-Unterbrechung umgehend der Übergang in den Ruhezustand.

Das Initiieren einer Spot-Instance-Unterbrechung wird in allen Ländern AWS-Regionen außer im asiatisch-pazifischen Raum (Jakarta), im asiatisch-pazifischen Raum (Osaka), in China (Peking), in China (Ningxia) und im Nahen Osten (VAE) unterstützt.

Themen

Initiieren einer Spot-Instance-Unterbrechung

Mithilfe der EC2-Konsole können Sie schnell eine Spot-Instance-Unterbrechung initiieren. Wenn Sie eine Spot-Instance-Anfrage auswählen, können Sie die Unterbrechung einer Spot-Instance einleiten. Wenn Sie eine Spot-Flotte-Anfrage auswählen, können Sie die Unterbrechung mehrerer Spot-Instances gleichzeitig einleiten.

Für komplexere Experimente zum Testen von Spot-Instance-Unterbrechungen können Sie mit der Konsole Ihre eigenen Experimente erstellen. AWS FIS

So initiieren Sie eine Spot-Instance-Unterbrechung in einer Spot-Instance-Anforderung über die EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests (Spot-Anforderungen) aus.
3. Wählen Sie eine Spot-Instance-Anforderung und dann Actions (Aktionen) sowie Initiate interruption (Unterbrechung beginnen) aus. Sie können nicht mehrere Spot-Instance-Anfragen auswählen, um eine Unterbrechung einzuleiten.

4. Verwenden Sie im Dialogfeld Initiate Spot Instance interruption (Spot-Instance-Unterbrechung initiieren) unter Service access (Service-Zugriff) entweder die Standardrolle oder wählen Sie eine vorhandene Rolle aus. Um eine Rolle auszuwählen, klicken Sie auf Use an existing service role (Vorhandene Servicerolle verwenden). Wählen Sie dann unter IAM role (IAM-Rolle) die zu verwendende Rolle aus.
5. Wenn Sie bereit sind, die Spot-Instance-Unterbrechung zu initiieren, wählen Sie Initiate interruption (Unterbrechung initiieren) aus.

Um die Unterbrechung einer oder mehrerer Spot-Instances in einer Spot-Flottenanforderung mithilfe der EC2-Konsole zu initiieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests (Spot-Anforderungen) aus.
3. Wählen Sie eine Spot-Flotten-Anforderung und dann Actions (Aktionen) sowie Initiate interruption (Unterbrechung beginnen) aus. Sie können nicht mehrere Spot-Flotten-Anfragen auswählen, um eine Unterbrechung einzuleiten.
4. Geben Sie im Dialogfeld „Anzahl der Spot-Instances angeben“ unter Anzahl der zu unterbrechenden Instances die Anzahl der zu unterbrechenden Spot-Instances ein und wählen Sie dann „Bestätigen“.

> **Note**
>
> Die Anzahl darf die Anzahl der Spot-Instances in der Flotte oder Ihr Kontingent für die Anzahl der Spot-Instances, die pro Experiment unterbrochen AWS FIS werden können, nicht überschreiten.

5. Verwenden Sie im Dialogfeld Initiate Spot Instance interruption (Spot-Instance-Unterbrechung initiieren) unter Service access (Service-Zugriff) entweder die Standardrolle oder wählen Sie eine vorhandene Rolle aus. Um eine Rolle auszuwählen, klicken Sie auf Use an existing service role (Vorhandene Servicerolle verwenden). Wählen Sie dann unter IAM role (IAM-Rolle) die zu verwendende Rolle aus.
6. Wenn Sie bereit sind, die Spot-Instance-Unterbrechung zu initiieren, wählen Sie Initiate interruption (Unterbrechung initiieren) aus.

So erstellen Sie weitergehende Experimente zum Testen von Spot-Instance-Unterbrechungen über die AWS FIS -Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests (Spot-Anforderungen) aus.
3. Wählen Sie Actions (Aktionen) und dann Create advanced experiments (Erweiterte Experimente erstellen) aus.

   Die AWS FIS Konsole wird geöffnet. Weitere Informationen finden Sie unter Tutorial: Testen von Spot-Instance-Unterbrechungen mit AWS FIS im Benutzerhandbuch von AWS Fault Injection Service .

Überprüfen der Spot-Instance-Unterbrechung

Nach Initiierung der Unterbrechung geschieht Folgendes:

- Für die Spot Instance wird eine Empfehlung zum Neuausgleich der Instance ausgesprochen.
- Zwei Minuten vor der Unterbrechung Ihrer Instance wird eine Benachrichtigung zur AWS FIS Unterbrechung der Spot-Instance ausgegeben.
- Nach zwei Minuten wird die Spot Instance unterbrochen.
- Eine Spot-Instance, die gestoppt wurde, AWS FIS bleibt gestoppt, bis Sie sie neu starten.

So überprüfen Sie, ob die Instance nach Initiierung der Unterbrechung unterbrochen wurde

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Öffnen Sie im Navigationsbereich Spot Requests (Spot-Anforderungen) und Instances in separaten Browser-Registerkarten oder -Fenstern.
3. Wählen Sie für Spot-Anfragen die Spot-Instance-Anfrage oder die Spot-Flotten-Anfrage aus. Der ursprüngliche Status ist `fulfilled`. Nach Unterbrechung der Instance ändert sich der Status je nach Unterbrechungsverhalten wie folgt:
   - `terminate` – Der Status ändert sich zu `instance-terminated-by-experiment`.
   - `stop` – Der Status ändert sich zu `marked-for-stop-by-experiment` und dann zu `instance-stopped-by-experiment`.
4. Wählen Sie unter Instances die Spot Instance aus. Der ursprüngliche Status ist `Running`. Zwei Minuten nach Erhalt der Benachrichtigung über eine Spot-Instance-Unterbrechung ändert sich der Status je nach Unterbrechungsverhalten wie folgt:

- `stop` – Der Status ändert sich zu `Stopping` und dann zu `Stopped`.
- `terminate` – Der Status ändert sich zu `Shutting-down` und dann zu `Terminated`.

Kontingente

Ihre AWS-Konto hat das folgende Standardkontingent für die Anzahl der Spot-Instances, die pro Experiment unterbrochen AWS FIS werden können.

Name	Standard	Anpassbar	Beschreibung
Ziel SpotInstances für aws:ec2:send-spot-instance-interruptions	Jede unterstützte Region: 5	Yes (Ja)	Die maximale Anzahl von Spot-Instances, auf die aws:ec2: abzielen kann, wenn Sie Ziele mithilfe von Tags identifizieren, pro Experiment. send-spot-instance-interruptions

Sie können eine Kontingenterhöhung beantragen. Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Um alle Kontingente für anzuzeigen AWS FIS, öffnen Sie die Konsole Service Quotas. Wählen Sie im Navigationsbereich AWS -Services und dann AWS Fault Injection Service aus. Sie können sich auch alle Kontingente für AWS Fault Injection Service im AWS Fault Injection Service Benutzerhandbuch ansehen.

Spot-Instance-Unterbrechungsbenachrichtigungen

Eine Benachrichtigung über die Unterbrechung der Spot-Instance ist eine Warnung, die zwei Minuten vor dem Anhalten oder Beenden einer Spot-Instance durch Amazon EC2 ausgegeben wird. Wenn Sie den Ruhezustand als Verhalten bei Unterbrechungen festlegen, erhalten Sie eine Benachrichtigung über die Unterbrechung. Sie erhalten jedoch eine zweiminütige Warnung, da sofort in den Ruhezustand übergegangen wird.

Der beste Weg, um Spot-Instance-Unterbrechungen ordnungsgemäß zu handhaben, besteht darin, Ihre Anwendung so zu konzipieren, dass sie eine Fehlertoleranz aufweist. Um dies zu erreichen, können Sie die Vorteile von Benachrichtigungen über die Unterbrechung der Spot-Instance nutzen. Wir empfehlen, alle 5 Sekunden zu prüfen, ob derartige Benachrichtigungen über die Unterbrechung vorliegen.

Die Unterbrechungsbenachrichtigungen werden als EventBridge Ereignis und als Elemente in den Instance-Metadaten auf der Spot-Instance zur Verfügung gestellt. Unterbrechungsmitteilungen werden nach bestem Bemühen ausgegeben.

EC2 Spot Instance interruption notice

Wenn Amazon EC2 Ihre Spot-Instance unterbrechen wird, gibt es zwei Minuten vor der eigentlichen Unterbrechung ein Ereignis aus (außer für den Ruhezustand, der die Benachrichtigung über die Unterbrechung erhält, aber nicht zwei Minuten im Voraus, weil der Ruhezustand sofort beginnt). Dieses Ereignis kann von Amazon erkannt werden EventBridge. Weitere Informationen zu EventBridge Veranstaltungen finden Sie im EventBridge Amazon-Benutzerhandbuch. Ein detailliertes Beispiel, das Sie durch das Erstellen und Verwenden von Ereignisregeln führt, finden Sie unter Taking AdvanTage of Amazon EC2 Spot Instance Interruption Notices.

Das folgende Beispiel zeigt ein Ereignis für eine Spot-Instance-Unterbrechung. Die möglichen Werte für `instance-action` sind `hibernate`, `stop` und `terminate`.

```
{
    "version": "0",
    "id": "12345678-1234-1234-1234-123456789012",
    "detail-type": "EC2 Spot Instance Interruption Warning",
    "source": "aws.ec2",
    "account": "123456789012",
    "time": "yyyy-mm-ddThh:mm:ssZ",
    "region": "us-east-2",
    "resources": ["arn:aws:ec2:us-east-2a:instance/i-1234567890abcdef0"],
    "detail": {
        "instance-id": "i-1234567890abcdef0",
        "instance-action": "action"
    }
}
```

> **Note**
>
> Das ARN-Format des Spot-Instance-Unterbrechungsereignisses ist `arn:aws:ec2:`*`availability-zone`*`:instance/`*`instance-id`*. Dieses Format unterscheidet sich vom ARN-Format der EC2-Ressource.

instance-action

Wenn Ihre Spot-Instance durch Amazon EC2 für das Anhalten oder Beenden markiert wird, ist das `instance-action`-Element in den Instance-Metadaten vorhanden. Andernfalls ist es nicht vorhanden. Sie können den `instance-action` Instance Metadata Service Version 2 (IMDSv2) wie folgt abrufen.

Verwenden Sie den Befehl für Ihr Betriebssystem.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/spot/instance-action
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/instance-action
```

Das Element `instance-action` gibt die Aktion sowie den ungefähren Zeitpunkt in UTC an, an dem die Aktion ausgeführt wird.

Die folgende Beispielausgabe zeigt den Zeitpunkt an, an dem diese Instance angehalten wird.

```
{"action": "stop", "time": "2017-09-18T08:22:00Z"}
```

Die folgende Beispielausgabe zeigt den Zeitpunkt an, an dem diese Instance beendet wird.

```
{"action": "terminate", "time": "2017-09-18T08:22:00Z"}
```

Wenn Amazon EC2 keine Vorbereitungen vornimmt, die Instance anzuhalten oder zu beenden oder wenn Sie die Instance selbst beendet haben, ist das Element `instance-action` nicht in den Instance-Metadaten vorhanden und es wird ein HTTP-Fehler 404 gemeldet, wenn Sie versuchen, es abzurufen.

termination-time

Dieses Element wird nur beibehalten, um die Abwärtskompatibilität zu gewährleisten. Sie sollten stattdessen `instance-action` verwenden.

Wenn Ihre Spot-Instance von Amazon EC2 zur Kündigung gekennzeichnet ist (entweder aufgrund einer Spot-Instance-Unterbrechung, auf die das Unterbrechungsverhalten eingestellt ist`terminate`, oder aufgrund der Stornierung einer persistenten Spot-Instance-Anfrage), ist das `termination-time` Element in Ihren Instance-Metadaten vorhanden. Andernfalls ist es nicht vorhanden. Sie können das `termination-time` mithilfe von IMDSv2 wie folgt abrufen.

Verwenden Sie den Befehl für Ihr Betriebssystem.

Linux

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"`
[ec2-user ~]$ if curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-data/spot/termination-time | grep -q .*T.*Z; then echo
 termination_scheduled; fi
```

Windows

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/meta-data/spot/termination-time
```

Das `termination-time` Element gibt die ungefähre Uhrzeit in UTC an, zu der die Instance das Shutdown-Signal empfängt. Es folgt eine Beispielausgabe.

```
2015-01-05T18:02:00Z
```

Wenn Amazon EC2 sich nicht darauf vorbereitet, die Instance zu beenden (entweder weil es keine Spot-Instance-Unterbrechung gibt oder weil Ihr Unterbrechungsverhalten auf `stop` oder eingestellt

is`hibernate`) oder wenn Sie die Spot-Instance selbst beendet haben, ist das `termination-time` Element entweder nicht in den Instance-Metadaten vorhanden (Sie erhalten also einen HTTP 404-Fehler) oder enthält einen Wert, der kein Zeitwert ist.

Wenn Amazon EC2 die Instance nicht beenden kann, wird der Anforderungsstatus auf `fulfilled` gesetzt. Beachten Sie, dass der `termination-time`-Wert mit der ursprünglichen ungefähren Zeit, die jetzt in der Vergangenheit liegt, in den Instance-Metadaten verbleibt.

Finden von unterbrochenen Spot-Instances

In der Konsole werden im Bereich Instances alle Instances angezeigt, einschließlich Spot-Instances. Der Instance-Lebenszyklus einer Spot Instance ist `spot`. Der Instance-Status einer Spot Instance ist entweder `stopped` oder `terminated`, abhängig vom von Ihnen konfigurierten Unterbrechungsverhalten. Bei einer Spot-Instance im Ruhezustand lautet der Instance-Status `stopped`.

So finden Sie eine unterbrochene Spot Instance mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wenden Sie den folgenden Filter an: Instance-Lebenszyklus=Spot.
4. Wenden Sie je nach dem von Ihnen konfigurierten Unterbrechungsverhalten den Filter Instance-Status=angehalten oder Instance-Status=beendet an.
5. Suchen Sie für jede Spot Instance auf der Registerkarte Details unter Instance-Details nach der Meldung zum Statusübergang. Die folgenden Codes geben an, dass die Spot Instance unterbrochen wurde.
   - `Server.SpotInstanceShutdown`
   - `Server.SpotInstanceTermination`
6. Weitere Informationen zum Grund der Unterbrechung finden Sie im Statuscode für Spot-Anfragen. Weitere Informationen finden Sie unter the section called “Spot-Anforderungsstatus”.

Um unterbrochene Spot-Instances mit dem zu finden AWS CLI

Sie können Ihre unterbrochenen Spot-Instances mit dem Befehl describe-instances und dem Parameter `--filters` auflisten. Um nur die Instance-IDs in der Ausgabe aufzulisten, fügen Sie den Parameter `--query` hinzu.

Wenn das Unterbrechungsverhalten der Instance darin besteht, die Spot Instances zu beenden, verwenden Sie den folgenden Befehl:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=terminated Name=state-reason-code,Values=Server.SpotInstanceTermination \
    --query "Reservations[*].Instances[*].InstanceId"
```

Wenn das Unterbrechungsverhalten der Instance darin besteht, die Spot Instances anzuhalten, verwenden Sie den folgenden Befehl:

```
aws ec2 describe-instances \
    --filters Name=instance-lifecycle,Values=spot Name=instance-state-
name,Values=stopped Name=state-reason-code,Values=Server.SpotInstanceShutdown \
    --query "Reservations[*].Instances[*].InstanceId"
```

Ermitteln, ob Amazon EC2 eine Spot-Instance beendet hat

Wenn eine Spot-Instance beendet wird, können Sie CloudTrail damit sehen, ob Amazon EC2 die Spot-Instance beendet hat. In AWS CloudTrail gibt der Ereignisname `BidEvictedEvent` an, dass Amazon EC2 die Spot-Instance beendet hat.

Um BidEvictedEvent Ereignisse anzuzeigen in CloudTrail

1. Öffnen Sie die CloudTrail Konsole unter https://console.aws.amazon.com/cloudtrail/.
2. Wählen Sie im Navigationsbereich Ereignisverlauf aus.
3. Wählen Sie in der Filter-Dropdown-Liste die Option Eventname aus und geben Sie dann in das Filterfeld auf der rechten Seite BidEvictedEvent ein.
4. Wählen Sie in der daraufhin angezeigten Liste BidEvictedEreignis aus, um dessen Details anzuzeigen. Unter Event Record (Event-Datensatz), finden Sie die Instance-ID.

Weitere Informationen zur Verwendung von CloudTrail finden Sie unterAmazon EC2 EC2-API-Aufrufe protokollieren mit AWS CloudTrail.

Fakturierung für unterbrochene Spot-Instances

Wenn eine Spot Instance unterbrochen wird, werden Ihnen die Kosten für die Nutzung der Instance und des EBS-Volumes in Rechnung gestellt und es können weitere Gebühren anfallen.

Instance-Nutzung

Wer die Spot-Instance unterbricht	Betriebssystem	Unterbrochen in der ersten Stunde	Unterbrochen in jeder beliebigen Stunde nach der ersten Stunde
Wenn Sie die Spot-Instance anhalten oder beenden	Windows und Linux (ohne SUSE)	Berechnung der genutzten Sekunden	Berechnung der genutzten Sekunden
	SUSE	Berechnung der vollen Stunde, selbst wenn Sie sie nicht ganz genutzt haben	Berechnung der vollen genutzten Stunden; Berechnung einer ganzen Stunde für die unterbrochene Teilstunde
Wenn Amazon EC2 die Spot-Instance unterbricht	Windows und Linux (ohne SUSE)	Keine Gebühren	Berechnung der genutzten Sekunden
	SUSE	Keine Gebühren	Berechnung der vollen genutzten Stunden, keine Berechnung für die unterbrochene Teilstunde

EBS-Volume-Nutzung

Während eine unterbrochene Spot-Instance angehalten wird, werden nur Gebühren für die EBS-Volumes berechnet, die beibehalten werden.

Wenn bei der Verwendung einer EC2-Flotte und Spot-Flotte viele Instances angehalten wurden, können Sie das Limit für die Anzahl der EBS-Volumes in Ihrem Konto überschreiten.

Weitere Änderungen

Wenn für Ihre laufende Spot-Instance Gebühren für andere Dienste anfallen, z. B. für Datenübertragung, Elastic IP-Adressen oder die Nutzung anderer AWS verwalteter Services, wird Ihnen deren Nutzung in Rechnung gestellt. Dies gilt unabhängig davon, wer die Spot Instance unterbricht oder wann sie unterbrochen wurde. Auch wenn Ihnen die Spot-Instance-Nutzung nicht in Rechnung gestellt wird, wenn Amazon EC2 Ihre Spot Instance in der ersten Stunde unterbricht, können weitere Gebühren anfallen.

Weitere Informationen über andere Gebühren finden Sie unter Amazon EC2 – On-Demand-Preise.

Spot-Platzierungsbewertung

Die Spot-Placement-Score-Funktion kann auf der Grundlage Ihrer Spot-Kapazitätsanforderungen eine AWS Region oder Availability Zone empfehlen. Die Spot-Kapazität schwankt und Sie können nicht sicher sein, dass Sie immer die Kapazität erhalten, die Sie benötigen. Eine Spot-Platzierungsbewertung gibt an, wie wahrscheinlich es ist, dass eine Spot-Anforderung in einer Region oder Availability Zone erfolgreich ist.

> **Note**
>
> Eine Spot-Platzierungsbewertung bietet keine Garantien in Bezug auf die verfügbare Kapazität oder das Risiko einer Unterbrechung. Eine Spot-Platzierungsbewertung dient nur als Empfehlung.

Vorteile

Sie können das Spot-Platzierungsbewertungsfeature für Folgendes verwenden:

- Verlagerung und Skalierung der Spot-Rechenkapazität nach Bedarf in einer anderen Region als Reaktion auf einen erhöhten Kapazitätsbedarf oder eine verringerte verfügbare Kapazität in der aktuellen Region.
- Um die optimale Availability Zone zu identifizieren, in der Single-Availability-Zone-Workloads ausgeführt werden sollen.
- Um zukünftige Spot-Kapazitätsanforderungen zu simulieren, damit Sie eine optimale Region für die Erweiterung Ihrer Spot-basierten Workloads auswählen können.
- Um eine optimale Kombination von Instance-Typen zu finden, Ihre Spot-Kapazitätsanforderungen erfüllen.

Themen

Kosten

Für die Nutzung des Spot-Platzierungsbewertungsfeatures fallen keine zusätzlichen Gebühren an.

So funktioniert die Spot-Platzierungsbewertung

Wenn Sie das Spot-Platzierungsbewertungsfeature verwenden, geben Sie zuerst die Rechenanforderungen für Ihre Spot-Instances an. Amazon EC2 gibt dann die 10 wichtigsten Regionen oder Availability Zones zurück, in denen Ihre Spot-Anfrage wahrscheinlich erfolgreich ist. Jede Region oder Availability Zone wird auf einer Skala von 1 bis 10 bewertet. 10 gibt an, dass Ihre Spot-Anforderung sehr wahrscheinlich erfolgreich ist und 1 zeigt an, dass Ihre Spot-Anforderung wahrscheinlich nicht erfolgreich sein wird.

Gehen Sie wie folgt vor, um das Spot-Platzierungsbewertungsfeature zu verwenden:

- Schritt 1: Geben Sie Ihre Spot-Anforderungen an
- Schritt 2: Filtern Sie die Antwort auf die Spot-Platzierungsbewertung
- Schritt 3: Überprüfen Sie die Empfehlungen
- Schritt 4: Nutzen Sie die Empfehlungen

Schritt 1: Geben Sie Ihre Spot-Anforderungen an

Zuerst geben Sie wie folgt Ihre gewünschte Ziel-Spot-Kapazität und die Rechenanforderungen an:

1. Geben Sie die Ziel-Spot-Kapazität und optional die Zielkapazitätseinheit an.

   Sie können Ihre gewünschte Ziel-Spot-Kapazität in Bezug auf die Anzahl der Instances oder vCPUs oder hinsichtlich der Speichermenge in MiB angeben. Um die Zielkapazität in der Anzahl der vCPUs oder der Speichermenge anzugeben, müssen Sie die Zielkapazitätseinheit auf `vcpu` oder `memory-mib` festlegen. Andernfalls wird standardmäßig die Anzahl der Instances angegeben.

   Indem Sie Ihre Zielkapazität in Bezug auf die Anzahl der vCPUs oder die Speichermenge angeben, können Sie diese Einheiten beim Zählen der Gesamtkapazität verwenden. Wenn Sie beispielsweise eine Mischung aus Instances unterschiedlicher Größe verwenden möchten, können Sie die Zielkapazität als Gesamtzahl von vCPUs angeben. Das Spot-Platzierungsbewertungsfeature berücksichtigt dann jeden Instance-Typ in der Anforderung nach der Anzahl von vCPUs und zählt die Gesamtzahl der vCPUs anstelle der Gesamtzahl der Instances bei der Summe der Zielkapazität.

Angenommen, Sie geben eine Gesamtzielkapazität von 30 vCPUs an und Ihre Instance-Typliste besteht aus c5.xlarge (4 vCPUs), m5.2xlarge (8 vCPUs) und r5.large (2 vCPUs). Um insgesamt 30 vCPUs zu erreichen, könnten Sie eine Mischung aus 2 c5.xlarge (2* 4 vCPUs), 2 m5.2xlarge (2* 8 vCPUs) und 3 r5.large (3* 2 vCPUs) erhalten.

2. Geben Sie Instance-Typen oder Instance-Attribute an.

   Sie können entweder die zu verwendenden Instance-Typen angeben oder die Instance-Attribute angeben, die Sie für Ihre Rechenanforderungen benötigen, und Amazon EC2 dann die Instance-Typen identifizieren lassen, die diese Attribute haben. Das wird als attributbasierte Instance-Typauswahl bezeichnet.

   Sie können nicht sowohl Instance-Typen als auch Instance-Attribute in derselben Anforderung einer Spot-Platzierungsbewertung angeben.

   Beim Festlegen von Instance-Typen müssen Sie mindestens drei verschiedene Instance-Typen angeben, andernfalls gibt Amazon EC2 eine niedrige Spot-Platzierungsbewertung zurück. Wenn Sie Instance-Aattribute angeben, müssen diese auf mindestens drei verschiedene Instance-Typen aufgelöst werden.

Beispiele für verschiedene Möglichkeiten zur Festlegung Ihrer Spot-Anforderungen finden Sie unter Beispielkonfigurationen.

Schritt 2: Filtern Sie die Antwort auf die Spot-Platzierungsbewertung

Amazon EC2 berechnet die Spot-Platzierungsbewertung für jede Region oder Availability Zone und gibt entweder die Top 10 Regionen oder die Top 10 Availability Zones zurück, in denen Ihre Spot-Anfrage wahrscheinlich erfolgreich ist. Standardmäßig wird eine Liste der bewerteten Regionen zurückgegeben. Wenn Sie planen, Ihre gesamte Spot-Kapazität in einer einzigen Availability Zone zu starten, ist es hilfreich, eine Liste der bewerteten Availability Zones anzufordern.

Sie können einen Regionsfilter angeben, um die Regionen einzugrenzen, die in der Antwort zurückgegeben werden.

Sie können den Regionsfilter und eine Anforderung für bewertete Availability Zones kombinieren. Auf diese Weise beschränken sich die bewerteten Availability Zones auf die Regionen, nach denen Sie gefiltert haben. Um die am höchsten bewertete Availability Zone in einer Region zu finden, geben Sie nur diese Region an. Die Antwort gibt eine Liste aller Availability Zones in dieser Region zurück.

Schritt 3: Überprüfen Sie die Empfehlungen

Die Spot-Platzierungsbewertung für jede Region oder Availability Zone wird basierend auf der Zielkapazität, der Zusammensetzung der Instance-Typen, den historischen und aktuellen Spot-Nutzungstrends und dem Zeitpunkt der Anfrage berechnet. Da die Spot-Kapazität ständig schwankt, kann dieselbe Anforderung der Spot-Platzierungsbewertung zu unterschiedlichen Bewertungen führen, wenn sie zu unterschiedlichen Zeiten berechnet wird.

Regionen und Availability Zones werden auf einer Skala von 1 bis 10 bewertet. Eine Punktzahl von 10 zeigt an, dass Ihre Spot-Anforderung sehr wahrscheinlich erfolgreich sein wird – sicher ist das aber nicht. Ein Ergebnis von 1 zeigt an, dass Ihre Spot-Anforderung sehr wahrscheinlich nicht erfolgreich sein wird. Dasselbe Ergebnis kann für verschiedene Regionen oder Availability Zones zurückgegeben werden.

Wenn niedrige Punktzahlen zurückgegeben werden, können Sie Ihre Berechnungsanforderungen bearbeiten und den Punktestand neu berechnen. Sie können auch Empfehlungen für die Spot-Bewertung für die gleichen Berechnungsanforderungen zu verschiedenen Tageszeiten anfordern.

Schritt 4: Nutzen Sie die Empfehlungen

Eine Spot-Platzierungsbewertung ist nur relevant, wenn Ihre Spot-Anforderung genau dieselbe Konfiguration wie die Spot-Platzierungsbewertung hat (Zielkapazität, Zielkapazitätseinheit und Instance-Typen oder Instance-Attribute) und für die Verwendung der `capacity-optimized`-Zuweisungsstrategie konfiguriert ist. Andernfalls stimmt die Wahrscheinlichkeit, die verfügbare Spot-Kapazität zu erhalten, nicht mit der Bewertung überein.

Während eine Spot-Platzierungsbewertung als Richtlinie dient und nicht garantiert, dass Ihre Spot-Anforderung vollständig oder teilweise erfüllt wird, können Sie die folgenden Informationen verwenden, um die besten Ergebnisse zu erzielen:

- Verwenden Sie dieselbe Konfiguration – Die Spot-Platzierungsbewertung ist nur relevant, wenn die Spot-Anforderungskonfiguration (Zielkapazität, Zielkapazitätseinheit und Instance-Typen oder Instance-Attribute) in Ihrer Auto-Scaling-Gruppe, EC2-Flotte oder Spot-Flotte mit dem übereinstimmt, was Sie zur Erzielung der Spot-Platzierungsbewertung eingegeben haben.

  Wenn Sie in Ihrer Anforderung der Spot-Platzierungsbewertung die attributbasierte Instance-Typauswahl verwendet haben, können Sie Ihre Auto-Scaling-Gruppe, EC2-Flotte oder Spot-Flotte mithilfe der attributbasierten Instance-Typauswahl konfigurieren. Weitere Informationen finden Sie unter Erstellen einer Auto-Scaling-Gruppe mit einer Reihe von Anforderungen für die verwendeten

Instance-Typen , Attributbasierte Auswahl von Instance-Typen für EC2-Flotte und Attributbasierte Auswahl von Instance-Typen für Spot-Flotte.

> **Note**
>
> Wenn Sie Ihre Zielkapazität in Bezug auf die Anzahl der vCPUs oder die Speichermenge angegeben haben und Instance-Typen in Ihrer Konfiguration der Spot-Platzierungsbewertung angegeben haben, beachten Sie, dass Sie diese Konfiguration derzeit nicht in Ihrer Auto-Scaling-Gruppe, EC2-Flotte oder Spot-Flotte erstellen können. Stattdessen müssen Sie die Instance-Gewichtung manuell festlegen, indem Sie den `WeightedCapacity`-Parameter verwenden.

- Verwenden der **`capacity-optimized`**-Zuweisungsstrategie – Bei jeder Bewertung wird davon ausgegangen, dass Ihre Flotten-Anforderung so konfiguriert ist, dass alle Availability Zones (für die Anforderung von Kapazität über Regionen hinweg) oder eine einzelne Availability Zone (wenn Sie Kapazität in einer Availability Zone anfordern) und die `capacity-optimized`-Spot-Zuweisungsstrategie für Ihre Anforderung der Spot-Kapazität erfolgreich sind. Wenn Sie andere Zuweisungsstrategien verwenden, z. B. `lowest-price`, stimmt die Wahrscheinlichkeit, dass Spot-Kapazität verfügbar ist, nicht mit der Bewertung überein.
- Handeln Sie sofort bei einer Punktzahl – Die Empfehlung der Spot-Platzierungsbewertung spiegelt die verfügbare Spot-Kapazität zum Zeitpunkt der Anforderung wider und dieselbe Konfiguration kann zu unterschiedlichen Ergebnissen führen, wenn sie aufgrund von Spot-Kapazitätsschwankungen zu unterschiedlichen Zeiten berechnet wird. Eine Punktzahl von 10 bedeutet zwar, dass Ihre Spot-Kapazitätsanforderung mit hoher Wahrscheinlichkeit – aber nicht garantiert – erfolgreich ist, aber für beste Ergebnisse empfehlen wir Ihnen, sofort auf eine Punktzahl zu reagieren. Wir empfehlen Ihnen auch, bei jedem Erstellen einer Kapazitätsanforderung eine neue Bewertung einzuholen.

Einschränkungen

- Zielkapazitätslimit – Ihr Zielkapazitätslimit für die Spot-Platzierung basiert auf Ihrer jüngsten Spot-Nutzung und berücksichtigt gleichzeitig ein potenzielles Nutzungswachstum. Wenn Sie in letzter Zeit keine Spot-Nutzung haben, bieten wir Ihnen ein niedriges Standardlimit, das auf Ihr Spot-Anfragelimit abgestimmt ist.
- Limit für Konfigurationen anfordern – Wir können die Anzahl neuer Anforderungskonfigurationen innerhalb eines Zeitraums von 24 Stunden begrenzen, wenn wir Muster erkennen, die nicht mit der beabsichtigten Verwendung des Spot-Platzierungsbewertungsfeatures verbunden sind. Wenn

Sie das Limit erreicht haben, können Sie die bereits verwendeten Anforderungskonfigurationen wiederholen, aber neue Anforderungskonfigurationen lassen sich erst im nächsten Zeitraum von 24 Stunden angeben.

- Mindestanzahl der Instance-Typen – Wenn Sie Instance-Typen angeben, müssen Sie mindestens drei verschiedene Instance-Typen angeben, andernfalls gibt Amazon EC2 einen niedrigen Spot-Platzierungswert zurück. Wenn Sie Instance-Aattribute angeben, müssen diese auf mindestens drei verschiedene Instance-Typen aufgelöst werden. Instance-Typen gelten als unterschiedlich, wenn sie einen anderen Namen haben. Zum Beispiel gelten m5.8xlarge, m5a.8xlarge und m5.12xlarge als unterschiedlich.

Erforderliche IAM-Berechtigung

IAM-Identitäten (Benutzer, Rollen oder Gruppen) sind standardmäßig nicht berechtigt, das Feature Spot-Platzierung zu verwenden. Damit IAM-Identitäten das Spot-Platzierungsbewertungsfeature verwenden können, müssen Sie eine IAM-Richtlinie erstellen, die die Berechtigung zur Verwendung der `ec2:GetSpotPlacementScores`-EC2-API-Aktion erteilt. Anschließend fügen Sie die Richtlinie an die IAM-Identitäten an, die diese Berechtigung erfordern.

Im Folgenden finden Sie ein Beispiel für eine IAM-Richtlinie, die die Berechtigung zur Verwendung der `ec2:GetSpotPlacementScores`-EC2-API-Aktion erteilt.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:GetSpotPlacementScores",
            "Resource": "*"
        }
    ]
}
```

Informationen zum Bearbeiten einer IAM-Richtlinie finden Sie unter Bearbeiten von IAM-Richtlinien im IAM-Benutzerhandbuch.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Berechnen Sie eine Spot-Platzierungsbewertung

Sie können eine Spot-Platzierungsbewertung berechnen, indem Sie die Amazon-EC2-Konsole oder AWS CLI verwenden.

Themen

- Berechnen einer Spot-Platzierungsbewertung durch Angabe von Instance-Attributen (Konsole)
- Berechnen Sie eine Spot-Platzierungsbewertung durch Angabe von Instance-Typen (Konsole)
- Berechnen Sie eine Spot-Platzierungsbewertung (AWS CLI)

Berechnen einer Spot-Platzierungsbewertung durch Angabe von Instance-Attributen (Konsole)

So berechnen Sie eine Spot-Platzierungsbewertung durch Angabe von Instance-Attributen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Spot-Platzierungsbewertung aus.
4. Wählen Sie Anforderungen eingeben aus.
5. Geben Sie unter Zielkapazität Ihre gewünschte Kapazität in Bezug auf die Anzahl der Instances oder vCPUs oder die Arbeitsspeichermenge (MiB) ein.
6. Wählen Sie für Instance type requirements (Anforderungen hinsichtlich des Instance-Typs) die Option Specify instance attributes that match your compute requirements (Instance-Attribute

angeben, die Ihren Rechenanforderungen entsprechen) aus, damit Amazon EC2 die optimalen Instance-Typen für diese Anforderungen identifiziert.

7. Geben Sie für vCPUs die gewünschte minimale und maximale Anzahl der vCPUs ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beides.
8. Geben Sie für Arbeitsspeicher (GiB) den gewünschten Mindest- und Höchstwert ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beides.
9. Wählen Sie für CPU-Architektur die erforderliche Instance-Architektur aus.
10. (Optional) Für Zusätzliche Instance-Attribute können Sie optional ein oder mehrere Attribute angeben, um Ihre Computinganforderungen genauer auszudrücken. Jedes zusätzliche Attribut fügt Ihrer Anforderung weitere Einschränkungen hinzu. Sie können die zusätzlichen Attribute weglassen. In diesem Fall werden die Standardwerte verwendet. Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-spot-placement-scores in der Amazon-EC2-Befehlszeilenreferenz.
11. (Optional) Um die Instance-Typen mit Ihren angegebenen Attributen anzuzeigen, erweitern Sie Vorschau der übereinstimmenden Instance-Typen. Um Instance-Typen von der Verwendung in der Platzierungsauswertung auszuschließen, wählen Sie die Instances aus und wählen Sie dann Ausgewählte Instance-Typen ausschließen.
12. Klicken Sie auf Platzierungsbewertungen laden und überprüfen Sie die Ergebnisse.
13. (Optional) Um die Spot-Platzierungsbewertung für bestimmte Regionen anzuzeigen, wählen Sie für Auszuwertende Regionen die zu bewertenden Regionen und dann Platzierungsbewertungen berechnen aus.
14. (Optional) Um die Spot-Platzierungsbewertung für die Availability Zones in den angezeigten Regionen anzuzeigen, aktivieren Sie das Kontrollkästchen Provide placement scores per Availability Zone (Platzierungsbewertungen pro Availability Zone bereitstellen). Eine Liste der bewerteten Availability Zones ist nützlich, wenn Sie Ihre gesamte Spot-Kapazität in einer einzigen Availability Zone starten möchten.
15. (Optional) Um Ihre Rechenanforderungen zu bearbeiten und einen neuen Platzierungswert zu erhalten, wählen Sie Bearbeiten, nehmen Sie die notwendigen Anpassungen vor und wählen Sie dann Berechnen von Platzierungswerten aus.

Berechnen Sie eine Spot-Platzierungsbewertung durch Angabe von Instance-Typen (Konsole)

So berechnen Sie eine Spot-Platzierungsbewertung durch Angabe von Instance-Typen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Spot-Platzierungsbewertung aus.
4. Wählen Sie Anforderungen eingeben aus.
5. Geben Sie unter Zielkapazität Ihre gewünschte Kapazität in Bezug auf die Anzahl der Instances oder vCPUs oder die Arbeitsspeichermenge (MiB) ein.
6. Um die zu verwendenden Instance-Typen anzugeben, wählen Sie unter Instance-Typanforderungen die Option Instance-Typen manuell auswählen aus.
7. Klicken Sie auf Instance-Typen auswählen, wählen Sie die Instance-Typen aus, die verwendet werden sollen und klicken Sie dann auf Auswählen. Um Instance-Typen schnell zu finden, können Sie die Instance-Typen mithilfe der Filterleiste nach verschiedenen Eigenschaften filtern.
8. Klicken Sie auf Platzierungsbewertungen laden und überprüfen Sie die Ergebnisse.
9. (Optional) Um die Spot-Platzierungsbewertung für bestimmte Regionen anzuzeigen, wählen Sie für Auszuwertende Regionen die zu bewertenden Regionen und dann Platzierungsbewertungen berechnen aus.
10. (Optional) Um die Spot-Platzierungsbewertung für die Availability Zones in den angezeigten Regionen anzuzeigen, aktivieren Sie das Kontrollkästchen Provide placement scores per Availability Zone (Platzierungsbewertungen pro Availability Zone bereitstellen). Eine Liste der bewerteten Availability Zones ist nützlich, wenn Sie Ihre gesamte Spot-Kapazität in einer einzigen Availability Zone starten möchten.
11. (Optional) Um die Liste der Instance-Typen zu bearbeiten und einen neuen Platzierungswert zu erhalten, wählen Sie Bearbeiten, nehmen Sie die notwendigen Anpassungen vor und wählen Sie dann Berechnen von Platzierungswerten aus.

Berechnen Sie eine Spot-Platzierungsbewertung (AWS CLI)

Berechnen Sie die Spot-Platzierungsbewertung

1. (Optional) Um alle möglichen Parameter zu generieren, die für die Konfiguration der Spot-Platzierungsbewertung angegeben werden können, verwenden Sie den Befehl get-spot-placement-scores und den `--generate-cli-skeleton`-Parameter.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --generate-cli-skeleton
```

Erwartete Ausgabe


```
{
    "InstanceTypes": [
        ""
    ],
    "TargetCapacity": 0,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "RegionNames": [
        ""
    ],
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": [
            "x86_64_mac"
        ],
        "VirtualizationTypes": [
            "hvm"
        ],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 0,
                "Max": 0
            },
            "MemoryMiB": {
                "Min": 0,
                "Max": 0
            },
            "CpuManufacturers": [
                "amd"
            ],
            "MemoryGiBPerVCpu": {
                "Min": 0.0,
                "Max": 0.0
            },
            "ExcludedInstanceTypes": [
                ""
            ],
            "InstanceGenerations": [
                "previous"
            ],
            "SpotMaxPricePercentageOverLowestPrice": 0,
            "OnDemandMaxPricePercentageOverLowestPrice": 0,
```

```
            "BareMetal": "excluded",
            "BurstablePerformance": "excluded",
            "RequireHibernateSupport": true,
            "NetworkInterfaceCount": {
                "Min": 0,
                "Max": 0
            },
            "LocalStorage": "included",
            "LocalStorageTypes": [
                "hdd"
            ],
            "TotalLocalStorageGB": {
                "Min": 0.0,
                "Max": 0.0
            },
            "BaselineEbsBandwidthMbps": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorTypes": [
                "fpga"
            ],
            "AcceleratorCount": {
                "Min": 0,
                "Max": 0
            },
            "AcceleratorManufacturers": [
                "amd"
            ],
            "AcceleratorNames": [
                "vu9p"
            ],
            "AcceleratorTotalMemoryMiB": {
                "Min": 0,
                "Max": 0
            }
        }
    },
    "DryRun": true,
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Erstellen Sie eine JSON-Konfigurationsdatei mit der Ausgabe des vorherigen Schritts und konfigurieren Sie sie wie folgt:

   a. Geben Sie für `TargetCapacity` Ihre gewünschte Spot-Kapazität in Bezug auf die Anzahl der Instances oder vCPUs oder die Speichermenge (MiB) ein.

   b. Geben Sie für `TargetCapacityUnitType` die Einheit für die Zielkapazität ein. Wenn Sie diesen Parameter weglassen, wird standardmäßig `units` verwendet.

      Zulässige Werte: `units` (bedeutet eine Anzahl der Instances) | `vcpu` | `memory-mib`

   c. Geben Sie für `SingleAvailabilityZone` `true` für eine Antwort an, die eine Liste bewerteter Availability Zones zurückgibt. Eine Liste der bewerteten Availability Zones ist nützlich, wenn Sie Ihre gesamte Spot-Kapazität in einer einzigen Availability Zone starten möchten. Wenn Sie diesen Parameter weglassen, wird standardmäßig `false` verwendet und die Antwort gibt eine Liste der bewerteten Regionen zurück.

   d. (Optional) Geben Sie für `RegionNames` die Regionen an, die als Filter verwendet werden soll(en). Sie müssen den Regionscode angeben, z. B. `us-east-1`.

      Bei einem Regionsfilter gibt die Antwort nur die von Ihnen angegebenen Regionen zurück. Wenn Sie `true` für `SingleAvailabilityZone` angegeben haben, gibt die Antwort nur die Availability Zones in den angegebenen Regionen zurück.

   e. Sie können entweder `InstanceTypes` oder `InstanceRequirements` aufnehmen, jedoch nicht beide in derselben Konfiguration.

      Geben Sie in Ihrer JSON-Konfiguration eine der folgenden Optionen an:

      - Um eine Liste der Instance-Typen anzugeben, geben Sie die Instance-Typen im `InstanceTypes`-Parameter an. Geben Sie mindestens drei verschiedene Instance-Typen an. Wenn Sie nur einen oder zwei Instance-Typen angeben, gibt die Spot-Bewertungsplatzierung eine niedrige Bewertung zurück. Eine Liste der Instance-Typen finden Sie unter Amazon-EC2-Instance-Typen.
      - Um die Instance-Attribute anzugeben, damit Amazon EC2 die Instance-Typen identifiziert, die diesen Attributen entsprechen, geben Sie die Attribute an, die sich in der `InstanceRequirements`-Struktur befinden.

        Sie müssen Werte für `VCpuCount`, `MemoryMiB` und `CpuManufacturers` angeben. Sie können die anderen Attribute weglassen. In diesem Fall werden die Standardwerte

verwendet. Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-spot-placement-scores in der Amazon-EC2-Befehlszeilenreferenz.

Beispielkonfigurationen finden Sie unter Beispielkonfigurationen.

3. Um die Spot-Platzierungsbewertung für die in der JSON-Datei angegebenen Anforderungen abzurufen, verwenden Sie den Befehl get-spot-placement-scores und geben Sie mithilfe des `--cli-input-json`-Parameters den Namen und den Pfad zu Ihrer JSON-Datei an.

```
aws ec2 get-spot-placement-scores \
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

Beispielausgabe, wenn `SingleAvailabilityZone` auf `false` gesetzt oder weggelassen ist (in diesem Fall wird standardmäßig `false` verwendet) – eine bewertete Liste von Regionen wird zurückgegeben

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "Score": 7
    },
    {
        "Region": "us-west-1",
        "Score": 5
    },
   ...
```

Beispielausgabe, wenn `SingleAvailabilityZone` auf `true` gesetzt ist – eine bewertete Liste von Availability Zones wird zurückgegeben

```
"SpotPlacementScores": [
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "use1-az1"
        "Score": 8
    },
    {
        "Region": "us-east-1",
        "AvailabilityZoneId": "usw2-az3"
```

```
        "Score": 6
    },
   ...
```

Beispielkonfigurationen

Bei der AWS CLI Verwendung von können Sie die folgenden Beispielkonfigurationen verwenden.

Beispielkonfigurationen

- Beispiel: Instance-Typen und Zielkapazität angeben
- Beispiel: Instance-Typen und Zielkapazität in Bezug auf Arbeitsspeicher angeben
- Beispiel: Angeben von Attributen für die attributbasierte Instance-Typauswahl
- Beispiel: Geben Sie Attribute für die attributbasierte Instance-Typauswahl an und geben Sie eine bewertete Liste von Availability Zones zurück

Beispiel: Instance-Typen und Zielkapazität angeben

Die folgende Beispielkonfiguration gibt drei verschiedene Instance-Typen und eine Ziel-Spot-Kapazität von 500 Spot-Instances an.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500
}
```

Beispiel: Instance-Typen und Zielkapazität in Bezug auf Arbeitsspeicher angeben

Die folgende Beispielkonfiguration gibt drei verschiedene Instance-Typen und eine Ziel-Spot-Kapazität von 500 000 MiB Speicher an, wobei die Anzahl der zu startenden Spot-Instances insgesamt 500 000 MiB Speicher bereitstellen muss.

```
{
    "InstanceTypes": [
        "m5.4xlarge",
```

```
        "r5.2xlarge",
        "m4.4xlarge"
    ],
    "TargetCapacity": 500000,
    "TargetCapacityUnitType": "memory-mib"
}
```

Beispiel: Angeben von Attributen für die attributbasierte Instance-Typauswahl

Die folgende Beispielkonfiguration ist für die attributbasierte Instance-Typauswahl konfiguriert, gefolgt von einer Texterklärung der Beispielkonfiguration.

```
{
    "TargetCapacity": 5000,
    "TargetCapacityUnitType": "vcpu",
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

`InstanceRequirementsWithMetadata`

Um die attributbasierte Instance-Typauswahl zu verwenden, müssen Sie die `InstanceRequirementsWithMetadata`-Struktur in Ihre Konfiguration aufnehmen und die gewünschten Attribute für die Spot-Instances angeben.

Im vorherigen Beispiel werden die folgenden erforderlichen Instance-Attribute angegeben:

- `ArchitectureTypes` – Der Architekturtyp der Instance-Typen muss `arm64` sein.
- `VirtualizationTypes` – Der Virtualisierungstyp der Instance-Typen muss `hvm` sein.
- `VCpuCount` – Die Instance-Typen müssen mindestens 1 und maximal 12 vCPUs aufweisen.

- `MemoryMiB` – Die Instance-Typen müssen mindestens 512 MiB Speicher aufweisen. Indem Sie den `Max`-Parameter weglassen, geben Sie an, dass es keine Höchstgrenze gibt.

Beachten Sie, dass es mehrere andere optionale Attribute gibt, die Sie angeben können. Eine Liste der Attribute finden Sie unter get-spot-placement-scores in der Amazon-EC2-Befehlszeilenreferenz..

`TargetCapacityUnitType`

Der `TargetCapacityUnitType`-Parameter gibt die Einheit für die Zielkapazität an. Im Beispiel ist die Zielkapazität `5000` und der Einheitentyp der Zielkapazität `vcpu`. Zusammen wird eine gewünschte Zielkapazität von 5000 vCPUs angegeben, wobei die Anzahl der zu startenden Spot-Instances insgesamt 5000 vCPUs bereitstellen muss.

Beispiel: Geben Sie Attribute für die attributbasierte Instance-Typauswahl an und geben Sie eine bewertete Liste von Availability Zones zurück

Die folgende Beispielkonfiguration ist für die attributbasierte Instance-Typauswahl konfiguriert. Indem Sie `"SingleAvailabilityZone": true` angeben, gibt die Antwort eine Liste der bewerteten Availability Zones zurück.

```
{
    "TargetCapacity": 1000,
    "TargetCapacityUnitType": "vcpu",
    "SingleAvailabilityZone": true,
    "InstanceRequirementsWithMetadata": {
        "ArchitectureTypes": ["arm64"],
        "VirtualizationTypes": ["hvm"],
        "InstanceRequirements": {
            "VCpuCount": {
                "Min": 1,
                "Max": 12
            },
            "MemoryMiB": {
                "Min": 512
            }
        }
    }
}
```

Spot-Instance-Daten-Feed

Damit Sie die Gebühren für Ihre Spot-Instance besser überblicken können, stellt Amazon EC2 einen Daten-Feed zu Ihrer Spot-Instance-Nutzung und dem entsprechenden Preisverlauf bereit. Dieser Daten-Feed wird an den Amazon S3-Bucket gesendet, den Sie beim Abonnieren des Daten-Feeds angegeben haben.

Daten-Feed-Dateien treffen in der Regel einmal pro Stunde in Ihrem Bucket ein und jede Nutzungsstunde wird in der Regel in einer einzelnen Datendatei abgedeckt. Diese Dateien werden komprimiert (gzip), bevor sie an Ihren Bucket geliefert werden. Amazon EC2 kann mehrere Dateien für eine bestimmte Nutzungsstunde schreiben, wenn die Dateien groß sind (beispielsweise wenn die Dateiinhalte für die Stunde vor der Komprimierung 50 MB überschreiten).

> **Note**
>
> Sie können jeweils nur einen Spot-Instance-Datenfeed erstellen AWS-Konto. Wenn während einer bestimmten Stunde keine Spot-Instance ausgeführt wird, erhalten Sie für diese Stunde keine Daten-Feed-Datei.

Der Spot-Instance-Datenfeed wird in allen AWS Regionen außer China (Peking), China (Ningxia), AWS GovCloud (USA) und den Regionen unterstützt, die standardmäßig deaktiviert sind.

Inhalt

Name und Format der Daten-Feed-Datei

Der Name der Daten-Feed-Datei für eine Spot-Instance weist das folgende Format auf (Datum und Uhrzeit in UTC):

```
bucket-name.s3.amazonaws.com/optional-prefix/aws-account-id.YYYY-MM-DD-HH.n.unique-id.gz
```

Wenn Ihr Bucket-Name beispielsweise **my-bucket-name** lautet und Ihr Präfix **my-prefix**, dann sehen Ihre Dateinamen in etwa wie folgt aus:

```
my-bucket-name.s3.amazonaws.com/my-prefix/111122223333.2023-12-09-07.001.b959dbc6.gz
```

Weitere Informationen zu Bucket-Namen finden Sie unter Regeln für die Bucket-Benennung im Benutzerhandbuch für Amazon S3.

Die Daten-Feed-Dateien für die Spot-Instance verwenden Tabulatoren als Trennzeichen. Jede Zeile in der Datendatei entspricht einer Instance-Stunde und enthält die in der folgenden Tabelle aufgeführten Felder.

Feld	Beschreibung
`Timestamp`	Der Zeitstempel, der zur Berechnung des Preises für diese Instance-Nutzung verwendet wird.
`UsageType`	Die Art der Nutzung und der Instance-Typ, für die diese Kosten anfallen. Für `m1.small` Spot-Instances ist dieses Feld auf `SpotUsage` festgelegt. Bei allen anderen Instance-Typen ist dieses Feld auf `SpotUsage:` {Instance-type} eingestellt. z. B. `SpotUsage:c1.medium` .
`Operation`	Das Produkt, für das diese Kosten anfallen. Bei Linux-Spot-Instances ist dieses Feld auf `RunInstances` eingestellt. Bei Windows-Spot-Instances ist dieses Feld auf `RunInstances:0002` eingestellt. Die Spot-Nutzung wird nach den Availability Zones gruppiert.
`InstanceID`	Die ID der Spot-Instance, die diese Instance-Nutzung generiert hat.
`MyBidID`	Die ID der Spot-Instance-Anforderung, die diese Instance-Nutzung generiert hat.

Feld	Beschreibung
`MyMaxPrice`	Der für diese Spot-Anforderung angegebene Höchstpreis.
`MarketPrice`	Der Spot-Preis zu dem im Feld `Timestamp` angegebenen Zeitpunkt.
`Charge`	Der für diese Instance-Nutzung berechnete Preis
`Version`	Die Version des Datenfeeds. Die mögliche Version ist 1.0.

Anforderungen für den Amazon S3-Bucket

Beim Abonnieren des Daten-Feeds müssen einen Amazon S3-Bucket angeben, in dem die Daten-Feed-Dateien gespeichert werden sollen.

Beachten Sie bei der Auswahl eines Amazon S3-Buckets für den Daten-Feed Folgendes:

- Sie müssen eine `FULL_CONTROL`-Berechtigung für den Bucket haben. Wenn Sie der Bucket-Eigentümer sind, verfügen Sie standardmäßig über diese Berechtigung. Andernfalls muss der Bucket-Besitzer Ihnen AWS-Konto diese Erlaubnis erteilen.
- Wenn Sie einen Datenfeed abonnieren, werden diese Berechtigungen verwendet, um die Bucket-ACL zu aktualisieren, sodass dem AWS Datenfeed-Konto die entsprechenden `FULL_CONTROL` Berechtigungen erteilt werden. Das AWS Datenfeed-Konto schreibt Datenfeed-Dateien in den Bucket. Wenn Ihr Konto nicht über die erforderlichen Berechtigungen verfügt, können die Daten-Feed-Dateien nicht in den Bucket geschrieben werden. Weitere Informationen finden Sie unter An Amazon S3 gesendete Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

  > **Note**
  >
  > Wenn Sie die ACL aktualisieren und die Berechtigungen für das AWS Datenfeed-Konto entfernen, können die Datenfeed-Dateien nicht in den Bucket geschrieben werden. Sie müssen den Daten-Feed erneut abonnieren, um die Daten-Feed-Dateien zu erhalten.

- Jede Daten-Feed-Datei verfügt über eine eigene ACL (unabhängig von der ACL für den Bucket). Der Bucket-Eigentümer verfügt über eine `FULL_CONTROL`-Berechtigung für die Datendateien. Das AWS Datenfeed-Konto hat Lese- und Schreibberechtigungen.

- Wenn Sie deaktivierte ACLs für Ihre Buckets angewendet haben, fügen Sie eine Bucket-Richtlinie hinzu, die Benutzern mit Vollzugriff das Schreiben in den Bucket ermöglicht. Weitere Informationen finden Sie unter Bucket-Richtlinien überprüfen und aktualisieren.
- Wenn Sie Ihr Datenfeed-Abonnement löschen, entfernt Amazon EC2 die Lese- und Schreibberechtigungen für das AWS Datenfeed-Konto weder für den Bucket noch für die Datendateien. Sie müssen diese Berechtigungen selbst entfernen.
- Sie müssen einen vom Kunden verwalteten Schlüssel verwenden, wenn Sie Ihren Amazon S3 S3-Bucket mit serverseitiger Verschlüsselung mit einem in AWS Key Management Service (SSE-KMS) gespeicherten AWS KMS Schlüssel verschlüsseln. Weitere Informationen finden Sie unter serverseitige Amazon S3 S3-Bucket-Verschlüsselung im Amazon CloudWatch Logs-Benutzerhandbuch.

> **Note**
>
> Für den Spot-Instance-Datenfeed ist die Ressource, die die S3-Dateien generiert, nicht mehr Amazon CloudWatch Logs. Daher müssen Sie die `aws:SourceArn` aus der S3-Bucket-Berechtigungsrichtlinie und aus der KMS-Richtlinie entfernen.

Abonnieren eines Spot-Instance-Date-Feeds

Verwenden Sie den Befehl create-spot-datafeed-subscription, um Ihren Daten-Feed zu abonnieren.

```
aws ec2 create-spot-datafeed-subscription \
    --bucket my-bucket-name \
    [--prefix my-prefix]
```

Beispielausgabe

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "111122223333",
        "Bucket": "my-bucket-name",
        "Prefix": "my-prefix",
        "State": "Active"
    }
}
```

Beschreiben Ihres Spot-Instance-Daten-Feeds

Verwenden Sie den Befehl create-spot-datafeed-subscription, um Ihr Daten-Feed-Abonnement zu beschreiben.

```
aws ec2 describe-spot-datafeed-subscription
```

Beispielausgabe

```
{
    "SpotDatafeedSubscription": {
        "OwnerId": "123456789012",
        "Prefix": "spotdata",
        "Bucket": "my-s3-bucket",
        "State": "Active"
    }
}
```

Daten in Ihrem Datenfeed anzeigen

In der AWS Management Console, öffne AWS CloudShell. Verwenden Sie den folgenden s3-Sync-Befehl, um die .gz-Dateien für Ihren Datenfeed aus dem S3-Bucket abzurufen und sie in dem von Ihnen angegebenen Ordner zu speichern.

```
aws s3 sync s3://my-s3-bucket ./data-feed
```

Um den Inhalt einer .gz-Datei anzuzeigen, wechseln Sie zu dem Ordner, in dem Sie den Inhalt des S3-Buckets gespeichert haben.

```
cd data-feed
```

Verwenden Sie den ls-Befehl, um die Namen der Dateien anzuzeigen. Verwenden Sie den zcat-Befehl mit dem Namen der Datei, um den Inhalt der komprimierten Datei anzuzeigen. Nachfolgend finden Sie ein Beispielbefehl.

```
zcat  111122223333.2023-12-09-07.001.b959dbc6.gz
```

Es folgt eine Beispielausgabe.

```
#Version: 1.0
#Fields: Timestamp UsageType Operation InstanceID MyBidID MyMaxPrice MarketPrice Charge
 Version
2023-12-09 07:13:47 UTC USE2-SpotUsage:c7a.medium       RunInstances:SV050
 i-0c3e0c0b046e050df     sir-pwq6nmfp    0.0510000000 USD        0.0142000000 USD
  0.0142000000 USD        1
```

Löschen Ihres Spot-Instance-Daten-Feeds

Verwenden Sie den Befehl delete-spot-datafeed-subscription, um Ihren Daten-Feed zu löschen.

```
aws ec2 delete-spot-datafeed-subscription
```

Kontingente für Spot-Instances

Es gibt Kontingente für die Anzahl von ausgeführten Spot-Instances und von ausstehenden Spot-Instance-Anforderungen pro AWS-Konto und Region. Sobald eine ausstehende Spot-Instance-Anforderung erfüllt wurde, wird die Anforderung nicht mehr auf das Kontingent angerechnet, da die ausgeführte Instance auf das Kontingent angerechnet wird.

Spot-Instance-Kontingente werden im Hinblick auf die Anzahl der virtuellen Zentralprozessoreinheiten (vCPUs) verwaltet, die Ihre ausgeführten Spot-Instances entweder verwenden oder bis zur Erfüllung offener Spot-Instance-Anforderungen verwenden werden. Wenn Sie Ihre Spot-Instances beenden, die Spot-Instance-Anforderungen aber nicht abbrechen, werden die Anforderungen auf Ihr vCPU-Kontingent für Spot Instances angerechnet, bis Amazon EC2 das Beenden der Spot-Instance erkennt und die Anforderungen schließt.

Wir bieten die folgenden Kontingenttypen für Spot-Instances:

- Alle DL-Spot-Instance-Anforderungen
- Alle F-Spot-Instance-Anforderungen
- Alle G- und VT-Spot-Instance-Anforderungen
- Alle Inf-Spot-Instance-Anforderungen
- Alle P-Spot-Instance-Anforderungen
- Alle Spot-Instance-Standard-Anforderungen (A, C, D, H, I, M, R, T, Z)
- Alle Anforderungen von Trn-Spot-Instances
- Alle X-Spot-Instance-Anforderungen

Jeder Kontingenttyp gibt die maximale Anzahl von vCPUs für eine oder mehrere Instance-Familien an. Weitere Informationen zu den unterschiedlichen Instance-Familien, Generationen und Größen finden Sie unter Amazon EC2-Instance-Typen.

Sie können jede beliebige Kombination von Instance-Typen starten, die Ihren wechselnden Anwendungsanforderungen entspricht. Bei einem Kontingent für alle Spot-Instance-Standardanforderungen von 256 vCPUs können Sie beispielsweise 32 `m5.2xlarge`-Spot-Instances (32 x 8 vCPUs) oder 16 `c5.4xlarge`-Spot-Instances (16 x 16 vCPUs) anfordern.

Aufgaben

- Überwachen von Kontingenten für Spot Instances und der Nutzung
- Anfordern einer Kontingenterhöhung

Überwachen von Kontingenten für Spot Instances und der Nutzung

Sie können Ihre Spot-Instance-Kontingente mit den folgenden Optionen anzeigen und verwalten:

- Die Amazon EC2-Service Quotas-Seite in der Service Quotas-Konsole
- Das Get-Service-Quota AWS CLI

Weitere Informationen finden Sie unter Amazon-EC2-Service Quotas Service Quotas anzeigen im Servicekontingents-Benutzerhandbuch.

Mit der Integration von Amazon CloudWatch Metrics können Sie die EC2-Nutzung anhand Ihrer Kontingente überwachen. Sie können auch Alarme konfigurieren, um vor beinahe erreichten Kontingenten zu warnen. Weitere Informationen finden Sie unter Service Quotas und CloudWatch Amazon-Alarme im Service-Kontingents-Benutzerhandbuch .

Anfordern einer Kontingenterhöhung

Auch wenn Amazon EC2 Ihre Kontingente für Spot Instances automatisch basierend auf Ihrer Nutzung erhöht, können Sie bei Bedarf eine Kontingenterhöhung anfordern. Wenn Sie beispielsweise mehr Spot Instances starten möchten, als Ihr aktuelles Kontingent zulässt, können Sie eine Kontingenterhöhung anfordern. Sie können auch eine Kontingenterhöhung anfordern, wenn Sie eine Spot-Instance-Anforderung senden und der Fehler `Max spot instance count exceeded` angezeigt wird. Zum Anfordern einer Kontingenterhöhung können Sie die in Amazon-EC2-Service Quotas beschriebene Service-Quotas-Konsole verwenden.

Burstable Performance Instances

Bei den T-Instance-Typen handelt es sich um Instances mit Spitzenleistung. Wenn Sie Ihre Spot Instances mit einem Burstable-Performance-Instance-Typ starten, und wenn Sie planen, Ihre Spot Instances mit Spitzenlastleistung sofort und für eine kurze Dauer zu verwenden, ohne Leerlaufzeit für die Anrechnung von CPU-Guthaben, empfiehlt sich, diese im Standardmodus zu starten, um höhere Kosten zu vermeiden. Wenn Sie die Spot-Instances mit Spitzenlastleistung im Unlimited mode (Unbegrenzten Modus) starten und die Spitzenlastleistung der CPU sofort nutzen, geben Sie überschüssiges Guthaben für Spitzen aus. Wenn Sie die Instance für eine kurze Zeit nutzen, hat die Instance keine Zeit, CPU-Guthaben zu sammeln, um das überschüssige Guthaben zu bezahlen. Das überschüssige Guthaben wir beim Beenden der Instance abgerechnet.

Der unbegrenzte Modus für Spot-Instances mit Spitzenlastleistung ist nur dann geeignet, wenn die Instance lange genug läuft, um CPU-Guthaben für Spitzen zu erhalten. Andernfalls macht das Bezahlen für überzähliges Guthaben die Spot-Instances mit Spitzenlastleistung teurer als die Verwendung anderer Instances. Weitere Informationen finden Sie unter Verwendung des unbegrenzten Modus im Vergleich zu einer festen CPU.

T2-Instances erhalten bei Konfiguration im Standardmodus Startguthaben. T2-Instances sind die einzigen Instances mit Spitzenleistung, die Startguthaben erhalten. Startguthaben sollen eine produktive erste Starterfahrung für T2-Instances bieten, indem sie ausreichende Rechenressourcen zur Verfügung gestellt werden, um die Instance zu konfigurieren. Wiederholte Starts von T2-Instances, um neue Startguthaben zu erhalten, sind nicht zulässig. Wenn Sie dauerhaft eine CPU benötigen, können Sie Guthaben verdienen (durch Leerlauf über einen gewissen Zeitraum), Unbegrenzten Modus für T2 Spot-Instances verwenden oder einen Instance-Typ mit dedizierter CPU verwenden.

Dedicated Hosts

Ein Amazon EC2 Dedicated Host ist ein physischer Server, der vollständig für Ihre Nutzung reserviert ist. Sie können sich optional dafür entscheiden, die Instanzkapazität mit anderen AWS Konten zu teilen. Weitere Informationen finden Sie unter Arbeiten mit freigegebenen Dedicated Hosts.

Dedicated Hosts bieten Transparenz und Kontrolle über die Platzierung von Instances und unterstützen die Host-Affinität. Das bedeutet, dass Sie Instances auf bestimmten Hosts starten und ausführen können und dass Sie sicherstellen können, dass Instances nur auf bestimmten Hosts ausgeführt werden. Weitere Informationen finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.

Dedicated Hosts bieten umfassenden Support für Bring Your Own License (BYOL). Sie ermöglichen es Ihnen, Ihre vorhandenen Softwarelizenzen pro Socket, pro Kern oder pro VM, einschließlich Windows Server, SQL Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux oder andere Softwarelizenzen, die an VMs, Sockets oder physische Kerne gebunden sind, gemäß Ihren Lizenzbedingungen zu verwenden.

Wenn Sie möchten, dass Ihre Instances auf dedizierter Hardware ausgeführt werden, Sie aber keine Transparenz oder Kontrolle über die Instance-Platzierung benötigen und Sie keine Softwarelizenzen pro Socket oder pro Core verwenden müssen, können Sie stattdessen die Verwendung von Dedicated Instances in Betracht ziehen. Dedicated Instances und Dedicated Hosts können beide verwendet werden, um Amazon EC2 EC2-Instances auf dedizierten physischen Servern zu starten. Es gibt keine leistungsbezogenen, sicherheitsrelevanten oder physischen Unterschiede zwischen Dedicated Instances und Instances auf Dedicated Hosts. Es gibt jedoch einige wichtige Unterschiede zwischen ihnen. Die folgende Tabelle hebt einige der wichtigsten Unterschiede zwischen Dedicated Hosts und Dedicated Instances hervor:

	Dedicated Host	Dedicated Instance
Dedizierter physischer Server	Physischer Server mit Instanzkapazität, die vollständig für Ihre Nutzung reserviert ist.	Physischer Server, der einem einzelnen Kundenkonto zugewiesen ist.
Gemeinsame Nutzung der Instanzkapazität	Kann die Instanzkapazität mit anderen Konten teilen.	Nicht unterstützt
Fakturierung	Abrechnung pro Host	Abrechnung pro Instance
Sichtbarkeit von Sockets, Kernen und Host-ID	Zeigt die Anzahl der Sockets und physischen Kerne	Keine Sichtbarkeit
Host- und Instance-Affinität	Gestattet Ihnen, Ihre Instances im Laufe der Zeit durchgängig auf demselben physischen Server bereitzustellen	Nicht unterstützt

	Dedicated Host	Dedicated Instance
Zielgerichtete Instance-Platzierung	Bietet zusätzliche Sichtbarkeit und Kontrolle darüber, wie Instances auf einem physischen Server platziert werden.	Nicht unterstützt
Automatische Instance-Wiederherstellung	Unterstützt. Weitere Informationen finden Sie unter Host-Wiederherstellung.	Unterstützt
Bring Your Own License (BYOL)	Unterstützt	Teilweise Unterstützung*
Kapazitätsreservierungen	Nicht unterstützt	Unterstützt

* Microsoft SQL Server mit Lizenzmobilität über Software Assurance und Windows Virtual Desktop Access (VDA)-Lizenzen können mit Dedicated Instance verwendet werden.

Weitere Informationen über Dedicated Instances finden Sie unter Dedicated Instances.

Inhalt

- Host-Wartung
- Verfolgen von Konfigurationsänderungen

Konfigurationen der Instance-Kapazität

Dedicated Hosts unterstützen verschiedene Konfigurationen (physische Kerne, Sockets und VCPUs), mit denen Sie Instances verschiedener Familien und Größen ausführen können.

Wenn Sie Ihrem Konto einen Dedicated Host zuweisen, können Sie eine Konfiguration auswählen, die entweder einen einzelnen Instance-Typ oder mehrere Instance-Typen innerhalb derselben Instance-Familie unterstützt. Die Anzahl der Instances, die Sie auf einem Host ausführen können, hängt von der ausgewählten Konfiguration ab.

Inhalt

- Unterstützung für einzelne Instance-Typen
- Unterstützung mehrerer Instance-Typen

Unterstützung für einzelne Instance-Typen

Sie können einen Dedicated Host zuweisen, der nur einen Instance-Typ unterstützt. Bei dieser Konfiguration muss jede Instance, die Sie auf dem Dedicated Host starten, vom gleichen Instance-Typ sein, den Sie bei der Zuweisung des Hosts angeben.

Sie können beispielsweise einen Host zuweisen, der nur den `m5.4xlarge`-Instance-Typ unterstützt. In diesem Fall können Sie nur `m5.4xlarge`-Instances auf diesem Host ausführen.

Die Anzahl der Instances, die Sie auf dem Host starten können, hängt von der Anzahl der vom Host bereitgestellten physischen Kerne und der Anzahl der vom angegebenen Instance-Typ verbrauchten Kerne ab. Wenn Sie beispielsweise einen Host für `m5.4xlarge`-Instances zuweisen, stellt der Host 48 physische Kerne bereit und jede `m5.4xlarge`-Instance verbraucht 8 physische Kerne. Dies bedeutet, dass Sie bis zu 6 Instances auf diesem Host starten können (48 physische Kerne / 8 Kerne pro Instance = 6 Instances).

Unterstützung mehrerer Instance-Typen

Sie können einen Dedicated Host zuweisen, der mehrere Instance-Typen innerhalb derselben Instance-Familie unterstützt. Auf diese Weise können Sie verschiedene Instance-Typen auf demselben Host ausführen, sofern sie sich in derselben Instance-Familie befinden und der Host über ausreichend Instance-Kapazität verfügt.

Sie können beispielsweise einen Host zuweisen, der verschiedene R5-Instance-Typen innerhalb der Instance-Familie unterstützt. In diesem Fall können Sie auf diesem Host eine beliebige Kombination von R5-Instance-Typen, wie z. B. `r5.large`, `r5.xlarge`, `r5.2xlarge` und `r5.4xlarge`, starten, bis zur physischen Kernkapazität des Hosts.

Die folgenden Instance-Familien unterstützen Dedicated Hosts mit Unterstützung mehrerer Instance-Typen:

- Universell: A1, M5, M5n, M6i, and T3
- Für Datenverarbeitung optimiert: C5, C5n, and C6i
- Speicheroptimiert: R5, R5n, and R6i

Die Anzahl der Instances, die Sie auf dem Host ausführen können, hängt von der Anzahl der vom Host bereitgestellten physischen Kerne und der Anzahl der von jedem Instance-Typ, den Sie auf dem Host ausführen, verbrauchten Kerne ab. Wenn Sie beispielsweise einen R5-Host zuweisen, der 48 physische Kerne bereitstellt, und Sie zwei `r5.2xlarge`-Instances (4 Kerne x 2 Instances) und drei `r5.4xlarge`-Instances (8 Kerne x 3 Instances) ausführen, verbrauchen diese Instances insgesamt 32 Kerne. Sie können eine beliebige Kombination von R5-Instances ausführen, solange diese die verbleibenden 16 Kerne nicht überschreiten.

Für jede Instance-Familie gibt es jedoch ein Limit für die Anzahl der Instances, die für jede Instance-Größe ausgeführt werden können. Beispielsweise unterstützt ein R5 Dedicated Host maximal 2 `r5.8xlarge`-Instances, die 32 der physischen Kerne nutzen. In diesem Fall können dann zusätzliche R5-Instances kleinerer Größe verwendet werden, um den Host auf die Kernkapazität zu füllen. Informationen zur unterstützten Anzahl von Instance-Größen für jede Instance-Familie finden Sie unter Konfigurationstabelle für Dedicated Hosts.

Die folgende Tabelle zeigt Beispielkombinationen von Instance-Typen:

Instance-Familie	Beispiel für Instance-Größenkombinationen
R5	• Beispiel 1: 4 x `r5.4xlarge` + 4 x `r5.2xlarge` • Beispiel 2: 1 x `r5.12xlarge` + 1 x `r5.4xlarge` + 1 x `r5.2xlarge` + 5 x `r5.xlarge` + 2 x `r5.large`
C5	

Instance-Familie	Beispiel für Instance-Größenkombinationen
	• Beispiel 1: 1 x `c5.9xlarge` + 2 x `c5.4xlarge` + 1 x `c5.xlarge` • Beispiel 2: 4 x `c5.4xlarge` + 1 x `c5.xlarge` + 2 x `c5.large`
M5	• Beispiel 1: 4 x `m5.4xlarge` + 4 x `m5.2xlarge` • Beispiel 2: 1 x `m5.12xlarge` + 1 x `m5.4xlarge` + 1 x `m5.2xlarge` + 5 x `m5.xlarge` + 2 x `m5.large`

Überlegungen

Beachten Sie beim Arbeiten mit Dedicated Hosts, die mehrere Instance-Typen unterstützen, Folgendes:

- Mit Dedicated Hosts vom Typ N wie C5n, M5n und R5n können Sie kleinere Instance-Größen (`2xlarge` und kleiner) nicht mit größeren Instance-Größen (`4xlarge` und größer, einschließlich `metal`) kombinieren. Wenn Sie gleichzeitig kleinere und größere Instance-Größen auf Hosts vom Typ N gleichzeitig benötigen, müssen Sie separate Hosts für die kleineren und größeren Instance-Größen zuweisen.
- Es wird empfohlen, zunächst größere Instance-Typen zu starten und dann die verbleibende Instance-Kapazität bei Bedarf mit kleineren Instance-Typen zu füllen.

Bring your own license (BYOL, Verwendung der eigenen Lizenz)

Dedicated Hosts gestatten Ihnen, Ihre vorhandenen Lizenzen pro Socket, pro Kern oder pro VM-Software zu verwenden. Wenn Sie BYOL verwenden, sind Sie für die Verwaltung Ihrer eigenen Lizenzen verantwortlich. Amazon EC2 verfügt jedoch über Features, die Sie bei der Aufrechterhaltung Ihrer Lizenz-Compliance unterstützen. Dazu zählen die Instance-Affinität und die zielgerichtete Platzierung.

Dies sind die allgemeinen Schritte, die Sie befolgen müssen, um Ihr eigenes Computer-Image per Volumenlizenz in Amazon EC2 zu übertragen.

1. Prüfen Sie, ob die Lizenzbedingungen, die die Nutzung Ihrer Computer-Images regeln, die Nutzung in einer virtualisierten Cloud-Umgebung erlauben. Weitere Informationen über die Microsoft-Lizenzierung finden Sie unter Amazon Web Services- und Microsoft-Lizenzierung.
2. Nachdem Sie überprüft haben, ob Ihr Computer-Image in Amazon EC2 verwendet werden kann, importieren Sie es mit VM Import/Export. Weitere Informationen zum Importieren Ihres Computer-Image finden Sie im Benutzerleitfaden für VM Import/Export.
3. Nach dem Importieren Ihres Machine Image können Sie Instances davon auf aktiven Dedicated Hosts in Ihrem Konto starten.
4. Wenn Sie diese Instances ausführen, müssen Sie je nach Betriebssystem diese Instances auf Ihrem eigenen KMS-Server aktivieren (Beispiel: Windows Server oder Windows SQL Server). Sie können Ihr importiertes Windows-AMI nicht über den Amazon Windows KMS-Server aktivieren.

> **Note**
>
> Um zu verfolgen, wie Ihre Bilder verwendet werden AWS, aktivieren Sie die Host-Aufzeichnung in AWS Config. Sie können AWS Config damit Konfigurationsänderungen auf einem Dedicated Host aufzeichnen und die Ausgabe als Datenquelle für Lizenzberichte verwenden. Weitere Informationen finden Sie unter Verfolgen von Konfigurationsänderungen.

Preise und Fakturierung

Der Preis für eine Dedicated Host variiert in Abhängigkeit von der Zahlungsoption.

Zahlungsoptionen

- On-Demand Dedicated Hosts
- Dedicated Host Reservations
- Savings Plans
- Preise für Windows Server auf Dedicated Hosts

On-Demand Dedicated Hosts

Die On-Demand-Abrechnung wird automatisch aktiviert, wenn Sie Ihrem Konto einen Dedicated Host zuweisen.

Der On-Demand-Preis für einen Dedicated Host variiert abhängig von Instance-Familie und Region. Sie zahlen pro Sekunde (mit einem Minimum von 60 Sekunden) für den aktiven Dedicated Host, unabhängig von der Menge oder der Größe der Instances, die Sie darauf starten möchten. Weitere Informationen zu On-Demand-Preisen erhalten Sie unter Amazon EC2 Dedicated Hosts On-Demand-Preise.

Sie können einen On-Demand Dedicated Host jederzeit freigeben, sodass keine Gebühren mehr dafür anfallen. Weitere Informationen über die Freigabe eines Dedicated Host finden Sie unter Freigeben von Dedicated Hosts.

Dedicated Host Reservations

Dedicated Host-Reservierungen bietet einen Abrechnungsrabatt im Vergleich zur Ausführung von On-Demand-Dedicated Hosts. Reservierungen sind in drei Zahlungsoptionen verfügbar:

- Keine Vorauszahlung:— Reservierungen vom Typ "Keine Vorauszahlung" bieten Ihnen einen Rabatt auf Ihre Dedicated Host-Nutzung in einem bestimmten Zeitraum und erfordern keine Vorauszahlung. Verfügbar mit einer Laufzeit von einem Jahr und drei Jahren. Nur einige Instance-Familien unterstützen die dreijährige Laufzeit für „Keine Vorabreservierungen“.
- Teilweise Vorauszahlung:— Ein Teil der Reservierung muss im Voraus bezahlt werden und die restlichen Stunden während der Laufzeit werden zu einem ermäßigten Satz abgerechnet. Verfügbar mit einer Laufzeit von einem Jahr und drei Jahren.
- Komplette Vorauszahlung:— Bietet den günstigsten effektiven Preis. Ist verfügbar mit einer Laufzeit von einem Jahr und drei Jahren und deckt die gesamten Kosten für die Laufzeit im Voraus ab, ohne weitere, künftig anfallende Kosten.

Sie müssen über aktive Dedicated Hosts in Ihrem Konto verfügen, bevor Sie Reservierungen kaufen können. Jede Reservierung kann einen oder mehrere Hosts abdecken, die dieselbe Instance-Familie in einer einzelnen Availability Zone unterstützen. Reservierungen werden auf die Instance-Familie auf dem Host angewendet, nicht auf die Instance-Größe. Falls Sie über drei Dedicated Hosts mit verschiedenen Instance-Größen (`m4.xlarge`, `m4.medium` und `m4.large`) verfügen, können Sie eine einzelne `m4`-Reservierung all diesen Dedicated Hosts zuordnen. Die Instance-Familie und Availability Zone müssen mit denen der Dedicated Hosts übereinstimmen, denen Sie sie zuordnen möchten.

Wenn eine Reservierung einem Dedicated Host zugeordnet wird, kann der Dedicated Host erstellt freigestellt werden, wenn die Laufzeit der Reservierung vorüber ist.

Weitere Informationen zu Reservierungspreisen erhalten Sie unter Amazon EC2 Dedicated Hosts – Preise.

Savings Plans

Savings Plans sind ein flexibles Preismodell, das erhebliche Einsparungen gegenüber On-Demand-Instances bietet. Mit Savings Plans verpflichten Sie sich zu einer konstanten Nutzung (in USD pro Stunde) für eine Laufzeit von einem oder drei Jahren. Dadurch erhalten Sie die Flexibilität, die Dedicated Hosts zu nutzen, die Ihren Anforderungen am besten entsprechen. Zugleich können Sie weiterhin Geld sparen, statt sich auf eine bestimmte Dedicated Host festzulegen. Weitere Informationen finden Sie im AWS Savings Plans User Guide.

> **Note**
>
> Savings Plans werden mit `u-6tb1.metal`-, `u-9tb1.metal`-, `u-12tb1.metal`-, `u-18tb1.metal`- und `u-24tb1.metal`-Dedicated-Hosts nicht unterstützt.

Preise für Windows Server auf Dedicated Hosts

Vorbehaltlich der Microsoft-Lizenzbedingungen können Sie Ihre vorhandenen Windows Server- und SQL Server-Lizenzen zu Dedicated Hosts mitbringen. Wenn Sie Ihre eigenen Lizenzen mitbringen, fallen keine zusätzlichen Kosten für die Softwarenutzung an.

Darüber hinaus können Sie auch von Amazon bereitgestellte Windows Server AMIs verwenden, um die neuesten Versionen von Windows Server auf Dedicated Hosts auszuführen. Dies kommt häufig in Szenarien vor, in denen Sie über vorhandene SQL Server-Lizenzen verfügen, die zur Ausführung auf Dedicated Hosts berechtigt sind, aber Windows Server zur Ausführung der SQL Server-Workload benötigen. Von Amazon bereitgestellte Windows Server-AMIs werden nur auf Instance-Typen der aktuellen Generation unterstützt. Weitere Informationen finden Sie unter Amazon EC2 Dedicated Hosts-Preise.

Burstable T3-Instances auf Dedicated Hosts

Dedicated Hosts unterstützen T3-Instances mit burstable Leistung. T3-Instances bieten eine kosteneffiziente Möglichkeit, Ihre berechtigte BYOL-Lizenzsoftware auf dedizierter Hardware zu verwenden. Der geringere vCPU-Footprint von T3-Instances ermöglicht es Ihnen, Ihre Workloads auf weniger Hosts zu konsolidieren und Ihre Lizenzauslastung pro Kern zu maximieren.

T3-Dedicated-Hosts eignen sich am besten für die Ausführung von BYOL-Software mit geringer bis mittlerer CPU-Auslastung. Dies umfasst berechtigte Softwarelizenzen pro Socket, pro Kern oder pro VM (z. B. Windows Server, Windows Desktop, SQL Server, SUSE Enterprise Linux Server, Red Hat Enterprise Linux und Oracle Database). Beispiele für Workloads, die für T3-Dedicated-Hosts geeignet sind, sind kleine und mittlere Datenbanken, virtuelle Desktops, Entwicklungs- und Testumgebungen, Code-Repositorys und Produktprototypen. T3-Dedicated-Hosts werden nicht für Workloads mit anhaltender hoher CPU-Auslastung oder für Workloads empfohlen, bei denen gleichzeitig korrelierte CPU-Bursts auftreten.

T3-Instances auf Dedicated Hosts verwenden dasselbe Kreditmodell wie T3-Instances auf gemeinsam genutzter Tenancy-Hardware. Sie unterstützen jedoch nur den `standard`-Kredit-Modus; sie unterstützen nicht den `unlimited`-Kredit-Modus. Im `standard`-Modus verdienen, verbrauchen und sammeln T3-Instances auf Dedicated Hosts Guthaben auf dieselbe Weise wie Burst-fähige Instances auf gemeinsam genutzter Tenancy-Hardware. Sie bieten eine Basis-CPU-Leistung mit der Möglichkeit, über das Basisniveau zu steigen. Um die Basisleistung zu übersteigen, gibt die Instance Guthaben aus, die sie in ihrem CPU-Guthaben-Konto angesammelt hat. Wenn die aufgelaufenen Gutschriften erschöpft sind, wird die CPU-Auslastung auf die Basisebene gesenkt. Weitere Informationen zum `standard`-Modus finden Sie unter Funktionsweise der Standard-Instances mit Spitzenlastleistung.

T3-Dedicated-Hosts unterstützen alle Features von Amazon-EC2-Dedicated-Hosts, einschließlich mehrerer Instance-Größen auf einem einzigen Host, Host-Ressourcengruppen und BYOL.

Unterstützte T3-Instance-Größen und -konfigurationen

T3-Dedicated-Hosts führen universelle burstable T3-Instances aus, die CPU-Ressourcen des Hosts gemeinsam nutzen, indem sie eine Basis-CPU-Leistung und die Möglichkeit bieten, bei Bedarf auf ein höheres Niveau zu steigen. Dadurch können T3-Dedicated-Hosts mit 48 Kernen bis zu 192 Instances pro Host unterstützen. Um die Ressourcen des Hosts effizient zu nutzen und die beste Instance-Leistung zu bieten, berechnet der Amazon-EC2-Instance-Platzierungsalgorithmus automatisch die unterstützte Anzahl von Instances und Instance-Größenkombinationen, die auf dem Host gestartet werden können.

T3-Dedicated-Hosts unterstützen mehrere Instance-Typen auf demselben Host. Alle T3-Instance-Größen werden auf Dedicated Hosts unterstützt. Sie können verschiedene Kombinationen von T3-Instances bis zum CPU-Limit des Hosts ausführen.

In der folgenden Tabelle werden die unterstützten Instance-Typen aufgeführt, die Leistung jedes Instance-Typs zusammengefasst und die maximale Anzahl von Instances jeder Größe angegeben, die gestartet werden können.

Insta Typ	vCPUs	Arbeitsspeicher (GiB)	Basis-CPU-Auslastung pro vCPU	Netzwerk-Burst-Bandbreite (Gbit/s)	Amazon-EBS-Burst-Bandbreite (Mbit/s)	Maximale Anzahl von Instances pro Dedicated Host
t3.na	2	0.5	5 %	5	Bis zu 2 085	192
t3.m	2	1	10 %	5	Bis zu 2 085	192
t3.sn	2	2	20 %	5	Bis zu 2 085	192
t3.m	2	4	20 %	5	Bis zu 2 085	192
t3.la	2	8	30 %	5	2.780	96
t3.xla	4	16	40%	5	2.780	48
t3.2x e	8	32	40%	5	2.780	24

Überwachung der CPU-Auslastung für T3-Dedicated-Hosts

Sie können die `DedicatedHostCPUUtilization` CloudWatch Amazon-Metrik verwenden, um die vCPU-Auslastung eines Dedicated Hosts zu überwachen. Die Metrik ist im `EC2`-Namespace und der `Per-Host-Metrics`-Dimension verfügbar. Weitere Informationen finden Sie unter Dedicated-Host-Metriken.

Dedicated Hosts-Einschränkungen

Bevor Sie Dedicated Hosts zuordnen, beachten Sie die folgenden Begrenzungen und Einschränkungen:

- Um RHEL, SUSE Linux und SQL Server auf Dedicated Hosts ausführen zu können, müssen Sie eigene AMIs verwenden. RHEL-, SUSE Linux- und SQL Server-AMIs, die von angeboten werden

AWS oder auf verfügbar sind, AWS Marketplace können nicht mit Dedicated Hosts verwendet werden. Weitere Informationen zum Erstellen eines eigenen AMI finden Sie unter Bring your own license (BYOL, Verwendung der eigenen Lizenz).

Diese Einschränkung gilt nicht für Hosts, die für Instances mit hohem Arbeitsspeicher (`u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, und `u-24tb1.metal`) zugewiesen sind. RHEL- und SUSE-Linux-AMIs, die von angeboten werden AWS oder auf verfügbar sind, AWS Marketplace können mit diesen Hosts verwendet werden.

- Es gibt eine Begrenzung für die Anzahl der laufenden Dedicated Hosts pro Instance-Familie pro AWS -Konto pro Region. Kontingente gelten nur für laufende Instances. Wenn Ihre Instance aussteht, stoppt oder angehalten wird, wird sie nicht auf Ihr Kontingent angerechnet. Um die Kontingente für Ihr Konto einzusehen oder eine Kontingenterhöhung anzufordern, können Sie die Service-Quotas-Konsole verwenden.
- Die Instances, die auf einem Dedicated Host ausgeführt werden, können nur in einem VPC gestartet werden.
- Auto Scaling-Gruppen werden unterstützt, wenn eine Startvorlage verwendet wird, bei der eine Hostressourcengruppe angegeben wird. Weitere Informationen finden Sie unter Erstellen einer Startvorlage mit erweiterten Einstellungen im Amazon EC2 Auto Scaling-Benutzerhandbuch.
- Amazon RDS-Instances werden nicht unterstützt.
- Das AWS kostenlose Nutzungskontingent ist für Dedicated Hosts nicht verfügbar.
- Die Instance-Platzierungskontrolle bezieht sich auf die Verwaltung von Instance-Starts auf Dedicated Hosts. Sie können Dedicated Hosts nicht in Placement-Gruppen starten.
- Wenn Sie einen Host für einen virtualisierten Instance-Typ zuweisen, können Sie den Instance-Typ nicht in einen `.metal`-Instance-Typ ändern, nachdem der Host zugewiesen wurde. Wenn Sie beispielsweise einen Host für den `m5.large`-Instance-Typ zuweisen, können Sie den Instance-Typ nicht in `m5.metal` ändern.

  Ebenso können Sie, wenn Sie einen Host für einen `.metal`-Instance-Typ zuweisen, den Instance-Typ nicht in einen virtualisierten Instance-Typ ändern, nachdem der Host zugewiesen wurde. Wenn Sie beispielsweise einen Host für den `m5.metal`-Instance-Typ zuweisen, können Sie den Instance-Typ nicht in `m5.large` ändern.

Arbeiten mit Dedicated Hosts

Zur Verwendung eines Dedicated Host ordnen Sie zuerst Hosts für die Nutzung in Ihrem Konto zu. Anschließend starten Sie Instances auf den Hosts, indem Sie die host-Tenancy für die Instance

festlegen. Sie müssen einen spezifischen Host auswählen, auf dem die Instance gestartet werden soll oder Sie können zulassen, dass sie auf einem beliebigen Host gestartet wird, für den die automatische Platzierung aktiviert ist, und der für den Instance-Typ geeignet ist. Wenn eine Instance angehalten und neu gestartet wurde, bestimmt die Einstellung Host-Affinity, ob sie auf demselben oder auf einem anderen Host neu gestartet werden soll.

Falls Sie keinen On-Demand-Host mehr benötigen, können Sie die auf dem Host ausgeführten Instances anhalten, sie auf einem anderen Host starten und dann den Host freigeben.

Dedicated Hosts sind ebenfalls in integriert AWS License Manager. Mit License Manager können Sie eine Hostressourcengruppe erstellen, bei der es sich um eine Sammlung von Dedicated Hosts handelt, die als einzelne Entity verwaltet werden. Beim Erstellen einer Hostressourcengruppe geben Sie die Einstellungen für die Hostverwaltung an, z. B. automatische Zuweisung und automatische Freigabe für die Dedicated Hosts. Auf diese Weise können Sie Instances auf Dedicated Hosts starten, ohne diese Hosts manuell zuzuweisen und zu verwalten. Weitere Informationen finden Sie unter Hostressourcengruppen im AWS License Manager Benutzerhandbuch.

Inhalt

Zuordnen von Dedicated Hosts

Um mit der Verwendung von Dedicated Hosts zu beginnen, müssen Sie über die Amazon EC2-Konsole oder die Befehlszeilen-Tools Dedicated Hosts zu Ihrem Konto zuweisen. Nachdem den Dedicated Host zugewiesen haben, wird die Dedicated Host-Kapazität sofort in Ihrem Konto verfügbar gemacht und Sie können mit dem Starten von Instances über den Dedicated Host beginnen.

Wenn Sie Ihrem Konto einen Dedicated Host zuweisen, können Sie eine Konfiguration auswählen, die entweder einen einzelnen Instance-Typ oder mehrere Instance-Typen innerhalb derselben Instance-Familie unterstützt. Die Anzahl der Instances, die Sie auf dem Host ausführen können, hängt von der ausgewählten Konfiguration ab. Weitere Informationen finden Sie unter Konfigurationen der Instance-Kapazität.

Console

So weisen Sie ein Dedicated Host zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts und dann Allocate Dedicated Host (Dedicated Host zuweisen) aus.
3. Wählen Sie für Instance (Instance-Familie) die Instance-Familie für die Dedicated Host aus.
4. Geben Sie an, ob der Dedicated Host mehrere Instance-Größen innerhalb der ausgewählten Instance-Familie oder nur einen bestimmten Instance-Typ unterstützt. Führen Sie eine der folgenden Aufgaben aus.

   - Um den Dedicated Host so zu konfigurieren, dass mehrere Instance-Typen in der ausgewählten Instance-Familie unterstützt werden, wählen Sie für Support multiple instance types (Mehrere Instance-Typen unterstützen) die Option Enable (Aktivieren) aus. Wenn Sie diese Option aktivieren, können Sie verschiedene Instance-Größen aus derselben Instance-Familie auf dem Dedicated Host starten. Wenn Sie die Instance-Familie `m5` und diese Option auswählen, können Sie beispielsweise `m5.xlarge`- und `m5.4xlarge`-Instances auf dem Dedicated Host starten.
   - Um das Dedicated Host so zu konfigurieren, dass ein einzelner Instance-Typ innerhalb der ausgewählten Instance-Familie unterstützt wird, deaktivieren Sie Support multiple instance types (Mehrere Instance-Typen unterstützen) und wählen Sie dann für Instance type (Instance-Typ) den zu unterstützenden Instance-Typ. Damit können Sie einen einzelnen Instance-Typ auf dem Dedicated Host starten. Wenn Sie diese Option wählen

und `m5.4xlarge` als unterstützten Instance-Typ angeben, können Sie beispielsweise nur `m5.4xlarge`-Instances auf dem Dedicated Host starten.

5. Wählen Sie für Availability Zone die Availability Zone aus, in der der Dedicated Host zugewiesen werden soll.
6. Damit der Dedicated Host nicht zielgerichtete Instance-Starts akzeptiert, die seinem Instance-Typ entsprechen, wählen Sie für Instance auto-placement (Automatische Instance-Platzierung) Enable (Aktiveren) aus. Weitere Informationen zur automatischen Platzierung finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.
7. Zur Aktivierung der Host-Wiederherstellung für den Dedicated Host wählen Sie für Host recovery (Host-Wiederherstellung) Enable (Aktivieren) aus. Weitere Informationen finden Sie unter Host-Wiederherstellung.
8. Geben Sie für Quantity (Menge) die Anzahl der zuzuordnenden Dedicated Hosts ein.
9. (Optional) Wählen Sie Add new Tags (Neuen Tags (Markierungen) hinzufügen) aus. Geben Sie einen Tag (Markierung)-Schlüssel und einen Tag (Markierung)-Wert ein.
10. Wählen Sie Allocate aus.

AWS CLI

So weisen Sie ein Dedicated Host zu

Verwenden Sie den Befehl allocate-hosts AWS CLI . Der folgende Befehl weist einen Dedicated Host zu, der mehrere Instance-Typen aus der `m5`-Instance-Familie in der Availability Zone `us-east-1a` unterstützt. Für den Host ist außerdem die Host-Wiederherstellung aktiviert und die automatische Platzierung deaktiviert.

```
aws ec2 allocate-hosts --instance-family "m5" --availability-zone "us-east-1a" --
auto-placement "off" --host-recovery "on" --quantity 1
```

Der folgende Befehl ordnet einen Dedicated Host zu, der nicht zielgerichtete Starts von `m4.large`-Instances in der Availability Zone `eu-west-1a` unterstützt, aktiviert eine Host-Wiederherstellung und wendet ein Tag (Markierung) mit einem Schlüssel namens „`purpose`“ und einem Wert von „`production`“ an.

```
aws ec2 allocate-hosts --instance-type "m4.large" --availability-zone "eu-west-1a"
 --auto-placement "on" --host-recovery "on" --quantity 1 --tag-specifications
 'ResourceType=dedicated-host,Tags=[{Key=purpose,Value=production}]'
```

PowerShell

So weisen Sie ein Dedicated Host zu

Verwenden Sie den Befehl. New-EC2Host AWS Tools for Windows PowerShell Der folgende Befehl weist einen Dedicated Host zu, der mehrere Instance-Typen aus der `m5`-Instance-Familie in der Availability Zone `us-east-1a` unterstützt. Für den Host ist außerdem die Host-Wiederherstellung aktiviert und die automatische Platzierung deaktiviert.

```
PS C:\> New-EC2Host -InstanceFamily m5 -AvailabilityZone us-east-1a -
AutoPlacement Off -HostRecovery On -Quantity 1
```

Die folgenden Befehle ordnen einen Dedicated Host zu, der nicht zielgerichtete Starts von `m4.large`-Instances in der Availability Zone `eu-west-1a` unterstützt, aktivieren eine Host-Wiederherstellung und wenden ein Tag (Markierung) mit einem Schlüssel namens `purpose` und einen Wert von `production` an.

Der `TagSpecification`-Parameter, der bei der Erstellung von einem Dedicated Host zum Markieren genutzt wird, erfordert ein Objekt, das den Typ der zu markierenden Ressource, den Tag (Markierung)-Schlüssel und den Tag (Markierung)-Wert angibt. Mit den folgenden Befehlen wird das erforderliche Objekt erstellt.

```
PS C:\> $tag = @{ Key="purpose"; Value="production" }
PS C:\> $tagspec = new-object Amazon.EC2.Model.TagSpecification
PS C:\> $tagspec.ResourceType = "dedicated-host"
PS C:\> $tagspec.Tags.Add($tag)
```

Der folgende Befehl ordnet den Dedicated Host zu und wendet den im `$tagspec`-Objekt angegebene Tag (Markierung) an.

```
PS C:\> New-EC2Host -InstanceType m4.large -AvailabilityZone eu-west-1a -
AutoPlacement On -HostRecovery On -Quantity 1 -TagSpecification $tagspec
```

Starten Sie Instances auf einem Dedicated Host

Nach dem Zuordnen eines Dedicated Host können Sie Instances darauf starten. Sie können keine Instances mit `host`-Tenancy starten, wenn Sie nicht Dedicated Hosts aktiviert haben und über genügend Kapazität für den von Ihnen gestarteten Instance-Typ verfügen.

> **Tip**
>
> Für Dedicated Hosts, die mehrere Instance-Größen unterstützen, wird empfohlen, zuerst die größeren Instance-Größen zu starten und dann die verbleibende Instance-Kapazität nach Bedarf mit den kleineren Instance-Größen zu füllen.

Beachten Sie vor dem Start Ihrer Instances die Einschränkungen. Weitere Informationen finden Sie unter Dedicated Hosts-Einschränkungen.

Sie können eine Instance mithilfe der folgenden Methoden auf einem Dedicated Host starten.

Console

So starten Sie eine Instances auf einem spezifischen Dedicated Host über die Dedicated Hosts-Seite

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie auf der Seite Dedicated Hosts einen Host aus. Wählen Sie dann Actions (Aktionen) und Launch Instance(s) onto Host (Instance(s) auf Host starten) aus.
4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus der Liste aus.

   > **Note**
   >
   > SQL Server-, SUSE- und RHEL-AMIs, die von Amazon EC2 bereitgestellt werden, können nicht mit Dedicated Hosts verwendet werden.

5. Wählen Sie im Bereich Instance type (Instance-Typ) den zu startenden Instance-Typ aus.

   > **Note**
   >
   > Wenn der Dedicated Host nur einen einzelnen Instance-Typ unterstützt, ist der unterstützte Instance-Typ standardmäßig ausgewählt und kann nicht geändert werden.
   > Wenn der Dedicated Host mehrere Instance-Typen unterstützt, müssen Sie einen Instance-Typ innerhalb der unterstützten Instance-Familie basierend auf der

verfügbaren Instance-Kapazität des Dedicated Host auswählen. Es wird empfohlen, zuerst die größeren Instance-Größen zu starten und dann die verbleibende Instance-Kapazität nach Bedarf mit den kleineren Instance-Größen zu füllen.

6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das der Instance zugeordnet werden soll.
7. Führen Sie im Bereich Advanced details (Erweiterte Details) unter Tenancy affinity (Tenancy-Affinität) einen der folgenden Schritte aus:

   - Wählen Sie Off (Aus). Die Instance wird auf dem angegebenen Host gestartet, es ist aber nicht garantiert, dass sie nach dem Anhalten wieder auf demselben Dedicated Host gestartet wird.
   - Wählen Sie die ID des Dedicated Host aus. Falls die Instance angehalten wird, wird sie immer wieder auf diesem spezifischen Host neu gestartet.

   Weitere Informationen zur Affinität finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.

   > **Note**
   >
   > Die Optionen Tenancy und Host sind abhängig von dem ausgewählten Host vorkonfiguriert.

8. Konfigurieren Sie die verbleibenden Instance-Optionen nach Bedarf. Weitere Informationen finden Sie unter Starten einer Instance mit definierten Parametern.
9. Wählen Sie Launch Instance (Instance starten) aus.

So starten Sie eine Instance auf einem Dedicated Host unter Verwendung des Launch Instance Wizard

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Launch Instance (Instance starten) aus.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus der Liste aus.

> **Note**
>
> SQL Server-, SUSE- und RHEL-AMIs, die von Amazon EC2 bereitgestellt werden, können nicht mit Dedicated Hosts verwendet werden.

4. Wählen Sie im Bereich Instance type (Instance-Typ) den zu startenden Instance-Typ aus.
5. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das der Instance zugeordnet werden soll.
6. Führen Sie im Bereich Advanced details (Erweiterte Details) folgende Schritte aus:
   a. Wählen Sie unter Tenancy die Option Dedicated Host aus.
   b. Wählen Sie unter Target host by (Ziel-Host durch) die Option Host ID (Host-ID) aus.
   c. Wählen Sie unter Target host ID (Ziel-Host-ID) den Host aus, auf dem die Instance gestartet werden soll.
   d. Führen Sie unter Tenancy affinity (Tenancy-Affinität) einen der folgenden Schritte aus:
      - Wählen Sie Off (Aus). Die Instance wird auf dem angegebenen Host gestartet, es ist aber nicht garantiert, dass sie nach dem Anhalten wieder auf demselben Dedicated Host gestartet wird.
      - Wählen Sie die ID des Dedicated Host aus. Falls die Instance angehalten wird, wird sie immer wieder auf diesem spezifischen Host neu gestartet.

      Weitere Informationen zur Affinität finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.
7. Konfigurieren Sie die verbleibenden Instance-Optionen nach Bedarf. Weitere Informationen finden Sie unter Starten einer Instance mit definierten Parametern.
8. Wählen Sie Launch Instance (Instance starten) aus.

AWS CLI

So starten Sie eine Instance in einem Dedicated Host

Verwenden Sie den AWS CLI Befehl run-instances und geben Sie die Instanzaffinität, den Tenancy und den Host im Anforderungsparameter an. `Placement`

PowerShell

So starten Sie eine Instance in einem Dedicated Host

Verwenden Sie den New-EC2Instance AWS Tools for Windows PowerShell Befehl und geben Sie die Instanzaffinität, den Tenancy und den Host im Anforderungsparameter an. `Placement`

Starten Sie Instances in einer Hostressourcengruppe

Wenn Sie eine Instance in einer Hostressourcengruppe starten, in der ein Dedicated Host mit verfügbarer Instance-Kapazität vorhanden ist, startet Amazon EC2 die Instance auf diesem Host. Wenn die Hostressourcengruppe keinen Host mit verfügbarer Instance-Kapazität besitzt, weist Amazon EC2 automatisch einen neuen Host in der Hostressourcengruppe zu und startet die Instance dann auf diesem Host. Weitere Informationen finden Sie unter Hostressourcengruppen im AWS License Manager Benutzerhandbuch.

Voraussetzungen und Einschränkungen

- Sie müssen dem AMI eine core- oder socket-basierte Lizenzkonfiguration zuordnen.
- Sie können SQL Server-, SUSE- oder RHEL-AMIs, die von Amazon EC2 mit Dedicated Hosts bereitgestellt werden, nicht verwenden.
- Sie können nicht auf einen bestimmten Host abzielen, indem Sie eine Host-ID auswählen, und Sie können die Instance-Affinität beim Starten einer Instance in eine Hostressourcengruppe nicht aktivieren.

Mit den folgenden Methoden können Sie eine Instance in einer Host-Ressourcengruppe starten.

Console

So starten Sie eine Instance in einer Hostressourcengruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Launch Instance (Instance starten) aus.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus der Liste aus.

> **Note**
>
> SQL Server-, SUSE- und RHEL-AMIs, die von Amazon EC2 bereitgestellt werden, können nicht mit Dedicated Hosts verwendet werden.

4. Wählen Sie im Bereich Instance type (Instance-Typ) den zu startenden Instance-Typ aus.
5. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das der Instance zugeordnet werden soll.
6. Führen Sie im Bereich Advanced details (Erweiterte Details) folgende Schritte aus:

   a. Wählen Sie unter Tenancy die Option Dedicated Host aus.

   b. Wählen Sie unter Target host by (Ziel-Host durch) die Option Host resource group (Host-Ressourcengruppe) aus.

   c. Wählen Sie unter Tenancy host resource group (Tenancy-Host-Ressourcengruppe) die Host-Ressourcengruppe aus, in der die Instance gestartet werden soll.

   d. Führen Sie unter Tenancy affinity (Tenancy-Affinität) einen der folgenden Schritte aus:

      - Wählen Sie Off (Aus). Die Instance wird auf dem angegebenen Host gestartet, es ist aber nicht garantiert, dass sie nach dem Anhalten wieder auf demselben Dedicated Host gestartet wird.
      - Wählen Sie die ID des Dedicated Host aus. Falls die Instance angehalten wird, wird sie immer wieder auf diesem spezifischen Host neu gestartet.

      Weitere Informationen zur Affinität finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.
7. Konfigurieren Sie die verbleibenden Instance-Optionen nach Bedarf. Weitere Informationen finden Sie unter Starten einer Instance mit definierten Parametern.
8. Wählen Sie Launch Instance (Instance starten) aus.

AWS CLI

So starten Sie eine Instance in einer Hostressourcengruppe

Verwenden Sie den AWS CLI Befehl run-instances, lassen Sie im `Placement` Anforderungsparameter die Option Tenancy weg und geben Sie den ARN der Hostressourcengruppe an.

PowerShell

So starten Sie eine Instance in einer Hostressourcengruppe

Verwenden Sie den New-EC2Instance AWS Tools for Windows PowerShell Befehl, lassen Sie im `Placement` Anforderungsparameter die Option Tenancy weg und geben Sie den ARN der Hostressourcengruppe an.

Grundlagen zur automatischen Platzierung und Affinität

Die Platzierungssteuerung für Dedicated Hosts erfolgt sowohl auf Instance- als auch auf Hostebene.

Automatische Platzierung

Die automatische Platzierung ist auf Host-Ebene konfiguriert. Mit ihr können Sie steuern, ob gestartete Instances auf einem bestimmten Host oder auf einem beliebigen verfügbaren Host mit passender Konfiguration gestartet werden.

Wenn die automatische Platzierung eines Dedicated Host deaktiviert ist, akzeptiert er nur Host-Tenancy-Instance-Starts, die seine eindeutige Host-ID angeben. Dies ist die Standardeinstellung für neue Dedicated Hosts.

Wenn die automatische Platzierung eines Dedicated Host aktiviert ist, akzeptiert er alle nicht zielgerichteten Instance-Starts, die mit seiner Instance-Typ-Konfiguration übereinstimmen.

Beim Starten einer Instance müssen Sie Ihre Tenancy konfigurieren. Wenn eine Instance auf einem Dedicated Host gestartet wird, ohne eine spezifische `HostId` anzugeben, kann sie auf jedem beliebigen Dedicated Host gestartet werden, für den automatische Platzierung aktiviert ist, und der für den Instance-Typ geeignet ist.

Host-Affinität

Host-Affinität wird auf Instance-Ebene konfiguriert. Sie schafft eine Start-Beziehung zwischen einer Instance und einem Dedicated Host.

Wenn die Affinität auf `Host` festgelegt ist, wird eine Instance, die auf einem spezifischen Host gestartet wurde, immer auf demselben Host neu gestartet, wenn sie einmal angehalten wurde. Dies gilt für gezielte und nicht gezielte Starts.

Wenn die Affinität auf `Default` gesetzt ist, und Sie den Neustart der Instance anhalten, kann sie auf jedem verfügbaren Host gestartet werden. Es wird jedoch versucht, sie auf dem letzten Dedicated Host zu starten, auf dem sie ausgeführt wurde (auf Best Effort-Basis).

Ändern der automatischen Platzierung Dedicated Host

Sie können die Einstellungen für die automatische Platzierung eines Dedicated Hosts ändern, nachdem Sie ihn Ihrem AWS Konto zugewiesen haben. Verwenden Sie dazu eine der folgenden Methoden.

Console

So ändern Sie die automatische Platzierung eines Dedicated Host

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie einen Host und Actions (Aktionen), Modify host (Host ändern) aus.
4. Wählen Sie bei Instance auto-placement (Automatische Platzierung der Instance) die Option Enable (Aktivieren) aus, um die automatische Platzierung zu aktivieren oder deaktivieren Sie Enable (Aktivieren), um die automatische Platzierung zu deaktivieren. Weitere Informationen finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.
5. Wählen Sie Save (Speichern) aus.

AWS CLI

So ändern Sie die automatische Platzierung eines Dedicated Host

Verwenden Sie den Befehl modify-hosts AWS CLI . Das folgende Beispiel aktiviert die automatische Platzierung für den angegebenen Dedicated Host

```
aws ec2 modify-hosts --auto-placement on --host-ids h-012a3456b7890cdef
```

PowerShell

So ändern Sie die automatische Platzierung eines Dedicated Host

Verwenden Sie den Befehl. Edit-EC2Host AWS Tools for Windows PowerShell Das folgende Beispiel aktiviert die automatische Platzierung für den angegebenen Dedicated Host

```
PS C:\> Edit-EC2Host --AutoPlacement 1 --HostId h-012a3456b7890cdef
```

Ändern der unterstützten Instance-Typen

Support für mehrere Instance-Typen auf demselben Dedicated Host ist für die folgenden Instance-Familien verfügbar: C5, M5, R5, C5n, R5n, M5n und T3. Andere Instance-Familien unterstützen nur einen einzelnen Instance-Typ auf demselben Dedicated Host.

Sie können einen Dedicated Host mit den folgenden Methoden zuweisen.

Sie können einen Dedicated Host bearbeiten, um die von ihm unterstützten Instance-Typen zu ändern. Wenn er derzeit einen einzelnen Instance-Typ unterstützt, können Sie ihn so ändern, dass er mehrere Instance-Typen innerhalb der Instance-Familie unterstützt. Wenn er derzeit mehrere Instance-Typen unterstützt, können Sie ihn so ändern, dass er nur einen bestimmten Instance-Typ unterstützt.

Um einen Dedicated Host zum Support mehrerer Instance-Typen zu ändern, müssen Sie zunächst alle laufenden Instances auf dem Host stoppen. Die Änderung dauert ca. 10 Minuten. Der Dedicated Host wechselt in den Status `pending`, während die Änderung durchgeführt wird. Sie können keine gestoppten Instances starten oder neue Instances auf dem Dedicated Host starten, während er sich im Status `pending` befinden.

Um ein Dedicated Host, das mehrere Instance-Typen unterstützt, so zu ändern, dass es nur einen einzigen Instance-Typ unterstützt, muss der Host entweder keine ausgeführten Instances haben oder die ausgeführten Instances müssen von dem Instance-Typ sein, den der Host unterstützen soll. Um beispielsweise einen Host für mehrere Instance-Typen der `m5`-Instance-Familie so zu ändern, dass er nur `m5.large`-Instances unterstützt, darf der Dedicated Host entweder keine laufenden Instances haben oder es dürfen nur `m5.large`-Instances darauf laufen.

Wenn Sie einen Host für einen virtualisierten Instance-Typ zuweisen, können Sie den Instance-Typ nicht in einen `.metal`-Instance-Typ ändern, nachdem der Host zugewiesen wurde. Wenn Sie beispielsweise einen Host für den `m5.large`-Instance-Typ zuweisen, können Sie den Instance-Typ nicht in `m5.metal` ändern. Ebenso können Sie, wenn Sie einen Host für einen `.metal`-Instance-Typ zuweisen, den Instance-Typ nicht in einen virtualisierten Instance-Typ ändern, nachdem der Host zugewiesen wurde. Wenn Sie beispielsweise einen Host für den `m5.metal`-Instance-Typ zuweisen, können Sie den Instance-Typ nicht in `m5.large` ändern.

Sie können die unterstützten Instance-Typen mit einer der folgenden Methoden ändern.

Console

SO ändern Sie die unterstützten Instance-Typen für einen Dedicated Host

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Host (Dedizierter Host) aus.
3. Wählen Sie den zu ändernden Dedicated Host und Actions (Aktionen), Modify host (Host ändern) aus.
4. Führen Sie je nach der aktuellen Konfiguration des Dedicated Host einen der folgenden Schritte aus:

   - Wenn der Dedicated Host derzeit einen bestimmten Instance-Typ unterstützt, ist Support multiple instance types (Unterstützung mehrerer Instance-Typen) nicht aktiviert und Instance type (Instance-Typ) führt den unterstützten Instance-Typ auf. Um den Host so zu ändern, dass er mehrere Typen in der aktuellen Instance-Familie unterstützt, wählen Sie für Support multiple instance types (Unterstützung mehrerer Instance-Typen) die Option Enable (Aktivieren) aus.

     Sie müssen zunächst alle Instances stoppen, die auf dem Host laufen, bevor Sie ihn so ändern, dass er mehrere Instance-Typen unterstützt.
   - Wenn Dedicated Host derzeit mehrere Instance-Typen in einer Instance-Familie unterstützt, wird Enabled (Aktiviert) für Support multiple instance types (Mehrere Instance-Typen unterstützen) ausgewählt. Um den Host so zu ändern, dass er einen bestimmten Instance-Typ unterstützt, löschen Sie bei Support multiple instance types (Unterstützung mehrerer Instance-Typen) die Option Enable (Aktivieren) und wählen dann bei Instance type (Instance-Typ) den spezifischen zu unterstützenden Instance-Typ aus.

     Sie können die vom Dedicated Host unterstützte Instance-Familie nicht ändern.
5. Wählen Sie Save (Speichern) aus.

AWS CLI

SO ändern Sie die unterstützten Instance-Typen für einen Dedicated Host

Verwenden Sie den Befehl modify-hosts AWS CLI .

Der folgende Befehl ändert einen Dedicated Host für die Unterstützung mehrerer Instance-Typen innerhalb der `m5`-Instance-Familie.

```
aws ec2 modify-hosts --instance-family m5 --host-ids h-012a3456b7890cdef
```

Der folgende Befehl ändert ein Dedicated Host so, dass nur `m5.xlarge`-Instances unterstützt werden.

```
aws ec2 modify-hosts --instance-type m5.xlarge --instance-family --host-
ids h-012a3456b7890cdef
```

PowerShell

SO ändern Sie die unterstützten Instance-Typen für einen Dedicated Host

Verwenden Sie den Befehl. Edit-EC2Host AWS Tools for Windows PowerShell

Der folgende Befehl ändert einen Dedicated Host für die Unterstützung mehrerer Instance-Typen innerhalb der `m5`-Instance-Familie.

```
PS C:\> Edit-EC2Host --InstanceFamily m5 --HostId h-012a3456b7890cdef
```

Der folgende Befehl ändert ein Dedicated Host so, dass nur `m5.xlarge`-Instances unterstützt werden.

```
PS C:\> Edit-EC2Host --InstanceType m5.xlarge --HostId h-012a3456b7890cdef
```

Ändern der Instance-Tenancy und der Affinität

Die Tenancy einer Instance kann geändert werden, nachdem sie gestartet wurde. Sie können die Affinität für Ihre Instance auch ändern, um einen bestimmten Host als Ziel festzulegen, oder das Starten auf einem beliebigen verfügbaren Dedicated Host mit passenden Attributen in Ihrem Konto zulassen. Um entweder die Instance-Tenancy oder die Affinität der Instance zu ändern, muss sich die Instance im Status `stopped` befinden.

Welche Konvertierungen unterstützt werden, hängt von den Betriebssystemdetails Ihrer Instance sowie davon ab, ob SQL Server installiert ist. Weitere Informationen zu den für Ihre Instance verfügbaren Tenancy-Konvertierungspfaden finden Sie im License Manager-Benutzerhandbuch unter Tenancy-Konvertierung.

> **Note**
>
> Bei T3-Instances muss die Instance auf einem Dedicated Host gestartet werden, um eine Tenancy vom Typ `host` zu verwenden. Bei T3-Instances kann die Tenancy nicht von `host` in `dedicated` oder `default` geändert werden. Wenn Sie versuchen, eine dieser nicht unterstützten Tenancy-Änderungen vorzunehmen, wird der `InvalidRequest`-Fehlercode angezeigt.

Sie können die Tenancy und die Affinität einer Instance mit den folgenden Methoden ändern.

Console

So ändern Sie Instance-Tenancy oder die Affinität

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Instances und die Instances aus, die zu ändern sind.
3. Wählen Sie Instance state (Instance-Status), Stop (Anhalten).
4. Wählen Sie bei ausgewählter Instance Aktionen, Instance-Einstellungen und Instance-Platzierung ändern.
5. Konfigurieren Sie auf der Seite Instanzplatzierung ändern Folgendes:
   - Tenancy:— Wählen Sie eine der folgenden Optionen:
     - Run a dedicated hardware instance (Eine dedizierte Hardware-Instance ausführen) — Startet die Instance als eine Dedicated Instance. Weitere Informationen finden Sie unter Dedicated Instances.
     - Launch the instance on a Dedicated Host (Starten der Instance auf einem) — Startet die Instance auf einem Dedicated Host mit konfigurierbarer Affinität.
   - Affinity (Affinität):— Wählen Sie eine der folgenden Optionen:
     - This instance can run on any one of my hosts (Diese Instance kann auf allen meinen Hosts ausgeführt werden) – Die Instance startet auf einem beliebigen, in Ihrem Konto verfügbaren Dedicated Host, der ihren Instance-Typ unterstützt.
     - This instance can only run on the selected host (Diese Instance kann nur auf dem ausgewählten Host gestartet werden) – Die Instance kann nur auf dem Dedicated Host ausgeführt werden, der als Target Host (Ziel-Host) bestimmt wurde.

- Target Host (Ziel-Host) — Wählen Sie den Dedicated Host aus, auf dem die Instance ausgeführt werden muss. Falls kein Ziel-Host aufgelistet ist, verfügen Sie möglicherweise über keine verfügbaren, kompatiblen Dedicated Hosts in Ihrem Konto.

Weitere Informationen finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.

6. Wählen Sie Save (Speichern) aus.

AWS CLI

So ändern Sie Instance-Tenancy oder die Affinität

Verwenden Sie den Befehl modify-instance-placement AWS CLI . Das folgende Beispiel ändert die Affinität der angegebenen Instance von `default` in `host` und gebt den Dedicated Host an, zu dem die Instance eine Affinität hat.

```
aws ec2 modify-instance-placement --instance-id i-1234567890abcdef0 --affinity host
 --tenancy host --host-id h-012a3456b7890cdef
```

PowerShell

So ändern Sie Instance-Tenancy oder die Affinität

Verwenden Edit-EC2InstancePlacement AWS Tools for Windows PowerShell Sie den Befehl. Das folgende Beispiel ändert die Affinität der angegebenen Instance von `default` in `host` und gebt den Dedicated Host an, zu dem die Instance eine Affinität hat.

```
PS C:\> Edit-EC2InstancePlacement -InstanceId i-1234567890abcdef0 -Affinity host -
Tenancy host -HostId h-012a3456b7890cdef
```

Dedicated Hosts anzeigen

Mit den folgenden Methoden können Sie Details zu einem Dedicated Host und den einzelnen Instances darauf anzeigen.

Console

So zeigen Sie die Details eines Dedicated Host an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie auf der Seite Dedicated Hosts einen Host aus.
4. Um Informationen über den Host anzuzeigen, wählen Sie Details aus.

   Available vCPUs (Verfügbare vCPUs) zeigt die vCPUs an, die auf dem Dedicated Host für den Start neuer Instances verfügbar sind. Ein Dedicated Host, der beispielsweise mehrere Instance-Typen innerhalb der c5-Instance-Familie unterstützt und auf dem keine Instances laufen, verfügt über 72 verfügbare vCPUs. Das bedeutet, dass Sie verschiedene Kombinationen von Instance-Typen auf dem Dedicated Host starten können, um die 72 verfügbaren vCPUs zu nutzen.

   Um Informationen über die Instances anzuzeigen, die auf Ihrem Host ausgeführt werden, wählen Sie Running instances (Ausgeführte Instances) aus.

AWS CLI

So zeigen Sie die Kapazität eines Dedicated Host an

Verwenden Sie den Befehl describe-hosts AWS CLI .

Das folgende Beispiel verwendet den Befehl describe-hosts (AWS CLI), um die verfügbare Instance-Kapazität für einen Dedicated Host anzuzeigen, der mehrere Instance-Typen innerhalb der Instance-Familie `c5` unterstützt. Auf dem Dedicated Host laufen bereits zwei `c5.4xlarge`-Instances und vier `c5.2xlarge`-Instances.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

```
"AvailableInstanceCapacity": [
    { "AvailableCapacity": 2,
      "InstanceType": "c5.xlarge",
      "TotalCapacity": 18 },
    { "AvailableCapacity": 4,
      "InstanceType": "c5.large",
      "TotalCapacity": 36 }
```

```
  ],
"AvailableVCpus": 8
```

PowerShell

So zeigen Sie die Instance-Kapazität eines Dedicated Host an

Verwenden Sie den Befehl Get-EC2Host AWS Tools for Windows PowerShell .

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Dedicated Hosts markieren

Sie können Ihren vorhandenen Dedicated Hosts benutzerdefinierte Tags (Markierungen) zuweisen, um sie auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. So können Sie einen bestimmten Dedicated Host basierend auf den zugewiesenen benutzerdefinierten Tags (Markierungen) schnell finden. Dedicated Host-Tags (Markierungen) können auch für die Kostenzuordnungsverfolgung verwendet werden.

Sie können zum Zeitpunkt der Erstellung Dedicated Hosts auch Tags (Markierungen) zuordnen. Weitere Informationen finden Sie unter Zuordnen von Dedicated Hosts.

Sie können ein Dedicated Host anhand der folgenden Methoden markieren:

Console

So markieren Sie ein Dedicated Host

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den zu markierenden Dedicated Host und dann Actions (Aktionen), Manage Tags (Tags (Markierungen) verwalten) aus.
4. Wählen Sie im Fenster Manage Tags (Tags (Markierungen) verwalten) die Option Add Tags (Tags (Markierungen) hinzufügen) aus und geben Sie dann den Schlüssel und den Wert für den Tag (Markierung) an.
5. (Optional) Wählen Sie Add Tags (Tags (Markierungen) hinzufügen), um dem Dedicated Host zusätzliche Tags (Markierungen) hinzuzufügen.
6. Wählen Sie Save Changes.

AWS CLI

So markieren Sie ein Dedicated Host

Verwenden Sie den Befehl create-tags AWS CLI .

Der folgende Befehl markiert den angegebenen Dedicated Host mit `Owner=TeamA`.

```
aws ec2 create-tags --resources h-abc12345678909876 --tags Key=Owner,Value=TeamA
```

PowerShell

So markieren Sie ein Dedicated Host

Verwenden Sie den Befehl New-EC2Tag AWS Tools for Windows PowerShell .

Der Befehl `New-EC2Tag` benötigt ein `Tag`-Objekt, das den Schlüssel und das Schlüsselpaar angibt, die für den Dedicated Host-Tag (Markierung) verwendet werden. Die folgenden Befehle erstellen ein `Tag`-Objekt mit dem Namen `$tag` und dem Schlüssel-Wert-Paar `Owner` bzw. `TeamA`:

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

Der folgende Befehl markiert den angegebenen Dedicated Host mit dem `$tag`-Objekt.

```
PS C:\> New-EC2Tag -Resource h-abc12345678909876 -Tag $tag
```

Dedicated Hosts überwachen

Amazon EC2 überwacht permanent den Status Ihrer Dedicated Hosts. Aktualisierungen werden in der Amazon EC2-Konsole angezeigt. Sie können Informationen zu einem Dedicated Host mit den folgenden Methoden anzeigen.

Console

So zeigen Sie den Status eines Dedicated Host an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Suchen Sie den Dedicated Host in der Liste und sehen Sie sich den Wert in der Spalte State (Status) an.

AWS CLI

So zeigen Sie den Status eines Dedicated Host an

Verwenden Sie den AWS CLI Befehl describe-hosts und überprüfen Sie dann die `state` Eigenschaft im `hostSet` Antwortelement.

```
aws ec2 describe-hosts --host-id h-012a3456b7890cdef
```

PowerShell

So zeigen Sie den Status eines Dedicated Host an

Verwenden Sie den Get-EC2Host AWS Tools for Windows PowerShell Befehl und überprüfen Sie dann die `state` Eigenschaft im `hostSet` Antwortelement.

```
PS C:\> Get-EC2Host -HostId h-012a3456b7890cdef
```

Die folgende Tabelle erklärt die möglichen Dedicated Host-Statuswerte.

Status	Beschreibung
`available`	AWS hat kein Problem mit dem Dedicated Host festgestellt. Es sind keine Wartungen oder Reparaturen geplant. Instances können auf diesem Dedicated Host gestartet werden.
`released`	Der Dedicated Host wurde freigegeben. Die Host-ID wird nicht mehr verwendet. Freigegebene Hosts können nicht wiederverwendet werden.
`under-assessment`	AWS untersucht ein mögliches Problem mit dem Dedicated Host. Wenn Maßnahmen ergriffen werden müssen, werden Sie per E-Mail AWS Management Console oder per E-Mail benachrichtigt. In diesem Status können keine Instances auf dem Dedicated Host gestartet werden.

Status	Beschreibung
`pending`	Der Dedicated Host kann nicht für den Start neuer Instances verwendet werden. Er wird entweder geändert, um mehrere Instance-Typen zu unterstützen oder es wird eine Host-Wiederherstellung durchgeführt.
`permanent-failure`	Ein unwiederbringlicher Fehler ist aufgetreten. Sie erhalten einen Bereinigungshinweis über Ihre Instances und per E-Mail. Ihre Instances werden möglicherweise weiter ausgeführt. Wenn Sie alle Instances auf einem Dedicated Host mit diesem Status beenden oder beenden, wird der AWS Host außer Betrieb genommen. AWS startet Instanzen in diesem Status nicht neu. In diesem Status können keine Instances auf dem Dedicated Hosts gestartet werden.
`released-permanent-failure`	AWS gibt Dedicated Hosts, die ausgefallen sind und auf denen keine laufenden Instances mehr laufen, dauerhaft frei. Die Dedicated Host-ID steht nicht mehr zur Nutzung zur Verfügung.

Freigeben von Dedicated Hosts

Sämtliche auf dem Dedicated Host ausgeführten Instances müssen angehalten werden, bevor Sie den Host freigeben können. Diese Instances können auf andere Dedicated Hosts in Ihrem Konto migriert werden, damit Sie deren Nutzung fortsetzen können. Diese Schritte gelten nur für On-Demand Dedicated Hosts.

Sie können einen Dedicated Host mit den folgenden Methoden freigeben.

Console

So veröffentlichen Sie ein Dedicated Host

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie auf der Seite Dedicated Hosts den freizugebenden Dedicated Host aus.
4. Wählen Sie Actions (Aktionen), Release host (Host veröffentlichen).
5. Wählen Sie zur Bestätigung Release (Freigeben) aus.

AWS CLI

So veröffentlichen Sie ein Dedicated Host

Verwenden Sie den Befehl release-hosts AWS CLI .

```
aws ec2 release-hosts --host-ids h-012a3456b7890cdef
```

PowerShell

So veröffentlichen Sie ein Dedicated Host

Verwenden Sie den Befehl Remove-EC2Hosts AWS Tools for Windows PowerShell .

```
PS C:\> Remove-EC2Hosts -HostId h-012a3456b7890cdef
```

Nachdem Sie einen Dedicated Host freigegeben haben, können Sie denselben Host oder dieselbe Host-ID nicht mehr wiederverwenden. Es werden Ihnen keine On-Demand-Abrechnungstarife mehr berechnet. Der Status des Dedicated Host wird in `released` geändert, und Sie können keine Instances mehr auf diesem Host starten.

> **Note**
>
> Falls Sie vor kurzem Dedicated Hosts freigegeben haben, kann es etwas dauern, bis diese nicht mehr zu Ihrem Limit hinzugezählt werden. Während dieser Zeit können `LimitExceeded`-Fehler auftreten, wenn Sie versuchen, neue Dedicated Hosts zuzuordnen. Wenn das der Fall ist, versuchen Sie nach ein paar Minuten noch einmal, neue Hosts zuzuordnen.

Die Instances, die angehalten wurden, sind immer noch zur Verwendung verfügbar und werden auf der Seite Instances aufgeführt. Sie behalten ihre `host`-Tenancy-Einstellung.

Kaufen von Dedicated Host-Reservierungen

Sie können Reservierungen mit den folgenden Methoden kaufen:

Console

So kaufen Sie Reservierungen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Dedicated Hosts, Dedicated Host-Reservierungen, Purchase Dedicated Host-Reservierung (Dedicated Host-Reservierung erwerben).
3. Gehen Sie auf dem Bildschirm „Angebote suchen“ wie folgt vor:
   a. Wählen Sie unter Instance-Familie die Instance-Familie des Dedicated Hosts aus, für den Sie die Dedicated Host-Reservierung erwerben möchten.
   b. Wählen und konfigurieren Sie unter Zahlungsoption Ihre bevorzugte Zahlungsoption.
4. Wählen Sie Weiter aus.
5. Wählen Sie die Dedicated Hosts aus, denen Sie die Dedicated Host-Reservierung zuordnen möchten, und klicken Sie dann auf Weiter.
6. (Optional) Weisen Sie der Dedicated Host-Reservierung Tags zu.
7. Überprüfen Sie Ihre Bestellung und wählen Sie Kaufen.

AWS CLI

So kaufen Sie Reservierungen

1. Verwenden Sie den AWS CLI Befehl describe-host-reservation-offers, um die verfügbaren Angebote aufzulisten, die Ihren Anforderungen entsprechen. Das folgende Beispiele listet die Angebote auf, die Instances in der Instance-Familie `m4` unterstützen und eine einjährige Laufzeit haben.

> **Note**
>
> Die Laufzeit wird in Sekunden angegeben. Eine einjährige Laufzeit umfasst 31 536 000 Sekunden und eine dreijährige Laufzeit 94 608 000 Sekunden.

```
aws ec2 describe-host-reservation-offerings --filter Name=instance-
family,Values=m4 --max-duration 31536000
```

Die Befehle geben eine Liste mit Angeboten zurück, die Ihren Kriterien entsprechen. Schreiben Sie sich die `offeringId` des zu kaufenden Angebots auf.

2. Verwenden Sie den AWS CLI Befehl purchase-host-reservation, um das Angebot zu erwerben und die im vorherigen Schritt angegebenen Daten bereitzustellen. `offeringId` Das folgende Beispiel kauft die angegebene Reservierung und ordnet sie einem bestimmten Dedicated Host zu, der dem AWS Konto bereits zugewiesen ist. Außerdem wird ein Tag mit dem Schlüssel `purpose` und dem Wert von zugewiesen. `production`

```
aws ec2 purchase-host-reservation --offering-id hro-03f707bf363b6b324 --
host-id-set h-013abcd2a00cbd123 --tag-specifications 'ResourceType=host-
reservation,Tags={Key=purpose,Value=production}'
```

PowerShell

So kaufen Sie Reservierungen

1. Verwenden Sie den Get-EC2HostReservationOffering AWS Tools for Windows PowerShell Befehl, um die verfügbaren Angebote aufzulisten, die Ihren Anforderungen entsprechen. Die folgenden Beispiele listen die Angebote auf, die Instances in der Instance-Familie `m4` unterstützen und eine einjährige Laufzeit haben.

> **Note**
>
> Die Laufzeit wird in Sekunden angegeben. Eine einjährige Laufzeit umfasst 31 536 000 Sekunden und eine dreijährige Laufzeit 94 608 000 Sekunden.

```
PS C:\> $filter = @{Name="instance-family"; Value="m4"}
```

```
PS C:\> Get-EC2HostReservationOffering -filter $filter -MaxDuration 31536000
```

Die Befehle geben eine Liste mit Angeboten zurück, die Ihren Kriterien entsprechen. Schreiben Sie sich die `offeringId` des zu kaufenden Angebots auf.

2. Verwenden Sie den New-EC2HostReservation AWS Tools for Windows PowerShell Befehl, um das Angebot zu erwerben und die `offeringId` im vorherigen Schritt angegebenen

Informationen bereitzustellen. Das folgende Beispiel kauft die angegebene Reservierung und ordnet sie einem bestimmten Dedicated Host zu, der dem AWS Konto bereits zugewiesen ist.

```
PS C:\> New-EC2HostReservation -OfferingId hro-03f707bf363b6b324 -
HostIdSet h-013abcd2a00cbd123
```

Anzeigen von Reservierungen Dedicated Host

Sie können Informationen zu den Dedicated Hosts anzeigen, die Ihrer Reservierung zugeordnet wurden, einschließlich:

- Die Laufzeit der Reservierung
- Die Zahlungsoption
- Das Start- und Enddatum

Sie können Details Ihrer Dedicated Host-Reservierungen mit den folgenden Methoden einsehen.

Console

So zeigen Sie die Details einer Dedicated Host-Reservierung an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Klicken Sie auf der Seite Dedicated Hosts auf Dedicated Host Reservations (Dedicated Host-Reservierungen) und wählen Sie die Reservierung aus der bereitgestellten Liste aus.
4. Wählen Sie Details für Informationen zu der Reservierung.
5. Wählen Sie Hosts aus, um Informationen über Dedicated Hosts zu erhalten, denen die Reservierung zugeordnet ist.

AWS CLI

So zeigen Sie die Details einer Dedicated Host-Reservierung an

Verwenden Sie den Befehl describe-host-reservations AWS CLI .

```
aws ec2 describe-host-reservations
```

PowerShell

So zeigen Sie die Details einer Dedicated Host-Reservierung an

Verwenden Sie den Befehl. Get-EC2HostReservation AWS Tools for Windows PowerShell

```
PS C:\> Get-EC2HostReservation
```

Markieren von Dedicated Host-Reservierungen

Sie können Ihren Dedicated Host-Reservierungen benutzerdefinierte Tags (Markierungen) zuweisen, um sie auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. So können Sie eine bestimmte Dedicated Host-Reservierung basierend auf den zugewiesenen benutzerdefinierten Tag (Markierung) schnell finden.

Sie können eine Dedicated Host-Reservierung nur mit Befehlszeilen-Tools markieren.

AWS CLI

So markieren Sie ein Dedicated Host-Reservierung

Verwenden Sie den Befehl create-tags AWS CLI .

```
aws ec2 create-tags --resources hr-1234563a4ffc669ae --tags Key=Owner,Value=TeamA
```

PowerShell

So markieren Sie ein Dedicated Host-Reservierung

Verwenden Sie den Befehl New-EC2Tag AWS Tools for Windows PowerShell .

Der Befehl `New-EC2Tag` benötigt einen `Tag`-Parameter, der das Schlüssel-Wert-Paar angibt, das für den Dedicated Host-Reservierung-Tag verwendet werden soll. Die folgenden Befehle erstellen den Parameter `Tag`.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
PS C:\> $tag.Key = "Owner"
PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource hr-1234563a4ffc669ae -Tag $tag
```

Arbeiten mit freigegebenen Dedicated Hosts

Dedicated Host Sharing ermöglicht es Besitzern von Dedicated Hosts, ihre Dedicated Hosts mit anderen AWS Konten oder innerhalb einer AWS Organisation zu teilen. Auf diese Weise können Sie Dedicated Hosts zentral erstellen und verwalten und den Dedicated Host für mehrere AWS Konten oder innerhalb Ihrer AWS Organisation gemeinsam nutzen.

Bei diesem Modell teilt sich das AWS Konto, dem der Dedicated Host gehört (Eigentümer), ihn mit anderen AWS Konten (Verbrauchern). Konsumenten können beim Starten der für sie freigegebenen Instances auf Dedicated Hosts so vorgehen, wie sie dies beim Starten von Instances auf Dedicated Hosts tun würden, die sie in ihrem eigenen Konto zuweisen. Der Besitzer ist für die Verwaltung des Dedicated Host und der Instances, die von ihm darin gestartet werden, verantwortlich. Besitzer können Instances, die Konsumenten auf freigegebenen Dedicated Hosts starten, nicht ändern. Konsumenten sind für die Verwaltung der Instances verantwortlich, die sie in den für sie freigegebenen Dedicated Hosts starten. Konsumenten können sich keine Instances anzeigen lassen oder ändern, die anderen Konsumenten oder dem Besitzer des Dedicated Host gehören, und sie können keine Dedicated Hosts ändern, die für sie freigegeben sind.

Ein Dedicated Host-Besitzer kann einen Dedicated Host freigeben für:

- Bestimmte AWS Konten innerhalb oder außerhalb der AWS Organisation
- Eine Organisationseinheit innerhalb ihrer AWS Organisation
- Es ist die gesamte AWS Organisation

Inhalt

- Fakturierung und Messung
- Dedicated Host-Limits
- Hostwiederherstellung und Dedicated Host-Freigabe

Voraussetzungen für die Freigabe von Dedicated Hosts

- Um einen Dedicated Host zu teilen, musst du ihn in deinem AWS Konto besitzen. Sie können keinen Dedicated Host freigeben, der für Sie freigegeben wurde.
- Um einen Dedicated Host mit deiner AWS Organisation oder einer Organisationseinheit in deiner AWS Organisation zu teilen, musst du das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.

Einschränkungen für die Freigabe von Dedicated Hosts

Sie können Dedicated Hosts nicht freigeben, die für die folgenden Instance-Typen zugewiesen wurden: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal` und `u-24tb1.metal`.

Zugehörige Services

AWS Resource Access Manager

Die gemeinsame Nutzung von Dedicated Hosts ist in AWS Resource Access Manager (AWS RAM) integriert. AWS RAM ist ein Dienst, mit dem Sie Ihre AWS Ressourcen mit einem beliebigen AWS Konto oder über dieses teilen können AWS Organizations. Mit können Sie Ressourcen AWS RAM, die Ihnen gehören, gemeinsam nutzen, indem Sie eine gemeinsame Nutzung erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Bei Verbrauchern kann es sich um einzelne AWS Konten, Organisationseinheiten oder eine gesamte Organisation handeln AWS Organizations.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Freigeben in mehreren Availability Zones

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. Beispielsweise hat die Availability Zone `us-`

`east-1a` für Ihr AWS Konto möglicherweise nicht denselben Standort wie `us-east-1a` für ein anderes AWS Konto.

Um den Ort Ihrer Dedicated Hosts relativ zu Ihren Konten zu bestimmen, verwenden Sie die Availability-Zone-ID (AZ-ID). Die Availability Zone ID ist eine eindeutige und konsistente Kennung für eine Availability Zone für alle AWS Konten. Beispielsweise ist `use1-az1` eine Availability-Zone-ID für die `us-east-1`-Region und ist derselbe Speicherort in jedem AWS -Konto.

So lassen Sie sich die Availability-Zone-IDs für Availability Zones in Ihrem Konto anzeigen

1. Öffnen Sie die AWS RAM Konsole unter https://console.aws.amazon.com/ram.
2. Die Availability-Zone-IDs für die aktuelle Region werden im Feld Your AZ ID (Ihre AZ-ID) rechts im Bildschirm angezeigt.

Freigeben eines Dedicated Host

Gibt ein Besitzer einen Dedicated Host frei, können Konsumenten Instances auf dem Host starten. Konsumenten können so viele Instances auf dem freigegebenen Host starten, wie es die verfügbare Kapazität zulässt.

> **Important**
>
> Beachten Sie, dass Sie dafür verantwortlich sind, sicherzustellen, dass Sie über die entsprechenden Lizenzrechte verfügen, um BYOL-Lizenzen auf Ihren Dedicated Hosts freizugeben.

Wenn Sie einen Dedicated Host freigeben, bei dem die automatische Platzierung aktiviert ist, beachten Sie Folgendes, da dies zu einer unbeabsichtigten Dedicated Host-Nutzung führen könnte:

- Wenn Konsumenten Instances mit Dedicated Host-Tenancy starten und über keine Kapazität auf einem Dedicated Host verfügen, den sie in ihrem Konto besitzen, wird die Instance automatisch auf dem freigegebenen Dedicated Host gestartet.

Um einen Dedicated Host freigeben zu können, müssen Sie ihn einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM Ressource, mit der Sie Ihre Ressourcen für mehrere AWS Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden

Ressourcen und die Konsumenten an, für die sie freigegeben werden. Sie können den Dedicated Host zu einer vorhandenen Ressource oder zu einer neuen Ressourcenfreigabe hinzufügen.

Wenn du Teil einer Organisation bist AWS Organizations und das Teilen innerhalb deiner Organisation aktiviert ist, erhalten Verbraucher in deiner Organisation automatisch Zugriff auf den gemeinsam genutzten Dedicated Host. Andernfalls erhalten Konsumenten eine Einladung zur Teilnahme an der Ressourcenfreigabe und nach Annahme der Einladung wird ihnen Zugriff auf den freigegebenen Dedicated Host gewährt.

> **Note**
>
> Nach der Freigabe eines Dedicated Host kann es einige Minuten dauern, bis Konsumenten darauf zugreifen können.

Sie können mithilfe einer der folgenden Methoden einen Dedicated Host, den Sie besitzen, freigeben.

Amazon EC2 console

So geben Sie einen Dedicated Host in Ihrem Besitz mithilfe der Amazon EC2-Konsole frei

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus, der freigegeben werden soll, und wählen Sie Aktionen, Host freigeben aus.
4. Wählen Sie die Ressourcenfreigabe aus, der der Dedicated Host hinzugefügt werden soll, aus und wählen Sie dann Freigeben aus.

   Es kann einige Minuten dauern, bis Konsumenten Zugriff auf den freigegebenen Host gewährt wird.

AWS RAM console

Um einen Dedicated Host, den Sie besitzen, über die AWS RAM Konsole gemeinsam zu nutzen

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

AWS CLI

Um einen Dedicated Host, den Sie besitzen, mit dem AWS CLI

Verwenden Sie den Befehl create-resource-share.

Freigeben eines freigegebenen Dedicated Host rückgängig machen

Der Dedicated Host-Besitzer kann die Freigabe eines freigegebenen Dedicated Host jederzeit aufheben. Wenn Sie die Freigabe eines freigegebenen Dedicated Host aufheben, gelten die folgenden Regeln:

- Verbraucher, für die der Dedicated Host freigegeben wurde, können darauf keine neuen Instances mehr starten.
- Instances im Besitz von Konsumenten, die zum Zeitpunkt der Freigabe auf dem Dedicated Host ausgeführt wurden, werden weiterhin ausgeführt, sind jedoch für die Ausmusterung vorgesehen. Konsumenten erhalten für die Instances Benachrichtigungen über die Ausmusterung und haben zwei Wochen Zeit, um entsprechende Maßnahmen zu ergreifen. Wird der Dedicated Host dem Konsumenten jedoch innerhalb der Ausmusterungsbenachrichtigungszeitraums erneut freigegeben, erfolgt ein Abbruch der Instance-Ausmusterungen.

Um die Freigabe eines freigegebenen Dedicated Host in Ihrem Besitz aufheben zu können, müssen Sie ihn aus der Ressourcenfreigabe entfernen. Sie können dies mit einer der folgenden Methoden durchführen:

Amazon EC2 console

So heben Sie die Freigabe eines freigegebenen Dedicated Host in Ihrem Besitz mithilfe der Amazon EC2-Konsole auf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus, dessen Freigabe aufgehoben werden soll, und wählen Sie dann die Registerkarte Freigabe aus.
4. Auf der Registerkarte Freigabe werden die Ressourcenfreigaben aufgelistet, zu denen der Dedicated Host hinzugefügt wurde. Wählen Sie die Ressourcenfreigabe aus, aus der der Dedicated Host entfernt werden soll, und wählen Sie Host aus Ressourcenfreigabe entfernen aus.

AWS RAM console

Freigabe eines Dedicated Host in Ihrem Besitz über die AWS RAM -Konsole aufheben

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Command line

Um die gemeinsame Nutzung eines gemeinsam genutzten Dedicated Hosts, den Sie besitzen, rückgängig zu machen, verwenden Sie AWS CLI

Verwenden Sie den Befehl disassociate-resource-share.

Identifizieren eines freigegebenen Dedicated Host

Besitzer und Konsumenten können freigegebene Dedicated Hosts mit einer der folgenden Methoden identifizieren.

Amazon EC2 console

So identifizieren Sie einen freigegebenen Dedicated Host mithilfe der Amazon EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus. Im Bildschirm werden die Dedicated Hosts in Ihrem Besitz und Dedicated Hosts, die für Sie freigegeben werden, aufgelistet. In der Spalte Owner (Besitzer) wird die AWS -Konto-ID des Dedicated Host-Besitzers angezeigt.

Command line

Um einen gemeinsam genutzten Dedicated Host zu identifizieren, verwenden Sie den AWS CLI

Verwenden Sie den Befehl describe-hosts. Der Befehl gibt die Dedicated Hosts zurück, die Sie besitzen und die Dedicated Hosts, die für Sie freigegeben sind.

Anzeigen von Instances, die auf einem freigegebenen Dedicated Host ausgeführt werden

Besitzer und Konsumenten können die Instances, die auf einem freigegebenen Dedicated Host ausgeführt werden, jederzeit mit einer der folgenden Methoden anzeigen.

Amazon EC2 console

So lassen Sie sich die auf einem freigegebenen Dedicated Host ausgeführten Instances mithilfe der Amazon EC2-Konsole anzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus, für den die Instances angezeigt werden sollen, und klicken Sie auf Instances. Auf der Registerkarte werden die Instances aufgeführt, die auf dem Host ausgeführt werden. Besitzer sehen alle Instances, die auf dem Host ausgeführt werden, einschließlich der Instances, die von Konsumenten gestartet werden. Konsumenten sehen nur ausgeführte Instances, die sie auf dem Host gestartet haben. In der Spalte Owner (Besitzer) wird die AWS -Konto-ID des Kontos angezeigt, über das die Instance gestartet wurde.

Command line

Instances, die auf freigegebenem Dedicated Host ausgeführt werden, über die AWS CLI anzeigen

Verwenden Sie den Befehl describe-hosts. Der Befehl gibt die Instances zurück, die auf jedem Dedicated Host ausgeführt werden. Besitzer sehen alle Instances, die auf dem Host ausgeführt werden. Konsumenten sehen nur ausgeführte Instances, die sie auf den freigegebenen Hosts gestartet haben. `InstanceOwnerId` zeigt die AWS -Konto-ID des Instance-Besitzers an.

Berechtigungen für freigegebene Dedicated Host

Berechtigungen für Besitzer

Besitzer sind verantwortlich für die Verwaltung ihrer freigegebenen Dedicated Hosts und der Instances, die sie auf ihnen starten. Besitzer können sich alle Instances anzeigen lassen, die auf dem freigegebenen Dedicated Host ausgeführt werden, dazu gehören auch die von Konsumenten gestarteten. Besitzer können jedoch keine Maßnahmen für ausgeführte Instances ergreifen, die von Konsumenten gestartet wurden.

Berechtigungen für Konsumenten

Konsumenten sind für die Verwaltung der Instances verantwortlich, die sie in dem für sie freigegebenen Dedicated Host starten. Konsumenten können den freigegebenen Dedicated

Host keinesfalls ändern und können keine Instances anzeigen oder bearbeiten, die von anderen Konsumenten oder dem Dedicated Host-Besitzer gestartet wurden.

Fakturierung und Messung

Für die Freigabe von Dedicated Hosts fallen keine zusätzlichen Gebühren an.

Besitzern werden die Dedicated Hosts in Rechnung gestellt, die sie freigeben. Konsumenten werden keine Instances in Rechnung gestellt, die sie auf freigegebenen Dedicated Hosts starten.

Dedicated Host-Reservierungen bieten weiterhin Abrechnungsrabatte für freigegebene Dedicated Hosts. Nur Dedicated Host-Besitzer können Dedicated Host-Reservierungen für freigegebene Dedicated Hosts kaufen, die sie besitzen.

Dedicated Host-Limits

Freigegebene Dedicated Hosts werden nur auf die Dedicated Hosts-Limits des Besitzers angerechnet. Die Dedicated Hosts-Limits von Konsumenten sind nicht von Dedicated Hosts betroffen, die ihnen freigegeben wurden. Ebenso werden Instances, die Konsumenten auf freigegebenen Dedicated Hosts starten, nicht auf ihre Instance-Limits angerechnet.

Hostwiederherstellung und Dedicated Host-Freigabe

Die Hostwiederherstellung stellt Instances wieder her, die vom Dedicated Host-Besitzer und den Konsumenten gestartet wurden, für die er freigegeben wurde. Der Ersatz-Dedicated Host wird dem Konto des Besitzers zugeordnet. Er wird zu den gleichen Ressourcenfreigaben wie der ursprüngliche Dedicated Host hinzugefügt und den gleichen Konsumenten freigegeben.

Weitere Informationen finden Sie unter Host-Wiederherstellung.

Dedizierte Hosts auf AWS Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur, Dienste, APIs und Tools auf Ihre Räumlichkeiten ausdehnt. Durch den lokalen Zugriff auf die AWS verwaltete Infrastruktur AWS Outposts können Sie Anwendungen vor Ort mit denselben Programmierschnittstellen wie in AWS Regionen erstellen und ausführen und gleichzeitig lokale Rechen- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen nutzen.

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazität, der am Standort eines Kunden bereitgestellt wird. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS Region.

Sie können Dedicated Hosts auf Outposts zuweisen, die Sie in Ihrem Konto besitzen. Dies erleichtert es Ihnen, Ihre vorhandenen Softwarelizenzen und Workloads, die einen dedizierten physischen Server erfordern, nach AWS Outposts zu bringen. Sie können auch auf bestimmte Hardwareressourcen auf einem Outpost ausrichten, um die Latenz zwischen Ihren Workloads zu minimieren.

Dedicated Hosts ermöglichen es Ihnen, Ihre berechtigten Softwarelizenzen auf Amazon EC2 zu verwenden, damit Sie die Flexibilität und Kosteneffizienz der Verwendung Ihrer eigenen Lizenzen erhalten. Andere Softwarelizenzen, die an virtuelle Maschinen, Sockets oder physische Kerne gebunden sind, können vorbehaltlich ihrer Lizenzbedingungen auch auf Dedicated Hosts verwendet werden. Während Outposts schon immer eine Einzelmandanten-Umgebung waren, die für BYOL-Workloads in Frage kommen, können Sie mit Dedicated Hosts die erforderlichen Lizenzen auf einen einzelnen Host im Gegensatz zur gesamten Outpost-Bereitstellung beschränken.

Darüber hinaus bietet Ihnen die Verwendung von Dedicated Hosts in einem Outpost eine größere Flexibilität bei der Instance-Typ-Bereitstellung und eine detailliertere Kontrolle über die Platzierung von Instances. Sie können beispielsweise auf einen bestimmten Host zielen und Host-Affinität verwenden, um sicherzustellen, dass die Instance immer auf diesem Host ausgeführt wird oder Sie können die automatische Platzierung verwenden, um eine Instance auf jedem verfügbaren Host zu starten, der über übereinstimmende Konfigurationen und verfügbare Kapazität verfügt.

Inhalt

Voraussetzungen

Sie müssen einen Outpost an Ihrem Standort installiert haben. Weitere Informationen finden Sie unter Outpost erstellen und die Kapazität dafür bestellen im AWS Outposts -Benutzerhandbuch.

Unterstützte Features

- Die folgenden Instance-Familien werden unterstützt: `C5`, `M5`, `R5`, `C5d`, `M5d`, `R5d`, `G4dn` und `i3en`.
- Dedicated Hosts on Outposts können so konfiguriert werden, dass sie mehrere Instance-Größen unterstützen. Unterstützung für mehrere Instance-Größen ist für die folgenden Instance-Familien

verfügbar: C5, M5, R5, C5d, M5d und R5d. Weitere Informationen finden Sie unter Konfigurationen der Instance-Kapazität.

- Dedicated Hosts on Outposts unterstützen die automatische Platzierung und gezielte Instance-Starts. Weitere Informationen finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.
- Dedicated Hosts auf Outposts unterstützen Host-Affinität. Weitere Informationen finden Sie unter Grundlagen zur automatischen Platzierung und Affinität.
- Dedizierte Hosts auf Outposts unterstützen das Teilen mit AWS RAM. Weitere Informationen finden Sie unter Arbeiten mit freigegebenen Dedicated Hosts.

Überlegungen

- Dedicated-Host-Reservierungen werden auf Outposts nicht unterstützt.
- Hosten Ressourcengruppen und AWS License Manager werden auf Outposts nicht unterstützt.
- Dedicated Hosts auf Outposts unterstützen keine Burstable T3-Instances.
- Dedicated Hosts auf Outposts unterstützen keine Host-Wiederherstellung.
- Eine vereinfachte automatische Wiederherstellung wird für Instances mit Dedicated Host Tenancy auf Outposts nicht unterstützt.

Einen Dedicated Host auf einem Outpost zuweisen und verwenden

Sie weisen Dedicated Hosts auf Outposts auf die gleiche Weise zu und verwenden sie wie bei Dedicated Hosts in einer AWS -Region.

Voraussetzungen

Erstellen Sie ein Subnetz auf dem Outpost. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im AWS Outposts -Benutzerhandbuch.

Verwenden Sie eine der folgenden Methoden, um einen Dedicated Host für einen Outpost zuzuweisen:

AWS Outposts console

1. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
2. Wählen Sie im Navigationsbereich Outposts aus. Wählen Sie den Outpost aus und wählen Sie dann Actions (Aktionen), Allocate Dedicated Host (Dedicated Host zuweisen).

3. Konfigurieren Sie den Dedicated Host nach Bedarf. Weitere Informationen finden Sie unter Zuordnen von Dedicated Hosts.

   > **Note**
   >
   > Availability Zone (Verfügbarkeitszone) und Outpost ARN (Outpost-ARN) sollte mit der Availability Zone und dem ARN des ausgewählten Outposts vorausgefüllt werden.

4. Wählen Sie Allocate aus.

Amazon EC2 console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts und dann Allocate Dedicated Host (Dedicated Host zuweisen) aus.
3. Als Availability Zon (Verfügbarkeitszone) wählen Sie die Availability Zone aus, die dem Outpost zugewiesen ist.
4. Als Outpost ARN (Outpost-ARN) geben Sie den ARN des Outposts ein.
5. Um auf bestimmte Hardwareressourcen auf dem Outpost auszurichten, wählen Sie für Gezielt auf spezifische Hardwareressourcen auf Outpost ausrichten die Option Aktivieren aus. Wählen Sie für jede Hardwareressource, die Sie als Ziel verwenden möchten, Ressourcen-ID hinzufügen aus, und geben Sie dann die ID der Hardwareressource ein.

   > **Note**
   >
   > Der Wert, den Sie für Menge angeben, muss der Anzahl der von Ihnen angegebenen Ressourcen-IDs entsprechen. Wenn Sie beispielsweise 3 Ressourcen-IDs angeben, muss die Menge ebenfalls 3 sein.

6. Konfigurieren Sie die verbleibenden Dedicated-Host-Einstellungen nach Bedarf. Weitere Informationen finden Sie unter Zuordnen von Dedicated Hosts.
7. Wählen Sie Allocate aus.

AWS CLI

Verwenden Sie den Befehl allocate-hosts AWS CLI . Geben Sie bei `--availability-zone` die Availability Zone an, die dem Outpost zugewiesen ist. Geben Sie bei `--outpost-arn` den ARN

des Ouposts an. Geben Sie optional für `--asset-ids` die IDs der Outpost-Hardwareressourcen an, auf die ausgerichtet werden soll.

```
aws ec2 allocate-hosts --availability-zone "us-east-1a" --outpost-arn
 "arn:aws:outposts:us-east-1a:111122223333:outpost/op-4fe3dc21baEXAMPLE" --asset-
ids asset_id --instance-family "m5" --auto-placement "off" --quantity 1
```

So starten Sie eine Instance in einem Dedicated Host auf einem Outpost

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus. Wählen Sie den Dedicated Host aus, den Sie im vorherigen Schritt zugewiesen haben, und wählen Sie Actions (Aktionen), Launch instance onto host (Instance auf Host launchen).
3. Konfigurieren Sie die Instance nach Bedarf und launchen Sie dann die Instance. Weitere Informationen finden Sie unter Starten Sie Instances auf einem Dedicated Host.

Host-Wiederherstellung

Die automatische Wiederherstellung des Dedicated Hosts startet Ihre Instances auf einem neuen Ersatzhost neu, wenn bestimmte problematische Bedingungen auf Ihrem Dedicated Host erkannt werden. Die Host-Wiederherstellung reduziert den Bedarf an manuellen Eingriffen und verringert die Betriebsbelastung, wenn ein unerwarteter Ausfall des Dedicated Hosts im Zusammenhang mit Systemstrom- oder Netzwerkkonnektivitätsereignissen auftritt. Andere Dedicated-Host-Probleme erfordern manuelle Eingriffe, um sie zu beheben.

Inhalt

Grundlagen zur Host-Wiederherstellung

Dedicated Hosts und der Wiederherstellungsprozess von Hostressourcengruppen verwenden Zustandsprüfungen auf Hostebene, um die Verfügbarkeit von Dedicated Hosts zu bewerten und zugrunde liegende Systemfehler zu erkennen. Die Art des Dedicated-Host-Fehlers bestimmt, ob die automatische Wiederherstellung des Dedicated Hosts möglich ist. Zu den Problemen, die zu Prüfungen auf Hostebene führen können, zählen:

- Verlust der Netzwerkverbindung
- Systemstromausfall
- Hardware- oder Softwareprobleme auf dem physischen Host

> **Important**
>
> Die automatische Wiederherstellung eines Dedicated Hosts findet nicht statt, wenn der Host für die Außerbetriebnahme vorgesehen ist.

Automatische Wiederherstellung für Dedicated Hosts

Wenn auf Ihrem Dedicated Host ein Ausfall der Systemleistung oder der Netzwerkverbindung festgestellt wird, wird die auto Wiederherstellung des Dedicated Hosts initiiert und Amazon EC2 weist automatisch einen Ersatz-Dedicated Host in derselben Availability Zone wie der ursprüngliche Dedicated Host zu. Dieser Dedicated Host erhält eine neue Host-ID, hat aber dieselben Attribute wie der ursprüngliche Dedicated Host, einschließlich:

- Availability Zone
- Instance-Typ
- Tags (Markierungen)
- Einstellungen zur automatischen Platzierung
- Reservation (Reservierung)

Nachdem der ersatzmäßige Dedicated Host zugeordnet wurde, werden die Instances auf dem ersatzmäßigen Dedicated Host wiederhergestellt. Die wiederhergestellten Instances haben dieselben Attribute wie der ursprüngliche Host, einschließlich:

- Instance-ID

- Private IP-Adressen
- Elastic IP-Adressen
- EBS-Volume-Anhänge
- Alle Instance-Metadaten

Darüber hinaus automatisiert die integrierte Integration mit AWS License Manager die Nachverfolgung und Verwaltung Ihrer Lizenzen.

> **Note**
>
> AWS Die License Manager-Integration wird nur in Regionen unterstützt, in denen AWS License Manager verfügbar ist.

Wenn zwischen den Instances und dem nicht funktionierenden Dedicated Host eine Affinitätsbeziehung besteht, richten die wiederhergestellten Instances eine Host-Affinität mit dem ersatzmäßigen Dedicated Host ein.

Wenn alle Instances auf dem ersatzmäßigen Dedicated Host wiederhergestellt wurden, wird der beeinträchtigte Dedicated Host freigegeben und der ersatzmäßige Dedicated Host kann verwendet werden.

Wenn die Host-Wiederherstellung eingeleitet wird, wird der AWS Kontoinhaber per E-Mail und durch ein AWS Health Dashboard Ereignis benachrichtigt. Nachdem die Host-Wiederherstellung erfolgreich durchgeführt wurde, wird eine zweite Benachrichtigung gesendet.

Wenn Sie AWS License Manager verwenden, um Ihre Lizenzen nachzuverfolgen, weist AWS License Manager neue Lizenzen für den Ersatz-Dedicated Host auf der Grundlage der Lizenzkonfigurationslimits zu. Wenn die Lizenzkonfiguration feste Grenzwerte hat, die durch die Host-Wiederherstellung überschritten werden, ist der Wiederherstellungsprozess nicht zulässig und Sie werden über eine Amazon SNS SNS-Benachrichtigung über den Fehler bei der Host-Wiederherstellung informiert (sofern die Benachrichtigungseinstellungen für AWS License Manager konfiguriert wurden). Gelten für die Lizenzkonfiguration weiche Limits, die aufgrund der Host-Wiederherstellung überschritten werden, kann der Wiederherstellungsprozess fortgesetzt werden und Sie werden per Amazon SNS-Benachrichtigung über die Limit-Überschreitung informiert. Weitere Informationen finden Sie unter Verwenden von Lizenzkonfigurationen und Einstellungen in License Manager im AWS -License-Manager-Benutzerhandbuch.

Szenarien ohne automatische Wiederherstellung für Dedicated Hosts

Die automatische Wiederherstellung eines Dedicated Hosts findet nicht statt, wenn der Host für die Außerbetriebnahme vorgesehen ist. Sie erhalten im Rahmen eines CloudWatch Amazon-Events eine Benachrichtigung zur Kündigung, und die E-Mail-Adresse des AWS Kontoinhabers erhält eine Nachricht über den Ausfall des Dedicated Hosts. AWS Health Dashboard Führen Sie die in der Benachrichtigung über die Außerbetriebnahme beschriebenen Abhilfemaßnahmen innerhalb der angegebenen Zeitspanne durch, um die Instances auf dem außerbetriebgenommenen Host manuell wiederherzustellen.

Angehaltene Instances werden auf dem Dedicated Host nicht wiederhergestellt. Wenn Sie versuchen, eine angehaltene Instance zu starten, die auf den beeinträchtigten Dedicated Host ausgerichtet ist, schlägt der Start fehl. Wir empfehlen, die angehaltene Instance so zu ändern, dass sie auf einen anderen Dedicated Host ausgerichtet ist oder so, dass sie auf einem verfügbaren Dedicated Host mit passender Konfiguration und aktivierter automatischer Platzierung gestartet wird.

Instances mit Instance-Speicher werden auf dem Ersatz-Dedicated Host nicht wiederhergestellt. Im Rahmen einer Korrekturmaßnahme wird der beeinträchtigte Dedicated Host für die Ausmusterung gekennzeichnet und Sie erhalten eine entsprechende Benachrichtigung, wenn die Host-Wiederherstellung abgeschlossen ist. Befolgen Sie die Korrekturmaßnahmen aus der Benachrichtigung innerhalb des angegebenen Zeitraums, um die verbliebenen Instances auf dem beeinträchtigten Dedicated Host wiederherzustellen.

Unterstützte Instance-Typen

Die Host-Wiederherstellung wird für die folgenden Instance-Familien unterstützt: A1, C3, C4, C5, C5n, C6a, C6g, C6i, Inf1, G3, G5g, M3, M4, M5, M5n, M5zn, M6a, M6g, M6i, P2, P3, R3, R4, R5, R5b, R5n, R6g, R6i, T3, X1, X1e, X2IEZN, u-6tb1, u-9tb1, u-12tb1, u-18tb1 und u-24tb1.

Informationen zum Wiederherstellen nicht unterstützter Instances finden Sie unter Manuelles Wiederherstellen nicht unterstützter Instances.

> **Note**
>
> Die automatische Wiederherstellung von unterstützten Metal-Instance-Typen für Dedicated Hosts dauert länger als die von Nicht-Metal-Instance-Typen zum Erkennen und Wiederherstellen.

Konfigurieren der Host-Wiederherstellung

Sie können die Host-Wiederherstellung zum Zeitpunkt der Dedicated Host-Zuweisung oder nach der Zuweisung mithilfe der Amazon EC2 EC2-Konsole oder AWS Command Line Interface (CLI) konfigurieren.

Inhalt

Aktivieren der Host-Wiederherstellung

Sie können die Host-Wiederherstellung zum Zeitpunkt der Dedicated Host-Zuordnung oder hinterher aktivieren.

Weitere Informationen zum Aktivieren der Host-Wiederherstellung zum Zeitpunkt der Dedicated Host-Zuordnung finden Sie unter Zuordnen von Dedicated Hosts.

So aktivieren Sie die Host-Wiederherstellung nach der Zuweisung über die Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus, für den die Host-Wiederherstellung aktiviert werden soll, und wählen Sie dann Actions (Aktionen), Modify Host Recovery (Host-Wiederherstellung ändern) aus.
4. Wählen Sie für Host recovery (Host-Wiederherstellung) die Optionen Enable (Aktivieren) und Save (Speichern) aus.

Um die Host-Wiederherstellung nach der Zuweisung zu aktivieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl modify-hosts und geben Sie den Parameter `host-recovery` an.

```
$ aws ec2 modify-hosts --host-recovery on --host-ids h-012a3456b7890cdef
```

Deaktivieren der Host-Wiederherstellung

Sie können die Host-Wiederherstellung jederzeit nach der Zuordnung des Dedicated Host deaktivieren.

So deaktivieren Sie die Host-Wiederherstellung nach der Zuweisung über die Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus, für den die Host-Wiederherstellung deaktiviert werden soll, und wählen Sie dann Actions (Aktionen), Modify Host Recovery (Host-Wiederherstellung ändern) aus.
4. Wählen Sie für Host recovery (Host-Wiederherstellung) die Optionen Disable (Deaktivieren) und Save (Speichern) aus.

Um die Host-Wiederherstellung nach der Zuweisung zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl modify-hosts und geben Sie den Parameter `host-recovery` an.

```
$ aws ec2 modify-hosts --host-recovery off --host-ids h-012a3456b7890cdef
```

Anzeigen der Host-Wiederherstellungskonfiguration

Sie können die Konfiguration der Host-Wiederherstellung für einen Dedicated Host jederzeit anzeigen.

So zeigen Sie die Host-Wiederherstellungskonfiguration für eine Dedicated Host über die Konsole an:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus und überprüfen Sie auf der Registerkarte Description (Beschreibung) das Feld Host Recovery (Host-Wiederherstellung).

Host-Wiederherstellungskonfiguration für Dedicated Host über die AWS CLI anzeigen

Verwenden Sie den Befehl describe-hosts.

```
$ aws ec2 describe-hosts --host-ids h-012a3456b7890cdef
```

Das `HostRecovery`-Antwortelement zeigt an, ob die Host-Wiederherstellung aktiviert oder deaktiviert ist.

Status der Host-Wiederherstellung

Wird ein Dedicated Host-Ausfall entdeckt, wechselt der beeinträchtigte Dedicated Host in den Status „`under-assessment`“ und die betroffenen Instances in den Status „`impaired`“. Sie können keine Instances auf dem gestörten Dedicated Host starten, während er sich im Status `under-assessment` befindet.

Nachdem der ersatzmäßige Dedicated Host zugeordnet wurde, wechselt er in den Status `pending`. Er bleibt in diesem Status, bis die Host-Wiederherstellung abgeschlossen ist. Sie können keine Instances auf den Ersatz-Dedicated Host starten, während er sich im Status `pending` befindet. Wiederhergestellte Instances auf dem ersatzmäßigen Dedicated Host verbleiben während der Wiederherstellung im Status `impaired`.

Nach Abschluss der Host-Wiederherstellung wechselt der ersatzmäßige Dedicated Host in den Status `available` und die wiederhergestellten Instances erhalten wieder den Status `running`. Sie können Instances auf dem ersatzmäßigen Dedicated Host starten, sobald dieser wieder den Status `available` hat. Der ursprüngliche, beeinträchtigte Dedicated Host wird dauerhaft freigegeben und wechselt in den Status `released-permanent-failure`.

Verfügt der beeinträchtigte Dedicated Host über Instances, die keine Host-Wiederherstellung unterstützen, beispielsweise solche mit Instance-Speicher-gestützten Volumes, wird der Dedicated Host nicht freigegeben. Stattdessen wird er für die Ausmusterung gekennzeichnet und erhält den Status `permanent-failure`.

Manuelles Wiederherstellen nicht unterstützter Instances

Die Host-Wiederherstellung unterstützt nicht die Wiederherstellung von Instances, die Instance-Speicher-Volumes verwenden. Befolgen Sie die unten stehende Anleitung, um manuell die Instances wiederherzustellen, die nicht automatisch wiederhergestellt werden konnten.

> **Warning**
>
> Alle Daten, die auf Instance-Speicher-Volumes gespeichert sind, gehen verloren, wenn eine Instance angehalten, in den Ruhezustand versetzt oder beendet wird. Dies gilt auch für Instance-Speicher-Volumes, die an eine Instance mit einem EBS-Volume als Root-Gerät

angefügt sind. Wenn Sie Daten von Instance-Speicher-Volumes schützen möchten, sichern Sie diese auf einem persistenten Speicher, ehe die Instance angehalten oder beendet wird.

Manuelles Wiederherstellen von EBS-gestützten Instances

EBS-gestützte Instances, die nicht automatisch wiederhergestellt werden, sollten Sie manuell anhalten und starten, damit sie auf einem neuen Dedicated Host wiederhergestellt werden. Weitere Informationen zum Anhalten Ihrer Instance und zu den Änderungen an der Instance-Konfiguration nach dem Anhalten finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.

Manuelles Wiederherstellen von Instance-Speicher-gestützten Instances

Bei Instance-Speicher-gestützten Instances, die nicht automatisch wiederhergestellt werden können, sollten Sie wie folgt vorgehen:

1. Starten Sie eine Ersatz-Instance auf einem neuen Dedicated Host über Ihr neuestes AMI.
2. Migrieren Sie alle notwendigen Daten zur Ersatz-Instance.
3. Beenden Sie die Original-Instance auf dem beeinträchtigten Dedicated Host.

Zugehörige Services

Dedicated Host kann in folgende Services integriert werden:

- AWS License Manager — Verfolgt Lizenzen auf Ihren Amazon EC2 Dedicated Hosts (wird nur in Regionen unterstützt, in denen AWS License Manager verfügbar ist). Weitere Informationen finden Sie im AWS License-Manager-Benutzerhandbuch.

Preisgestaltung

Für die Host-Wiederherstellung fallen keine weiteren Kosten an. Es gelten die üblichen Dedicated Host-Gebühren. Weitere Informationen finden Sie unter Amazon EC2 Dedicated Hosts-Preise.

Sobald die Host-Wiederherstellung gestartet wurde, fallen keine Gebühren mehr für den beeinträchtigten Dedicated Host an. Kosten für den ersatzmäßigen Dedicated Host fallen erst an, wenn er den Status `available` hat.

Wenn der beeinträchtigte Dedicated Host nach Bedarf abgerechnet wurde, wird der ersatzmäßige Dedicated Host ebenso abgerechnet. Verfügte der beeinträchtigte Dedicated Host über einen aktiven Dedicated Host-Reservierung, wird er an den ersatzmäßigen Dedicated Host weitergegeben.

Host-Wartung

Bei der Host-Wartung werden Ihre Amazon EC2 EC2-Instances auf dem heruntergestuften Dedicated Host während eines geplanten Wartungsereignisses automatisch auf einem Ersatz-Dedicated Host neu gestartet. Dies trägt dazu bei, die Ausfallzeiten von Anwendungen zu reduzieren und den undifferenzierten Aufwand der Wartung auf AWS auszulagern. Host-Wartung wird auch für geplante und routinemäßige Amazon-EC2-Wartung durchgeführt.

Host-Wartung wird auf allen neuen Dedicated-Host-Zuweisungen unterstützt, die über die Amazon-EC2-Konsole vorgenommen werden. Für jeden Dedicated Host in Ihrem AWS-Konto oder für jeden neuen Dedicated Host, der über die AllocateHosts API zugewiesen wurde, können Sie die Host-Wartung für unterstützte Dedicated Hosts konfigurieren. Weitere Informationen finden Sie unter the section called “Konfigurieren der Host-Wartung”.

Inhalt

Grundlagen zur Host-Wartung

Wenn bei einem Dedicated Host eine Beeinträchtigung festgestellt wird, wird ein neuer Dedicated Host zugewiesen. Eine Beeinträchtigung kann durch eine Beeinträchtigung der zugrunde liegenden Hardware oder durch die Erkennung bestimmter problematischer Bedingungen verursacht werden. Es ist geplant, dass Ihre Instances auf dem heruntergestuften Dedicated Host automatisch auf dem Ersatz-Dedicated Host neu gestartet werden.

Der Ersatz-Dedicated-Host erhält eine neue Host-ID, behält aber die gleichen Attribute wie der ursprüngliche Dedicated Host. Diese Attribute beinhalten Folgendes.

- Einstellungen zur automatischen Platzierung
- Availability Zone
- Reservation (Reservierung)
- Host-Affinität
- Einstellungen für die Host-Wartung
- Einstellungen für die Host-Wiederherstellung
- Instance-Typ
- Tags

Die Host-Wartung ist insgesamt AWS-Regionen für alle unterstützten Dedicated Hosts verfügbar. Weitere Informationen zu Dedicated Hosts, bei denen Host-Wartung nicht unterstützt wird, finden Sie unter the section called “Einschränkungen”.

Ihr beeinträchtigter Dedicated Host wird freigegeben, nachdem alle Ihre Instances auf einem neuen Dedicated Host neu gestartet oder beendet wurden. Sie können vor dem geplanten Wartungsvorgang auf Ihre Instances auf dem beeinträchtigten Dedicated Host zugreifen, aber das Starten von Instances auf dem beeinträchtigten Dedicated Host wird nicht unterstützt.

Sie können den Ersatz-Dedicated Host verwenden, um vor dem geplanten Wartungsereignis neue Instances auf dem Host zu starten. Ein Teil der Instance-Kapazität auf dem Ersatzhost ist jedoch für die Instances reserviert, die vom heruntergestuften Host migriert werden müssen. Sie können keine neuen Instances in dieser reservierten Kapazität starten. Weitere Informationen finden Sie unter the section called “Instances auf Dedicated Host”.

Einschränkungen

- Die Host-Wartung wird in AWS Outposts AWS Local Zones und AWS Wavelength Zones nicht unterstützt.
- Die Host-Wartung kann für Hosts, die sich bereits in einer Host-Ressourcengruppe befinden, nicht aktiviert oder deaktiviert werden. Hosts, die einer Host-Ressourcengruppe hinzugefügt wurden, behalten ihre Host-Wartungseinstellung bei. Weitere Informationen finden Sie unter Host-Ressourcengruppen.

- Host-Wartung wird nur auf bestimmten Instance-Typen unterstützt. Weitere Informationen finden Sie unter the section called “Unterstützte Instance-Typen”.

Host-Wartung im Vergleich zur Host-Wiederherstellung

Die folgende Tabelle zeigt die Hauptunterschiede zwischen Host-Wiederherstellung und Host-Wartung.

	Host-Wiederherstellung	Host-Wartung
Zugriffsmöglichkeiten	Unerreichbar	Erreichbar
Status	`under-assessment`	`permanent-failure`
Aktion	Die Wiederherstellung erfolgt sofort	Die Wartung ist geplant
Flexibilität bezüglich der Zeitplanung	Kann nicht verschoben werden	Kann nicht verschoben werden
Host-Ressourcengruppe	Unterstützt	Nicht unterstützt

Weitere Informationen zur Host-Wiederherstellung finden Sie unter Host-Wiederherstellung.

Unterstützte Instance-Typen

Die Host-Wartung wird für die folgenden Instance-Familien unterstützt:

- Universell: `A1` | `M4` | `M5` | `M5a` | `M5n` | `M5zn` | `M6a` | `M6g` | `M6i` | `M6in` | `M7a` | `M7g` | `M7i` | `T3`
- Für Datenverarbeitung optimiert: `C4` | `C5` | `C5a` | `C5n` | `C6a` | `C6g` | `C6gn` | `C6i` | `C6in` | `C7g` | `C7gn` | `C7i`
- Arbeitsspeicheroptimiert: `R4` | `R5` | `R5a` | `R5b` | `R5n` | `R6a` | `R6g`| `R6i` | `R6in` | `R7a` | `R7g` | `R7iz` | `u-12tb1` | `u-18tb1` | `u-24tb1` | `u-3tb1` | `u-6tb1` | `u-9tb1` | `X2iezn`
- Beschleunigtes Computing: `G3` | `G5g` | `Inf1` | `P2` | `P3`

Instances auf Dedicated Host

Amazon EC2 reserviert automatisch Kapazität auf dem Ersatzhost für die Instances, die automatisch vom heruntergestuften Host migriert werden. Amazon EC2 reserviert keine Kapazität auf dem Ersatzhost für Instances, die nicht automatisch migriert werden können, wie z. B. Instances mit Instance-Speicher-Root-Volumes. Die reservierte Kapazität kann nicht zum Starten neuer Instances verwendet werden.

> **Note**
>
> Die Amazon EC2 EC2-Konsole zeigt die reservierte Kapazität als genutzte Kapazität an. Es könnte den Anschein haben, dass die Instances sowohl auf dem heruntergestuften Host als auch auf dem Ersatzhost laufen. Die Instances werden jedoch weiterhin nur auf dem heruntergestuften Host ausgeführt, bis sie gestoppt oder in die reservierte Kapazität auf dem Ersatzhost migriert werden.

Wenn Sie eine Instanz auf dem heruntergestuften Host, die automatisch migriert werden kann, manuell beenden, wird die Kapazität, die für diese Instance auf dem Ersatzhost reserviert war, freigegeben und steht wieder zur Verfügung.

Während des geplanten Wartungsereignisses werden die Instanzen auf dem heruntergestuften Host neu gestartet und in die reservierte Kapazität auf dem Ersatz-Dedicated Host migriert. Die migrierten Instances behalten dieselben Attribute wie die Instanzen auf Ihrem heruntergestuften Host, einschließlich der folgenden.

- Anhänge von Amazon-EBS-Volumes
- Elastic-IP-Adressen
- Instance-ID
- Instance-Metadaten
- Private IP-Adresse

Sie können eine Instance auf dem beeinträchtigten Host zu einem beliebigen Zeitpunkt beenden und starten, bevor der geplante Wartungsvorgang initiiert wird. Dadurch wird Ihre Instance auf einem anderen Host neu gestartet und Ihre Instance wird nicht planmäßig gewartet. Sie müssen die Host-Affinität Ihrer Instance auf den neuen Host aktualisieren, auf dem Sie Ihre Instance neu starten möchten. Wenn Sie alle Instanzen auf dem heruntergestuften Host beenden, bevor

das Wartungsereignis ausgelöst wird, wird der heruntergestufte Host freigegeben und das Wartungsereignis wird abgebrochen. Weitere Informationen finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.

> **Note**
>
> Die Daten auf einem lokalen Speicher-Volume werden nicht beibehalten, wenn Sie Ihre Instance beenden und starten.

Instances mit einem Instance-Speicher-Volume als Root-Gerät werden nach dem angegebenen Beendigungsdatum beendet. Alle Daten auf den Instance-Speicher-Volumes werden gelöscht, wenn die Instances beendet werden. Beendete Instances werden dauerhaft gelöscht und können nicht erneut gestartet werden. Für Instances mit Instance-Stamm-Volumes empfehlen wir, Ersatz-Instances auf einem anderen Dedicated Host zu starten. Verwenden Sie dazu das aktuellste Amazon Machine Image und migrieren Sie alle verfügbaren Daten vor dem angegebenen Beendigungsdatum auf die Ersatz-Instances. Weitere Informationen finden Sie unter Maßnahmen zur Außerbetriebnahme einer Instanz.

Instances, die nicht automatisch neu gestartet werden können, werden nach dem angegebenen Datum beendet. Sie können diese Instances auf einem anderen Host erneut starten. Instances, die ein Amazon-EBS-Volume als Stamm-Gerät verwenden, verwenden weiterhin dasselbe Amazon EBS-Volume, nachdem sie auf einem neuen Host gestartet wurden.

Sie können die Reihenfolge des Instance-Neustarts festlegen, indem Sie die Startzeit eines Instance-Neustarts in https://console.aws.amazon.com/ec2/ neu planen.

Konfigurieren der Host-Wartung

Sie können die Host-Wartung für alle unterstützten Dedicated Hosts über AWS Management Console oder konfigurieren AWS CLI. Weitere Einzelheiten finden Sie in der folgenden Tabelle.

AWS Management Console

Um die Host-Wartung für Ihren Dedicated Host zu aktivieren, verwenden Sie AWS Management Console.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie Dedicated Host > Aktionen > Host ändern aus.

4. Wählen Sie die Option ein im Feld Host-Wartung aus.

So deaktivieren Sie die Host-Wartung für Ihren Dedicated Host mit der AWS Management Console.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie Dedicated Host > Aktionen > Host ändern aus.
4. Wählen Sie die Option aus im Feld Host-Wartung aus.

So zeigen Sie die Host-Wartungskonfiguration für Ihren Dedicated Host mit der AWS Management Console an.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Dedicated Hosts aus.
3. Wählen Sie den Dedicated Host aus und überprüfen Sie auf der Registerkarte Beschreibung das Feld Host-Wartung.

AWS CLI

So aktivieren oder deaktivieren Sie die Host-Wartung für Ihren neuen Dedicated Host während der Zuweisung mit AWS CLI.

Verwenden Sie den allocate-hosts-Befehl.

Aktivieren

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance on
```

Deaktivieren

```
aws ec2 allocate-hosts --region us-east-1 --quantity 1 --instance-type m3.large --
availability-zone us-east-1b --host-maintenance off
```

Um die Host-Wartung für Ihren vorhandenen Dedicated Host zu aktivieren oder zu deaktivieren, verwenden Sie AWS CLI.

Verwenden Sie den modify-hosts-Befehl.

Aktivieren

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance on --host-
ids h-0d123456bbf78910d
```

Deaktivieren

```
aws ec2 modify-hosts --region us-east-1 --host-maintenance off --host-
ids h-0d123456bbf78910d
```

So zeigen Sie die Host-Wartungskonfiguration für Ihren Dedicated Host mit der AWS CLI an.

Verwenden Sie den Befehl describe-hosts.

```
aws ec2 describe-hosts --region us-east-1 --host-ids h-0d123456bbf78910d
```

> **Note**
>
> Wenn Sie die Host-Wartung deaktivieren, erhalten Sie eine E-Mail-Benachrichtigung, um den beeinträchtigten Host zu entfernen und Ihre Instances innerhalb von 28 Tagen manuell auf einen anderen Host zu migrieren. Wenn Sie über eine Dedicated-Host-Reservierung verfügen, wird ein Ersatz-Host zugewiesen. Nach 28 Tagen werden die auf dem beeinträchtigten Host ausgeführten Instances beendet und der Host wird automatisch freigegeben.

Wartungsereignis

Wenn eine Beeinträchtigung festgestellt wird, wird 14 Tage später ein Wartungsvorgang geplant, bei dem Ihre Instances auf einem neuen Dedicated Host neu gestartet werden. Sie erhalten eine E-Mail-Benachrichtigung mit Details über den beeinträchtigten Host, den geplanten Wartungsvorgang und die Zeitfenster für die Wartung. Weitere Informationen finden Sie unter Anzeigen von geplanten Ereignissen.

Sie können den Wartungsvorgang auf einen beliebigen Tag bis zu sieben Tage nach dem Datum des geplanten Ereignisses verschieben. Weitere Informationen zur Neuplanung finden Sie unter Neuplanung eines geplanten Ereignisses.

Der Wartungsvorgang dauert in der Regel einige Minuten. Im seltenen Fall eines erfolglosen Ereignisses erhalten Sie eine E-Mail-Benachrichtigung, um die Instances auf dem beeinträchtigten Host innerhalb eines bestimmten Zeitrahmens zu entfernen.

Status der Host-Wartung

Ihr Dedicated Host wird in den `permanent-failure`-Status versetzt, wenn eine Beeinträchtigung festgestellt wird. Sie können keine Instances auf einem Dedicated Host im Status `permanent-failure` starten. Nach Abschluss des Wartungsvorgangs wird der beeinträchtigte Host freigegeben und in den `released, permanent-failure`-Status versetzt.

Nachdem bei einem Dedicated Host eine Leistungsminderung festgestellt wurde und bevor ein Wartungsereignis geplant wurde, weist die Host-Wartung Ihrem Konto automatisch einen Ersatz-Dedicated Host zu. Dieser Ersatzhost bleibt so lange in seinem `pending` Zustand, bis ein Wartungsereignis geplant ist. Nachdem das Wartungsereignis geplant wurde, wechselt der Ersatz-Dedicated Host in den `available` Status.

Sie können den Ersatz-Dedicated Host verwenden, um vor dem geplanten Wartungsereignis neue Instances auf dem Host zu starten. Ein Teil der Instance-Kapazität auf dem Ersatzhost ist jedoch für die Instances reserviert, die vom heruntergestuften Host migriert werden müssen. Sie können keine neuen Instances in dieser reservierten Kapazität starten. Weitere Informationen finden Sie unter the section called “Instances auf Dedicated Host”.

Zugehörige Services

Dedicated Host ist in AWS License Manager integriert — Verfolgt Lizenzen auf Ihren Amazon EC2 Dedicated Hosts (wird nur in Regionen unterstützt, in denen AWS License Manager verfügbar ist). Weitere Informationen finden Sie im AWS License-Manager-Benutzerhandbuch.

Sie müssen über ausreichend Lizenzen AWS-Konto für Ihren neuen Dedicated Host verfügen. Die Ihrem beeinträchtigten Host zugeordneten Lizenzen werden freigegeben, wenn der Host nach Abschluss des geplanten Wartungsvorgangs freigegeben wird.

Preisgestaltung

Für die Host-Wartung fallen keine zusätzlichen Gebühren an. Es fallen jedoch die üblichen Dedicated-Host-Gebühren an. Weitere Informationen finden Sie unter Amazon EC2 Dedicated Hosts-Preise.

Sobald die Host-Wartung eingeleitet wird, wird Ihnen der beeinträchtigte Dedicated Host nicht mehr in Rechnung gestellt. Kosten für den ersatzmäßigen Dedicated Host fallen erst an, wenn er den Status `available` hat.

Wenn der eingeschränkte Dedicated Host mit dem On-Demand-Tarif abgerechnet wurde, wird der Ersatz-Dedicated Host ebenfalls mit dem On-Demand-Tarif abgerechnet. Wenn der beeinträchtigte Dedicated Host über eine aktive Dedicated-Host-Reservierung verfügt, wird diese auf den neuen Dedicated Host übertragen.

Verfolgen von Konfigurationsänderungen

Sie können AWS Config damit Konfigurationsänderungen für Dedicated Hosts und für Instances aufzeichnen, die auf diesen gestartet, gestoppt oder beendet werden. Sie können dann die von AWS Config erfassten Informationen als Datenquelle für die Lizenzberichterstellung verwenden.

AWS Config zeichnet Konfigurationsinformationen für Dedicated Hosts und Instances einzeln auf und verknüpft diese Informationen anhand von Beziehungen. Es gibt drei Berichtsbedingungen.

- AWS Config Aufzeichnungsstatus — Wenn aktiviert, AWS Config werden ein oder mehrere AWS Ressourcentypen aufgezeichnet, zu denen Dedicated Hosts und Dedicated Instances gehören können. Um die erforderlichen Informationen für die Lizenzberichterstattung zu erfassen, prüfen Sie, dass Hosts und Instances mit den folgenden Feldern aufgenommen werden.
- Host recording status (Hostaufnahmestatus):— Bei Enabled (Aktiviert) werden die Konfigurationsinformationen für Dedicated Hosts aufgenommen.
- Instance recording status (Instance-Erfassungsstatus) – Bei Enabled (Aktiviert) werden die Konfigurationsinformationen für Dedicated Instances erfasst.

Falls mindestens eine dieser drei Bedingungen deaktiviert ist, ist das Symbol auf der Schaltfläche Edit Config Recording (Konfigurationsaufnahme bearbeiten) rot. Um den vollständigen Nutzen dieses Tools zu erhalten, müssen Sie gewährleisten, dass alle drei Aufnahmemethoden aktiviert sind. Wenn alle drei aktiviert sind, ist das Symbol grün. Zum Bearbeiten der Einstellungen wählen Sie Edit Config Recording (Konfigurationsaufnahme bearbeiten). Sie werden zur AWS Config Einrichtungsseite in der AWS Config Konsole weitergeleitet, auf der Sie die Aufzeichnung für Ihre Hosts, Instances AWS Config und andere unterstützte Ressourcentypen einrichten und starten können. Weitere Informationen finden Sie im AWS Config Entwicklerhandbuch AWS Config unter Einrichtung mithilfe der Konsole.

> **Note**
>
> AWS Config zeichnet Ihre Ressourcen auf, nachdem sie erkannt wurden. Dies kann mehrere Minuten dauern.

Nach AWS Config Beginn der Aufzeichnung von Konfigurationsänderungen an Ihren Hosts und Instances können Sie den Konfigurationsverlauf aller Hosts abrufen, die Sie zugewiesen oder freigegeben haben, sowie aller Instances, die Sie gestartet, gestoppt oder beendet haben. Beispiel: Sie können an jedem beliebigen Punkt im Konfigurationsverlauf eines Dedicated Host neben der Anzahl der Sockets und Kerne im Host auch nachsehen, wie viele Instances auf dem Host gestartet werden. Sie können für all diese Instances die ID des zugehörigen Amazon Machine Image (AMI) nachsehen. Sie können diese Informationen verwenden, um einen Bericht über die Lizenzierung Ihrer eigenen servergebundenen Software zu erstellen, die auf Socket- oder Kernbasis lizenziert ist.

Sie können die Konfigurationsverläufe auf eine der folgenden Arten anzeigen:

- Mithilfe der AWS Config Konsole. Für jede aufgenommene Ressource können Sie eine Timeline-Seite anzeigen, die einen Verlauf der Konfigurationsdetails bietet. Wählen Sie zum Anzeigen dieser Seite das graue Symbol in der Spalte Config Timeline (Konfig.-Timeline) der Seite Dedicated Hosts. Weitere Informationen finden Sie im AWS Config Entwicklerhandbuch unter Konfigurationsdetails in der AWS Config Konsole anzeigen.
- Durch das Ausführen von AWS CLI Befehlen. Zuerst können Sie den Befehl list-discovered-resources verwenden, um eine Liste aller Hosts und Instances zu erhalten. Danach verwenden Sie den Befehl get-resource-config-history, um die Konfigurationsdetails eines Hosts oder einer Instance für ein spezifisches Zeitintervall zu erhalten. Weitere Informationen finden Sie unter View Configuration Details Using the CLI (Anzeigen von Konfigurationsdetails mithilfe der Befehlszeilenschnittstelle (CLI)) im AWS Config -Developer-Handbuch.
- Indem Sie die AWS Config API in Ihren Anwendungen verwenden. Zunächst können Sie die Aktion ListDiscoveredRessourcen verwenden, um eine Liste aller Hosts und Instanzen abzurufen. Anschließend können Sie die GetResourceConfigHistoryAktion verwenden, um die Konfigurationsdetails eines Hosts oder einer Instanz für ein bestimmtes Zeitintervall abzurufen.

Um beispielsweise eine Liste all Ihrer Dedicated Hosts von abzurufen AWS Config, führen Sie einen CLI-Befehl wie den folgenden aus.

```
aws configservice list-discovered-resources --resource-type AWS::EC2::Host
```

Um den Konfigurationsverlauf eines Dedicated Hosts von abzurufen AWS Config, führen Sie einen CLI-Befehl wie den folgenden aus.

```
aws configservice get-resource-config-history --resource-type AWS::EC2::Instance --
resource-id i-1234567890abcdef0
```

Um AWS Config Einstellungen mit der Konsole zu verwalten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Seite Dedicated Hosts die Option Edit Config Recording (Konfigurationsaufnahme bearbeiten).
3. Folgen Sie in der AWS Config Konsole den angegebenen Schritten, um die Aufnahme zu aktivieren. Weitere Informationen finden Sie unter Einrichtung AWS Config über die Konsole.

Weitere Informationen finden Sie unter Konfigurationsdetails in der AWS Config Konsole anzeigen.

Zur Aktivierung AWS Config über die Befehlszeile oder API

- AWS CLI: Konfigurationsdetails (AWS CLI) im AWS Config Entwicklerhandbuch anzeigen.
- Amazon EC2 EC2-API: GetResourceConfigHistory.

Dedicated Instances

EC2-Instances werden standardmäßig auf gemeinsam genutzter Tenancy-Hardware ausgeführt. Das bedeutet, dass sich mehrere AWS Konten möglicherweise dieselbe physische Hardware teilen.

Dedicated Instances sind EC2-Instances, die auf Hardware ausgeführt werden, die einem einzelnen AWS Konto zugewiesen ist. Das bedeutet, dass Dedicated Instances auf Host-Hardwareebene physisch von Instances isoliert sind, die zu anderen gehören AWS-Konten, auch wenn diese Konten mit einem einzigen Zahlerkonto verknüpft sind. Dedicated Instances können sich jedoch Hardware mit anderen Instances derselben Instanz teilen AWS-Konto , bei denen es sich nicht um Dedicated Instances handelt.

Dedicated Instances bieten weder Transparenz noch Kontrolle über die Platzierung von Instances und unterstützen keine Host-Affinität. Wenn Sie eine Dedicated Instance beenden und starten,

läuft sie möglicherweise nicht auf demselben Host. Ebenso können Sie nicht auf einen bestimmten Host abzielen, auf dem eine Instance gestartet oder ausgeführt werden soll. Darüber hinaus bieten Dedicated Instances eingeschränkte Unterstützung für Bring Your Own License (BYOL).

Wenn Sie Transparenz und Kontrolle über die Platzierung von Instanzen und einen umfassenderen BYOL-Support benötigen, sollten Sie stattdessen einen Dedicated Host verwenden. Dedicated Instances und Dedicated Hosts können beide verwendet werden, um Amazon EC2 EC2-Instances auf dedizierten physischen Servern zu starten. Es gibt keine leistungsbezogenen, sicherheitsrelevanten oder physischen Unterschiede zwischen Dedicated Instances und Instances auf Dedicated Hosts. Es gibt jedoch einige wichtige Unterschiede zwischen ihnen. Die folgende Tabelle hebt einige der wichtigsten Unterschiede zwischen Dedicated Hosts und Dedicated Instances hervor:

	Dedicated Host	Dedicated Instance
Dedizierter physischer Server	Physischer Server mit Instanzkapazität, die vollständig für Ihre Nutzung reserviert ist.	Physischer Server, der für ein einzelnes Kundenkonto reserviert ist.
Gemeinsame Nutzung der Instanzkapazität	Kann die Instanzkapazität mit anderen Konten teilen.	Nicht unterstützt
Fakturierung	Abrechnung pro Host	Abrechnung pro Instance
Sichtbarkeit von Sockets, Kernen und Host-ID	Zeigt die Anzahl der Sockets und physischen Kerne	Keine Sichtbarkeit
Host- und Instance-Affinität	Gestattet Ihnen, Ihre Instances im Laufe der Zeit durchgängig auf demselben physischen Server bereitzustellen	Nicht unterstützt
Zielgerichtete Instance-Platzierung	Bietet zusätzliche Sichtbarkeit und Kontrolle darüber, wie Instances auf	Nicht unterstützt

	Dedicated Host	Dedicated Instance
	einem physischen Server platziert werden.	
Automatische Instance-Wiederherstellung	Unterstützt. Weitere Informationen finden Sie unter Host-Wiederherstellung.	Unterstützt
Bring Your Own License (BYOL)	Unterstützt	Teilweise Unterstützung*
Kapazitätsreservierungen	Nicht unterstützt	Unterstützt

* Microsoft SQL Server mit Lizenzmobilität über Software Assurance und Windows Virtual Desktop Access (VDA)-Lizenzen können mit Dedicated Instance verwendet werden.

Weitere Informationen über Dedicated Instances finden Sie unter Dedicated Hosts.

Themen

- Grundlagen von Dedicated Instance
- Unterstützte Features
- Dedicated Instances-Einschränkungen
- Preise für Dedicated Instances
- Arbeiten mit Dedicated Instances

Grundlagen von Dedicated Instance

Eine VPC kann eine Tenancy von `default` oder `dedicated` haben. Ihre VPCs haben standardmäßig eine `default`-Tenancy und Instances, die in einer `default`-Tenancy-VPC gestartet werden, haben eine `default`-Tenancy. Starten Sie Dedicated Instances wie folgt:

- Erstellen Sie eine VPC mit einer Tenancy `dedicated`, sodass alle Instances in der VPC als Dedicated Instances ausgeführt werden. Weitere Informationen finden Sie unter Erstellen einer VPC mit einer Dedicated-Instance-Tenancy.
- Erstellen Sie eine VPC mit der Tenancy `default` und geben Sie manuell die Tenancy `dedicated` für die Instances an, die als Dedicated Instances ausgeführt werden sollen. Weitere Informationen finden Sie unter Starten von Dedicated Instances in eine VPC.

Unterstützte Features

Dedicated Instances unterstützen die folgenden Funktionen und AWS Serviceintegrationen:

Themen

- Reserved Instances
- Auto Scaling
- Automatische Wiederherstellung
- Dedicated Spot Instances
- Burstable Performance Instances

Reserved Instances

Um Kapazität für Ihre Dedicated Instances zu reservieren, können Sie Dedicated Reserved Instances oder Capacity Reservations erwerben. Weitere Informationen finden Sie unter Reserved Instances und On-Demand Capacity Reservations.

Wenn Sie eine Dedicated Reserved Instance kaufen, erwerben Sie die Kapazität zum Starten einer Dedicated Instance in einer VPC zu deutlich reduzierten Nutzungsgebühren. Der Preisunterschied in der nutzungsabhängigen Gebühr gilt nur, wenn Sie eine Instance mit Dedicated Tenancy starten. Wenn Sie eine Reserved Instance mit Standard-Tenancy erwerben, gilt sie nur für eine aktive Instance mit `default`-Tenancy; sie gilt nicht für eine aktive Instance mit `dedicated`-Tenancy.

Darüber hinaus können Sie die Tenancy einer Reserved Instance nach dem Kauf nicht mit dem Änderungsverfahren ändern. Sie können jedoch auch eine Convertible Reserved Instance gegen eine neue Convertible Reserved Instance mit einer anderen Tenancy austauschen.

Auto Scaling

Mit Amazon EC2 Auto Scaling können Sie Dedicated Instances starten. Weitere Informationen finden Sie unter Starten von Auto Scaling-Instances in einer VPC im Amazon EC2 Auto Scaling-Benutzerhandbuch.

Automatische Wiederherstellung

Sie können die automatische Wiederherstellung für eine Dedicated Instance konfigurieren, wenn sie aufgrund eines zugrunde liegenden Hardwarefehlers oder eines Problems, das eine Reparatur AWS erfordert, beeinträchtigt wird. Weitere Informationen finden Sie unter Resilienz der Instanz.

Dedicated Spot Instances

Sie können eine Dedicated Spot-Instance ausführen, indem Sie beim Erstellen einer Spot-Instance-Anfrage die Tenancy `dedicated` angeben. Weitere Informationen finden Sie unter Angeben einer Tenancy für Ihre Spot-Instances.

Burstable Performance Instances

Sie können die Vorteile der Ausführung auf Dedicated-Tenancy-Hardware mit nutze the section called “Burstable Performance Instances”. T3 Dedicated Instances werden standardmäßig im unbegrenzten Modus gestartet und sie stellen eine CPU-Basisleistung mit der Fähigkeit bereit, die CPU-Leistung je nach Erfordernis Ihrer Workload itslast zu steigern. Die T3-Basisleistung und die Steigerbarkeit unterliegen dem CPU-Guthaben. Aufgrund der Steigerbarkeit der T3-Instance-Typen empfehlen wir, zu überwachen, wie Ihre T3-Instances die CPU-Ressourcen der dedizierten Hardware für die beste Leistung verwenden. T3 Dedicated Instances sind für Kunden mit unterschiedlichen Workloads gedacht, die ein zufälliges CPU-Verhalten aufweisen, aber idealerweise eine durchschnittliche CPU-Auslastung bei oder unterhalb der Basisnutzung haben. Weitere Informationen finden Sie unter the section called “Die wichtigsten Konzepte”.

Amazon EC2 verfügt über Systeme zur Identifizierung und Korrektur von Leistungsschwankungen. Es ist jedoch immer noch möglich, dass es zu kurzfristigen Schwankungen kommt, wenn Sie mehrere T3 Dedicated Instances starten, die korrelierte CPU-Auslastungsmuster aufweisen. Für diese anspruchsvolleren oder korrelierten Workloads empfehlen wir die Verwendung von M5 oder M5a Dedicated Instances anstelle von T3 Dedicated Instances.

Dedicated Instances-Einschränkungen

Berücksichtigen Sie bei Verwendung von Dedicated Instances Folgendes:

- Einige AWS Dienste oder ihre Funktionen werden mit einer VPC nicht unterstützt, bei der die Instance-Tenancy auf eingestellt ist. `dedicated` Lesen Sie die Dokumentation zum entsprechenden Service, um zu bestätigen, ob es Einschränkungen gibt.
- Einige Instance-Typen können nicht in einer VPC gestartet werden, deren Instance-Tenancy auf `dedicated` festgelegt ist. Weitere Informationen zu den unterstützten Instance-Typen finden Sie unter Amazon EC2 Dedicated Instances.
- Wenn Sie eine Dedicated-Instance-gestützte Amazon EBS starten, wird das EBS-Volume nicht auf einer Single-Tenant-Hardware ausgeführt.

Preise für Dedicated Instances

Die Preise für Dedicated Instances unterscheiden sich von den Preisen für On-Demand-Instances. Weitere Informationen finden Sie auf der Produktseite für Amazon EC2 – Dedicated Instances.

Arbeiten mit Dedicated Instances

Sie können eine VPC mit der Instance-Tenancy `dedicated` erstellen, um sicherzustellen, dass alle in der VPC gestarteten Instances Dedicated Instances sind. Alternativ können Sie die Tenancy der Instance beim Start angeben.

Themen

- Erstellen einer VPC mit einer Dedicated-Instance-Tenancy
- Starten von Dedicated Instances in eine VPC
- Anzeigen der Tenancy-Informationen
- Ändern der Tenancy einer Instance
- Ändern der Tenancy einer VPC

Erstellen einer VPC mit einer Dedicated-Instance-Tenancy

Beim Erstellen einer VPC haben Sie die Option, eine Instance-Tenancy anzugeben. Wenn Sie eine Instance in einer VPC starten, die eine Instance-Tenancy von `dedicated` hat, wird die Instance immer als Dedicated Instance auf Hardware ausgeführt, die für Ihre Verwendung bestimmt ist.

Weitere Informationen zum Erstellen einer VPC und zur Auswahl der Tenancy-Optionen finden Sie unter Erstellen einer VPC im Amazon-VPC-Benutzerhandbuch.

Starten von Dedicated Instances in eine VPC

Sie können eine Dedicated Instance mit dem Amazon EC2 Launch Instance Wizard starten.

Console

So starten Sie eine Dedicated Instance mithilfe der Konsole in einer VPC mit einer Standard-Tenancy

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Launch Instance (Instance starten) aus.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus der Liste aus.
4. Wählen Sie im Bereich Instance type (Instance-Typ) den zu startenden Instance-Typ aus.

   > **Note**
   >
   > Stellen Sie sicher, dass Sie einen Instance-Typ auswählen, der als Dedicated Instance unterstützt wird;. Weitere Informationen finden Sie unter Amazon EC2 Dedicated Instances.

5. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das der Instance zugeordnet werden soll.
6. Wählen Sie im Bereich Advanced details (Erweiterte Details) unter Tenancy die Option Dedicated aus.
7. Konfigurieren Sie die verbleibenden Instance-Optionen nach Bedarf. Weitere Informationen finden Sie unter Starten einer Instance mit definierten Parametern.
8. Wählen Sie Launch Instance (Instance starten) aus.

Command line

So stellen Sie die Tenancy-Option für eine Instance beim Start mithilfe der Befehlszeile ein

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Weitere Informationen zum Starten einer Instance mit der Tenancy `host` finden Sie unter Starten Sie Instances auf einem Dedicated Host.

Anzeigen der Tenancy-Informationen

Console

So zeigen Sie Tenancy-Informationen für Ihre VPC mithilfe der Konsole an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs.
3. Überprüfen Sie die Instance-Tenancy Ihrer VPC in der Spalte Tenancy.
4. Wenn die Spalte Tenancy nicht angezeigt wird, wählen Sie in der oberen rechten Ecke Einstellungen (), aktivieren Sie Tenancy und wählen Sie Confirm.

So zeigen Sie Tenancy-Informationen für Ihre Instance mithilfe der Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Überprüfen Sie Tenancy Ihrer Instance in der Spalte Tenancy.
4. Wenn die Spalte „Mietverhältnis“ nicht angezeigt wird, führen Sie einen der folgenden Schritte aus:
   - Wählen Sie in der oberen rechten Ecke Einstellungen (), aktivieren Sie Tenancy und wählen Sie Bestätigen.
   - Wählen Sie die Instance aus. Überprüfen Sie auf der Registerkarte Details unten auf der Seite unter Host and Placement group (Host- und Platzierungsgruppe) den Wert für Tenancy.

Command line

So beschreiben Sie die Tenancy Ihrer VPC mithilfe der Befehlszeile

- describe-vpcs (AWS CLI)

- Get-EC2Vpc (AWS Tools for Windows PowerShell)

So beschreiben Sie die Tenancy Ihrer Instance mithilfe der Befehlszeile

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

So beschreiben Sie den Tenancy-Wert einer Reserved Instance mithilfe der Befehlszeile

- describe-reserved-instances (AWS CLI)
- Get-EC2ReservedInstance (AWS Tools for Windows PowerShell)

So beschreiben Sie den Tenancy-Wert eines Reserved Instance-Angebots mithilfe der Befehlszeile

- describe-reserved-instances-offerings (AWS CLI)
- Get-EC2ReservedInstancesOffering (AWS Tools for Windows PowerShell)

Ändern der Tenancy einer Instance

Sie können die Tenancy einer angehaltenen Instance nach dem Start ändern. Ihre Änderungen werden wirksam, wenn die Instance das nächste Mal gestartet wird.

Welche Konvertierungen unterstützt werden, hängt von den Betriebssystemdetails Ihrer Instance sowie davon ab, ob SQL Server installiert ist. Weitere Informationen zu den für Ihre Instance verfügbaren Tenancy-Konvertierungspfaden finden Sie im License Manager-Benutzerhandbuch unter Tenancy-Konvertierung.

> **Note**
>
> Bei T3-Instances muss die Instance auf einem Dedicated Host gestartet werden, um eine Tenancy vom Typ `host` zu verwenden. Die Tenancy kann nicht von `host` in `dedicated` oder `default` geändert werden. Wenn Sie versuchen, eine dieser nicht unterstützten Tenancy-Änderungen vorzunehmen, wird der `InvalidRequest`-Fehlercode angezeigt.

Console

So ändern Sie die Tenancy einer Instance mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten), Stop (Anhalten).
4. Wählen Sie Actions (Aktionen), Instance Settings (Instance-Einstellungen) und Modify Instance Placement (Instance-Platzierung ändern).
5. Wählen Sie für Tenancy aus, ob Ihre Instance auf dedizierter Hardware oder auf einem Dedicated Host ausgeführt werden soll. Wählen Sie Save (Speichern) aus.

Command line

So ändern Sie den Tenancy-Wert einer Instance mithilfe der Befehlszeile

- modify-instance-placement (AWS CLI)
- Edit-EC2InstancePlacement (AWS Tools for Windows PowerShell)

Ändern der Tenancy einer VPC

Die Tenancy der Instance einer VPC kann nach dem Erstellen von `dedicated` in `default` geändert werden. Die Änderung der Instance-Tenancy der VPC hat keine Auswirkungen auf die Tenancy der in der VPC vorhandenen Instances. Beim nächsten Start einer Instance in der VPC wird dieser die Tenancy `default` zugewiesen, wenn beim Start kein anderer Wert angegeben wird.

> **Note**
>
> Sie können die Instance-Tenancy einer VPC nicht von `default` in `dedicated` in ändern, nachdem sie erstellt wurde.

Sie können die Instance-Tenancy einer VPC nur mithilfe der AWS CLI, eines AWS SDK oder der Amazon EC2 EC2-API ändern.

Command line

Um das Instance-Tenancy-Attribut einer VPC zu ändern, verwenden Sie den AWS CLI

Verwenden Sie den Befehl modify-vpc-tenancy und geben Sie die ID der VPC und den Instance-Tenancy-Wert an. Der einzige unterstützte Wert ist `default`.

```
aws ec2 modify-vpc-tenancy --vpc-id vpc-1a2b3c4d --instance-tenancy default
```

Kapazitätsreservierungen

Mit Kapazitätsreservierungen können Sie Rechenkapazität für Amazon-EC2-Instances in einer bestimmten Availability Zone reservieren. Es gibt zwei Arten von Kapazitätsreservierungen für unterschiedliche Anwendungsfälle.

Arten von Kapazitätsreservierungen

- On-Demand Capacity Reservations
- Kapazitätsblöcke für ML

Im Folgenden sind einige häufige Anwendungsfälle für On-Demand-Kapazitätsreservierungen aufgeführt:

- Skalierung von Ereignissen – Erstellen Sie vor Ihren geschäftskritischen Ereignissen bedarfsgesteuerte Kapazitätsreservierungen, um sicherzustellen, dass Sie bei Bedarf skalieren können.
- Regulatorische Anforderungen und Notfallwiederherstellung – Verwenden Sie On-Demand-Kapazitätsreservierungen, um regulatorische Anforderungen für Hochverfügbarkeit zu erfüllen und Kapazität in einer anderen Availability Zone oder Region für die Notfallwiederherstellung zu reservieren.

Im Folgenden sind einige häufige Anwendungsfälle für Kapazitätsblöcke für ML aufgeführt:

- Modell-Training und Feinabstimmung für Machine Learning (ML) – Erhalten Sie ununterbrochenen Zugriff auf die GPU-Instances, die Sie für das Training und die Feinabstimmung von ML-Modellen reserviert haben.

- ML-Experimente und Prototypen – Führen Sie Experimente durch und erstellen Sie Prototypen, die kurzfristig GPU-Instances erfordern.

Wann sollte die On-Demand-Kapazitätsreservierung verwendet werden?

Verwenden Sie On-Demand-Kapazitätsreservierungen, wenn Sie strenge Kapazitätsanforderungen haben und geschäftskritische Workloads ausführen, die eine Kapazitätssicherung erfordern. Mit On-Demand-Kapazitätsreservierungen können Sie sicherstellen, dass Sie immer Zugriff auf die von Ihnen reservierte Amazon-EC2-Kapazität haben, solange Sie diese benötigen.

Wann sollten Kapazitätsblöcke für ML verwendet werden?

Verwenden Sie Kapazitätsblöcke für ML, wenn Sie sicherstellen müssen, dass Sie ab einem zukünftigen Datum für einen definierten Zeitraum ununterbrochenen Zugriff auf GPU-Instances haben. Kapazitätsblöcke eignen sich ideal für das Training und die Feinabstimmung von ML-Modellen, für kurze Ausführungen von Experimenten und für die Bewältigung eines vorübergehenden Anstiegs der Inferenznachfrage in der Zukunft. Mit Kapazitätsblöcken können Sie sicherstellen, dass Sie zu einem bestimmten Datum Zugriff auf GPU-Ressourcen haben, um Ihre ML-Workloads auszuführen.

On-Demand Capacity Reservations

On-Demand-Kapazitätsreservierungen ermöglichen das Reservieren von Rechenkapazität für Ihre Amazon EC2-Instances in einer bestimmten Availability Zone für eine beliebige Dauer. Kapazitätsreservierungen mindern das Risiko, bei Kapazitätsengpässen keine On-Demand-Kapazitäten abrufen zu können. Wenn Sie strenge Kapazitätsanforderungen haben und geschäftskritische Workloads ausführen, die ein gewisses Maß an langfristiger oder kurzfristiger Kapazitätssicherung erfordern, empfehlen wir Ihnen, eine Kapazitätsreservierung zu erstellen, um sicherzustellen, dass Sie immer Zugriff auf Amazon-EC2-Kapazität haben; wenn und so lange Sie sie benötigen.

Sie können Kapazitätsreservierungen jederzeit erstellen, ohne einen Vertrag mit einjähriger oder dreijähriger Laufzeit abzuschließen. Die Kapazität ist sofort verfügbar und die Abrechnung beginnt, sobald die Kapazitätsreservierung in Ihrem Konto bereitgestellt wird. Wenn Sie sie nicht mehr benötigen, stornieren Sie die Kapazitätsreservierung, damit die Kapazität freigegeben wird und keine weiteren Gebühren anfallen. Sie können auch die von Savings Plans und Regional Reserved Instances angebotenen Abrechnungsrabatte nutzen, um die Kosten einer Kapazitätsreservierung zu senken.

Beim Erstellen einer Kapazitätsreservierung geben Sie Folgendes an:

- Availability Zone, in der die Kapazität reserviert werden soll
- Anzahl der Instances, für die Kapazität reserviert werden soll
- Die Instance-Attribute, einschließlich Instance-Typ, Plattform, Availability Zone und Tenancy

Kapazitätsreservierungen können nur von Instances mit entsprechenden Attributen verwendet werden. Standardmäßig werden sie automatisch von laufenden Instances verwendet, die den Attributen entsprechen. Wenn Sie keine laufenden Instances haben, die den Attributen der Kapazitätsreservierung entsprechen, bleibt sie unbenutzt, bis Sie eine Instance mit übereinstimmenden Attributen starten.

Inhalt

Unterschiede zwischen Kapazitätsreservierungen, Reserved Instances und Savings Plans

Die folgende Tabelle hebt einige der wichtigsten Unterschiede zwischen Kapazitätsreservierungen, Reserved Instances und Savings Plans hervor:

	Capacity Reservations	Zonengebundene Reserved Instances	Regionsgebundene Reserved Instances	Savings Plans
Laufzeit	Keine Vertragsbindung erforderlich. Kann bei Bedarf erstellt und storniert werden.	Setzen eine feste ein- oder dreijährige Laufzeit voraus.		
Kapazitätsnutzen	In einer bestimmten Availability Zone reservierte Kapazität.		Keine Kapazität reserviert.	
Fakturierungsrabatt	Kein Fakturierungsrabatt. †	Bietet einen Fakturierungsrabatt.		
Instance-Limits	Es gelten Ihre Limits On-Demand-Instance pro Region.	Der Standardwert ist 20 pro Availability Zone. Sie können eine Erhöhung des Limits anfordern.	Der Standardwert ist 20 pro Region. Sie können eine Erhöhung des Limits anfordern.	Kein Limit.

† Sie können Kapazitätsreservierungen mit Savings Plans oder Regional Reserved Instances kombinieren, um einen Rabatt zu erhalten.

Weitere Informationen finden Sie unter:

- Reserved Instances
- Savings Plans-Benutzerhandbuch

Unterstützte Plattformen

Sie müssen die Kapazitätsreservierung mit der richtigen Plattform erstellen, um sicherzustellen, dass sie optimal mit Ihren Instances abgestimmt ist. Kapazitätsreservierungen unterstützen die folgenden Plattformen:

- Linux/Unix
- Linux mit SQL Server-Standard
- Linux mit SQL Server Web
- Linux mit SQL Server Enterprise
- SUSE Linux
- Red Hat Enterprise Linux
- RHEL mit SQL Server Standard
- RHEL mit SQL Server Enterprise
- RHEL mit SQL Server Web
- RHEL mit HA
- RHEL mit HA und SQL Server Standard
- RHEL mit HA und SQL Server Enterprise
- Ubuntu Pro
- Windows
- Windows mit SQL Server
- Windows mit SQL Server Web
- Windows mit SQL Server-Standard
- Windows mit SQL Server Enterprise

Wenn Sie ein Kapazitätsreservierung kaufen, müssen Sie die Plattform angeben, die das Betriebssystem für Ihre Instance darstellt.

- Für SUSE-Linux- und RHEL-Verteilungen, mit Ausnahme von BYOL, müssen Sie die spezifische Plattform auswählen. Zum Beispiel die SUSE-Linux- oder Red-Hat-Enterprise-Linux-Plattform .
- Bei allen anderen Linux-Distributionen (einschließlich Ubuntu) wählen Sie die Linux/UNIX-Plattform.
- Wenn Sie Ihr bestehendes RHEL-Abonnement (BYOL) mitbringen, müssen Sie die Linux/UNIX-Plattform wählen.
- Bei Windows mit SQL Standard, Windows mit SQL Server Enterprise und Windows mit SQL Server Web müssen Sie die spezielle Plattform auswählen.
- Wählen Sie für alle anderen Windows-Versionen, mit Ausnahme von BYOL, die nicht unterstützt wird, die Windows-Plattform aus.

Kontingente

Die Anzahl der Instances, für die Sie Kapazität reservieren dürfen, richtet sich nach dem On-Demand-Instance-Kontingent Ihres Kontos. Sie können Kapazität für so viele Instances reservieren, wie es dieses Kontingent erlaubt, abzüglich der Anzahl der bereits ausgeführten Instances.

Kontingente gelten nur für laufende Instances. Wenn Ihre Instance aussteht, stoppt, gestoppt wird oder im Ruhezustand ist, wird sie nicht auf Ihr Kontingent angerechnet.

Einschränkungen

Bevor Sie Kapazitätsreservierungen erstellen, beachten Sie bitte die folgenden Begrenzungen und Einschränkungen.

- Aktive und ungenutzte Kapazitätsreservierungen werden auf On-Demand-Instance-Limits angerechnet.
- Kapazitätsreservierungen sind nicht von einem AWS Konto auf ein anderes übertragbar. Sie können Kapazitätsreservierungen jedoch mit anderen AWS Konten teilen. Weitere Informationen finden Sie unter Arbeiten mit freigegebenen Kapazitätsreservierungen.
- Zonengebundene Reserved Instance-Fakturierungsrabatte gelten nicht für Kapazitätsreservierungen.
- Kapazitätsreservierungen können in Cluster-Placement-Gruppen erstellt werden. Spread- und Partition-Placement-Gruppen werden nicht für unterstützt.
- Kapazitätsreservierungen kann nicht mit Dedicated Hosts verwendet werden. Kapazitätsreservierungen können nicht mit Dedicated Instances verwendet werden.
- [Windows-Instanzen] Kapazitätsreservierungen können nicht mit Bring Your Own License (BYOL) verwendet werden.
- Kapazitätsreservierungen stellen nicht sicher, dass eine Instance im Ruhezustand fortgesetzt werden kann, nachdem Sie versucht haben, sie zu starten.

Preise und Fakturierung für Kapazitätsreservierung

Themen

- Preisgestaltung
- Fakturierung
- Fakturierungsrabatte

- Anzeigen Ihrer Rechnung

Preisgestaltung

Für Kapazitätsreservierungen wird Ihnen der entsprechende On-Demand-Tarif in Rechnung gestellt, unabhängig davon, ob Sie Instances mit der reservierten Kapazität ausführen oder nicht. Wenn Sie die Reservierung nicht nutzen, erscheint diese als ungenutzte Reservierung auf Ihrer Amazon-EC2-Rechnung. Wenn Sie eine Instance ausführen, die den Attributen einer Reservierung entspricht, bezahlen Sie nur für die Instance und nichts für die Reservierung. Es gibt keine Vorab- oder Zusatzgebühren.

Wenn Sie beispielsweise eine Kapazitätsreservierung für zwanzig `m4.large`-Linux-Instances erstellen und fünfzehn `m4.large`-Linux-Instances in derselben Availability Zone ausführen, werden Ihnen fünfzehn aktive Instances und fünf ungenutzte Instances in der Reservierung berechnet.

Fakturierungsrabatte für Savings Plans und regionale Reserved Instances gelten für Kapazitätsreservierungen. Weitere Informationen finden Sie unter Fakturierungsrabatte.

Weitere Informationen finden Sie unter Amazon EC2 – Preise.

Fakturierung

Die Abrechnung beginnt, sobald die Kapazitätsreservierung in Ihrem Konto bereitgestellt wurde, und wird fortgesetzt, solange die Kapazitätsreservierung in Ihrem Konto bereitgestellt bleibt.

Kapazitätsreservierungen werden mit sekundengenauer Granularität berechnet. Das bedeutet, dass Ihnen angefangene Stunden in Rechnung gestellt werden. Wenn eine Kapazitätsreservierung beispielsweise `24` Stunden und `15` Minuten lang in Ihrem Konto bereitgestellt bleibt, werden Ihnen `24.25` Reservierungsstunden in Rechnung gestellt.

Das folgende Beispiel zeigt, wie eine Kapazitätsreservierung abgerechnet wird. Die Kapazitätsreservierung wurde für eine `m4.large`-Linux-Instance mit einem On-Demand-Tarif von 0,10 USD pro Nutzungsstunde erstellt. In diesem Beispiel wird die Kapazitätsreservierung im Konto für fünf Stunden lang bereitgestellt. Die Kapazitätsreservierung wird in der ersten Stunde nicht genutzt, sodass in diesem Fall eine ungenutzte Stunde mit dem standardmäßigen On-Demand-Tarif des Instance-Typs `m4.large` abgerechnet wird. In der zweiten bis fünften Stunde wird die Kapazitätsreservierung von einer `m4.large`-Instance belegt. In dieser Zeit fallen für die Kapazitätsreservierung keine Gebühren an, stattdessen wird dem Konto die `m4.large`-Instance in Rechnung gestellt, die diese Kapazitätsreservierung belegt. In der sechsten Stunde wird die

Kapazitätsreservierung storniert und die `m4.large`-Instance arbeitet normalerweise außerhalb der reservierten Kapazität. Für diese Stunde wird der On-Demand-Tarif des Instance-Typs `m4.large` berechnet.

Hour	1	2	3	4	5	6	Total cost
Unused Capacity Reservation	$0.10	$0.00	$0.00	$0.00	$0.00	$0.00	**$0.10**
On-demand Instance Usage	$0.00	$0.10	$0.10	$0.10	$0.10	$0.10	**$0.50**
Hourly cost	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.10**	**$0.60**

Fakturierungsrabatte

Abrechnungsrabatte für Savings Plans und Regional Reserved Instances gelten für Kapazitätsreservierungen. AWS wendet diese Rabatte automatisch auf Kapazitätsreservierungen mit übereinstimmenden Attributen an. Wenn eine Kapazitätsreservierung von einer Instance verwendet wird, wird der Rabatt auf die Instance angewendet. Rabatte werden vorzugsweise auf die Instance-Nutzung angewendet, bevor ungenutzte Kapazitätsreservierungen abgedeckt werden.

Fakturierungsrabatte für zonengebundene Reserved Instances gelten nicht für Kapazitätsreservierungen.

Weitere Informationen finden Sie unter:

- Reserved Instances
- Savings Plans-Benutzerhandbuch
- Fakturierungs- und Kaufoptionen

Anzeigen Ihrer Rechnung

Sie können die Gebühren und Gebühren für Ihr Konto auf der AWS Billing and Cost Management Konsole überprüfen.

- Das Dashboard zeigt eine Ausgabenzusammenfassung für Ihr Konto an.
- Erweitern Sie auf der Seite Bills (Rechnungen) unter Details den Bereich Elastic Compute Cloud und die Region, um Fakturierungsdaten zu Ihren Kapazitätsreservierungen abzurufen.

Sie können die Gebühren online anzeigen oder eine CSV-Datei herunterladen. Weitere Informationen finden Sie unter Kapazitätsreservierung-Zeilenposten im AWS Billing and Cost Management - Benutzerhandbuch.

Arbeiten mit Kapazitätsreservierungen

Um mit der Verwendung von Kapazitätsreservierungen zu beginnen, müssen Sie die Kapazitätsreservierung in der gewünschten Availability Zone erstellen. Nun können Sie Instances in der reservierten Kapazität starten, die Kapazitätsauslastung in Echtzeit anzeigen und die Kapazität nach Bedarf erhöhen oder verringern.

Standardmäßig ordnen Kapazitätsreservierungen automatisch neuen Instances und laufenden Instances mit passenden Attributen (Instance-Typ, Plattform, Availability Zone und Tenancy) zu. Dies bedeutet, dass eine Instance mit übereinstimmenden Attributen automatisch in der Kapazitätsreservierung ausgeführt wird. Sie können jedoch auch eine Kapazitätsreservierung für bestimmte Workloads festlegen. Auf diese Weise können Sie explizit steuern, welche Instances in der reservierten Kapazität ausgeführt werden dürfen.

Sie können angeben, wie die Reservierung endet. Sie können wählen, ob Sie Kapazitätsreservierung manuell abbrechen oder es zu einer bestimmten Uhrzeit automatisch beendet werden soll. Wenn Sie eine Endzeit angeben, wird die Kapazitätsreservierung innerhalb einer Stunde von der angegebenen Uhrzeit abgebrochen. Wenn Sie beispielsweise den 31.05.2019, 13:30:55 Uhr angeben, endet die Kapazitätsreservierung garantiert am 31.05.2019 zwischen 13:30:55 und 14:30:55 Uhr. Nach dem Ende einer Reservierung können Sie Instances nicht mehr zielgerichtet in der Kapazitätsreservierung aufnehmen. In der reservierten Kapazität ausgeführte Instances werden weiterhin ununterbrochen ausgeführt. Wenn Instances, die auf eine Kapazitätsreservierung ausgerichtet sind, beendet werden, können Sie sie erst dann neu starten, wenn Sie ihre Ziel-Präferenz für die Kapazitätsreservierung entfernt oder sie für eine andere Kapazitätsreservierung konfiguriert haben.

Inhalt

Erstellen eines Kapazitätsreservierung

Wenn Ihre Anfrage zum Erstellen einer Kapazitätsreservierung erfolgreich ist, ist die Kapazität sofort verfügbar. Die Kapazität bleibt für Ihren Gebrauch reserviert, solange die Kapazitätsreservierung aktiv

ist. Sie können jederzeit Instances darin starten. Wenn die Kapazitätsreservierung offen ist, werden neue Instances und vorhandene Instances mit übereinstimmenden Attributen automatisch in der Kapazität der Kapazitätsreservierung ausgeführt. Wenn die Kapazitätsreservierung `targeted` ist, müssen die Instances speziell für die Ausführung in der reservierten Kapazität ausgerichtet sein.

Ihre Anforderung, eine Kapazitätsreservierung zu erstellen, kann bei Eintreten einer der folgenden Bedingungen fehlschlagen:

- Die Kapazität von Amazon EC2 reicht nicht aus, um der Anforderung nachzukommen. Versuchen Sie es entweder zu einem späteren Zeitpunkt noch einmal, versuchen Sie es mit einer anderen Availability Zone oder versuchen Sie es mit einer kleineren Anfrage. Wenn Ihre Anwendung in Hinsicht auf Instance-Typen und -Größen flexibel ist, versuchen Sie es mit verschiedenen Instance-Attributen.
- Die angeforderte Menge überschreitet Ihr On-Demand-Instance-Limit für die ausgewählte Instance-Familie. Erhöhen Sie Ihr On-Demand-Instance-Limit für die Instance-Familie und versuchen Sie es erneut. Weitere Informationen finden Sie unter Kontingente für On-Demand-Instances.

So erstellen Sie eine Kapazitätsreservierung mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen (Kapazitätsreservierungen) und dann Create Kapazitätsreservierung (Kapazitätsreservierung erstellen) aus.
3. Konfigurieren Sie auf der Seite zum Erstellen einer Kapazitätsreservierung die folgenden Einstellungen im Abschnitt Instance details (Instance-Details): Der Instance-Typ, die Plattform, die Availability Zone und die Tenancy der Instances, die Sie starten, müssen mit dem Instance-Typ, der Plattform, der Availability Zone und der Tenancy übereinstimmen, die Sie hier angeben. Andernfalls wird die Kapazitätsreservierung nicht angewendet. Wenn beispielsweise eine offene Kapazitätsreservierung nicht übereinstimmt, schlägt ein Instance-Start, der explizit auf die betreffende Kapazitätsreservierung gerichtet ist, fehl.

    a. Instance Type (Instance-Typ) – Der Instance-Typ, mit dem in der reservierten Kapazität gestartet werden soll.

    b. Launch EBS-optimized instances (EBS-optimierte Instances starten) – Geben Sie an, ob die Kapazität für EBS-optimierte Instances reserviert werden soll. Diese Option ist standardmäßig für einige Instance-Typen ausgewählt. Weitere Informationen finden Sie unter the section called “EBS-Optimierung”.

c. Platform (Plattform) – Das Betriebssystem für Ihre Instances. Weitere Informationen finden Sie unter Unterstützte Plattformen.

d. Availability Zone – Die Availability Zone, in der die Kapazität reserviert werden soll.

e. Tenancy – Geben Sie an, ob eine gemeinsam genutzte Hardware-Instance (Standard) oder eine Dedicated Instance ausgeführt werden soll.Allgemeine Verwendungszwecke:

f. (Optional) ARN der Platzierungsgruppe – Der ARN der Cluster-Placement-Gruppe, in der die Kapazitätsreservierung erstellt werden soll.

   Weitere Informationen finden Sie unter Kapazitätsreservierungen in Cluster-Placement-Gruppen.

g. Quantity (Menge): Anzahl der Instances, für die Kapazität reserviert werden soll. Wenn Sie eine Menge angeben, die größer als Ihr restliches On-Demand-Instance-Limit für den ausgewählten Instance-Typ ist, wird die Anforderung abgelehnt.

4. Konfigurieren Sie die folgenden Einstellungen im Abschnitt Reservation details (Reservierungsdetails):

   a. Reservation Ends (Reservierung endet) – Wählen Sie eine der folgenden Optionen aus:

      - Manually (Manuell) – Reservieren Sie die Kapazität, bis Sie sie explizit stornieren.
      - Specific time (Bestimmter Zeitpunkt): hebt die Kapazitätsreservierung automatisch zum angegebenen Datum und zur festgelegten Uhrzeit auf.

   b. Instance eligibility (Instance-Berechtigung) – Wählen Sie eine der folgenden Optionen aus:

      - open — (Standard) Die Kapazitätsreservierung entspricht jeder Instance mit passenden Attributen (Instance-Typ, Plattform, Availability Zone und Tenancy). Wenn Sie eine Instance mit passenden Attributen starten, wird sie automatisch in der reservierten Kapazität platziert.
      - targeted — Die Kapazitätsreservierung akzeptiert nur Instances mit übereinstimmenden Attributen (Instance-Typ, Plattform, Availability Zone und Tenancy) und die explizit auf die Reservierung abzielen.

5. Wählen Sie Request reservation (Reservierung anfordern) aus.

Um eine Kapazitätsreservierung mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-capacity-reservation. Weitere Informationen finden Sie unter Unterstützte Plattformen.

Der folgende Befehl erstellt eine Kapazitätsreservierung, die Kapazität für drei `m5.2xlarge` Instances reserviert, auf denen Red Hat Enterprise Linux-AMIs in der `us-east-1a` Availability Zone ausgeführt werden.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-platform Red
 Hat Enterprise Linux --availability-zone us-east-1a --instance-count 3
```

Der folgende Befehl erstellt eine Kapazitätsreservierung, die Kapazität für drei `m5.2xlarge` Instances reserviert, auf denen Windows mit SQL Server-AMIs in der `us-east-1a` Availability Zone ausgeführt wird.

```
aws ec2 create-capacity-reservation --instance-type m5.2xlarge --instance-
platform Windows with SQL Server --availability-zone us-east-1a --instance-count 3
```

Starten von Instances in einer bestehenden Kapazitätsreservierung

Wenn Sie eine Instance starten, können Sie angeben, ob die Instance in einer `open` Kapazitätsreservierung, in einer bestimmten Kapazitätsreservierung oder in einer Gruppe von Kapazitätsreservierungen gestartet werden soll. Sie können eine Instance nur in einer Kapazitätsreservierung starten, die über übereinstimmende Attribute (Instance-Typ, Plattform, Availability Zone und Tenancy) und ausreichend Kapazität verfügt. Alternativ können Sie die Instance so konfigurieren, dass sie nicht in einem Kapazitätsreservierung ausgeführt wird, selbst wenn Sie über eine `open`Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügen.

Das Starten einer Instance in einer Kapazitätsreservierung reduziert ihre verfügbare Kapazität um die Anzahl der gestarteten Instances. Wenn Sie beispielsweise drei Instances starten, wird die verfügbare Kapazität der Kapazitätsreservierung um drei reduziert.

So starten Sie eine Instance in einer bestehenden Kapazitätsreservierung mithilfe einer Konsole

1. Gehen Sie wie folgt vor, um eine Instance zu starten, starten Sie die Instance jedoch erst, wenn Sie die folgenden Schritte abgeschlossen haben, um die Einstellungen für die Platzierungsgruppe und die Kapazitätsreservierung anzugeben.
2. Erweitern Sie Erweiterte Details und gehen Sie wie folgt vor:

    a. Wählen Sie unter Platzierungsgruppe die Cluster-Placement-Gruppe aus, in der die Instance gestartet werden soll.

b. Wählen Sie für Capacity Reservation (Kapazitätsreservierung) je nach Konfiguration der Kapazitätsreservierung eine der folgenden Optionen aus:

   - Keine — Verhindert, dass die Instances im Rahmen einer Kapazitätsreservierung gestartet werden. Die Instances werden in On-Demand-Kapazität ausgeführt.
   - Öffnen — Startet die Instances in einer beliebigen Kapazitätsreservierung, die über übereinstimmende Attribute und ausreichend Kapazität für die Anzahl der von Ihnen ausgewählten Instances verfügt. Wenn keine passende Kapazitätsreservierung mit ausreichender Kapazität vorhanden ist, verwendet die Instance On-Demand-Kapazität.
   - Targeting by ID — Startet die Instances in der ausgewählten Kapazitätsreservierung. Wenn die ausgewählte Kapazitätsreservierung nicht über genügend Kapazität für die Anzahl der von Ihnen ausgewählten Instances verfügt, schlägt das Starten der Instances fehl.
   - Zielgruppenweise — Startet die Instances in eine beliebige Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität in der ausgewählten Kapazitätsreservierungsgruppe. Wenn die ausgewählte Gruppe nicht über eine Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügt, werden die Instances in der On-Demand-Kapazität gestartet.

3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Um eine Instance für eine bestehende Kapazitätsreservierung zu starten, verwenden Sie den AWS CLI

Geben Sie mit dem Befehl run-instances den Parameter `--capacity-reservation-specification` an.

Das folgende Beispiel startet eine `t2.micro`-Instance in jeder offenen Kapazitätsreservierung, die übereinstimmende Attribute und verfügbare Kapazität aufweist:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationPreference=open
```

Das folgende Beispiel startet eine `t2.micro`-Instance in einer Kapazitätsreservierung vom Typ `targeted`:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 --instance-type t2.micro
 --key-name MyKeyPair --subnet-id subnet-1234567890abcdef1 --capacity-reservation-
specification CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

Im folgenden Beispiel wird eine `t2.micro`-Instance in einer Kapazitätsreservierung-Gruppe gestartet:

```
aws ec2 run-instances --image-id ami-abc12345 --count 1
 --instance-type t2.micro --key-name MyKeyPair --subnet-
id subnet-1234567890abcdef1 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Ändern eines Kapazitätsreservierung

Sie können die Attribute einer aktiven Kapazitätsreservierung ändern, nachdem Sie sie erstellt haben. Sie können eine Kapazitätsreservierung nicht mehr ändern, nachdem sie abgelaufen ist oder nachdem Sie sie explizit storniert haben.

Bei der Änderung einer Kapazitätsreservierung können Sie nur die Menge erhöhen oder verringern und die Art ändern, in der sie freigegeben wurde. Sie können den Instance-Typ, die EBS-Optimierung, die Plattform, die Availability Zone und die Instance-Berechtigung einer Kapazitätsreservierung nicht ändern. Wenn Sie eines dieser Attribute ändern müssen, empfehlen wir Ihnen, die Reservierung zu stornieren und dann eine neue mit den erforderlichen Attributen zu erstellen.

Wenn Sie eine neue Menge angeben, die Ihr verbleibendes On-Demand-Instance-Limit für den ausgewählten Instance-Typ überschreitet, schlägt die Aktualisierung fehl.

So ändern Sie eine Kapazitätsreservierung mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen, die zu ändernde Kapazitätsreservierung und Edit (bearbeiten) aus.
3. Ändern Sie bei Bedarf die Optionen Quantity (Menge) oder Reservation ends (Reservierung endet) und wählen Sie im Anschluss Save changes (Änderungen speichern) aus.

Um eine Kapazitätsreservierung zu ändern, verwenden Sie AWS CLI

Verwenden Sie den Befehl modify-capacity-reservation:

Mit dem folgenden Befehl wird beispielsweise eine Kapazitätsreservierung geändert, um Kapazität für acht Instances zu reservieren.

```
aws ec2 modify-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0 --
instance-count 8
```

Ändern der Kapazitätsreservierung-Einstellungen einer Instance

Sie können die folgenden Kapazitätsreservierung-Einstellungen für eine angehaltene Instance jederzeit ändern:

- Beginnen Sie mit einer beliebigen Kapazitätsreservierung mit übereinstimmenden Attributen (Instanztyp, Plattform, Availability Zone und Tenancy) und verfügbarer Kapazität.
- Start der Instance in einer bestimmten Kapazitätsreservierung vornehmen.
- Beginnen Sie mit einer beliebigen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität in einer Kapazitätsreservierung-Gruppe.
- Start der Instance in einer Kapazitätsreservierung verhindern.

So ändern Sie die Kapazitätsreservierung-Einstellungen einer Instance mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Instances und wählen Sie die zu ändernde Instance aus. Halten Sie die Instance an, falls Sie das noch nicht getan haben.
3. Wählen Sie „Aktionen“, „Instanzeinstellungen“, „Einstellungen für die Kapazitätsreservierung ändern“.
4. Wählen Sie unter Kapazitätsreservierung eine der folgenden Optionen aus:

    - Open (Offen) – Startet die Instances in einer jeder Kapazitätsreservierung mit passenden Attributen und ausreichender Kapazität für die von Ihnen ausgewählte Anzahl von Instances. Wenn keine passende Kapazitätsreservierung mit ausreichender Kapazität vorhanden ist, verwendet die Instance On-Demand-Kapazität.
    - None (Keine) – Verhindert, dass Instances in einer Kapazitätsreservierung gestartet werden. Die Instances werden in On-Demand-Kapazität ausgeführt.
    - Specify Capacity Reservation (Kapazitätsreservierung angeben) — startet die Instances in der ausgewählten Kapazitätsreservierung. Wenn die ausgewählte Kapazitätsreservierung nicht

über genügend Kapazität für die Anzahl der von Ihnen ausgewählten Instances verfügt, schlägt das Starten der Instances fehl.

- Specify Capacity Reservation group (Kapazitätsreservierungsgruppe angeben) — startet die Instances in einer beliebigen Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität in der ausgewählten Kapazitätsreservierung-Gruppe. Wenn die ausgewählte Gruppe nicht über eine Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügt, werden die Instances in der On-Demand-Kapazität gestartet.

Um die Einstellungen für die Kapazitätsreservierung einer Instance zu ändern, verwenden Sie den AWS CLI

Verwenden Sie den Befehl modify-instance-capacity-reservation-attributes.

Mit dem folgenden Befehl wird beispielsweise die Kapazitätsreservierung-Einstellung einer Instance in open oder none geändert.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationPreference=none|open
```

Mit dem folgenden Befehl wird beispielsweise eine Instance so geändert, dass sie eine bestimmte Kapazitätsreservierung anvisiert.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-1234567890abcdef0}
```

Mit dem folgenden Befehl wird beispielsweise eine Instance so geändert, dass sie eine bestimmte Kapazitätsreservierung-Gruppe anvisiert.

```
aws ec2 modify-instance-capacity-reservation-attributes --instance-
id i-1234567890abcdef0 --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationResourceGroupArn=arn:aws:resource-
groups:us-west-1:123456789012:group/my-cr-group}
```

Anzeigen eines Kapazitätsreservierung

Kapazitätsreservierungen können die folgenden Status aufweisen:

- `active` – Die Kapazität ist zur Verwendung verfügbar.
- `expired` – Die Kapazitätsreservierung ist automatisch zu dem in Ihrer Reservierungsanforderung angegebenen Datum und der festgelegten Uhrzeit abgelaufen. Die reservierte Kapazität ist nicht mehr für Ihre Nutzung verfügbar.
- `cancelled`—Das Kapazitätsreservierung wurde abgebrochen. Die reservierte Kapazität ist nicht mehr für Ihre Nutzung verfügbar.
- `pending` – Die Kapazitätsreservierung-Anforderung war erfolgreich, aber die Kapazitätsbereitstellung steht noch aus.
- `failed` – Die Kapazitätsreservierung-Anforderung ist fehlgeschlagen. Eine Anforderung kann aufgrund ungültiger Anforderungsparameter, aufgrund von Kapazitätsbeschränkungen oder aufgrund von Instance-Limits fehlschlagen. Anforderungen können bis zu 60 Minuten nach ihrem Fehlschlagen angezeigt werden.

> **Note**
>
> Aufgrund des Eventuellen Konsistenzmodells, dem die Amazon EC2 APIs folgen, kann es nach der Erstellung einer Kapazitätsreservierung bis zu 5 Minuten dauern, bis die Konsole und die describe-capacity-reservations-Antwort anzeigen, dass die Kapazitätsreservierung den Status `active` hat. Während dieser Zeit können die Konsole und die `describe-capacity-reservations`-Antwort darauf hindeuten, dass die Kapazitätsreservierung den Status `pending` hat. Die Kapazitätsreservierung ist jedoch möglicherweise bereits verfügbar und Sie können versuchen, Instances darin zu starten.

So können Sie Ihre Kapazitätsreservierungen über die Konsole anzeigen lassen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie erst Kapazitätsreservierungen und dann eine Kapazitätsreservierung aus, um sie anzuzeigen.
3. Wählen Sie View launched instances for this reservation (Gestartete Instances für diese Reservierung anzeigen)aus.

Um Ihre Kapazitätsreservierungen einzusehen, verwenden Sie AWS CLI

Verwenden Sie den Befehl describe-capacity-reservations:

Mit dem folgenden Befehl werden beispielsweise alle Kapazitätsreservierungen beschrieben.

```
aws ec2 describe-capacity-reservations
```

Beispielausgabe.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-1234abcd56EXAMPLE ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-16T09:03:18.000Z",
            "AvailableInstanceCount": 1,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 1,
            "State": "active",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "a1.medium",
            "PlacementGroupArn": "arn:aws:ec2:us-east-1:123456789012:placement-group/
MyPG"
        },
        {
            "CapacityReservationId": "cr-abcdEXAMPLE9876ef ",
            "EndDateType": "unlimited",
            "AvailabilityZone": "eu-west-1a",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "EphemeralStorage": false,
            "CreateDate": "2019-08-07T11:34:19.000Z",
            "AvailableInstanceCount": 3,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 3,
            "State": "cancelled",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "m5.large"
        }
    ]
```

```
}
```

Abbrechen eines Kapazitätsreservierung

Sie können eine Kapazitätsreservierung jederzeit stornieren, wenn Sie die reservierte Kapazität nicht mehr benötigen. Wenn Sie eine Kapazitätsreservierung stornieren, wird die Kapazität sofort freigegeben und ist nicht mehr zu Ihrer Verwendung reserviert.

Sie können leere Kapazitätsreservierungen und Kapazitätsreservierungen mit laufenden Instances stornieren. Wenn Sie eine Kapazitätsreservierung mit ausgeführten Instances stornieren, werden die Instances normalerweise außerhalb der Kapazitätsreservierung zu On-Demand-Instance-Standardtarifen oder zu einem ermäßigten Tarif ausgeführt, falls ein entsprechender Savings Plan bzw. eine entsprechende regionale Reserved Instance vorliegt.

Nachdem Sie eine Kapazitätsreservierung storniert haben, können Instances, die auf sie ausgerichtet sind, nicht mehr starten. Ändern Sie diese Instances, sodass sie entweder auf eine andere Kapazitätsreservierung ausgerichtet sind, starten Sie sie in einer „geöffneten“ Kapazitätsreservierung mit passenden Attributen und ausreichender Kapazität oder vermeiden Sie den Start in einer Kapazitätsreservierung. Weitere Informationen finden Sie unter Ändern der Kapazitätsreservierung-Einstellungen einer Instance.

So stornieren Sie eine Kapazitätsreservierung mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie erst Kapazitätsreservierungen und dann die zu stornierende Kapazitätsreservierung aus.
3. Wählen Sie Cancel reservation (Reservierung stornieren) und Cancel reservation (Reservierung stornieren) aus.

Um eine Kapazitätsreservierung zu stornieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl cancel-capacity-reservation:

Mit dem folgenden Befehl wird beispielsweise eine Kapazitätsreservierung mit einer ID `cr-1234567890abcdef0` abgebrochen.

```
aws ec2 cancel-capacity-reservation --capacity-reservation-id cr-1234567890abcdef0
```

Arbeiten mit Kapazitätsreservierung-Gruppen

Sie können sie verwenden AWS Resource Groups , um logische Sammlungen von Kapazitätsreservierungen zu erstellen, die als Ressourcengruppen bezeichnet werden. Eine Ressourcengruppe ist eine logische Gruppierung von AWS Ressourcen, die sich alle in derselben AWS Region befinden. Weitere Informationen zu Ressourcengruppen finden Sie unter Was sind Ressourcengruppen? im AWS Resource Groups -Benutzerhandbuch.

Sie können Kapazitätsreservierungen, die Sie besitzen, in Ihr Konto aufnehmen, und Kapazitätsreservierungen, die von anderen AWS Konten mit Ihnen geteilt wurden, in eine einzige Ressourcengruppe aufnehmen. Sie können auch Kapazitätsreservierungen mit unterschiedlichen Attributen (Instanztyp, Plattform, Availability Zone und Tenancy) in eine einzige Ressourcengruppe aufnehmen.

Wenn Sie Ressourcengruppen für Kapazitätsreservierungen erstellen, können Sie Instances auf eine Gruppe von Kapazitätsreservierungen statt auf eine einzelne Kapazitätsreservierung ausrichten. Instances, die auf eine Gruppe von Kapazitätsreservierungen abzielen, stimmen mit jeder Kapazitätsreservierung in der Gruppe überein, deren Attribute (Instance-Typ, Plattform, Availability Zone und Tenancy) und die verfügbare Kapazität übereinstimmen. Wenn die Gruppe nicht über eine Kapazitätsreservierung mit übereinstimmenden Attributen und verfügbarer Kapazität verfügt, werden die Instances mit On-Demand-Kapazität ausgeführt. Wenn der Zielgruppe zu einem späteren Zeitpunkt eine übereinstimmende Kapazitätsreservierung hinzugefügt wird, wird die Instance automatisch mit ihrer reservierten Kapazität abgeglichen und in diese verschoben.

Um eine unbeabsichtigte Verwendung von Kapazitätsreservierungen in einer Gruppe zu verhindern, konfigurieren Sie die Kapazitätsreservierungen in der Gruppe so, dass nur Instances akzeptiert werden, die explizit die Kapazitätsreservierung anvisieren. Legen Sie dazu beim Erstellen der Kapazitätsreservierung mithilfe der Amazon EC2-Konsole die Instance-Berechtigung auf targeted (anvisiert) (alte Konsole) oder Only instances that specify this reservation (Nur Instances, bei denen diese Reservierung angegeben ist) (neue Konsole) fest. Geben Sie bei der Verwendung von an AWS CLI, `--instance-match-criteria targeted` wann Sie die Kapazitätsreservierung erstellen. Dadurch wird sichergestellt, dass nur Instances, die explizit die Gruppe oder eine Kapazitätsreservierung in der Gruppe anvisieren, in der Gruppe ausgeführt werden können.

Wenn eine Kapazitätsreservierung in einer Gruppe abgebrochen wird oder abläuft, während auf ihr Instances ausgeführt werden, werden die Instances automatisch in eine andere Kapazitätsreservierung in der Gruppe verschoben, die über übereinstimmende Attribute und verfügbare Kapazität verfügt. Wenn es in der Gruppe keine verbleibenden Kapazitätsreservierungen mit übereinstimmenden Attributen und verfügbarer Kapazität vorhanden sind, werden die Instances

in On-Demand-Kapazität ausgeführt. Wenn der anvisierten Gruppe zu einem späteren Zeitpunkt eine passende Kapazitätsreservierung hinzugefügt wird, wird die Instance automatisch in ihre reservierte Kapazität verschoben.

Themen

Erstellen einer Kapazitätsreservierungsgruppe

So erstellen Sie eine Kapazitätsreservierungsgruppe

Verwenden Sie den Befehl create-group AWS CLI . Geben Sie unter `name` einen beschreibenden Namen für die Gruppe an, und geben Sie unter`configuration` die beiden folgenden `Type`-Anforderungsparameter an:

- `AWS::EC2::CapacityReservationPool`,um sicherzustellen, dass die Ressourcengruppe für Instance-Starts anvisiert werden kann
- `AWS::ResourceGroups::Generic`, wobei `allowed-resource-types` auf `AWS::EC2::CapacityReservation` gesetzt ist, um sicherzustellen, dass die Ressourcengruppe nur Kapazitätsreservierungen akzeptiert.

Mit dem folgenden Befehl wird beispielsweise eine Gruppe namens `MyCRGroup` erstellt.

```
aws resource-groups create-group --name MyCRGroup --configuration
 '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Das folgende Beispiel zeigt eine Ausgabe.

```
{
```

```
    "GroupConfiguration": {
        "Status": "UPDATE_COMPLETE",
        "Configuration": [
            {
                "Type": "AWS::EC2::CapacityReservationPool"
            },
            {
                "Type": "AWS::ResourceGroups::Generic",
                "Parameters": [
                    {
                        "Values": [
                            "AWS::EC2::CapacityReservation"
                        ],
                        "Name": "allowed-resource-types"
                    }
                ]
            }
        ]
    },
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Hinzufügen einer Kapazitätsreservierung zu einer Gruppe

Wenn Sie eine für Sie freigegebene Kapazitätsreservierung zu einer Gruppe hinzufügen und diese Kapazitätsreservierung nicht freigegeben ist, wird sie automatisch aus der Gruppe entfernt.

So fügen Sie eine Kapazitätsreservierung zu einer Gruppe hinzu

Verwenden Sie den AWS CLI -Befehl group-resources. Geben Sie unter `group` den Namen der Gruppe an, der die Kapazitätsreservierungen hinzugefügt werden soll und geben Sie unter `resources` die ARNs der Kapazitätsreservierungen an, die hinzugefügt werden sollen. Wenn Sie mehrere Kapazitätsreservierungen hinzufügen möchten, trennen Sie die ARNs durch ein Leerzeichen. Um die ARNs der hinzuzufügenden Kapazitätsreservierungen abzurufen, verwenden Sie den AWS CLI Befehl describe-capacity-reservations und geben Sie die IDs der Kapazitätsreservierungen an.

Mit dem folgenden Befehl werden beispielsweise zwei Kapazitätsreservierungen zu einer Gruppe namens `MyCRGroup` hinzugefügt.

```
aws resource-groups group-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Das folgende Beispiel zeigt eine Ausgabe.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Anzeigen von Kapazitätsreservierungen in einer Gruppe

So zeigen Sie die Kapazitätsreservierungen in einer bestimmten Gruppe an

Verwenden Sie den Befehl list-group-resources. AWS CLI Geben Sie unter `group` den Namen der Gruppe an.

Mit dem folgenden Befehl werden beispielsweise die Kapazitätsreservierungen in einer Gruppe namens `MyCRGroup` aufgeführt.

```
aws resource-groups list-group-resources --group MyCRGroup
```

Das folgende Beispiel zeigt eine Ausgabe.

```
{
    "QueryErrors": [],
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
```

```
    ]
}
```

> **Note**
>
> Die Befehlsausgabe enthält Kapazitätsreservierungen, die Sie besitzen, und Kapazitätsreservierungen, die für Sie freigegeben sind.

Anzeigen der Gruppen, zu denen eine Kapazitätsreservierung gehört

AWS CLI

So zeigen Sie die Gruppen an, denen eine bestimmte Kapazitätsreservierung hinzugefügt wurde

Verwenden Sie den AWS CLI -Befehl get-groups-for-capacity-reservation.

Mit dem folgenden Befehl werden beispielsweise die Gruppen aufgeführt, denen Kapazitätsreservierung `cr-1234567890abcdef1` hinzugefügt wurde.

```
aws ec2 get-groups-for-capacity-reservation --capacity-reservation-
id cr-1234567890abcdef1
```

Das folgende Beispiel zeigt eine Ausgabe.

```
{
    "CapacityReservationGroups": [
        {
            "OwnerId": "123456789012",
            "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/
MyCRGroup"
        }
    ]
}
```

> **Note**
>
> Wenn Sie eine Kapazitätsreservierung angeben, die für Sie freigegeben ist, gibt der Befehl nur Gruppen von Kapazitätsreservierungen zurück, die Sie besitzen.

Amazon EC2 console

So zeigen Sie die Gruppen an, denen eine bestimmte Kapazitätsreservierung hinzugefügt wurde

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Kapazitätsreservierungen, wählen Sie die anzuzeigende Kapazitätsreservierung aus und klicken Sie anschließend auf Anzeigen.

   Die Gruppen, zu denen die Kapazitätsreservierung hinzugefügt wurde, werden auf der Karte Gruppen aufgeführt.

> **Note**
>
> Wenn Sie eine Kapazitätsreservierung auswählen, die für Sie freigegeben ist, zeigt die Konsole nur Gruppen von Kapazitätsreservierungen an, die Sie besitzen.

Entfernen einer Kapazitätsreservierung aus einer Gruppe

So entfernen Sie eine Kapazitätsreservierung aus einer Gruppe

Verwenden Sie den Befehl ungroup-resources. AWS CLI Geben Sie unter `group` den ARN der Gruppe an, aus der die Kapazitätsreservierung entfernt werden soll, und bei `resources` den ARN der zu entfernenden Kapazitätsreservierungen. Um mehrere Kapazitätsreservierungen zu entfernen, trennen Sie die ARNs durch ein Leerzeichen.

Im folgenden Beispiel werden zwei Kapazitätsreservierungen aus einer Gruppe mit dem Namen `MyCRGroup` entfernt.

```
aws resource-groups ungroup-resources --group MyCRGroup --resource-arns arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Das folgende Beispiel zeigt eine Ausgabe.

```
{
    "Failed": [],
    "Succeeded": [
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-0e154d26a16094dd",
```

```
        "arn:aws:ec2:sa-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
    ]
}
```

Löschen einer Kapazitätsreservierungsgruppe

So löschen Sie eine Gruppe

Verwenden Sie den Befehl delete-group. AWS CLI Geben Sie unter `group` den Namen der zu löschenden Gruppe an.

Mit dem folgenden Befehl wird beispielsweise eine Gruppe namens `MyCRGroup` gelöscht.

```
aws resource-groups delete-group --group MyCRGroup
```

Das folgende Beispiel zeigt eine Ausgabe.

```
{
    "Group": {
        "GroupArn": "arn:aws:resource-groups:sa-east-1:123456789012:group/MyCRGroup",
        "Name": "MyCRGroup"
    }
}
```

Kapazitätsreservierungen in Cluster-Placement-Gruppen

Sie können Kapazitätsreservierungen in einer Cluster-Placement-Gruppe erstellen, um Amazon-EC2-Rechenkapazität für Ihre Workloads zu reservieren. Cluster-Placement-Gruppen bieten die Vorteile einer geringen Netzwerklatenz und eines hohen Netzwerkdurchsatzes.

Durch das Erstellen einer Kapazitätsreservierung in einer Cluster-Placement-Gruppe stellen Sie sicher, dass Sie bei Bedarf so lange wie nötig auf Rechenkapazität in Ihren Cluster-Placement-Gruppen zugreifen können. Dies ist ideal zum Reservieren von Kapazitäten für High-Performance-Computing-Workloads (HPC-Workloads), die eine Skalierung erfordern. So skalieren Sie Ihren Cluster nach unten und stellen gleichzeitig sicher, dass die Kapazität für Ihre Verwendung verfügbar bleibt, sodass Sie bei Bedarf wieder nach oben skalieren können.

Themen

- Einschränkungen
- Arbeiten mit Kapazitätsreservierungen in Cluster-Placement-Gruppen

Einschränkungen

Beachten Sie beim Erstellen von Kapazitätsreservierungen in Cluster-Placement-Gruppen Folgendes:

- Wenn sich eine bestehende Kapazitätsreservierung nicht in einer Platzierungsgruppe befindet, können Sie die Kapazitätsreservierung nicht ändern, um Kapazität in einer Platzierungsgruppe zu reservieren. Um Kapazität in einer Platzierungsgruppe zu reservieren, müssen Sie die Kapazitätsreservierung in der Platzierungsgruppe erstellen.
- Nachdem Sie eine Kapazitätsreservierung in einer Platzierungsgruppe erstellt haben, können Sie diese nicht ändern, um Kapazität außerhalb der Platzierungsgruppe zu reservieren.
- Sie können die reservierte Kapazität in einer Platzierungsgruppe erhöhen, indem Sie eine vorhandene Kapazitätsreservierung in der Platzierungsgruppe bearbeiten oder zusätzliche Kapazitätsreservierungen in der Platzierungsgruppe erstellen. Dadurch steigt jedoch das Risiko eines Fehlers wegen unzureichender Kapazität.
- Sie können keine Kapazitätsreservierungen freigeben, die in einer Cluster-Placement-Gruppe erstellt wurden.
- Sie können Cluster-Placement-Gruppen mit `active` Kapazitätsreservierungen nicht löschen. Sie müssen alle Kapazitätsreservierungen in der Cluster-Placement-Gruppe stornieren, bevor Sie sie löschen können.

Arbeiten mit Kapazitätsreservierungen in Cluster-Placement-Gruppen

Führen Sie die folgenden Schritte aus, um Kapazitätsreservierungen in Cluster-Placement-Gruppen zu verwenden.

> **Note**
>
> Wenn Sie eine Kapazitätsreservierung in einer vorhandenen Cluster-Placement-Gruppe erstellen möchten, überspringen Sie Schritt 1. Geben Sie dann für die Schritte 2 und 3 den ARN der vorhandenen Cluster-Placement-Gruppe an. Informationen darüber, wie Sie den ARN Ihrer vorhandenen Cluster-Platzierungsgruppe ermitteln können, finden Sie unterInformationen zur Platzierungsgruppe anzeigen.

Themen

- Schritt 1: (Bedingt) Erstellen einer Cluster-Placement-Gruppe zur Verwendung mit einer Kapazitätsreservierung
- Schritt 2: Erstellen einer Kapazitätsreservierung in einer Cluster-Placement-Gruppe
- Schritt 3: Starten von Instances in einer Cluster-Placement-Gruppe

Schritt 1: (Bedingt) Erstellen einer Cluster-Placement-Gruppe zur Verwendung mit einer Kapazitätsreservierung

Führen Sie diesen Schritt nur aus, wenn Sie eine neue Cluster-Placement-Gruppe erstellen müssen. Um eine vorhandene Cluster-Placement-Gruppe zu verwenden, überspringen Sie diesen Schritt und verwenden Sie dann für die Schritte 2 und 3 den ARN dieser Cluster-Placement-Gruppe. Informationen darüber, wie Sie den ARN Ihrer vorhandenen Cluster-Platzierungsgruppe ermitteln können, finden Sie unterInformationen zur Platzierungsgruppe anzeigen.

Sie können eine Cluster-Placement-Gruppe mit einer der folgenden Methoden erstellen.

Console

So erstellen Sie eine Cluster-Placement-Gruppe mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Placement Groups (Placement-Gruppen) und Create Placement Group (Placement-Gruppe erstellen) aus.
3. Geben Sie unter Name einen beschreibenden Namen für die Platzierungsgruppe an.
4. Legen Sie für die Platzierungsstrategie Cluster fest.
5. Wählen Sie Create group (Gruppe erstellen) aus.
6. Notieren Sie sich in der Tabelle Placement-Gruppen in der Spalte Gruppen-ARN den ARN der Cluster-Placement-Gruppe, die Sie erstellt haben. Sie benötigen ihn für den nächsten Schritt.

AWS CLI

Um eine Cluster-Platzierungsgruppe mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-placement-group. Geben Sie unter `--group-name` einen beschreibenden Namen für die Platzierungsgruppe an und legen Sie unter `--strategy cluster` fest.

Im folgenden Beispiel wird eine Platzierungsgruppe mit dem Namen `MyPG` erstellt, die die `cluster`-Platzierungsstrategie verwendet.

```
aws ec2 create-placement-group \
    --group-name MyPG \
    --strategy cluster
```

Notieren Sie sich den ARN der Platzierungsgruppe, die in der Befehlsausgabe zurückgegeben wurde, da Sie ihn für den nächsten Schritt benötigen.

Schritt 2: Erstellen einer Kapazitätsreservierung in einer Cluster-Placement-Gruppe

Eine Kapazitätsreservierung in einer Cluster-Placement-Gruppe erstellen Sie auf die gleiche Weise wie eine Kapazitätsreservierung. Sie müssen jedoch auch den ARN der Cluster-Placement-Gruppe angeben, in der die Kapazitätsreservierung erstellt werden soll. Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.

Überlegungen

- Die angegebene Cluster-Placement-Gruppe muss sich im Zustand `available` befinden. Wenn sich die Cluster-Placement-Gruppe im Zustand `pending`, `deleting` oder `deleted` befindet, schlägt die Anforderung fehl.
- Die Kapazitätsreservierung und die Cluster-Placement-Gruppe müssen sich in derselben Availability Zone befinden. Wenn bei der Anforderung zum Erstellen der Kapazitätsreservierung eine Availability Zone angegeben wird, die sich von der der Cluster-Placement-Gruppe unterscheidet, schlägt die Anforderung fehl.
- Sie können Kapazitätsreservierungen nur für Instance-Typen erstellen, die von Cluster-Placement-Gruppen unterstützt werden. Wenn Sie einen nicht unterstützten Instance-Typ angeben, schlägt die Anforderung fehl. Weitere Informationen finden Sie unter Regeln und Einschränkungen für Cluster Placement-Gruppen.
- Wenn Sie eine `open` Kapazitätsreservierung in einer Cluster-Placement-Gruppe erstellen und ausgeführte Instances mit übereinstimmenden Attributen (ARN der Platzierungsgruppe, Instance-Typ, Availability Zone, Plattform und Tenancy) vorhanden sind, werden diese Instances automatisch in der Kapazitätsreservierung ausgeführt.
- Ihre Anforderung, eine Kapazitätsreservierung zu erstellen, kann bei Eintreten einer der folgenden Bedingungen fehlschlagen:

- Die Kapazität von Amazon EC2 reicht nicht aus, um der Anforderung nachzukommen. Versuchen Sie es entweder zu einem späteren Zeitpunkt erneut oder probieren Sie es erneut mit einer anderen Availability Zone oder einer kleineren Kapazität. Wenn Ihr Workload in Hinsicht auf Instance-Typen und -Größen flexibel ist, versuchen Sie es mit verschiedenen Instance-Attributen.
- Die angeforderte Menge überschreitet Ihr On-Demand-Instance-Limit für die ausgewählte Instance-Familie. Erhöhen Sie Ihr On-Demand-Instance-Limit für die Instance-Familie und versuchen Sie es erneut. Weitere Informationen finden Sie unter Kontingente für On-Demand-Instances.

Sie können die Kapazitätsreservierung in der Cluster-Placement-Gruppe mit einer der folgenden Methoden erstellen.

Console

So erstellen Sie eine Kapazitätsreservierung mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Kapazitätsreservierungen (Kapazitätsreservierungen) und dann Create Kapazitätsreservierung (Kapazitätsreservierung erstellen) aus.
3. Geben Sie auf der Seite „Kapazitätsreservierung erstellen“ den Instance-Typ, die Plattform, die Availability Zone, die Tenancy, die Menge und das Enddatum nach Bedarf an.
4. Wählen Sie unter Platzierungsgruppe den ARN der Cluster-Platzierungsgruppe aus, in der die Kapazitätsreservierung erstellt werden soll.
5. Wählen Sie Create (Erstellen) aus.

Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.

AWS CLI

Um eine Kapazitätsreservierung mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-capacity-reservation. Geben Sie für `--placement-group-arn` den ARN der Cluster-Placement-Gruppe an, in der die Kapazitätsreservierung erstellt werden soll.

```
$ aws ec2 create-capacity-reservation \
```

```
    --instance-type instance_type \
    --instance-platform platform \
    --availability-zone az \
    --instance-count quantity \
    --placement-group-arn placement_group_ARN
```

Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.

Schritt 3: Starten von Instances in einer Cluster-Placement-Gruppe

Sie starten eine Instance in der Kapazitätsreservierung einer Cluster-Placement-Gruppe auf die gleiche Weise, wie Sie eine Instance in eine Kapazitätsreservierung starten. Sie müssen jedoch auch den ARN der Cluster-Placement-Gruppe angeben, in der die Instance gestartet werden soll. Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.

Überlegungen

- Wenn die Kapazitätsreservierung open ist, müssen Sie die Kapazitätsreservierung in der Instance-Startanforderung nicht angeben. Wenn Attribute der Instance (ARN der Platzierungsgruppe, Instance-Typ, Availability Zone, Plattform und Tenancy) mit einer Kapazitätsreservierung in der angegebenen Platzierungsgruppe übereinstimmen, wird diese Instance automatisch in der Kapazitätsreservierung ausgeführt.
- Wenn von der Kapazitätsreservierung nur gezielte Instance-Starts akzeptiert werden, müssen Sie bei der Anforderung zusätzlich zur Cluster-Placement-Gruppe die Ziel-Kapazitätsreservierung angeben.
- Wenn sich die Kapazitätsreservierung in einer Kapazitätsreservierungsgruppe befindet, müssen Sie bei der Anforderung zusätzlich zur Cluster-Placement-Gruppe die Ziel-Kapazitätsreservierungsgruppe angeben. Weitere Informationen finden Sie unter Arbeiten mit Kapazitätsreservierung-Gruppen.

Mit einer der folgenden Methoden starten Sie eine Instance in einer Kapazitätsreservierung einer Cluster-Placement-Gruppe.

Console

So starten Sie eine Instance in einer bestehenden Kapazitätsreservierung mithilfe einer Konsole

1. Gehen Sie wie folgt vor, um eine Instance zu starten, starten Sie die Instance jedoch erst, wenn Sie die folgenden Schritte abgeschlossen haben, um die Einstellungen für die Platzierungsgruppe und die Kapazitätsreservierung festzulegen.
2. Erweitern Sie Erweiterte Details und gehen Sie wie folgt vor:
   a. Wählen Sie unter Platzierungsgruppe die Cluster-Placement-Gruppe aus, in der die Instance gestartet werden soll.
   b. Wählen Sie für Capacity Reservation (Kapazitätsreservierung) je nach Konfiguration der Kapazitätsreservierung eine der folgenden Optionen aus:
      - Öffnen — Um die Instances in einer beliebigen `open` Kapazitätsreservierung in der Cluster-Placement-Gruppe zu starten, die über passende Attribute und ausreichend Kapazität verfügt.
      - Targeting by ID — Um die Instances in einer Kapazitätsreservierung zu starten, die nur gezielte Instance-Starts akzeptiert.
      - Zielgruppenspezifisch — Um die Instances für eine beliebige Kapazitätsreservierung mit passenden Attributen und verfügbarer Kapazität in der ausgewählten Kapazitätsreservierungsgruppe zu starten.
3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.

AWS CLI

Um Instances für eine bestehende Kapazitätsreservierung zu starten, verwenden Sie den AWS CLI

Verwenden Sie den Befehl run-instances. Wenn Sie eine bestimmte Kapazitätsreservierung oder eine Kapazitätsreservierungsgruppe anvisieren müssen, geben Sie den Parameter `--capacity-reservation-specification` an. Geben Sie für `--placement` den Parameter `GroupName`

und dann dann den Namen der Platzierungsgruppe an, die Sie in den vorherigen Schritten erstellt haben.

Mit dem folgenden Befehl starten Sie eine Instance in einer `targeted` Kapazitätsreservierung einer Cluster-Placement-Gruppe.

```
$ aws ec2 run-instances \
    --image-id ami_id \
    --count quantity \
    --instance-type instance_type \
    --key-name key_pair_name \
    --subnet-id subnetid \
    --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=capacity_reservation_id} \
    --placement "GroupName=cluster_placement_group_name"
```

Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.

Capacity Reservations in Local Zones

Eine lokale Zone ist eine Erweiterung einer AWS Region, die sich geografisch in der Nähe Ihrer Benutzer befindet. Ressourcen, die in einer Local Zone erstellt wurden, können von lokalen Benutzern mit sehr latenzarmen Verbindungen genutzt werden. Weitere Informationen finden Sie unter AWS -Local Zones.

Sie können eine VPC von ihrer übergeordneten AWS Region in eine lokale Zone erweitern, indem Sie in dieser lokalen Zone ein neues Subnetz erstellen. Wenn Sie ein Subnetz in einer Local Zone erstellen, wird Ihre VPC auf diese Local Zone erweitert. Das Subnetz in der Local Zone funktioniert genauso wie andere Subnetze in Ihrer VPC.

Mithilfe von Local Zones können Sie Kapazitätsreservierungen an mehreren Speicherorten platzieren, die näher an Ihren Benutzern liegen. Sie erstellen und verwenden Kapazitätsreservierungen in Local Zones auf die gleiche Weise, wie Sie Kapazitätsreservierungen in regulären Availability Zones erstellen und verwenden. Es gelten dieselben Features und dasselbe Verhalten der Instance-Übereinstimmung. Weitere Informationen zu den in Local Zones unterstützten Preismodellen finden Sie unter Häufig gestellte Fragen zu AWS Local Zones.

Überlegungen

Sie können in einer Local Zone keine Kapazitätsreservierung-Gruppen verwenden.

Verwenden einer Kapazitätsreservierung in einer Local Zone

1. Aktivieren Sie die lokale Zone für die Verwendung in Ihrem AWS Konto. Weitere Informationen finden Sie unter Anmelden für Local Zones.
2. Erstellen Sie eine Kapazitätsreservierung in der Local Zone. Wählen Sie für Availability Zone die Local Zone aus. Die lokale Zone wird beispielsweise durch einen AWS Regionalcode gefolgt von einer Kennung dargestellt, die den Standort angibt`us-west-2-lax-1a`. Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.
3. Erstellen Sie ein Subnetz in der Local Zone. Wählen Sie für Availability Zone die Local Zone aus. Weitere Informationen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC im Amazon-VPC-Benutzerhandbuch.
4. Starten Sie eine Instance. Wählen Sie als Subnetz das Subnetz in der Local Zone (z. B. `subnet-123abc | us-west-2-lax-1a`) aus und wählen Sie bei Kapazitätsreservierung die Spezifikation (entweder `open` oder finden Sie sie nach ID), die für die Kapazitätsreservierung erforderlich ist, die Sie in der Local Zone erstellt haben. Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.

Kapazitätsreservierungen in Wavelength-Zonen

Mit AWS Wavelength können Entwickler Anwendungen mit ultra-niedriger Latenz für Mobilgeräte und Endbenutzer erstellen. Wavelength stellt standardmäßige AWS -Datenverarbeitungs- und -Speicherservices am Edge der 5G-Netze von Telekommunikationsanbietern bereit. Sie können eine Amazon Virtual Private Cloud (VPC) auf eine oder mehrere Wavelength-Zonen erweitern. Sie können dann AWS Ressourcen wie Amazon EC2 EC2-Instances verwenden, um Anwendungen auszuführen, die eine extrem niedrige Latenz und eine Verbindung zu AWS Diensten in der Region erfordern. Weitere Informationen finden Sie unter AWS Wavelength Zonen.

Wenn Sie On-Demand Kapazitätsreservierungen erstellen, können Sie die Wavelength-Zone auswählen und Instances Kapazitätsreservierung in einer Wavelength-Zone starten, indem Sie das mit der Wavelength-Zone verknüpfte Subnetz angeben. Die Wavelength-Zone wird durch einen AWS -Regionscode dargestellt, gefolgt von einer ID, die den Standort angibt, z. B. `us-east-1-wl1-bos-wlz-1`.

Wavelength Zones sind nicht in jeder Region verfügbar. Weitere Informationen zu den Regionen, die Wavelength Zones unterstützen, finden Sie unter Verfügbare Wavelength Zones im AWS Wavelength Developerhandbuch.

Überlegungen

Sie können in einer Wavelength-Zone keine Kapazitätsreservierung-Gruppen verwenden.

Verwenden einer Kapazitätsreservierung in einer Wavelength-Zone

1. Aktivieren Sie die Wellenlängenzone für die Verwendung in Ihrem AWS Konto. Weitere Informationen finden Sie unter the section called “Aktivieren von Wavelength Zones”.
2. Erstellen Sie eine Kapazitätsreservierung in der Wavelength-Zone. Wählen Sie für Availability Zone die Wavelength aus. Die Wavelength wird beispielsweise durch einen AWS Regionalcode gefolgt von einer Kennung dargestellt, die den Standort angibt`us-east-1-wl1-bos-wlz-1`. Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.
3. Erstellen Sie ein Subnetz in der Wavelength-Zone. Wählen Sie für Availability Zone die Zone Wavelength aus. Weitere Informationen finden Sie unter Erstellen eines Subnetzes in Ihrer VPC im Amazon-VPC-Benutzerhandbuch.
4. Starten Sie eine Instance. Wählen Sie als Subnetz das Subnetz in der Zone Wavelength (z. B. `subnet-123abc | us-east-1-wl1-bos-wlz-1`) aus und wählen Sie bei Kapazitätsreservierung die Spezifikation (entweder `open` oder finden Sie sie nach ID), die für die Kapazitätsreservierung erforderlich ist, die Sie in der Wavelength erstellt haben. Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.

Kapazitätsreservierungen am AWS Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur, Dienste, APIs und Tools auf Kundenstandorte ausdehnt. Durch den lokalen Zugriff auf die AWS verwaltete Infrastruktur AWS Outposts können Kunden Anwendungen vor Ort mit denselben Programmierschnittstellen wie in AWS Regionen erstellen und ausführen und gleichzeitig lokale Rechen- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen nutzen.

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazitäten, der am Standort eines Kunden bereitgestellt wird. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS Region.

Sie können Kapazitätsreservierungen auf Outposts erstellen, die Sie in Ihrem Konto erstellt haben. Auf diese Weise können Sie Rechenkapazität auf einem Outpost an Ihrem Standort reservieren. Sie erstellen und verwenden Kapazitätsreservierungen in Outposts auf die gleiche Weise, wie Sie Kapazitätsreservierungen in regulären Availability Zones erstellen und verwenden. Es gelten dieselben Features und dasselbe Verhalten der Instance-Übereinstimmung.

Sie können Kapazitätsreservierungen auf Outposts auch mit anderen AWS Konten innerhalb Ihrer Organisation teilen, indem AWS Resource Access Manager Sie. Weitere Informationen zum Freigeben von Kapazitätsreservierungen finden Sie unter Arbeiten mit freigegebenen Kapazitätsreservierungen.

Voraussetzung

Sie müssen einen Outpost an Ihrem Standort installiert haben. Weitere Informationen finden Sie unter Outpost erstellen und die Kapazität dafür bestellen im AWS Outposts -Benutzerhandbuch.

Überlegungen

- Sie können auf einem Outpost keine Kapazitätsreservierung-Gruppen verwenden.

Verwenden einer Kapazitätsreservierung auf einem Outpost

1. Erstellen Sie ein Subnetz auf dem Outpost. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im AWS Outposts -Benutzerhandbuch.
2. Erstellen Sie eine Kapazitätsreservierung auf dem Outpost.
   a. Öffnen Sie die AWS Outposts Konsole unter https://console.aws.amazon.com/outposts/.
   b. Wählen Sie im Navigationsbereich Outposts aus und klicken Sie danach auf Aktionen, Kapazitätsreservierung erstellen.
   c. Konfigurieren Sie die Kapazitätsreservierung nach Bedarf und wählen Sie Create (Erstellen) aus. Weitere Informationen finden Sie unter Erstellen eines Kapazitätsreservierung.

   > **Note**
   >
   > In der Dropdown-Liste Instance-Typ werden nur Instance-Typen aufgeführt, die vom ausgewählten Outpost unterstützt werden. In der Dropdown-Liste Availability Zone wird nur die Availability Zone aufgeführt, die dem ausgewählten Outpost zugeordnet ist.

3. Starten einer Instance in einer Kapazitätsreservierung. Wählen Sie für Subnetz das Subnetz aus, das Sie in Schritt 1 erstellt haben, und für Kapazitätsreservierung wählen Sie die Kapazitätsreservierung aus, die Sie in Schritt 2 erstellt haben. Weitere Informationen finden Sie unter Launch an Instance on your Outpost (Starten einer Instance auf Ihrem Outpost) im AWS Outposts -Benutzerhandbuch.

Arbeiten mit freigegebenen Kapazitätsreservierungen

Die gemeinsame Nutzung von Kapazitätsreservierungen ermöglicht es Besitzern von Kapazitätsreservierungen, ihre reservierte Kapazität mit anderen AWS Konten oder innerhalb einer AWS Organisation zu teilen. Auf diese Weise können Sie Kapazitätsreservierungen zentral erstellen und verwalten und die reservierte Kapazität auf mehrere AWS Konten oder innerhalb Ihrer AWS Organisation verteilen.

Bei diesem Modell teilt sich das AWS Konto, dem die Kapazitätsreservierung gehört (Eigentümer), diese mit anderen AWS Konten (Verbrauchern). Konsumenten können beim Starten von Instances in den für sie freigegebenen Kapazitätsreservierungen so vorgehen, wie sie dies beim Starten von Instances in Kapazitätsreservierungen tun würden, die zu ihrem Konto gehören. Der Kapazitätsreservierung-Besitzer ist für die Verwaltung der Kapazitätsreservierung und der Instances, die von ihm darin gestartet werden, verantwortlich. Besitzer sind nicht dazu befugt Instances, die Konsumenten in den von ihnen freigegebenen Kapazitätsreservierungen starten, zu ändern. Konsumenten sind für die Verwaltung der Instances verantwortlich, die sie in den für sie freigegebenen Kapazitätsreservierungen starten. Konsumenten können keine Instances anzeigen oder ändern, die sich im Besitz anderer Konsumenten oder des Besitzers der Kapazitätsreservierung befinden.

Ein Kapazitätsreservierung-Besitzer kann eine Kapazitätsreservierung freigeben für:

- Bestimmte AWS Konten innerhalb oder außerhalb der AWS Organisation
- Eine Organisationseinheit innerhalb ihrer AWS Organisation
- Es ist die gesamte AWS Organisation

Inhalt

- Instance-Limits

Voraussetzungen für die Freigabe von Kapazitätsreservierungen

- Um eine Kapazitätsreservierung teilen zu können, müssen Sie sie in Ihrem AWS Konto besitzen. Sie können keine Kapazitätsreservierung freigeben, die für Sie freigegeben wurde.
- Sie können Kapazitätsreservierungen ausschließlich für freigegebene Tenancy-Instances freigeben. Sie können Kapazitätsreservierungen nicht für Dedicated Tenancy-Instances freigeben.
- Die gemeinsame Nutzung von Kapazitätsreservierungen ist nicht für neue AWS Konten oder AWS Konten mit begrenzter Abrechnungshistorie verfügbar.
- Um eine Kapazitätsreservierung mit Ihrer AWS Organisation oder einer Organisationseinheit in Ihrer AWS Organisation zu teilen, müssen Sie die gemeinsame Nutzung mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM -Benutzerhandbuch.

Zugehörige Services

Die gemeinsame Nutzung von Kapazitätsreservierungen ist in AWS Resource Access Manager (AWS RAM) integriert. AWS RAM ist ein Dienst, mit dem Sie Ihre AWS Ressourcen mit einem beliebigen AWS Konto oder über dieses teilen können AWS Organizations. Mit können Sie Ressourcen AWS RAM, die Ihnen gehören, gemeinsam nutzen, indem Sie eine gemeinsame Nutzung erstellen. Eine Ressourcenfreigabe legt die freizugebenden Ressourcen und die Konsumenten fest, für die sie freigegeben werden sollen. Bei Verbrauchern kann es sich um einzelne AWS Konten, Organisationseinheiten oder eine gesamte Organisation handeln AWS Organizations.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM Benutzerhandbuch.

Freigeben in mehreren Availability Zones

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. Beispielsweise hat die Availability Zone `us-east-1a` für Ihr AWS Konto möglicherweise nicht denselben Standort wie `us-east-1a` für ein anderes AWS Konto.

Um den Ort Ihrer Kapazitätsreservierungen relativ zu Ihren Konten zu bestimmen, verwenden Sie die Availability Zone-ID (AZ-ID). Die AZ-ID ist eine eindeutige und konsistente Kennung für eine

Availability Zone für alle AWS Konten. Dies `use1-az1` ist beispielsweise eine AZ-ID für die `us-east-1` Region und es handelt sich in jedem AWS Konto um denselben Standort.

So zeigen Sie die AZ-IDs für die Availability Zones in Ihrem Konto an

1. Öffnen Sie die AWS RAM Konsole unter https://console.aws.amazon.com/ram.
2. Die AZ-IDs für die aktuelle Region werden im Feld Your AZ ID (Ihre AZ-ID) rechts im Bildschirm angezeigt.

Freigeben einer Kapazitätsreservierung

Wenn Sie eine Kapazitätsreservierung, die Sie besitzen, mit anderen AWS Konten teilen, ermöglichen Sie diesen, Instances für Ihre reservierte Kapazität zu starten. Berücksichtigen Sie bei der Freigabe einer offenen Kapazitätsreservierung Folgendes, da dies zu einer unvorhergesehenen Nutzung der Kapazitätsreservierung führen könnte:

- Konsumenten mit ausgeführten Ressourcen, die den Attributen der Kapazitätsreservierung entsprechen, für die der Parameter `CapacityReservationPreference` auf `open` eingestellt ist und die noch nicht in reservierter Kapazität ausgeführt werden, verwenden automatisch die freigegebene Kapazitätsreservierung.
- Wenn Verbraucher Instances mit übereinstimmenden Attributen (Instance-Typ, Plattform, Availability Zone und Tenancy) starten und deren `CapacityReservationPreference` Parameter auf gesetzt ist`open`, starten sie automatisch in die gemeinsame Kapazitätsreservierung.

Um eine Kapazitätsreservierung freigeben zu können, müssen Sie sie einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM Ressource, mit der Sie Ihre Ressourcen für mehrere AWS Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden. Wenn Sie eine Kapazitätsreservierung mithilfe der Amazon EC2-Konsole freigeben, fügen Sie sie zu einer vorhandenen Ressourcenfreigabe hinzu. Um die Kapazitätsreservierung einer neuen Ressourcenfreigabe hinzufügen zu können, müssen Sie die Ressourcenfreigabe mithilfe der AWS RAM -Konsole erstellen.

Wenn Sie Teil einer Organisation sind AWS Organizations und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation Zugriff auf die gemeinsame Kapazitätsreservierung, sofern die Voraussetzungen für die gemeinsame Nutzung erfüllt sind. Wenn die Kapazitätsreservierung für externe Konten freigegeben ist, erhalten Konsumenten eine Einladung

zur Teilnahme an der Ressourcenfreigabe und nach Annahme der Einladung wird ihnen Zugriff auf die freigegebene Kapazitätsreservierung gewährt.

> **Important**
>
> Bevor Sie Instances in einer Kapazitätsreservierung starten, die mit Ihnen geteilt wird, überprüfen Sie, ob Sie Zugriff auf die gemeinsam genutzte Kapazitätsreservierung haben, indem Sie sie in der Konsole anzeigen oder sie mit dem Befehl AWS CLI describe-capacity-reservations beschreiben. Wenn Sie sich die gemeinsam genutzte Kapazitätsreservierung in der Konsole ansehen oder sie mit dem beschreiben können AWS CLI, steht sie Ihnen zur Verfügung und Sie können Instances darin starten. Wenn Sie versuchen, Instances in die Kapazitätsreservierung zu starten, und diese aufgrund eines Freigabefehlers nicht zugänglich ist, werden die Instances in On-Demand-Kapazität gestartet.

Sie können eine Kapazitätsreservierung, die Sie besitzen, mithilfe der Amazon-EC2-Konsole, der AWS RAM -Konsole oder der AWS CLI freigeben.

So geben Sie eine Kapazitätsreservierung in Ihrem Besitz mithilfe der Amazon EC2-Konsole frei

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Wählen Sie die Kapazitätsreservierung aus, die freigegeben werden soll, und wählen Sie Actions (Aktionen), Share reservation (Reservierung freigeben).
4. Wählen Sie die Ressourcenfreigabe aus, der die Kapazitätsreservierunghinzugefügt werden soll, und wählen Sie Share Kapazitätsreservierung (Kapazitätsreservierung freigeben).

   Es kann einige Minuten dauern, bis Konsumenten Zugriff auf die freigegebene Kapazitätsreservierung gewährt wird.

Um eine Kapazitätsreservierung, die Ihnen gehört, über die AWS RAM Konsole zu teilen

Siehe Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um eine Kapazitätsreservierung, die Sie besitzen, zu teilen, verwenden Sie die AWS CLI

Verwenden Sie den Befehl create-resource-share.

Beenden der Freigabe einer Kapazitätsreservierung

Der Kapazitätsreservierung-Besitzer kann die gemeinsame Nutzung einer Kapazitätsreservierung jederzeit beenden. Es gelten die folgenden Regeln:

- Instances im Besitz von Konsumenten, die in freigegebener Kapazität ausgeführt wurden, als die Freigabe aufgehoben wurde, werden weiterhin normal außerhalb der reservierten Kapazität ausgeführt, und die Kapazität wird abhängig von der Verfügbarkeit an Amazon EC2-Kapazität als Kapazitätsreservierung wiederhergestellt.
- Konsumenten, für die die Kapazitätsreservierung freigegeben wurde, können keine neuen Instances mehr in der reservierten Kapazität starten.

Um die Freigabe einer Kapazitätsreservierung in Ihrem Besitz zu beenden, müssen Sie diese aus der Ressourcenfreigabe entfernen. Hierzu können Sie die Amazon-EC2-Konsole, die AWS RAM -Konsole oder die AWS CLI verwenden.

So beenden Sie die Freigabe einer Kapazitätsreservierung in Ihrem Besitz mithilfe der Amazon EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Wählen Sie die Kapazitätsreservierung aus und klicken Sie auf die Registerkarte Freigabe.
4. Auf der Registerkarte Sharing (Freigabe) werden die Ressorcenfreigaben aufgelistet, zu denen die Kapazitätsreservierung hinzugefügt wurde. Wählen Sie die Ressourcenfreigabe aus, aus der die Kapazitätsreservierung entfernt werden soll, und wählen Sie Remove from resource share (Aus Ressourcenfreigabe entfernen).

Um die gemeinsame Nutzung einer Kapazitätsreservierung, die Ihnen gehört, über die AWS RAM Konsole zu beenden

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Um die gemeinsame Nutzung einer Kapazitätsreservierung zu beenden, die Sie besitzen, verwenden Sie die AWS CLI

Verwenden Sie den Befehl disassociate-resource-share.

Identifizieren und Anzeigen einer gemeinsamen Kapazitätsreservierung

> **Important**
>
> Bevor Sie Instances in eine Kapazitätsreservierung starten, die für Sie freigegeben ist, überprüfen Sie, ob Sie Zugriff auf die gemeinsame Kapazitätsreservierung haben, indem Sie diese in der Konsole anzeigen oder mithilfe des AWS CLI-Befehls beschreiben. Wenn Sie die gemeinsame Kapazitätsreservierung in der Konsole einsehen oder sie mithilfe der beschreiben können AWS CLI, steht sie Ihnen zur Verfügung und Sie können Instances darin starten. Wenn Sie versuchen, Instances in die Kapazitätsreservierung zu starten, und diese aufgrund eines Freigabefehlers nicht zugänglich ist, wird die Instance in On-Demand-Kapazität gestartet.

Besitzer und Konsumenten können freigegebene Kapazitätsreservierungen mithilfe der Amazon-EC2-Konsole und AWS CLI identifizieren.

So identifizieren Sie eine freigegebene Kapazitätsreservierung mithilfe der Amazon EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus. Im Bildschirm werden die Kapazitätsreservierungen in Ihrem Besitz und Kapazitätsreservierungen, die für Sie freigegeben werden, aufgelistet. In der Spalte Besitzer wird die AWS Konto-ID des Besitzers der Kapazitätsreservierung angezeigt. `(me)`neben der AWS Konto-ID gibt an, dass Sie der Eigentümer sind.

Um eine gemeinsame Kapazitätsreservierung mit dem zu identifizieren AWS CLI

Verwenden Sie den Befehl describe-capacity-reservations. Der Befehl gibt die Kapazitätsreservierungen zurück, die Sie besitzen, und die Kapazitätsreservierungen, die mit Ihnen gemeinsam genutzt wurden. `OwnerId`zeigt die AWS Konto-ID des Besitzers der Kapazitätsreservierung an.

Anzeigen einer gemeinsamen Kapazitätsreservierung Nutzung

Der Besitzer einer freigegebenen Kapazitätsreservierung kann ihre Nutzung jederzeit mithilfe der Amazon-EC2-Konsole oder der AWS CLI anzeigen.

So zeigen Sie die Kapazitätsreservierung-Nutzung mithilfe der Amazon EC2-Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Wählen Sie die Kapazitätsreservierung aus, deren Nutzung angezeigt werden soll, und wählen Sie die Registerkarte Usage (Nutzung).

   Die Spalte AWS -Konto-ID zeigt die Konto-IDs der Konsumenten an, von denen die Kapazitätsreservierung derzeit genutzt wird. Die Spalte Launched instances (Gestartete Instances) zeigt die Anzahl von Instances, die jeder Konsument derzeit in der reservierten Kapazität ausführt.

Um die Nutzung der Kapazitätsreservierung mit dem AWS CLI

Verwenden Sie den Befehl get-capacity-reservation-usage. `AccountId` zeigt die Konto-ID des Kontos, von dem die Kapazitätsreservierung genutzt wird. `UsedInstanceCount` zeigt die Anzahl von Instances, die der Konsument derzeit in der reservierten Kapazität ausführt.

Berechtigungen für freigegebene Kapazitätsreservierung

Berechtigungen für Besitzer

Besitzer sind für die Verwaltung und Stornierung ihrer freigegebenen Kapazitätsreservierungen verantwortlich. Besitzer können keine Änderungen an Instances vornehmen, die in der freigegebenen Kapazitätsreservierung im Besitz anderer Konten ausgeführt werden. Besitzer sind weiterhin für die Verwaltung von Instances verantwortlich, die sie selbst in der freigegebenen Kapazitätsreservierung starten.

Berechtigungen für Konsumenten

Konsumenten sind für die Verwaltung ihrer Instances verantwortlich, die in der freigegebenen Kapazitätsreservierung ausgeführt werden. Konsumenten können die freigegebene Kapazitätsreservierung keinesfalls ändern und können keine Instances anzeigen oder bearbeiten, die sich im Besitz anderer Konsumenten oder des Kapazitätsreservierung-Besitzers befinden.

Fakturierung und Messung

Für die Freigabe von Kapazitätsreservierungen fallen keine zusätzlichen Gebühren an.

Dem Kapazitätsreservierung-Besitzer werden Instances, die er in der Kapazitätsreservierung ausführt, sowie nicht genutzte reservierte Kapazität in Rechnung gestellt. Konsumenten werden Instances in Rechnung gestellt, die Sie in der freigegebenen Kapazitätsreservierung ausführen.

Wenn der Besitzer der Kapazitätsreservierung einem anderen Zahlerkonto angehört und die Kapazitätsreservierung durch eine regionale Reserved Instance oder einen Savings Plan abgedeckt ist, werden dem Besitzer der Kapazitätsreservierung weiterhin die Kosten für die regionale Reserved Instance oder den Savings Plan in Rechnung gestellt. In diesen Fällen zahlt der Besitzer der Kapazitätsreservierung für die regionale Reserved Instance oder den Savings Plan, und den Verbrauchern werden die Instances in Rechnung gestellt, die in der gemeinsamen Kapazitätsreservierung ausgeführt werden.

Instance-Limits

Die gesamte Kapazitätsreservierung-Nutzung wird auf die On-Demand-Instance-Beschränkungen des Kapazitätsreservierung-Besitzers angerechnet. Dies umfasst:

- Ungenutzte reservierte Kapazität
- Nutzung durch Instances im Besitz des Kapazitätsreservierung-Besitzers
- Nutzung durch Instances im Besitz von Konsumenten

Instances, die von Konsumenten in der freigegebenen Kapazität gestartet werden, werden auf die On-Demand-Instance-Beschränkung des Kapazitätsreservierung-Besitzers angerechnet. Instance-Beschränkungen von Konsumenten sind die Summe aus ihren eigenen On-Demand-Instance-Beschränkungen und der in der freigegebenen Kapazitätsreservierungen verfügbaren Kapazität, auf die sie Zugriff haben.

Kapazitätsreservierungsflotten

Eine On-Demand-Kapazitätsreservierungsflotte ist eine Gruppe von Kapazitätsreservierungen.

Die Anforderung einer Kapazitätsreservierungsflotte enthält alle Konfigurationsinformationen, die zum Starten einer Kapazitätsreservierungsflotte erforderlich sind. Mit einer einzigen Anforderung können Sie für Ihre Workload große Amazon-EC2-Kapazitäten (bis zu einem angegebenen Zielwert) für verschiedene Instance-Typen reservieren.

Nachdem Sie eine Kapazitätsreservierungsflotte erstellt haben, können Sie die Kapazitätsreservierungen in der Flotte verwalten, indem Sie die Flotte ändern oder auflösen.

Themen

Funktionsweise von Kapazitätsreservierungsflotten

Wenn Sie eine Kapazitätsreservierungsflotte erstellen, versucht die Flotte, individuelle Kapazitätsreservierungen festzulegen, um die in Ihrer Flottenanforderung angegebene Gesamtzielkapazität zu erreichen.

Die Anzahl der Instances, für die die Flotte Kapazität reserviert, hängt von der Gesamtzielkapazität und den Instance-Typ-Gewichtungen ab, die Sie angeben. Der Instance-Typ, für den die Flotte Kapazität reserviert, hängt von der Zuweisungsstrategie und den Instance-Typ-Prioritäten ab, die Sie verwenden.

Wenn zum Zeitpunkt der Erstellung nicht genügend Kapazität vorhanden ist und die Flotte ihre Gesamtzielkapazität nicht sofort erreichen kann, versucht sie auf asynchrone Weise, Kapazitätsreservierungen zu erstellen, bis die angeforderte Kapazitätsmenge reserviert ist.

Wenn die Flotte ihre Gesamtzielkapazität erreicht, versucht sie, diese Kapazität beizubehalten. Wird eine Kapazitätsreservierung in der Flotte storniert, erstellt die Flotte je nach Ihrer Flottenkonfiguration automatisch eine oder mehrere Kapazitätsreservierungen, um die verlorene Kapazität zu ersetzen und ihre Gesamtzielkapazität beizubehalten.

Die Kapazitätsreservierungen in der Flotte können nicht einzeln verwaltet werden. Sie müssen gemeinsam durch eine Änderung der Flotte verwaltet werden. Wenn Sie eine Flotte ändern, werden die Kapazitätsreservierungen in der Flotte automatisch den Änderungen entsprechend aktualisiert.

Derzeit unterstützen Kapazitätsreservierungsflotten die Übereinstimmungskriterien für open-Instances. Alle von einer Flotte gestarteten Kapazitätsreservierungen verwenden automatisch diese Übereinstimmungskriterien. Mit diesen Kriterien werden neue Instances und bestehende Instances mit übereinstimmenden Attributen (Instance-Typ, Plattform, Availability Zone und

Tenancy) automatisch in den von einer Flotte erstellten Kapazitätsreservierungen ausgeführt. Kapazitätsreservierungsflotten unterstützen keine Übereinstimmungskriterien für `target`-Instances.

Überlegungen

Bei der Arbeit mit Kapazitätsreservierungsflotten sollten Sie Folgendes bedenken:

- Eine Flotte mit Kapazitätsreservierungen kann mithilfe der AWS API und erstellt, geändert, angezeigt und storniert werden. AWS CLI
- Die Kapazitätsreservierungen in einer Flotte können nicht einzeln verwaltet werden. Sie müssen gemeinsam durch eine Änderung oder Stornierung der Flotte verwaltet werden.
- Eine Kapazitätsreservierungsflotte kann nicht für mehrere Regionen gelten.
- Eine Kapazitätsreservierungsflotte kann nicht für mehrere Availability Zones gelten.
- Kapazitätsreservierungen, die von einer Flotte mit Kapazitätsreservierungen erstellt wurden, werden automatisch mit dem folgenden AWS generierten Tag versehen:
  - Schlüssel: `aws:ec2-capacity-reservation-fleet`
  - Wert: *`fleet_id`*

  Anhand dieses Tags können Sie Kapazitätsreservierungen erkennen, die von einer Kapazitätsreservierungsflotte erstellt wurden.

Preisgestaltung

Für die Verwendung von Kapazitätsreservierungsflotten fallen keine zusätzlichen Gebühren an. Ihnen werden die einzelnen Kapazitätsreservierungen in Rechnung gestellt, die von Ihren Kapazitätsreservierungsflotten erstellt wurden. Weitere Informationen zur Abrechnung von Kapazitätsreservierungen finden Sie unter Preise und Fakturierung für Kapazitätsreservierung.

Konzepte von Kapazitätsreservierungsflotten

In diesem Thema werden einige der Konzepte von Kapazitätsreservierungsflotten beschrieben.

Themen

- Gesamtzielkapazität
- Zuweisungsstrategie
- Instance-Typ-Gewichtung
- Instance-Typ-Priorität

Gesamtzielkapazität

Die Gesamtzielkapazität definiert die Gesamtmenge der Rechenkapazität, den die Kapazitätsreservierungsflotte reserviert. Sie geben die Gesamtzielkapazität beim Erstellen der Kapazitätsreservierungsflotte an. Nachdem die Flotte erstellt wurde, erstellt Amazon EC2 automatisch Kapazitätsreservierungen, um Kapazitäten bis zur Gesamtzielkapazität zu reservieren.

Die Anzahl der Instances, für die die Kapazitätsreservierungsflotte Kapazität reserviert, wird durch die Gesamtzielkapazität und die Instance-Typ-Gewichtung bestimmt, die Sie für jeden Instance-Typ in der Kapazitätsreservierungsflotte angeben (`total target capacity` / `instance type weight` = `number of instances`).

Sie können die Gesamtzielkapazität basierend auf sinnvollen Einheiten für Ihre Workload zuweisen. Wenn Ihre Workload beispielsweise eine bestimmte Anzahl von vCPUs erfordert, können Sie die Gesamtzielkapazität basierend auf der Anzahl der erforderlichen vCPUs zuweisen. Wenn Ihre Workload `2048` vCPUs erfordert, geben Sie eine Gesamtzielkapazität von `2048` an und weisen anschließend Instance-Typ-Gewichtungen auf der Grundlage der Anzahl von vCPUs zu, die von den Instance-Typen in der Flotte bereitgestellt werden. Ein Beispiel finden Sie unter Instance-Typ-Gewichtung.

Zuweisungsstrategie

Die Zuweisungsstrategie für Ihre Kapazitätsreservierungsflotte bestimmt, wie die Anforderung von reservierter Kapazität aus den Instance-Typ-Spezifikationen in der Konfiguration der Kapazitätsreservierungsflotte erfüllt wird.

Derzeit wird nur die Zuweisungsstrategie `prioritized` unterstützt. Diese Strategie sieht vor, dass die Kapazitätsreservierungsflotte Kapazitätsreservierungen unter Verwendung der Prioritäten erstellt, die Sie den Instance-Typ-Spezifikationen in der Konfiguration der Kapazitätsreservierungsflotte zugewiesen haben. Niedrigere Prioritätswerte bedeuten eine höhere Priorität für die Verwendung. Angenommen, Sie erstellen eine Kapazitätsreservierungsflotte, die die folgenden Instance-Typen und Prioritäten verwendet:

- `m4.16xlarge` – Priorität = 1
- `m5.16xlarge` – Priorität = 3
- `m5.24xlarge` – Priorität = 2

Die Flotte versucht zunächst, Kapazitätsreservierungen für `m4.16xlarge` zu erstellen. Wenn Amazon EC2 keine ausreichende `m4.16xlarge`-Kapazität hat, versucht die Flotte,

Kapazitätsreservierungen für `m5.24xlarge` zu erstellen. Wenn Amazon EC2 keine ausreichende `m5.24xlarge`-Kapazität hat, erstellt die Flotte Kapazitätsreservierungen für `m5.16xlarge`.

Instance-Typ-Gewichtung

Die Instance-Typ-Gewichtung ist eine Gewichtung, die Sie jedem Instance-Typ in der Kapazitätsreservierungsflotte zuweisen. Die Gewichtung bestimmt, wie viele Kapazitätseinheiten jede Instance des jeweiligen Instance-Typs der Gesamtzielkapazität der Flotte anrechnet.

Sie können Gewichtungen basierend auf sinnvollen Einheiten für Ihre Workload zuweisen. Wenn Ihre Workload beispielsweise eine bestimmte Anzahl von vCPUs erfordert, können Sie Gewichtungen basierend auf der Anzahl von vCPUs zuweisen, die von jedem Instance-Typ in der Kapazitätsreservierungsflotte bereitgestellt werden. Wenn Sie in diesem Fall eine Kapazitätsreservierungsflotte mit `m4.16xlarge`- und `m5.24xlarge`-Instances erstellen, würden Sie Gewichtungen zuweisen, die der Anzahl von vCPUs für jede Instance entsprechen:

- `m4.16xlarge` – 64 vCPUs, Gewichtung = 64 Einheiten
- `m5.24xlarge` – 96 vCPUs, Gewichtung = 96 Einheiten

Die Instance-Typ-Gewichtung bestimmt die Anzahl der Instances, für die die Kapazitätsreservierungsflotte Kapazität reserviert. Wenn eine Kapazitätsreservierungsflotte mit einer Gesamtzielkapazität von 384 Einheiten beispielsweise die Instance-Typen und Gewichtungen aus dem vorhergehenden Beispiel verwendet, könnte die Flotte Kapazität für 6 `m4.16xlarge`-Instances reservieren (384 Gesamtzielkapazität / 64 Instance-Typ-Gewichtung = 6 Instances) oder 4 `m5.24xlarge`-Instances (384 / 96 = 4).

Weisen Sie keine Instance-Typ-Gewichtungen oder eine Gewichtung von 1 zu, basiert die Gesamtzielkapazität ausschließlich auf der Anzahl der Instances. Wenn eine Kapazitätsreservierungsflotte mit einer Gesamtzielkapazität von 384 Einheiten beispielsweise die Instance-Typen aus dem vorhergehenden Beispiel verwendet, aber die Gewichtungen weglässt oder eine Gewichtung von 1 für beide Instance-Typen angibt, könnte die Flotte Kapazität für 384 `m4.16xlarge`- oder 384 `m5.24xlarge`-Instances reservieren.

Instance-Typ-Priorität

Die Instance-Typ-Priorität ist ein Wert, den Sie den Instance-Typen in der Flotte zuweisen. Anhand der Prioritäten wird bestimmt, welcher der für die Flotte angegebenen Instance-Typen für die Verwendung priorisiert werden soll.

Niedrigere Prioritätswerte bedeuten eine höhere Priorität für die Verwendung.

Arbeiten mit Kapazitätsreservierungsflotten

Themen

Bevor Sie beginnen

Bevor Sie eine Kapazitätsreservierungsflotte erstellen:

1. Bestimmen Sie die Höhe der Rechenkapazität, die Ihre Workload erfordert.
2. Legen Sie die zu verwendenden Instance-Typen und Availability Zones fest.
3. Weisen Sie jedem Instance-Typ eine Priorität zu, die auf Ihren Anforderungen und Einstellungen basiert. Weitere Informationen finden Sie unter Instance-Typ-Priorität.
4. Erstellen Sie ein für Ihre Workload sinnvolles Kapazitätsgewichtungssystem. Weisen Sie jedem Instance-Typ eine Gewichtung zu und bestimmen Sie die Gesamtzielkapazität. Weitere Informationen finden Sie unter Instance-Typ-Gewichtung und Gesamtzielkapazität.
5. Bestimmen Sie, ob Sie die Kapazitätsreservierung auf unbestimmte Zeit oder nur für einen bestimmten Zeitraum benötigen.

Zustände von Kapazitätsreservierungsflotten

Eine Kapazitätsreservierungsflotte kann sich in einem der folgenden Zustände befinden:

- `submitted` – die Anforderung für die Kapazitätsreservierungsflotte wurde übermittelt und Amazon EC2 bereitet sich auf die Erstellung der Kapazitätsreservierungen vor.
- `modifying` – die Kapazitätsreservierungsflotte wird gerade geändert. Die Flotte bleibt in diesem Zustand, bis die Änderung abgeschlossen ist.

- `active` – die Kapazitätsreservierungsflotte hat ihre Gesamtzielkapazität erreicht und versucht, diese Kapazität beizubehalten. Die Flotte bleibt so lange in diesem Zustand, bis sie geändert oder gelöscht wird.
- `partially_fulfilled` – die Kapazitätsreservierungsflotte hat ihre Gesamtzielkapazität teilweise erfüllt. Es ist nicht genügend Amazon-EC2-Kapazität vorhanden, um die Gesamtzielkapazität zu erfüllen. Die Flotte versucht, ihre Gesamtzielkapazität asynchron zu erfüllen.
- `expiring` – die Kapazitätsreservierungsflotte hat ihr Enddatum erreicht und läuft gerade ab. Eine oder mehrere ihrer Kapazitätsreservierungen sind möglicherweise noch aktiv.
- `expired` – die Kapazitätsreservierungsflotte hat ihr Enddatum erreicht. Die Flotte und ihre Kapazitätsreservierungen sind abgelaufen. Die Flotte kann keine neuen Kapazitätsreservierungen erstellen.
- `cancelling` – die Kapazitätsreservierungsflotte wird gerade storniert. Eine oder mehrere ihrer Kapazitätsreservierungen sind möglicherweise noch aktiv.
- `cancelled` – die Kapazitätsreservierungsflotte wurde manuell storniert. Die Flotte und ihre Kapazitätsreservierungen wurden storniert und die Flotte kann keine neuen Kapazitätsreservierungen erstellen.
- `failed` – die Kapazitätsreservierungsflotte konnte die Kapazität für die angegebenen Instance-Typen nicht reservieren.

Erstellen einer Kapazitätsreservierungsflotte

Wenn Sie eine Kapazitätsreservierungsflotte erstellen, werden für die in der Flottenanforderung angegebenen Instance-Typen automatisch Kapazitätsreservierungen bis zur angegebenen Gesamtzielkapazität erstellt. Die Anzahl der Instances, für die die Kapazitätsreservierungsflotte Kapazität reserviert, hängt von der Gesamtzielkapazität und den Instance-Typ-Gewichtungen ab, die Sie in der Anforderung angeben. Weitere Informationen finden Sie unter Instance-Typ-Gewichtung und Gesamtzielkapazität.

Wenn Sie die Flotte erstellen, müssen Sie die zu verwendenden Instance-Typen und eine Priorität für jeden dieser Instance-Typen angeben. Weitere Informationen finden Sie unter Zuweisungsstrategie und Instance-Typ-Priorität.

> **Note**
>
> Die mit dem AWSServiceRoleForEC2CapacityReservationFleetService verknüpfte Rolle wird automatisch in Ihrem Konto erstellt, wenn Sie zum ersten Mal eine Flotte für

Kapazitätsreservierungen erstellen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Kapazitätsreservierungsflotten.

Derzeit unterstützen Kapazitätsreservierungsflotten nur die Übereinstimmungskriterien für open-Instances.

Sie können Kapazitätsreservierungsflotten nur über die Befehlszeile erstellen.

Kapazitätsreservierungsflotte erstellen

Verwenden Sie den Befehl AWS CLI create-capacity-reservation-fleet.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity capacity_units \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy dedicated|default \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

Im Folgenden sehen Sie den Inhalt von `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "instance_type",
        "InstancePlatform":"platform",
        "Weight": instance_type_weight,
        "AvailabilityZone":"availability_zone",
        "AvailabilityZoneId" : "az_id",
        "EbsOptimized": true|false,
        "Priority" : instance_type_priority
    }
]
```

Erwartete Ausgabe.

```
{
    "Status": "status",
    "TotalFulfilledCapacity": fulfilled_capacity,
    "CapacityReservationFleetId": "cr_fleet_id",
    "TotalTargetCapacity": capacity_units
```

```
}
```

Beispiel

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 24 \
--allocation-strategy prioritized \
--instance-match-criteria open \
--tenancy default \
--end-date 2021-12-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

`instanceTypeSpecification.json`

```
[
  {
    "InstanceType": "m5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "Weight": 3.0,
    "AvailabilityZone":"us-east-1a",
    "EbsOptimized": true,
    "Priority" : 1
  }
]
```

Beispielausgabe.

```
{
    "Status": "submitted",
    "TotalFulfilledCapacity": 0.0,
    "CapacityReservationFleetId": "crf-abcdef01234567890",
    "TotalTargetCapacity": 24
}
```

Anzeigen einer Kapazitätsreservierungsflotte

Sie können jederzeit Konfigurations- und Kapazitätsinformationen für eine Kapazitätsreservierungsflotte anzeigen. Beim Aufrufen einer Flotte werden auch Details zu den einzelnen Kapazitätsreservierungen angezeigt, die sich innerhalb der Flotte befinden.

Sie können Kapazitätsreservierungsflotten nur über die Befehlszeile anzeigen.

Kapazitätsreservierungsflotte anzeigen

Verwenden Sie den AWS CLI Befehl describe-capacity-reservation-fleets.

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Erwartete Ausgabe

```
{
    "CapacityReservationFleets": [
        {
            "Status": "status",
            "EndDate": "yyyy-mm-ddThh:mm:ss.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "cr_fleet_id",
            "Tenancy": "dedicated|default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr1_id",
                    "AvailabilityZone": "cr1_availability_zone",
                    "FulfilledCapacity": cr1_used_capacity,
                    "Weight": cr1_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr1_platform",
                    "TotalInstanceCount": cr1_number of instances,
                    "Priority": cr1_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr1_instance_type"
                },
    {
                    "CapacityReservationId": "cr2_id",
                    "AvailabilityZone": "cr2_availability_zone",
                    "FulfilledCapacity": cr2_used_capacity,
                    "Weight": cr2_instance_type_weight,
                    "CreateDate": "yyyy-mm-ddThh:mm:ss.000Z",
                    "InstancePlatform": "cr2_platform",
                    "TotalInstanceCount": cr2_number of instances,
                    "Priority": cr2_instance_type_priority,
                    "EbsOptimized": true|false,
                    "InstanceType": "cr2_instance_type"
                },
```

```
            ],
            "TotalTargetCapacity": total_target_capacity,
            "TotalFulfilledCapacity": total_target_capacity,
            "CreateTime": "yyyy-mm-ddThh:mm:ss.000Z",
            "AllocationStrategy": "prioritized"
        }
    ]
}
```

Beispiel

```
aws ec2 describe-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Beispielausgabe

```
{
    "CapacityReservationFleets": [
        {
            "Status": "active",
            "EndDate": "2021-12-31T23:59:59.000Z",
            "InstanceMatchCriteria": "open",
            "Tags": [],
            "CapacityReservationFleetId": "crf-abcdef01234567890",
            "Tenancy": "default",
            "InstanceTypeSpecifications": [
                {
                    "CapacityReservationId": "cr-1234567890abcdef0",
                    "AvailabilityZone": "us-east-1a",
                    "FulfilledCapacity": 5.0,
                    "Weight": 1.0,
                    "CreateDate": "2021-07-02T08:34:33.398Z",
                    "InstancePlatform": "Linux/UNIX",
                    "TotalInstanceCount": 5,
                    "Priority": 1,
                    "EbsOptimized": true,
                    "InstanceType": "m5.xlarge"
                }
            ],
            "TotalTargetCapacity": 5,
            "TotalFulfilledCapacity": 5.0,
            "CreateTime": "2021-07-02T08:34:33.397Z",
            "AllocationStrategy": "prioritized"
```

```
        }
    ]
}
```

Ändern einer Kapazitätsreservierungsflotte

Sie können die Gesamtzielkapazität und das Datum einer Kapazitätsreservierungsflotte jederzeit ändern. Wenn Sie die Gesamtzielkapazität einer Kapazitätsreservierungsflotte ändern, erstellt die Flotte automatisch neue Kapazitätsreservierungen oder ändert bzw. storniert bestehende Kapazitätsreservierungen in der Flotte, um die neue Gesamtzielkapazität zu erreichen. Wenn Sie das Enddatum für die Flotte ändern, werden die Enddaten für alle einzelnen Kapazitätsreservierungen entsprechend angepasst.

Nachdem Sie eine Flotte geändert haben, wechselt ihr Zustand zu `modifying`. Sie können keine zusätzlichen Änderungen an einer Flotte vornehmen, wenn sie sich im Zustand `modifying` befindet.

Sie können keine Änderungen bezüglich Tenancy, Availability Zone, Instance-Typen, Instance-Plattformen, Prioritäten oder Gewichtungen vornehmen, die von einer Kapazitätsreservierungsflotte verwendet werden. Wenn Sie einen dieser Parameter ändern möchten, müssen Sie die vorhandene Flotte stornieren und eine neue Flotte mit den erforderlichen Parametern erstellen.

Sie können Kapazitätsreservierungsflotten nur über die Befehlszeile ändern.

Kapazitätsreservierungsflotte ändern

Verwenden Sie den AWS CLI Befehl modify-capacity-reservation-fleet.

> **Note**
>
> Sie können `--end-date` und `--remove-end-date` nicht im selben Befehl angeben.

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id cr_fleet_ids \
--total-target-capacity capacity_units \
--end-date yyyy-mm-ddThh:mm:ss.000Z \
--remove-end-date
```

Erwartete Ausgabe

```
{
    "Return": true
}
```

Beispiel: Gesamtzielkapazität ändern

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--total-target-capacity 160
```

Beispiel: Enddatum ändern

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--end-date 2021-07-04T23:59:59.000Z
```

Beispiel: Enddatum entfernen

```
aws ec2 modify-capacity-reservation-fleet \
--capacity-reservation-fleet-id crf-01234567890abcedf \
--remove-end-date
```

Beispielausgabe

```
{
    "Return": true
}
```

Stornieren einer Kapazitätsreservierungsflotte

Wenn Sie eine Kapazitätsreservierungsflotte und die reservierte Kapazität nicht mehr benötigen, können Sie die Flotte stornieren. Wenn Sie eine Flotte stornieren, ändert sich ihr Zustand in `cancelled` und sie kann keine neuen Kapazitätsreservierungen mehr erstellen. Außerdem werden alle individuellen Kapazitätsreservierungen in der Flotte storniert und die Instances, die zuvor in der reservierten Kapazität ausgeführt wurden, werden mit gemeinsam genutzter Kapazität weiter ausgeführt.

Sie können Kapazitätsreservierungsflotten nur über die Befehlszeile stornieren.

Kapazitätsreservierungsflotte stornieren

Verwenden Sie den AWS CLI Befehl cancel-capacity-reservation-fleet.

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids cr_fleet_ids
```

Erwartete Ausgabe

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_1"
        },
        {
            "CurrentFleetState": "state",
            "PreviousFleetState": "state",
            "CapacityReservationFleetId": "cr_fleet_id_2"
        }
    ],
    "FailedFleetCancellations": [
        {
         "CapacityReservationFleetId": "cr_fleet_id_3",
         "CancelCapacityReservationFleetError": [
             {
              "Code": "code",
                    "Message": "message"
          }
         ]
     }
    ]
}
```

Beispiel: Erfolgreiche Stornierung

```
aws ec2 cancel-capacity-reservation-fleets \
--capacity-reservation-fleet-ids crf-abcdef01234567890
```

Beispielausgabe

```
{
    "SuccessfulFleetCancellations": [
        {
            "CurrentFleetState": "cancelling",
            "PreviousFleetState": "active",
            "CapacityReservationFleetId": "crf-abcdef01234567890"
        }
    ],
    "FailedFleetCancellations": []
}
```

Beispiel für Kapazitätsreservierungsflotten-Konfigurationen

Themen

- Beispiel 1: Kapazität basierend auf vCPUs reservieren

Beispiel 1: Kapazität basierend auf vCPUs reservieren

Im folgenden Beispiel wird eine Kapazitätsreservierungsflotte erstellt, die zwei Instance-Typen verwendet: `m5.4xlarge` und `m5.12xlarge`.

Sie verwendet ein Gewichtungssystem, das auf der Anzahl der vCPUs basiert, die von den angegebenen Instance-Typen bereitgestellt werden. Die Gesamtzielkapazität beträgt `480` vCPUs. `m5.4xlarge` stellt 16 vCPUs bereit und erhält eine Gewichtung von 16, `m5.12xlarge` stellt 48 vCPUs bereit und erhält eine Gewichtung von `48`. Mit diesem Gewichtungssystem wird die Kapazitätsreservierungsflotte dafür konfiguriert, Kapazität für 30 `m5.4xlarge`-Instances (480 / 16 = 30) oder 10 `m5.12xlarge`-Instances (480 / 48 = 10) zu reservieren.

Gemäß der Flottenkonfiguration wird die `m5.12xlarge`-Kapazität priorisiert und erhält die Priorität 1. Der `m5.4xlarge`-Instance hingegen wird eine niedrigere Priorität zugeteilt: 2. Die Flotte wird demnach zuerst versuchen, die `m5.12xlarge`-Kapazität zu reservieren. Nur wenn Amazon EC2 nicht genügend `m5.12xlarge`-Kapazität hat, versucht sie, die `m5.4xlarge`-Kapazität zu reservieren.

Die Flotte reserviert die Kapazität für `Windows`-Instances und die Reservierung läuft automatisch am `October 31, 2021` um`23:59:59` UTC ab.

```
aws ec2 create-capacity-reservation-fleet \
--total-target-capacity 480 \
--allocation-strategy prioritized \
```

```
--instance-match-criteria open \
--tenancy default \
--end-date 2021-10-31T23:59:59.000Z \
--instance-type-specifications file://instanceTypeSpecification.json
```

Im Folgenden sehen Sie den Inhalt von `instanceTypeSpecification.json`.

```
[
    {
        "InstanceType": "m5.4xlarge",
        "InstancePlatform":"Windows",
        "Weight": 16,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 2
    },
    {
        "InstanceType": "m5.12xlarge",
        "InstancePlatform":"Windows",
        "Weight": 48,
        "AvailabilityZone":"us-east-1a",
        "EbsOptimized": true,
        "Priority" : 1
 }
]
```

Verwenden von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Die On-Demand-Flotte für Kapazitätsreservierungen verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine spezielle IAM-Rolle, die direkt mit Kapazitätsreservierungsflotten verknüpft ist. Servicebezogene Rollen sind von Capacity Reservation Fleet vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Kapazitätsreservierungsflotten, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Kapazitätsreservierungsflotten definieren die Berechtigungen ihrer serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, können die Rollen nur von der jeweiligen Kapazitätsreservierungsflotte übernommen werden. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Kapazitätsreservierungsflotten-Ressourcen, da Sie die Berechtigung für den Zugriff auf die Ressourcen nicht versehentlich entfernen können.

Berechtigungen von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Capacity Reservation Fleet verwendet die angegebene dienstbezogene Rolle, AWSServiceRoleForEC2CapacityReservationFleetum Kapazitätsreservierungen, die zuvor von einer Kapazitätsreservierungsflotte erstellt wurden, in Ihrem Namen zu erstellen, zu beschreiben, zu ändern und zu stornieren.

Die AWSServiceRoleForEC2CapacityReservationFleet dienstbezogene Rolle vertraut darauf, dass die folgende Entität die Rolle übernimmt:. `capacity-reservation-fleet.amazonaws.com`

Die Rolle verwendet die AWSEC2CapacityReservationFleetRolePolicyRichtlinie, die die folgenden Berechtigungen umfasst:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeCapacityReservations",
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateCapacityReservation",
                "ec2:CancelCapacityReservation",
                "ec2:ModifyCapacityReservation"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:CapacityReservationFleet": "arn:aws:ec2:*:*:capacity-
reservation-fleet/crf-*"
                }
```

```
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:capacity-reservation/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateCapacityReservation"
                }
            }
        }
    ]
}
```

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Berechtigungen für serviceverknüpfte Rollen im IAM-Benutzerhandbuch.

Erstellen von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie mithilfe des `create-capacity-reservation-fleet` AWS CLI Befehls oder der `CreateCapacityReservationFleet` API eine Flotte für Kapazitätsreservierungen erstellen, wird die mit dem Service verknüpfte Rolle automatisch für Sie erstellt.

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie eine Kapazitätsreservierungsflotte erstellen, erstellt die Kapazitätsreservierungsflotte wieder die serviceverknüpfte Rolle für Sie.

Bearbeiten von serviceverknüpften Rollen für Kapazitätsreservierungsflotten

Mit der Kapazitätsreservierungsflotte können Sie die AWSServiceRoleForEC2CapacityReservationFleet servicebezogene Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die

Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Kapazitätsreservierungsflotten

Wenn Sie ein Feature oder einen Service, die bzw. der eine servicegebundene Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle löschen, bevor Sie sie manuell löschen können.

> **Note**
>
> Falls der Kapazitätsreservierungsflotten-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt der Löschvorgang möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um die AWSServiceRoleForEC2CapacityReservationFleet serviceverknüpfte Rolle zu löschen

1. Verwenden Sie den `delete-capacity-reservation-fleet` AWS CLI Befehl oder die `DeleteCapacityReservationFleet` API, um die Kapazitätsreservierungsflotten in Ihrem Konto zu löschen.
2. Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSServiceRoleForEC2CapacityReservationFleet serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Unterstützte Regionen für serviceverknüpfte Rollen für Kapazitätsreservierungsflotten

Kapazitätsreservierungsflotten unterstützen die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter AWS -Regionen und Endpunkte.

Überwachung von Kapazitätsreservierungen

Sie können die folgenden Features zum Überwachen Ihrer Kapazitätsreservierungen verwenden:

Themen

- Überwachen Sie Kapazitätsreservierungen mithilfe von Metriken CloudWatch

- Überwachen Sie Kapazitätsreservierungen mit EventBridge
- Benachrichtigungen zur Auslastung

Überwachen Sie Kapazitätsreservierungen mithilfe von Metriken CloudWatch

Mithilfe von CloudWatch Metriken können Sie Ihre Kapazitätsreservierungen effizient überwachen und ungenutzte Kapazitäten identifizieren, indem Sie CloudWatch Alarme einrichten, die Sie benachrichtigen, wenn die Nutzungsgrenzwerte erreicht werden. Dies kann Ihnen helfen, ein konstantes Kapazitätsreservierung-Volumen beizubehalten und eine höhere Auslastung zu erreichen.

Kapazitätsreservierungen auf Abruf senden CloudWatch alle fünf Minuten Metrikdaten. Metriken für Kapazitätsreservierungen werden nicht unterstützt, die weniger als fünf Minuten aktiv sind.

Weitere Informationen zum Anzeigen von Metriken in der CloudWatch Konsole finden Sie unter Amazon CloudWatch Metrics verwenden. Weitere Informationen zum Erstellen von Alarmen finden Sie unter CloudWatch Amazon-Alarme erstellen.

Inhalt

- Kapazitätsreservierung-Nutzungsmetriken
- Kapazitätsreservierung-Metrikdimensionen
- CloudWatch Kennzahlen für Kapazitätsreservierungen anzeigen

Kapazitätsreservierung-Nutzungsmetriken

Der `AWS/EC2CapacityReservations`-Namespace enthält die folgenden Nutzungsmetriken, mit denen Sie On-Demand-Kapazität innerhalb von Schwellenwerten überwachen und verwalten können, die Sie für Ihre Reservierung angeben.

Metrik	Beschreibung
`UsedInstanceCount`	Die Anzahl der Instances, die derzeit verwendet werden. Einheit: Anzahl
`AvailableInstanceCount`	Die Anzahl der verfügbaren Instances.

Metrik	Beschreibung
	Einheit: Anzahl
`TotalInstanceCount`	Die Gesamtzahl der reservierten Instances. Einheit: Anzahl
`InstanceUtilization`	Der Prozentsatz der Instances für reservierte Kapazität, die derzeit verwendet werden. Einheit: Prozent

Kapazitätsreservierung-Metrikdimensionen

Sie können die folgenden Dimensionen verwenden, um die in den vorherigen Tabellen aufgeführten Metriken zu verfeinern.

Dimension	Beschreibung
`CapacityReservationId`	Diese global eindeutige Dimension filtert nur die Daten, die Sie für die identifizierte Kapazitätsreservierung anfordern.

CloudWatch Kennzahlen für Kapazitätsreservierungen anzeigen

Metriken werden zuerst nach dem Service-Namespace und dann nach den unterstützten Dimensionen gruppiert. Sie können die folgenden Vorgehensweisen nutzen, um die Metriken für Kapazitätsreservierungen anzuzeigen.

Um Metriken zur Kapazitätsreservierung über die CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Ändern Sie, falls erforderlich, die Region. Wählen Sie auf der Navigationsleiste die Region aus, in der sich Ihr Kapazitätsreservierung befindet. Weitere Informationen finden Sie unter -Regionen und Endpunkte.
3. Wählen Sie im Navigationsbereich Metrics aus.

4. Wählen Sie für Alle Metriken die Option EC2-Kapazitätsreservierungen aus.
5. Wählen Sie die Metrik-Dimension Nach Kapazitätsreservierung. Metriken werden gruppiert nach `CapacityReservationId`.
6. Verwenden Sie die Spaltenüberschrift, um die Metriken zu sortieren. Um eine Metrik grafisch darzustellen, müssen Sie das Kontrollkästchen neben der Metrik aktivieren.

Metriken für Kapazitätsreservierung anzeigen (AWS CLI)

Verwenden Sie den folgenden list-metrics-Befehl:

```
aws cloudwatch list-metrics --namespace "AWS/EC2CapacityReservations"
```

Überwachen Sie Kapazitätsreservierungen mit EventBridge

AWS Health sendet Ereignisse an Amazon, EventBridge wenn eine Kapazitätsreservierung in Ihrem Konto in bestimmten Zeiträumen unter 20 Prozent ausgelastet ist. Mit EventBridge können Sie Regeln festlegen, die als Reaktion auf solche Ereignisse programmatische Aktionen auslösen. Sie können beispielsweise eine Regel erstellen, die eine Kapazitätsreservierung automatisch aufhebt, wenn ihre Auslastung über einen Zeitraum von 7 Tagen unter 20 Prozent fällt.

Ereignisse in EventBridge werden als JSON-Objekte dargestellt. Die Felder, die für das Ereignis einzigartig sind, sind im Abschnitt "Detail" des JSON-Objekt enthalten. Im Feld "Ereignis" ist der Name des Ereignisses enthalten. Das Feld "Ergebnis" enthält den vollständigen Status der Aktion, die zur Auslösung des Ereignisses führte. Weitere Informationen finden Sie unter Amazon EventBridge Event Patterns im EventBridge Amazon-Benutzerhandbuch.

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Diese Funktion wird in nicht unterstützt AWS GovCloud (US).

Inhalt

Ereignisse

AWS Health sendet die folgenden Ereignisse, wenn die Kapazitätsnutzung für eine Kapazitätsreservierung unter 20 Prozent liegt.

Ereignisse

- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION
- AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das generiert wird, wenn eine neu erstellte Kapazitätsreservierung über einen Zeitraum von 24 Stunden unter 20 Prozent Kapazitätsauslastung liegt.


```
{
    "version": "0",
    "id": "b3e00086-f271-12a1-a36c-55e8ddaa130a",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-10T12:03:38Z",
    "region": "ap-south-1",
    "resources": [
        "cr-01234567890abcdef"
    ],
    "detail": {
        "eventArn": "arn:aws:health:ap-south-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_cr-01234567890abcdef-6211-4d50-9286-0c9fbc243f04",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION",
        "eventTypeCategory": "accountNotification",
        "startTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "endTime": "Fri, 10 Mar 2023 12:03:38 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef"
            }
        ]
    }
```

```
    }
```

AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das generiert wird, wenn eine oder mehrere Kapazitätsreservierungen über einen Zeitraum von 7 Tagen unter 20 Prozent Kapazitätsauslastung liegen.

```
{
    "version": "0", "id":"7439d42b-3c7f-ad50-6a88-25e2a70977e2",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-03-07T06:06:01Z",
    "region": "us-east-1",
    "resources": [
        "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/UNIX | 0.0%",
        "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/UNIX | 0.0%"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY/
AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY_726c1732-d6f6-4037-b9b8-
bec3c2d3ba65",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION_SUMMARY",
        "eventTypeCategory": "accountNotification",
        "startTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "endTime": "Tue, 7 Mar 2023 06:06:01 GMT",
        "eventDescription": [
            {
                "language": "en_US",
                "latestDescription": "A description of the event will be provided
 here"
            }
        ],
        "affectedEntities": [
            {
                "entityValue": "cr-01234567890abcdef | us-east-1b | t3.medium | Linux/
UNIX | 0.0%"
            },
            {
```

```
                "entityValue": "cr-09876543210fedcba | us-east-1a | t3.medium | Linux/
UNIX | 0.0%"
            }
        ]
    }
}
```

Erstellen Sie eine EventBridge Regel

Um E-Mail-Benachrichtigungen zu erhalten, wenn Ihre Kapazitätsreservierungsauslastung unter 20 Prozent fällt, erstellen Sie ein Amazon SNS SNS-Thema und dann eine EventBridge Regel für das `AWS_EC2_ODCR_UNDERUTILIZATION_NOTIFICATION` Ereignis.

So erstellen Sie das Amazon-SNS-Thema

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Topics (Themen) und Create topic (Thema erstellen).
3. Wählen Sie unter Type (Typ) die Option Standard aus.
4. Geben Sie unter Name einen Namen für das neue Thema ein.
5. Wählen Sie Thema erstellen aus.
6. Wählen Sie Create subscription (Abonnement erstellen) aus.
7. Wählen Sie für Protokoll die Option E-Mail aus und geben Sie dann für Endpunkt die E-Mail-Adresse ein, die die Benachrichtigungen erhält.
8. Wählen Sie Create subscription (Abonnement erstellen) aus.
9. Die oben eingegebene E-Mail-Adresse erhält eine E-Mail-Nachricht mit der folgenden Betreffzeile: `AWS Notification - Subscription Confirmation`. Befolgen Sie die Anweisungen, um Ihr Abonnement zu bestätigen.

Um die Regel zu erstellen EventBridge

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie im Navigationsbereich Rules (Regeln) und anschließend Create rule (Regel erstellen) aus.
3. Geben Sie unter Name einen Namen für die neue Regel ein.
4. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.

5. Wählen Sie Weiter aus.
6. Gehen Sie bei Ereignismuster wie folgt vor:
    a. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.
    b. Wählen Sie unter AWS -Service die Option AWS Health aus.
    c. Wählen Sie als Ereignistyp die Option Benachrichtigung über EC2-ODCR-Unterauslastung aus.
7. Wählen Sie Weiter aus.
8. Gehen Sie bei Ziel 1 wie folgt vor:
    a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.
    b. Für Select a target (Wählen Sie ein Ziel aus), wählen Sie SNS-Thema aus.
    c. Wählen Sie für Thema das Thema aus, das Sie zuvor erstellt haben.
9. Wählen Sie Weiter und dann erneut Weiter.
10. Wählen Sie Regel erstellen aus.

Benachrichtigungen zur Auslastung

AWS Health sendet die folgende E-Mail und AWS Health Dashboard Benachrichtigungen, wenn die Kapazitätsauslastung für Kapazitätsreservierungen in Ihrem Konto unter 20 Prozent fällt.

- Individuelle Benachrichtigungen für jede neu erstellte Kapazitätsreservierung, die in den letzten 24 Stunden weniger als 20 Prozent ausgelastet war.
- Eine zusammenfassende Benachrichtigung für alle Kapazitätsreservierungen, die in den letzten 7 Tagen weniger als 20 Prozent ausgelastet waren.

Die E-Mail-Benachrichtigungen und AWS Health Dashboard Benachrichtigungen werden an die E-Mail-Adresse gesendet, die mit dem AWS Konto verknüpft ist, dem die Kapazitätsreservierungen gehören. Die Benachrichtigungen enthalten die folgenden Informationen:

- Die ID der Kapazitätsreservierung.
- Die Availability Zone der Kapazitätsreservierung.
- Die durchschnittliche Nutzungsrate für die Kapazitätsreservierung.
- Der Instance-Typ und die Plattform (Betriebssystem) der Kapazitätsreservierung.

Wenn die Kapazitätsauslastung für eine Kapazitätsreservierung in Ihrem Konto innerhalb von 24 Stunden und 7 Tagen unter 20 Prozent fällt, werden außerdem Ereignisse AWS Health an EventBridge gesendet. Mit können Sie Regeln erstellen EventBridge, die automatische Aktionen wie das Senden von E-Mail-Benachrichtigungen oder das Auslösen von AWS Lambda Funktionen als Reaktion auf solche Ereignisse aktivieren. Weitere Informationen finden Sie unter Überwachen Sie Kapazitätsreservierungen mit EventBridge.

Kapazitätsblöcke für ML

Mit Kapazitätsblöcken für ML können Sie stark nachgefragte GPU-Instances zu einem späteren Zeitpunkt reservieren, um Ihre kurzzeitigen Machine Learning (ML)-Workloads zu unterstützen. Instances, die innerhalb eines Kapazitätsblocks ausgeführt werden, werden in Amazon EC2 automatisch nahe beieinander platziert UltraClusters, um blockierungsfreie Netzwerke im Petabit-Bereich mit niedriger Latenz zu gewährleisten.

Mit Kapazitätsblöcken können Sie sehen, wann GPU-Instance-Kapazität an zukünftigen Terminen verfügbar ist, und Sie können einen Kapazitätsblock so planen, dass er zu einem Zeitpunkt startet, der für Sie am besten passt. Wenn Sie einen Kapazitätsblock reservieren, erhalten Sie eine vorhersehbare Kapazitätsgarantie für GPU-Instance und zahlen nur für die Zeit, die Sie benötigen. Wir empfehlen Kapazitätsblöcke, wenn Sie für Ihre ML-Workloads tage- oder wochenlang GPUs benötigen und nicht für eine Reservierung zahlen möchten, während Ihre GPU-Instances nicht verwendet werden.

Im Folgenden sind einige häufige Anwendungsfälle für Kapazitätsblöcke aufgeführt.

- Modell-Training und Feinabstimmung für Machine Learning (ML) – Erhalten Sie ununterbrochenen Zugriff auf die GPU-Instances, die Sie für die Durchführung des ML-Modell-Trainings und der Feinabstimmung reserviert haben.
- ML-Experimente und Prototypen – Führen Sie Experimente durch und erstellen Sie Prototypen, die kurzfristig GPU-Instances erfordern.

Kapazitätsblöcke sind derzeit für Und-Instances verfügbar. `p5.48xlarge` `p4d.24xlarge` Die `p5.48xlarge` Instances sind in den Regionen USA Ost (Ohio) und USA Ost (Nord-Virginia) verfügbar. Die `p4d.24xlarge` Instances sind in den Regionen USA Ost (Ohio) und USA West (Oregon) verfügbar. Sie können einen Kapazitätsblock mit einem Reservierungsstartzeitpunkt bis zu acht Wochen in der Zukunft reservieren.

Sie können Capacity Blocks für Reservierungen p5 und p4d Instances mit den folgenden Optionen für Reservierungsdauer und Anzahl der Instanzen verwenden.

- Reservierungsdauer in Schritten von einem Tag bis zu insgesamt 14 Tagen
- Optionen für die Anzahl der Reservierungs-Instances: 1, 2, 4, 8, 16, 32 oder 64 Instances

Um einen Kapazitätsblock zu reservieren, geben Sie zunächst Ihren Kapazitätsbedarf an, einschließlich des Instance-Typs, der Anzahl der Instances, der Dauer, des frühesten Startdatums und des spätesten Enddatums, die Sie benötigen. Anschließend wird Ihnen ein verfügbares Kapazitätsblock-Angebot angezeigt, das Ihren Spezifikationen entspricht. Das Angebot für den Kapazitätsblock enthält Details wie Startzeit, Availability Zone und Reservierungspreis. Der Angebotspreis eines Kapazitätsblocks hängt vom verfügbaren Angebot und der Nachfrage zum Zeitpunkt der Bereitstellung des Angebots ab. Nach der Reservierung eines Kapazitätsblocks ändert sich der Preis nicht. Weitere Informationen finden Sie unter Preise und Fakturierung für Kapazitätsblöcke.

Wenn Sie ein Angebot für ein Kapazitätsblock erwerben, wird Ihre Reservierung für das von Ihnen ausgewählte Datum und die Anzahl der Instances erstellt. Wenn Ihre Kapazitätsblock-Reservierung beginnt, können Sie Instances gezielt starten, indem Sie die Reservierungs-ID in Ihren Startanfragen angeben.

Sie können alle von Ihnen reservierten Instances bis 30 Minuten vor dem Endzeitpunkt des Kapazitätsblocks nutzen. Wenn noch 30 Minuten in Ihrer Kapazitätsblock-Reservierung verbleiben, beginnen wir mit der Beendigung aller Instances, die in dem Kapazitätsblock ausgeführt werden. Wir nutzen diese Zeit zur Bereinigung Ihrer Instances, bevor wir den Kapazitätsblock dem nächsten Kunden bereitstellen. Die letzten 30 Minuten der Reservierung werden nicht im Preis des Kapazitätsblocks berechnet. Bis zu EventBridge 10 Minuten vor Beginn des Kündigungsvorgangs senden wir ein Ereignis aus. Weitere Informationen finden Sie unter Überwachen Sie Kapazitätsblöcke mit EventBridge.

Themen

- Überwachung von Kapazitätsblöcken

Unterstützte Plattformen

Derzeit werden Kapazitätsblöcke für ML `p5.48xlarge` und `p4d.24xlarge` Instances mit Standard-Tenancy unterstützt. Wenn Sie den AWS Management Console zum Kauf eines Capacity Blocks verwenden, ist die Standard-Plattformoption Linux/UNIX. Wenn Sie das AWS Command Line Interface (AWS CLI) oder AWS SDK zum Kauf eines Capacity Blocks verwenden, sind die folgenden Plattformoptionen verfügbar:

- Linux/Unix
- Red Hat Enterprise Linux
- RHEL mit HA
- SUSE Linux
- Ubuntu Pro

Überlegungen

Berücksichtigen Sie vor der Verwendung von Kapazitätsblöcken die folgenden Details und Einschränkungen.

- Kapazitätsblöcke beginnen und enden um 11:30 Uhr koordinierte Weltzeit (UTC).
- Der Beendigungsprozess für Instances, die in einem Kapazitätsblock ausgeführt werden, beginnt um 11:00 Uhr koordinierter Weltzeit (UTC) am letzten Tag der Reservierung.
- Kapazitätsblöcke können mit einer Startzeit bis zu 8 Wochen in der Zukunft reserviert werden.
- Änderungen und Stornierungen von Kapazitätsblöcken sind nicht zulässig.
- Kapazitätsblöcke können nicht zwischen AWS Konten oder innerhalb Ihrer AWS Organisation gemeinsam genutzt werden.
- Kapazitätsblöcke können nicht in einer Gruppe von Kapazitätsreservierungen verwendet werden.
- Die Gesamtzahl der Instanzen, die in Kapazitätsblöcken für alle Konten in Ihrer AWS Organisation reserviert werden können, darf an einem bestimmten Datum 64 Instanzen nicht überschreiten.
- Um einen Kapazitätsblock zu verwenden, müssen Instances gezielt die Reservierungs-ID verwenden.
- Instances in einem Kapazitätsblock werden nicht auf Ihre On-Demand-Instances angerechnet.

- Stellen Sie für P5-Instances, die ein benutzerdefiniertes AMI verwenden, sicher, dass Sie über die erforderliche Software und Konfiguration für EFA verfügen.
- Kapazitätsblöcke können derzeit nicht mit von Amazon EKS verwalteten Knotengruppen oder verwendet werdenKarpenter. Weitere Informationen zum Erstellen einer selbstverwalteten Amazon EKS-Knotengruppe finden Sie unter Capacity Blocks for ML im Amazon EKS-Benutzerhandbuch.

Zugehörige Ressourcen

Nachdem Sie einen Kapazitätsblock erstellt haben, können Sie mit dem Kapazitätsblock Folgendes tun:

- Starten Sie Instances im Capacity Block. Weitere Informationen finden Sie unter Starten von Instances in Kapazitätsblöcken.
- Erstellen Sie eine Amazon EC2 Auto Scaling Scaling-Gruppe. Weitere Informationen finden Sie unter Verwenden von Kapazitätsblöcken für Machine-Learning-Workloads im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

> **Note**
>
> Wenn Sie Amazon EC2 Auto Scaling oder Amazon EKS verwenden, können Sie die Skalierung so planen, dass sie zu Beginn der Kapazitätsblockreservierung ausgeführt wird. Bei der geplanten Skalierung werden Wiederholungsversuche AWS automatisch für Sie erledigt, sodass Sie sich keine Gedanken über die Implementierung der Wiederholungslogik für vorübergehende Ausfälle machen müssen.

- Verbessern Sie ML-Workflows mit. AWS ParallelCluster Weitere Informationen finden Sie unter Verbesserung von ML-Workflows mit AWS ParallelCluster und Amazon EC2 Capacity Blocks for ML.

Weitere Informationen zu finden Sie AWS ParallelCluster unter Was ist AWS ParallelCluster.

Preise und Fakturierung für Kapazitätsblöcke

Themen

- Preisgestaltung
- Fakturierung

Preisgestaltung

Mit Amazon-EC2-Kapazitätsblöcken für ML zahlen Sie nur für das, was Sie reservieren. Der Preis eines Kapazitätsblocks hängt vom verfügbaren Angebot und der verfügbaren Nachfrage für Kapazitätsblöcke zum Zeitpunkt des Kaufs ab. Sie können den Preis eines Kapazitätsblockangebots anzeigen, bevor Sie es reservieren. Der Preis für den Kapazitätsblocks wird zum Zeitpunkt der Reservierung im Voraus berechnet. Wenn Sie über einen Zeitraum hinweg nach einem Kapazitätsblock suchen, erhalten Sie von uns das günstigste verfügbare Kapazitätsblockangebot. Nachdem Sie einen Kapazitätsblock reserviert haben, ändert sich der Preis nicht.

Wenn Sie einen Kapazitätsblock verwenden, zahlen Sie für das Betriebssystem, das Sie nutzen, wenn Ihre Instances ausgeführt werden. Weitere Informationen zu den Preisen für Betriebssysteme finden Sie unter Amazon EC2 Capacity Blocks for ML Pricing.

Fakturierung

Der Preis für das Angebot eines Kapazitätsblocks wird im Voraus berechnet. Die Zahlung wird innerhalb von 12 Stunden nach dem Kauf eines Kapazitätsblocks über Ihr AWS -Konto abgerechnet. Während Ihre Zahlung bearbeitet wird, verbleibt die Ressource für Ihre Kapazitätsblock-Reservierung im Status `payment-pending`. Wenn Ihre Zahlung nicht innerhalb von 12 Stunden bearbeitet werden kann, wird Ihre Kapazitätssperre freigegeben und der Reservierungsstatus ändert sich in `payment-failed`.

Nachdem Ihre Zahlung erfolgreich verarbeitet wurde, ändert sich der Status der Kapazitätsblock-Ressource von `payment-pending` in `scheduled`. Sie erhalten eine Rechnung mit der einmaligen Vorauszahlung. Auf der Rechnung können Sie den gezahlten Betrag der Kapazitätsblock-Reservierungs-ID zuordnen.

Wenn Ihre Kapazitätsblock-Reservierung beginnt, erfolgt die Abrechnung nur auf Grundlage des Betriebssystems, das Sie verwenden, während Ihre Instances in der Reservierung ausgeführt werden. Sie können Ihre Nutzung und die damit verbundenen Gebühren in Ihrer Jubiläumsrechnung für den Nutzungsmonat in Ihrem AWS Cost and Usage Report anzeigen.

> **Note**
>
> Savings Plans und Rabatte für Reserved Instances gelten nicht für Kapazitätsblöcke.

Anzeigen Ihrer Rechnung

Sie können Ihre Rechnung in der AWS Billing and Cost Management Konsole einsehen. Die Vorauszahlung für Ihren Kapazitätsblock erfolgt in dem Monat, in dem Sie die Reservierung erworben haben.

Nachdem Ihre Reservierung begonnen hat, werden auf Ihrer Rechnung separate Zeilen für die genutzte und ungenutzte Zeit der Blockreservierung angezeigt. Anhand dieser Einzelposten können Sie sehen, wie viel Zeit für Ihre Reservierung aufgewendet wurde. Wenn Sie ein Premium-Betriebssystem nutzen, wird Ihnen in der Zeile für die genutzte Zeit nur eine Nutzungsgebühr angezeigt. Weitere Informationen finden Sie unter Preisgestaltung. Für nicht genutzte Zeit fallen keine zusätzlichen Gebühren an.

Weitere Informationen finden Sie unter Anzeigen Ihrer Rechnung im AWS Billing and Cost Management -Benutzerhandbuch.

Wenn Ihr Kapazitätsblock in einem anderen Monat beginnt als dem, in dem Sie Ihre Reservierung erworben haben, werden der Vorabpreis und die Reservierungsnutzung in separaten Abrechnungsmonaten angezeigt. In Ihrem AWS Cost and Usage Report ist die Reservierungs-ID für den Kapazitätsblock in der Reservation/ReservationARN-Position Ihrer Vorausgebühr und unter LineItem/ResourceID in Ihrer Jubiläumsrechnung aufgeführt, sodass Sie die Nutzung dem entsprechenden Vorabpreis zuordnen können.

Arbeiten mit Kapazitätsblöcken

Um mit der Nutzung von Kapazitätsblöcken zu beginnen, müssen Sie zunächst einen verfügbaren Kapazitätsblock finden und erwerben, der Ihrer Reservierungsgröße, -dauer und Ihren zeitlichen Anforderungen entspricht. Wenn die Reservierung dann beginnt, können Sie den Kapazitätsblock verwenden, indem Sie Instances starten, die für die Reservierungs-ID bestimmt sind. Dreißig Minuten vor Ablauf der Reservierung beginnen wir mit der Beendigung aller Instances, die noch im Kapazitätsblock ausgeführt werden.

Kapazitätsblöcke werden als `targeted`-Kapazitätsreservierungen in einer einzigen Availability Zone bereitgestellt. Um Instances in einem Kapazitätsblock auszuführen, müssen Sie beim Starten Ihrer Instances die Reservierungs-ID angeben. Wenn Sie Instances von sich aus anhalten und der Kapazitätsblock abläuft, können Sie sie erst wieder starten, wenn Sie einen anderen Kapazitätsblock im Status `active` als Ziel festlegen.

Standardmäßig stellen Kapazitätsblöcke Netzwerkkonnektivität mit geringer Latenz und hohem Durchsatz zwischen den Instances innerhalb des Kapazitätsblocks bereit, sodass keine Notwendigkeit besteht, eine Cluster-Placement-Gruppe mit einem Kapazitätsblock zu verwenden.

Themen

Voraussetzungen

Sie müssen den entsprechenden Instanztyp AWS-Region für den Instanztyp verwenden, den Sie verwenden möchten. Weitere Informationen finden Sie unter Regionen.

Kapazitätsblöcke mit `p5.48xlarge` Instanzen sind im Folgenden verfügbar AWS-Regionen.

Name der Region	Regionscode
USA Ost (Ohio)	us-east-2
USA Ost (Nord-Virginia)	us-east-1

Kapazitätsblöcke mit `p4d.24xlarge` Instanzen sind im Folgenden verfügbar AWS-Regionen.

Name der Region	Regionscode
USA Ost (Ohio)	us-east-2
USA West (Oregon)	us-west-2

> **Note**
>
> Kapazitätsblockgrößen von 64 Instances werden nicht für alle Instance-Typen insgesamt unterstützt AWS-Regionen.

Suchen und Erwerben von Kapazitätsblöcken

Um einen Kapazitätsblock zu reservieren, müssen Sie zunächst einen Zeitblock finden, in dem Kapazität verfügbar ist, der Ihren Anforderungen entspricht. Um nach einen Kapazitätsblock zu suchen, der reserviert werden kann, geben Sie Folgendes an.

- Die Anzahl der von Ihnen benötigten Instances
- Die Zeitdauer, für die Sie die Instances benötigen
- Der Zeitraum, in dem Sie Ihre Reservierung benötigen

Um nach einem verfügbaren Kapazitätsblock-Angebot zu suchen, geben Sie eine Reservierungsdauer und die Anzahl der Instances an. Sie müssen eine der folgenden Optionen auswählen.

- Für die Reservierungsdauer – bis zu 14 Tage in Schritten von 1 Tag
- Zum Beispiel die Anzahl der Instanzen — 1, 2, 4, 8, 16, 32 oder 64 Instanzen

Wenn ein Kapazitätsblock verfügbar ist, der Ihren Spezifikationen entspricht, geben wir die Details eines einzelnen Kapazitätsblock-Angebots zurück. Zu den Angebotsdetails gehören die Startzeit der Reservierung, die Availability Zone für die Reservierung und der Preis der Reservierung. Weitere Informationen finden Sie unter Preisgestaltung.

Sie können das angezeigte Kapazitätsblock-Angebot erwerben oder Ihre Suchkriterien ändern, um andere verfügbaren Optionen anzuzeigen. Es gibt keine vordefinierte Verfallszeit für das Angebot, die Angebote sind jedoch nur nach dem Prinzip „Wer zuerst kommt, wird zuerst bedient“ verfügbar.

Wenn Sie ein Kapazitätsblock-Angebot erwerben, erhalten Sie sofort eine Antwort, die bestätigt, dass Ihr Kapazitätsblock reserviert wurde. Nach der Bestätigung wird in Ihrem Konto eine neue Kapazitätsreservierung mit dem Reservierungstyp `capacity-block` und einem `start-date` angezeigt, das auf die Startzeit des von Ihnen erworbenen Angebots festgelegt ist. Ihre Kapazitätsblock-Reservierung wurde mit dem Status `payment-pending` erstellt. Nachdem die Vorauszahlung erfolgreich verarbeitet wurde, ändert sich der Reservierungsstatus in `scheduled`. Weitere Informationen finden Sie unter Fakturierung.

Sie können eine der folgenden Methoden nutzen, um nach einen Kapazitätsblock zu suchen und zu erwerben.

Console

So suchen und erwerben Sie einen Kapazitätsblock mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste oben auf dem Bildschirm eine aus AWS-Region. Diese Auswahl ist wichtig, da Kapazitätsblockgrößen von 64 Instances nicht für alle Instance-Typen in allen Regionen unterstützt werden.
3. Wählen Sie im Navigationsbereich Kapazitätsreservierungen und dann Kapazitätsblöcke kaufen aus.
4. Unter Kapazitätsattributen können Sie Ihre Kapazitätsblock-Suchparameter definieren. Standardmäßig ist die Plattform Linux. Wenn Sie ein anderes Betriebssystem auswählen möchten, verwenden Sie die AWS CLI. Weitere Informationen finden Sie unter Unterstützte Plattformen.
5. Wählen Sie unter Gesamtkapazität die Anzahl der Instances aus, die Sie reservieren möchten.
6. Geben Sie unter Dauer die Anzahl der Tage ein, für die Sie die Reservierung benötigen.
7. Geben Sie unter Zeitraum für die Suche nach Kapazitätsblöcken das frühestmögliche Startdatum und das späteste akzeptable Enddatum für Ihre Reservierung ein.
8. Wählen Sie Kapazitätsblöcke suchen.
9. Wenn ein Kapazitätsblock verfügbar ist, der Ihren Spezifikationen entspricht, wird unter Empfohlene Kapazitätsblöcke ein Angebot angezeigt. Wenn mehrere Angebote Ihren Spezifikationen entsprechen, wird das preisgünstigste verfügbare Kapazitätsblock-Angebot angezeigt. Um andere Kapazitätsblock-Angebote anzuzeigen, passen Sie Ihre Sucheingaben an und wählen Sie erneut Kapazitätsblöcke suchen.
10. Wenn Sie ein Kapazitätsblock-Angebot finden, das Sie erwerben möchten, wählen Sie Weiter.
11. (Optional) Wählen Sie auf der Seite Tags hinzufügen die Option Neues Tag hinzufügen aus.
12. Auf der Seite Überprüfen und Kaufen werden das Start- und Enddatum, die Dauer, die Gesamtzahl der Instances und der Preis aufgeführt.

> **Note**
>
> Kapazitätsblöcke können nach der Reservierung nicht mehr geändert oder storniert werden.

13. Geben Sie im Popup-Fenster Einen Kapazitätsblock kaufen Bestätigen ein und wählen Sie dann Kaufen aus.

AWS CLI

Um einen Kapazitätsblock mit dem zu finden AWS CLI

Verwenden Sie den `describe-capacity-block-offerings`-Befehl.

Im folgenden Beispiel wird nach einem Kapazitätsblock gesucht, der über 16 `p5.48xlarge`-Instances mit einem Datumsbereich vom `2023-08-14` bis zum `2023-10-22` und einer Dauer von 48 Stunden verfügt. Die Instance-Anzahl muss eine Ganzzahl aus einem vordefinierten Satz von Optionen sein: 1, 2, 4, 8, 16, 32, 64. Die Kapazitätsdauer muss eine Ganzzahl sein, die ein Vielfaches von 24 zwischen 24 und 336 ist und die Anzahl der Tage in Stunden angibt.

```
aws ec2 describe-capacity-block-offerings --instance-type p5.48xlarge \
  --instance-count 16 --start-date-range 2023-08-14T00:00:00Z \
  --end-date-range 2023-10-22-T00:00:00Z --capacity-duration 48
```

Um einen Capacity-Block zu kaufen, verwenden Sie AWS CLI

Verwenden Sie den `purchase-capacity-block`-Befehl und geben Sie die Angebots-ID des Kapazitätsblocks, den Sie erwerben möchten, sowie die Instance-Plattform an.

```
aws ec2 purchase-capacity-block \
  --capacity-block-offering-id cbr-0123456789abcdefg \
  --instance-platform Linux/UNIX
```

Starten von Instances in Kapazitätsblöcken

Nachdem Sie einen Kapazitätsblock reserviert haben, können Sie die Kapazitätsblock-Reservierung in Ihrem AWS -Konto anzeigen. Sie können das `start-date` und `end-date` anzeigen, um zu sehen, wann Ihre Reservierung beginnt und endet. Vor Beginn einer Kapazitätsblock-Reservierung wird die verfügbare Kapazität als Null angezeigt. Wie viele Instances in Ihrem Kapazitätsblock verfügbar sein werden, können Sie anhand des Tag-Werts für den Tag-Schlüssel `aws:ec2capacityreservation:incrementalRequestedQuantity` anzeigen.

Wenn eine Kapazitätsblock-Reservierung beginnt, ändert sich der Reservierungsstatus von `scheduled` zu `active`. Wir senden ein Ereignis über Amazon EventBridge, um Sie darüber zu

informieren, dass der Capacity Block zur Verwendung verfügbar ist. Weitere Informationen finden Sie unter Überwachung von Kapazitätsblöcken.

Um Ihren Kapazitätsblock zu verwenden, müssen Sie beim Starten von Instances die Kapazitätsblock-Reservierungs-ID angeben. Das Starten einer Instance in einem Kapazitätsblock verringert die verfügbare Kapazität um die Anzahl der gestarteten Instances. Wenn Ihre erworbene Instance-Kapazität beispielsweise acht Instances beträgt und Sie vier Instances starten, verringert sich die verfügbare Kapazität um vier.

Wenn Sie eine im Kapazitätsblock ausgeführte Instance beenden, bevor die Reservierung endet, können Sie an ihrer Stelle eine neue Instance starten. Wenn Sie eine Instance in einem Kapazitätsblock anhalten oder beenden, dauert die Bereinigung Ihrer Instance mehrere Minuten, bevor Sie eine andere Instance starten können, um sie zu ersetzen. Während dieser Zeit befindet sich Ihre Instance im Anhalte- oder `shutting-down`-Status. Nachdem dieser Vorgang abgeschlossen ist, ändert sich Ihr Instance-Status in `stopped` oder `terminated`. Anschließend wird die verfügbare Kapazität in Ihrem Kapazitätsblock aktualisiert, um eine weitere zur Verwendung verfügbare Instance anzuzeigen.

In den folgenden Schritten wird erklärt, wie Sie Instances in einem Capacity-Block starten`active`, der den AWS Management Console oder den verwendet AWS CLI.

Informationen zum Einrichten einer EKS-Knotengruppe für die automatische Verwendung eines Kapazitätsblocks zu Beginn finden Sie unter Kapazitätsblöcke für ML im Amazon-EKS-Benutzerhandbuch.

Informationen zum Starten von Instances in einem Kapazitätsblock unter Verwendung der EC2-Flotte finden Sie unter Tutorial: Starten von Instances in Kapazitätsblöcken.

Informationen zum Erstellen einer Startvorlage für einen Kapazitätsblock finden Sie unter Starten einer Instance über eine Startvorlage.

Sie können eine der folgenden Methoden zum Starten von Instances in einem Kapazitätsblock verwenden.

Console

So starten Sie eine Instance in einem Kapazitätsblock mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste am oberen Bildschirmrand die Region für Ihre Kapazitätsblock-Reservierung aus.

3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.
4. (Optional) Unter Name und Tags können Sie Ihrer Instance einen Namen geben und die Instance mit einem Tag versehen. Informationen zu Tags finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen)
5. Wählen Sie unter Anwendungs- und Betriebssystem-Images ein Amazon Machine Image (AMI) aus.
6. Wählen Sie unter Instance-Typ den Instance-Typ aus, der Ihrer Kapazitätsblock-Reservierung entspricht.
7. Wählen Sie unter Schlüsselpaar (Login) ein vorhandenes Schlüsselpaar aus oder wählen Sie Neues Schlüsselpaar erstellen, um ein neues zu erstellen. Weitere Informationen finden Sie unter Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances.
8. Verwenden Sie unter Network settings (Netzwerkeinstellungen) die Standardeinstellungen oder wählen Sie Edit (Bearbeiten), um die Netzwerkeinstellungen nach Bedarf zu konfigurieren.

   > **Important**
   >
   > Ihre Instance kann nicht in einem Subnetz in einer anderen Availability Zone als der Availability Zone gestartet werden, in der sich Ihr Kapazitätsblock befindet.

9. Konfigurieren Sie die Instance unter Erweiterte Details wie folgt.
   a. Wählen Sie unter Kaufoption (Markttyp) die Option Kapazitätsblöcke aus.
   b. Wählen Sie unter Kapazitätsreservierung die Option Nach ID festlegen aus.
   c. Wählen Sie die Kapazitätsreservierungs-ID Ihrer Kapazitätsblock-Reservierung aus.
10. Geben Sie im Bereich Summary (Zusammenfassung) für Number of Instances (Anzahl der Instances) die Anzahl der Instances ein, die gelauncht werden sollen.
11. Wählen Sie Launch Instance (Instance starten) aus.

AWS CLI

Um Instances in einem Capacity-Block zu starten, verwenden Sie AWS CLI

- Verwenden Sie den `run-instances`-Befehl und geben Sie ein `MarketType` von `capacity-block` in der `instance-market-options`-Struktur an. Sie müssen außerdem den Parameter `capacity-reservation-specification` angeben.

Das folgende Beispiel startet eine einzelne `p5.48xlarge`-Instance in einem aktiven Kapazitätsblock, der über übereinstimmende Attribute und verfügbare Kapazität verfügt.

```
aws ec2 run-instances --image-id ami-abc12345 --count 1 \
  --instance-type p5.48xlarge --key-name MyKeyPair \
  --subnet-id subnet-1234567890abcdef1 \
  --instance-market-options MarketType='capacity-block'
  --capacity-reservation-specification
 CapacityReservationTarget={CapacityReservationId=cr-a1234567}
```

Anzeigen von Kapazitätsblöcken

Kapazitätsblöcke weisen die folgenden Status auf:

- `payment-pending` – Die Vorauszahlung wurde noch nicht verarbeitet.
- `payment-failed` – Die Zahlung konnte nicht innerhalb des 12-Stunden-Zeitraums verarbeitet werden. Ihr Kapazitätsblock wurde veröffentlicht.
- `scheduled` – Die Zahlung wurde verarbeitet und die Kapazitätsblock-Reservierung hat noch nicht begonnen.
- `active` – Die reservierte Kapazität steht Ihnen zur Nutzung zur Verfügung.
- `expired` – Die Kapazitätsblock-Reservierung ist automatisch zu dem in Ihrer Reservierungsanfrage angegebenen Datum und der angegebenen Uhrzeit abgelaufen. Die reservierte Kapazität ist nicht mehr für Ihre Nutzung verfügbar.

Sie können Ihre Kapazitätsblock-Reservierung mit einer der folgenden Methoden anzeigen.

Console

So zeigen Sie Kapazitätsblöcke mithilfe der Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Kapazitätsreservierungen aus.
3. Auf der Übersichtsseite für Kapazitätsreservierungen sehen Sie eine Ressourcentabelle mit Details zu allen Ihren Ressourcen für Kapazitätsreservierungen. Um nach Ihren Kapazitätsblock-Reservierungen zu suchen, wählen Sie Kapazitätsblöcke aus der Dropdown-

Liste über der Kapazitätsreservierungs-ID aus. In der Tabelle können Sie Informationen zu Ihren Kapazitätsblöcken anzeigen, z. B. Start- und Enddatum, Dauer und Status.

4. Für weitere Details zu einem Kapazitätsblock wählen Sie die Reservierungs-ID für den Kapazitätsblock aus, den Sie anzeigen möchten. Auf der Seite mit den Details zur Kapazitätsreservierung werden alle Eigenschaften der Reservierung sowie die Anzahl der genutzten und im Kapazitätsblock verfügbaren Instances angezeigt.

> **Note**
>
> Vor Beginn einer Kapazitätsblock-Reservierung wird die verfügbare Kapazität als Null angezeigt. Die Anzahl der verfügbaren Instances bei Beginn der Kapazitätsblockreservierung kann mithilfe des folgenden Tag-Werts für den Tag-Schlüssel ermittelt werden: `aws:ec2capacityreservation:incrementalRequestedQuantity`.

AWS CLI

Um Kapazitätsblöcke anzuzeigen, verwenden Sie AWS CLI

Wenn Sie den Befehl describe-capacity-reservations verwenden, werden standardmäßig sowohl On-Demand-Kapazitätsreservierungen als auch Kapazitätsblock-Reservierungen aufgelistet. Um nur Ihre Kapazitätsblock-Reservierungen anzuzeigen, filtern Sie mithilfe von `capacity-block` nach dem `capacity-reservation-type`-Parameter.

Der folgende Befehl beschreibt beispielsweise eine oder mehrere Ihrer aktuellen Kapazitätsblock-Reservierungen AWS-Region.

```
aws ec2 describe-capacity-reservations -reservation-type capacity-block
```

Beispielausgabe.

```
{
    "CapacityReservations": [
        {
            "CapacityReservationId": "cr-12345678",
            "EndDateType": "limited",
            "ReservationType": "capacity-block"
            "AvailabilityZone": "eu-east-2a",
            "InstanceMatchCriteria": "targeted",
```

```
            "EphemeralStorage": false,
            "CreateDate": "2023-11-29T14:22:45Z",
            "StartDate": "2023-12-15T12:00:00Z",
            "EndDate": "2023-08-19T12:00:00Z",
            "AvailableInstanceCount": 0,
            "InstancePlatform": "Linux/UNIX",
            "TotalInstanceCount": 16,
            "State": "payment-pending",
            "Tenancy": "default",
            "EbsOptimized": true,
            "InstanceType": "p5.48xlarge"
        },
        ...
```

Überwachung von Kapazitätsblöcken

Themen

- Überwachen Sie Kapazitätsblöcke mit EventBridge
- Kapazität protokollieren Blockiert API-Aufrufe mit AWS CloudTrail

Überwachen Sie Kapazitätsblöcke mit EventBridge

Wenn Ihre Kapazitätsblock-Reservierung beginnt, sendet Amazon EC2 ein Ereignis EventBridge , das anzeigt, dass Ihre Kapazität einsatzbereit ist. Vierzig Minuten vor dem Ende Ihrer Capacity Block-Reservierung erhalten Sie ein weiteres EventBridge Ereignis, das Sie darüber informiert, dass alle Instances, die im Rahmen der Reservierung laufen, in 10 Minuten beendet werden. Weitere Informationen zu EventBridge Veranstaltungen finden Sie unter Amazon EventBridge Events.

Die folgenden Ereignisstrukturen für von Kapazitätsblöcken ausgegebene Ereignisse:

Kapazitätsblock bereitgestellt

Das folgende Beispiel zeigt ein Ereignis für Kapazitätsblock bereitgestellt.

```
{
  "customer_event_id": "[Capacity Reservation Id]-delivered",
  "detail_type": "Capacity Block Reservation Delivered",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
```

```
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Warnung vor Ablauf des Kapazitätsblocks

Das folgende Beispiel zeigt ein Ereignis für die Warnung Kapazitätsblockablauf.

```
{
  "customer_event_id": "[Capacity Reservation Id]-approaching-expiry",
  "detail_type": "Capacity Block Reservation Expiration Warning",
  "source": "aws.ec2",
  "account": "[Customer Account ID]",
  "time": "[Current time]",
  "resources": [
    "[ODCR ARN]"
  ],
  "detail": {
    "capacity-reservation-id": "[ODCR ID]",
    "end-date": "[ODCR End Date]"
  }
}
```

Kapazität protokollieren Blockiert API-Aufrufe mit AWS CloudTrail

Capacity Blocks ist in einen Dienst integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst in Capacity Blocks ausgeführt wurden. CloudTrail erfasst API-Aufrufe für Capacity Blocks als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Kapazitätsblocks-Konsole und Cdeaufrufe der Kapazitätsblocks-API-Operationen. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Bereitstellung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Kapazitätsblöcke. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf anzeigen. Anhand der von CloudTrail gesammelten Informationen können Sie die Anfrage an Capacity Blocks, die IP-Adresse, von der aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Details ermitteln.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Kapazität: Blockiert Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn Aktivitäten in Kapazitätsblöcken auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem System AWS-Konto, einschließlich der Ereignisse für Kapazitätsblöcke, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Übersicht zum Erstellen eines Trails
- CloudTrail unterstützte Dienste und Integrationen
- Konfigurieren von Amazon SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Capacity Blocks-Aktionen werden von der Amazon EC2 API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Beispielsweise generieren Aufrufe von und `CapacityBlockActive` Aktionen Einträge in den CloudTrail Protokolldateien. `CapacityBlockScheduled`

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie unter dem CloudTrail UserIdentity-Element.

Grundlegendes zu den Protokolldateieinträgen für Kapazitätsblöcke

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Die folgenden Beispiele zeigen CloudTrail Protokolleinträge für:

- TerminateCapacityBlocksInstances
- CapacityBlockPaymentFailed
- CapacityBlockGeplant
- CapacityBlockAktiv
- CapacityBlockGescheitert
- CapacityBlockAbgelaufen

> **Note**
>
> Aus Datenschutzgründen wurden einige Felder aus den Beispielen geschwärzt.

TerminateCapacityBlocksInstances


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "TerminateCapacityBlockInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
```

```
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:instance/
i-1234567890abcdef0"
    }
    {
      "accountId": "123456789012",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws::ec2:US East (N. Virginia):123456789012:instance/
i-0598c7d356eba48d7"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      }
}
```


CapacityBlockPaymentFailed


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockPaymentFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
```

```
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "payment-failed"
      }
}
```

CapacityBlockGeplant

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockScheduled",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
```

```
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "scheduled"
      }
}
```

CapacityBlockAktiv

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockActive",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "active"
      }
 }
```

CapacityBlockGescheitert


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockFailed",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "failed"
      }
 }
```


CapacityBlockAbgelaufen

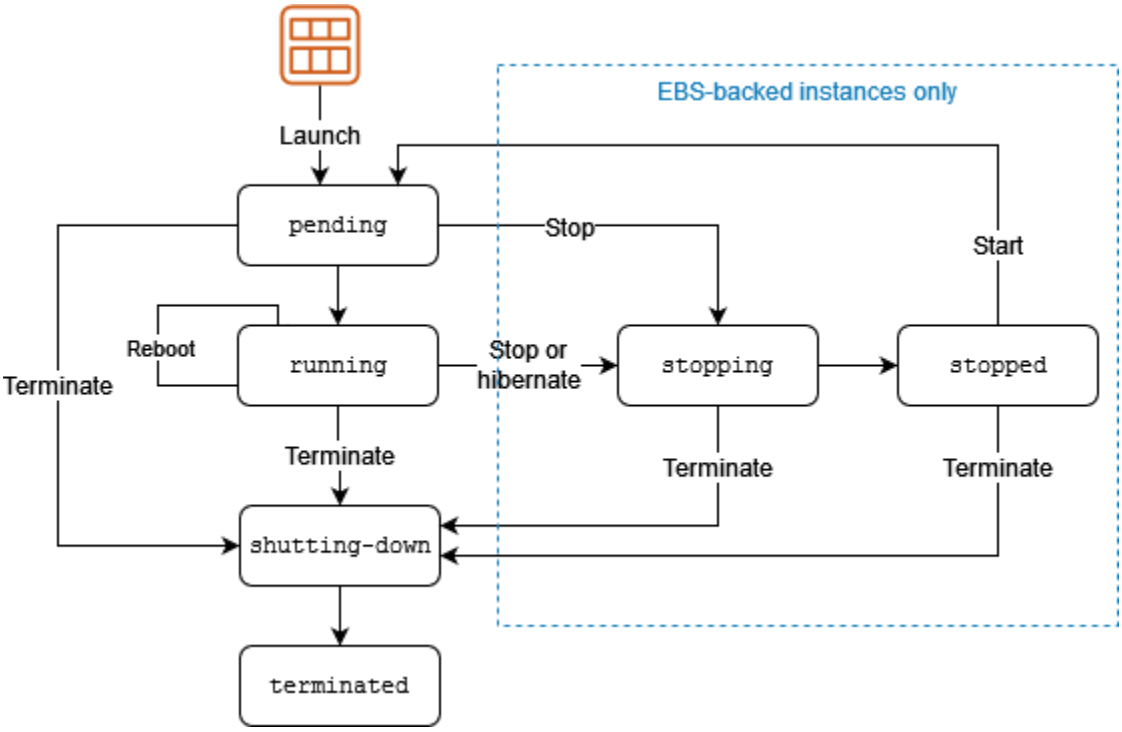

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "accountId": "123456789012",
    "invokedBy": "AWS Internal;"
  },
  "eventTime": "2023-10-02T00:06:08Z",
```

```
  "eventSource": "ec2.amazonaws.com",
  "eventName": "CapacityBlockExpired",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.25",
  "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
  "requestParameters": null,
  "responseElements": null,
  "eventID": "a1b2c3d4-EXAMPLE",
  "readOnly": false,
  "resources": [
    {
      "ARN": "arn:aws:ec2:US East (N. Virginia):123456789012:capacity-reservation/
cr-12345678",
      "accountId": "123456789012",
      "type": "AWS::EC2::CapacityReservation"
    }
  ],
  "eventType": "AwsServiceEvent",
  "recipientAccountId": "123456789012",
  "serviceEventDetails": {
      "capacityReservationId": "cr-12345678",
      "capacityReservationState": "expired"
      }
 }
```

Instance-Lebenszyklus

Eine Amazon EC2-Instance wechselt durch verschiedene Zustände von dem Zeitpunkt, an dem Sie sie starten, bis zu ihrer Beendigung.

In der folgenden Abbildung sind die Übergänge zwischen den Instances dargestellt. Beachten Sie, dass Sie eine Instance Store-Backed Instance nicht anhalten und starten können. Weitere Informationen zu Instance Store-Backed Instances erhalten Sie unter Speicher für das Root-Gerät.



Die folgende Tabelle enthält eine kurze Beschreibung der einzelnen Instance-Status und gibt an, ob die Instance-Nutzung in Rechnung gestellt wird. Für einige AWS Ressourcen, wie Amazon EBS-Volumes und Elastic IP-Adressen, fallen unabhängig vom Status der Instance Gebühren an. Weitere Informationen finden Sie unter Unerwartete Gebühren vermeiden im AWS Billing -Benutzerhandbuch.

Instance-Status	Beschreibung	Abrechnung für Instance-Nutzung
`pending`	Die Instance bereitet sich darauf vor, in den Status `running` überzugehen. Eine Instance wechselt in den Status `pending`, wenn sie gestartet wird oder wenn sie sich im Status `stopped` befand und dann gestartet wird.	Nicht berechnet

Instance-Status	Beschreibung	Abrechnung für Instance-Nutzung
running	Die Instance wird ausgeführt und ist bereit zur Nutzung.	Berechnet
stopping	Die Instance bereitet sich darauf vor, angehalten zu werden.	Nicht berechnet
stopped	Die Instance wird beendet und kann nicht genutzt werden. Die Instance kann jederzeit gestartet werden.	Nicht berechnet
shutting-down	Die Instance bereitet sich darauf vor, beendet zu werden.	Nicht berechnet
terminated	Die Instance wurde dauerhaft gelöscht und kann nicht gestartet werden.	Nicht berechnet **Note** Reserved Instances, die sich auf beendete Instances beziehen, werden bis zum Ende ihrer Laufzeit entsprechend ihrer Zahlungsoption abgerechnet. Weitere Informationen finden Sie unter Reserved Instances

Inhalt

- Unterschiede zwischen Neustart, Anhalten, Ruhezustand und Beenden
- Starten Ihrer Instance
- Beenden und starten Sie Amazon EC2 EC2-Instances
- Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand
- Durchführen eines Neustarts Ihrer Instance
- Amazon EC2 EC2-Instances beenden
- Ausmusterung einer Instance
- Resilienz der Instanz

Instance-Start

Wenn Sie eine Instance starten, erhält diese den Status `pending`. Der von Ihnen beim Start festgelegte Instance-Typ bestimmt die Hardware des Host-Computers für Ihre Instance. Um die Instance zu starten, verwenden wir das von Ihnen beim Start angegebene Amazon Machine Image (AMI). Wenn die Instance bereit ist, verfügt sie über den Status `running`. Sie können eine Verbindung mit Ihrer laufenden Instance herstellen und sie wie einen normalen Computer verwenden.

Sobald Ihre Instance in den Status `running` übergeht, wird Ihnen jede Sekunde (und mindestens eine Minute) der Betriebszeit der Instance in Rechnung gestellt, auch wenn sich die Instance im Leerlauf befindet und Sie keine Verbindung zu ihr herstellen.

Anhalten und Starten der Instance (nur Amazon EBS-gestützte Instances)

Wenn eine Statusprüfung Ihrer Instance fehlschlägt oder Ihre Anwendungen auf der Instance nicht wie erwartet ausgeführt werden und wenn das Stamm-Volume Ihrer Instance ein Amazon EBS-Volume ist, können Sie Ihre Instance anhalten und starten, um das Problem zu beheben.

Wenn Sie Ihre Instance anhalten, wird sie zunächst in den Status the `stopping` und anschließend in den Status `stopped` versetzt. Wenn Ihre Instance `stopped` ist, werden Ihnen keine Nutzungs- oder Datenübertragungsgebühren berechnet. Für die Speicherung etwaiger Amazon-EBS-Volumes fallen Gebühren an. Während sich die Instance im Status `stopped` befindet, können Sie bestimmte Attribute der Instance ändern, z. B. auch den Instance-Typ.

Wenn Sie Ihre Instance starten, wechselt sie in den `pending`-Status und wird auf einen neuen Host-Computer verschoben (in einigen Fällen verbleibt sie jedoch auf dem aktuellen Host). Wenn Sie Ihre Instance anhalten und starten, verlieren Sie alle Daten auf den Instance-Speicher-Volumes, die dem vorherigen Host-Computer angefügt waren.

Ihre Instance behält ihre private IPv4-Adresse, was bedeutet, dass eine Elastic-IP-Adresse, die der privaten IPv4-Adresse oder der Benutzeroberfläche zugeordnet ist, mit Ihrer Instance verbunden bleibt. Wenn Ihre Instance über eine IPv6-Adresse verfügt, behält sie die IPv6-Adresse bei.

Jedes Mal, wenn Sie eine Instance von `stopped` auf `running` umstellen, werden Ihnen Gebühren pro Sekunde bei Ausführung der Instance berechnet, mindestens jedoch eine Minute pro Instance-Start.

Weitere Informationen zum Anhalten und Starten von Instances finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.

Instance-Ruhezustand (nur durch Amazon EBS gesicherte Instances)

Wenn Sie eine Instance in den Ruhezustand versetzen, erhält das Betriebssystem ein Signal, die Instance in den Ruhezustand zu versetzen ("suspend-to-disk"). Hierdurch wird der Inhalt des Instance-Arbeitsspeichers (RAM) auf Ihrem Amazon EBS-Stamm-Volume gespeichert. Das Amazon EBS-Stamm-Volume der Instance und alle angefügten Amazon EBS-Daten-Volumens bleiben erhalten. Wenn Sie die Instance starten, wird das Amazon EBS-Stamm-Volume im vorherigen Zustand wiederhergestellt und der RAM-Inhalt wird neu geladen. Zuvor angefügte Daten-Volumes werden erneut zugewiesen und die Instance behält ihre Instance-ID bei.

Wenn Sie Ihre Instance in den Ruhezustand versetzen, wird sie zunächst in den Status the `stopping` und anschließend in den Status `stopped` versetzt. Wir berechnen keine Nutzung für eine im Ruhezustand befindliche Instance, wenn sie sich im Zustand `stopped` befindet. Während sie sich im Zustand `stopping` befindet wird jedoch eine Berechnung durchgeführt (im Gegensatz zum Anhalten einer Instance, ohne sie in den Ruhezustand zu versetzen). Wir stellen für die Datenübertragung keine Gebühren in Rechnung. Für Speicher für Amazon EBS-Volumes, einschließlich Speicher für den RAM-Daten, fallen jedoch Gebühren an.

Wenn Sie Ihre Instance im Ruhezustand starten, wird sie in den Zustand `pending` versetzt, und wir verschieben die Instance auf einen neuen Host-Computer (in einigen Fällen verbleibt sie jedoch auf dem aktuellen Host).

Ihre Instance behält ihre private IPv4-Adresse. Dies bedeutet, dass eine mit der privaten IPv4-Adresse oder Netzwerkschnittstelle verknüpfte Elastic IP-Adresse immer noch mit Ihrer Instance verknüpft ist. Wenn Ihre Instance über eine IPv6-Adresse verfügt, behält sie die IPv6-Adresse bei.

Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand.

Instance-Neustart

Sie können einen Neustart Ihrer Instance mit der Amazon EC2-Konsole, einem Befehlszeilen-Tool und der Amazon EC2-API durchführen. Wir empfehlen Ihnen, Amazon EC2 zum erneuten Starten Ihrer Instance zu verwenden, anstatt den Neustart-Befehl für das Betriebssystem auf Ihrer Instance auszuführen.

Ein Neustart einer Instance entspricht einem Neustart des Betriebssystems. Die Instance verbleibt auf demselben Host-Computer und behält ihren öffentlichen DNS-Namen, ihre private IP-Adresse sowie alle Daten auf ihren Instance-Speicher-Volumes. Es dauert i. d. R. einige Minuten, bis der Neustart abgeschlossen ist. Die Dauer des Neustarts hängt jedoch von der Konfiguration der Instance ab.

Beim Neustart einer Instance wird kein neuer Abrechnungszeitraum gestartet; es wird weiterhin sekundengenau und ohne weitere Mindestgebühr von einer Minute abgerechnet.

Weitere Informationen finden Sie unter Durchführen eines Neustarts Ihrer Instance.

Instance-Beendigung

Wenn Sie sich entschieden haben, dass Sie eine Instance nicht mehr benötigen, können Sie sie beenden. Sobald der Status einer Instance zu `shutting-down` oder `terminated` wechselt, fallen für diese Instance keine Gebühren mehr an.

Bei aktiviertem Beendigungsschutz können Sie die Instance nicht mithilfe der Konsole, der CLI oder der API beenden.

Nachdem Sie eine Instance beendet haben, bleibt sie in der Konsole noch für kurze Zeit sichtbar, bevor der Eintrag automatisch gelöscht wird. Sie können eine beendete Instance auch mithilfe der CLI und API beschreiben. Ressourcen (z. B. Tags (Markierungen)) werden nach und nach von der beendeten Instance getrennt, sodass sie nach kurzer Zeit auf der beendeten Instance ggf. nicht mehr sichtbar sind. Sie können keine Verbindung mehr mit einer beendeten Instance herstellen oder diese wiederherstellen.

Jede Amazon EBS-gestützte Instance unterstützt das `InstanceInitiatedShutdownBehavior` Attribut, das steuert, ob die Instance stoppt oder beendet wird, wenn Sie das Herunterfahren innerhalb der Instance selbst initiieren (z. B. mit dem shutdown Befehl unter Linux). Das Standardverhalten ist das Anhalten der Instance. Sie können die Einstellungen für dieses Attribut ändern, während die Instance in Betrieb oder angehalten ist.

Jedes Amazon EBS-Volume unterstützt das Attribut `DeleteOnTermination`. Hiermit wird gesteuert, ob das Volume gelöscht wird oder erhalten bleibt, wenn Sie die zugehörige Instance beenden. Standardmäßig wird der Root-Gerät-Volume gelöscht und alle anderen EBS-Volumes bleiben erhalten.

Weitere Informationen finden Sie unter Amazon EC2 EC2-Instances beenden.

Unterschiede zwischen Neustart, Anhalten, Ruhezustand und Beenden

In der folgenden Tabelle sind die wichtigsten Unterschiede zwischen Neustart, Anhalten, Ruhezustand und Beenden Ihrer Instance zusammengefasst.

Merkmal	Neustart	Anhalten/Starten (nur Amazon EBS-gestützte Instances)	Ruhezustand (nur durch Amazon EBS gesicherte Instances)	Beenden
Host-Computer	Die Instance verbleibt auf demselben Host-Computer.	Wir verschieben die Instance auf einen neuen Host-Computer (in einigen Fällen verbleibt sie jedoch auf dem aktuellen Host).	Wir verschieben die Instance auf einen neuen Host-Computer (in einigen Fällen verbleibt sie jedoch auf dem aktuellen Host).	Keine
Private und öffentliche IPv4-Adressen	Diese Adressen werden nicht geändert.	EC2-VPC: Die Instance behält ihre private IPv4-Adresse. Die Instance erhält nur dann eine neue öffentliche IPv4-Adresse, wenn sie über keine Elastic IP-Adresse verfügt. Diese ändert sich während des Anhalten-/	EC2-VPC: Die Instance behält ihre private IPv4-Adresse. Die Instance erhält nur dann eine neue öffentliche IPv4-Adresse, wenn sie über keine Elastic IP-Adresse verfügt. Diese ändert sich während des Anhalten-/Neustart-Vorgangs nicht.	Keine

Merkmal	Neustart	Anhalten/Starten (nur Amazon EBS-gestützte Instances)	Ruhezustand (nur durch Amazon EBS gesicherte Instances)	Beenden
		Neustart-Vorgangs nicht.		
Elastic IP-Adressen (IPv4)	Die Elastic IP-Adresse bleibt der Instance zugeordnet.	Die Elastic IP-Adresse bleibt der Instance zugeordnet.	Die Elastic IP-Adresse bleibt der Instance zugeordnet.	Die Zuordnung der Elastic IP-Adresse zur Instance wird aufgehoben.
IPv6-Adresse	Die Instance behält ihre IPv6-Adresse.	Die Instance behält ihre IPv6-Adresse.	Die Instance behält ihre IPv6-Adresse.	Keine
Instance-Speicher-Volumes	Die Daten bleiben erhalten.	Die Daten werden gelöscht.	Die Daten werden gelöscht.	Die Daten werden gelöscht.
Root-Gerät-Volume	Das Volume bleibt erhalten.	Das Volume bleibt erhalten.	Das Volume bleibt erhalten.	Das Volume wird standardmäßig gelöscht.
RAM (Inhalt des Speichers)	RAM wird gelöscht	RAM wird gelöscht	RAM wird in einer Datei auf dem Root-Volume gespeichert	RAM wird gelöscht

Merkmal	Neustart	Anhalten/Starten (nur Amazon EBS-gestützte Instances)	Ruhezustand (nur durch Amazon EBS gesicherte Instances)	Beenden
Fakturierung	Die Abrechnungszeit der Instance ändert sich nicht	Sobald der Status einer Instance zu wechselt, fallen für diese Instance keine Gebühren mehr a `stopping`. Bei jedem Übergang einer Instance von `stopped` zu `running` wird ein neuer Abrechnungszeitraum gestartet ; für jeden Start der Instance wird eine Mindestgebühr von einer Minute abgerechnet.	Ihnen werden Gebühren berechnet, während sich die Instance im Zustand `stopping` befindet. Es werden jedoch keine Gebühren berechnet, wenn sich die Instance im Zustand `stopped` befindet. Bei jedem Übergang einer Instance von `stopped` zu `running` wird ein neuer Abrechnungszeitraum gestartet ; für jeden Start der Instance wird eine Mindestgebühr von einer Minute abgerechnet.	Es fallen keine Gebühren mehr für eine Instance an, sobald sich ihr Status auf ändert `shutting-down`

Instance Store-Backed Instances werden durch den Befehl zum Herunterfahren des Betriebssystems immer beendet. Sie können steuern, ob Amazon EBS-gestützte Instances durch den Befehl zum Herunterfahren des Betriebssystems angehalten oder beendet werden sollen. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.

Starten Ihrer Instance

Eine Instanz ist ein virtueller Server in der AWS Cloud. Sie starten eine Instance von einem Amazon Machine Image (AMI) aus. Das AMI stellt das Betriebssystem, den Anwendungsserver und Anwendungen für Ihre Instance bereit.

Wenn Sie sich für registrieren AWS, können Sie Amazon EC2 kostenlos nutzen, indem Sie das AWS kostenlose Kontingent nutzen. Sie können das kostenlose Kontingent verwenden, um eine `t2.micro`-Instance 12 Monate lang kostenlos zu starten und zu verwenden (in Regionen, in denen `t2.micro` nicht verfügbar ist, können Sie eine `t3.micro`-Instance im Rahmen des kostenlosen Kontingents verwenden). Wenn Sie eine Instance starten, die nicht vom kostenlosen Kontingent abgedeckt ist, fallen die standardmäßigen Amazon EC2-Nutzungsgebühren für die Instance an. Weitere Informationen finden Sie unter Amazon EC2 – Preise.

Sie können eine Instance mithilfe der folgenden Methoden starten.

Art	Dokumentation
[Amazon EC2-Konsole] Verwenden Sie den Launch Instance Wizard zur Angabe der Startparameter.	Starten einer Instance mit dem alten Launch Instance Wizard
[Amazon EC2-Konsole] Erstellen Sie eine Startvorlage und starten Sie die Instance über die Startvorlage.	Starten einer Instance über eine Startvorlage
[Amazon EC2-Konsole] Verwenden Sie eine vorhandene Instance als Vorlage.	Starten einer Instance mit den Parametern einer vorhandenen Instance
[Amazon-EC2-Konsole] Verwenden Sie ein im AWS Marketplace erworbenes AMI.	Starten Sie eine AWS Marketplace Instanz
[AWS CLI] Verwenden Sie ein von Ihnen ausgewähltes AMI.	Verwenden von Amazon EC2 über die AWS -CLI
[AWS Tools for Windows PowerShell] Verwenden Sie ein von Ihnen ausgewähltes AMI.	Amazon EC2 von der AWS Tools for Windows PowerShell

Art	Dokumentation
[AWS CLI] Verwenden Sie eine EC2-Flotte, um Kapazitäten für verschiedene EC2-Instance-Typen und Availability Zones sowie für alle On-Demand-Instance-, Reserved-Instance- und Spot-Instance Kaufmodelle bereitzustellen.	EC2-Flotte
[AWS CloudFormation] Verwenden Sie eine AWS CloudFormation Vorlage, um eine Instanz anzugeben.	AWS::EC2::Instance im AWS CloudFormation - Benutzerhandbuch
[AWS SDK] Verwenden Sie ein sprachspezifisches AWS SDK, um eine Instanz zu starten.	AWS SDK for .NET AWS SDK for C++ AWS SDK for Go AWS SDK für Java AWS SDK für JavaScript AWS SDK for PHP V3 AWS SDK für Python AWS SDK for Ruby V3

Note

Um eine EC2-Instance in einem reinen IPv6-Subnetz zu starten, müssen Sie Instances verwenden, die auf dem Nitro-System basieren. AWS

Note

Beim Starten einer reinen IPv6-Instance ist es möglich, dass DHCPv6 die Instance möglicherweise nicht sofort mit dem IPv6-DNS-Nameserver versorgt. Während dieser

anfänglichen Verzögerung kann die Instance möglicherweise keine öffentlichen Domains auflösen.
Führen Sie für Instances, die unter Amazon Linux 2 laufen, wenn Sie die Datei /etc/resolv.conf sofort mit dem IPv6-DNS-Nameserver aktualisieren möchten, Folgendes beim Start aus: cloud-init-Direktive:

```
#cloud-config
bootcmd:
- /usr/bin/sed -i -E 's,^nameserver\s+[\.[:digit:]]+$,nameserver
 fd00:ec2::253,' /etc/resolv.conf
```

Eine andere Möglichkeit besteht darin, die Konfigurationsdatei zu ändern und Ihr AMI so neu zu gestalten, dass die Datei sofort beim Booten die IPv6-DNS-Nameserver-Adresse hat.

Wenn Sie die Instance starten, können Sie die Instance in einem Subnetz starten, das einer der folgenden Ressourcen zugeordnet ist:

- einer Availability Zone – diese Option ist die Standardeinstellung.
- einer lokalen Zone: Um eine Instance in einer Local Zone zu starten, müssen Sie sich bei der Local Zone anmelden und dann ein Subnetz in der Zone erstellen. Weitere Informationen finden Sie unter Erste Schritte mit Local Zones
- Eine Wavelength-Zone – Um eine Instance in einer Wavelength-Zone zu starten, müssen Sie sich für die Wavelength-Zone anmelden und dann ein Subnetz in der Zone erstellen. Informationen zum Starten einer Instance in einer Wellenlängenzone finden Sie unter Erste Schritte mit AWS Wavelength.
- einem Outpost –- um eine Instance in einem Outpost zu starten, müssen Sie einen Outpost erstellen. Informationen zum Erstellen eines Outposts finden Sie unter Erste Schritte mit AWS Outposts.

Nachdem Sie Ihre Instance gestartet haben, können Sie eine Verbindung zu ihr herstellen und sie verwenden. Zu Beginn lautet der Status der Instance `pending`. Wenn der Status der Instance `running` lautet, hat die Instance mit dem Hochfahren begonnen. Es kann möglicherweise kurz dauern, bis Sie eine Verbindung zur Instance herstellen können. Beachten Sie, dass der Start von Bare Metal-Instance-Typen möglicherweise länger dauern kann.

Die Instance erhält einen öffentlichen DNS-Namen, den Sie verwenden können, um über das Internet auf die Instance zuzugreifen. Außerdem erhält die Instance einen privaten DNS-Namen, den andere Instances innerhalb desselben VPC zum Herstellen der Verbindung zur Instance verwenden können.

Wenn Sie eine Instance nicht mehr benötigen, müssen Sie sie beenden. Weitere Informationen finden Sie unter Amazon EC2 EC2-Instances beenden.

Starten einer Instance mit dem neuen Launch Instance Wizard

Sie können eine Instance mit dem neuen Launch Instance Wizard starten. Der Launch Instance Wizard gibt alle Startparameter an, die zum Starten einer Instance erforderlich sind. Wenn der Launch Instance Wizard einen Standardwert bereitstellt, können Sie den Standardwert akzeptieren oder einen eigenen Wert angeben. Wenn Sie die Standardwerte akzeptieren, können Sie eine Instance starten, indem Sie nur ein Schlüsselpaar auswählen.

> **Important**
>
> Wenn Sie eine Instance starten, die nicht vom kostenlosen AWS -Kontingent abgedeckt ist, fallen für die Zeit, in der die Instance ausgeführt wird, Gebühren an, selbst wenn sie nicht genutzt wird.

Themen

Starten Sie schnell eine Instance

Gehen Sie folgendermaßen vor, um eine Instance zu Testzwecken schnell einzurichten. Sie wählen das Betriebssystem und Ihr Schlüsselpaar aus und akzeptieren die Standardwerte. Weitere Informationen zu allen Parametern im Launch Instance Wizard finden Sie unter Starten einer Instance mit definierten Parametern.

So starten Sie schnell eine Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. In der Navigationsleiste oben auf dem Bildschirm wird die aktuelle AWS Region angezeigt (z. B. USA Ost (Ohio)). Wählen Sie eine Region aus, in der die Instance gestartet werden soll. Die Auswahl ist wichtig, da nur bestimmte Amazon EC2-Ressourcen zwischen Regionen geteilt werden können. Weitere Informationen finden Sie unter Ressourcenstandorte.
3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.
4. (Optional) Geben Sie unter Name und Tags für Name einen beschreibenden Namen für Ihre Instance ein.
5. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) Quick Start und dann das Betriebssystem (OS) für Ihre Instance aus.
6. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
7. Wählen Sie in der Übersicht Launch instance (Instance starten) aus.

Starten einer Instance mit definierten Parametern

Mit Ausnahme des Schlüsselpaars stellt der Launch Instance Wizard Standardwerte für alle Parameter bereit. Sie können eine oder alle Standardeinstellungen akzeptieren oder eine Instance konfigurieren, indem Sie für jeden Parameter eigene Werte angeben. Die Parameter sind im Launch Instance Wizard gruppiert. Die folgenden Anweisungen führen Sie durch jede Parametergruppe.

Parameter für die Instance-Konfiguration

- Initiieren des Instance-Starts
- Name und Tags
- Anwendungs- und Betriebssystem-Images (Amazon Machine Image)
- Instance-Typ
- Schlüsselpaar (Anmeldung)
- Network settings (Netzwerkeinstellungen)
- Speicher konfigurieren
- Erweiterte Details
- Übersicht

Initiieren des Instance-Starts

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. In der Navigationsleiste oben auf dem Bildschirm wird die aktuelle AWS Region angezeigt (z. B. USA Ost (Ohio)). Wählen Sie eine Region aus, in der die Instance gestartet werden soll. Die Auswahl ist wichtig, da nur bestimmte Amazon EC2-Ressourcen zwischen Regionen geteilt werden können. Weitere Informationen finden Sie unter Ressourcenstandorte.
3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.

Name und Tags

Der Instance-Name ist ein Tag, wobei der Schlüssel Name ist und es sich bei dem Wert um den von Ihnen angegebenen Namen handelt. Sie können die Instance, Volumes und Netzwerkschnittstellen taggen. Bei Spot-Instances können Sie nur die Spot-Instance-Anforderung mit Tags (Markierungen) versehen. Informationen zu Tags siehe Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

Die Angabe eines Instance-Namens und zusätzlicher Tags ist optional.

- Geben Sie unter Name einen beschreibenden Namen für die Instance ein. Wenn Sie keinen Namen angeben, kann die Instance anhand der ID identifiziert werden, die beim Starten der Instance automatisch generiert wird.
- Wenn Sie zusätzliche Tags hinzufügen möchten, wählen Sie Add additional tags (Zusätzliche Tags hinzufügen) aus. Klicken Sie auf Tag hinzufügen, geben Sie dann einen Schlüssel und einen Wert ein und wählen Sie den Ressourcentyp aus, den Sie markieren möchten. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.

Anwendungs- und Betriebssystem-Images (Amazon Machine Image)

Ein Amazon Machine Image (AMI) enthält die Informationen, die zum Starten einer Instance erforderlich sind. Ein AMI kann beispielsweise die Software enthalten, die für die Funktion als Webserver erforderlich ist, z. B. Linux, Apache und Ihre Website.

Sie finden wie folgt ein passendes AMI. Bei jeder Option zum Aufrufen eines AMI können Sie Abbrechen (oben rechts) auswählen, um zum Launch Instance Wizard zurückzukehren, ohne ein AMI zu wählen.

Suchleiste

Um alle verfügbaren AMIs zu durchsuchen, geben Sie ein Schlüsselwort in die AMI-Suchleiste ein und drücken Sie dann die Eingabetaste. Wählen Sie Select (Auswählen) zum Auswählen des AMI aus.

Kürzlich gestartet

Die AMIs, die Sie kürzlich verwendet haben.

Wählen Sie Kürzlich gestartet oder Derzeit verwendet aus und wählen Sie dann unter Amazon Machine Image (AMI) ein AMI.

My AMIs

Die privaten AMIs, die Sie besitzen oder private AMIs, die für Sie freigegeben wurden

Klicken Sie auf Im Besitz von mir oder Mit mir geteilt und wählen Sie dann unter Amazon Machine Image (AMI) ein AMI aus.

Schnellstart

AMIs sind nach Betriebssystem (OS) gruppiert, damit Sie loslegen können.

Wählen Sie zuerst das benötigte Betriebssystem und dann unter Amazon Machine Image (AMI) ein AMI aus. Um ein AMI auszuwählen, das für das kostenlose Kontingent berechtigt ist, vergewissern Sie sich, dass das AMI als Für kostenloses Kontingent berechtigt markiert ist.

Durchsuchen Sie weitere AMIs

Wählen Sie Weitere AMIs durchsuchen aus, um den vollständigen AMI-Katalog zu durchsuchen.

- Um alle verfügbaren AMIs zu durchsuchen, geben Sie ein Schlüsselwort in die Suchleiste ein und drücken Sie dann die Eingabetaste.
- Um mit einem Systems-Manager-Parameter nach einem AMI zu suchen, wählen Sie die Pfeilschaltfläche rechts neben der Suchleiste und dann Search by Systems Manager parameter (Nach Systems-Manager-Parameter suchen) aus. Weitere Informationen finden Sie unter Finden Sie ein AMI mithilfe eines Systems Manager Manager-Parameters.
- Um nach Kategorie zu suchen, wählen Sie Schnellstart-AMIs, Meine AMIs, AWS Marketplace - AMIs oder Community-AMIs aus.

  Das AWS Marketplace ist ein Online-Shop, in dem Sie Software kaufen können, die darauf läuft AWS, einschließlich AMIs. Weitere Informationen zum Starten einer Instance vom AWS

Marketplace finden Sie unterStarten Sie eine AWS Marketplace Instanz. In Community AMIs finden Sie AMIs, die AWS -Community-Mitglieder anderen zur Verwendung zur Verfügung gestellt haben. AMIs von Amazon oder einem verifizierten Partner sind mit Verifizierter Anbieter gekennzeichnet.

- Um die Liste der AMIs zu filtern, aktivieren Sie ein oder mehrere Kontrollkästchen unter Ergebnisse verfeinern auf der linken Seite des Bildschirms. Die Filteroptionen unterscheiden sich in Abhängigkeit von der ausgewählten Suchkategorie.
- Prüfen Sie, welcher Root device type für die einzelnen AMIs aufgeführt ist. Achten Sie darauf, welche AMIs den benötigten Typ aufweisen: entweder ebs (unterstützt von Amazon EBS) oder instance-store (unterstützt durch Instance-Speicher). Weitere Informationen finden Sie unter Speicher für das Root-Gerät.
- Prüfen Sie, welcher Typ unter Virtualization type für die einzelnen AMIs aufgeführt ist. Achten Sie darauf, welche AMIs den benötigten Typ aufweisen: entweder hvm oder paravirtual. Manche Instance-Typen benötigen beispielsweise HVM. Weitere Informationen zu Linux-Virtualisierungstypen finden Sie unterAMI-Virtualisierungstypen.
- Prüfen Sie den für jedes AMI aufgelisteten Startmodus. Achten Sie darauf, welche AMIs den benötigten Startmodus aufweisen: entweder legacy-bios, uefi oder uefi-preferred. Weitere Informationen finden Sie unter Amazon EC2 EC2-Startmodi.
- Wählen Sie ein AMI aus, das Ihren Anforderungen entspricht, und klicken Sie auf Select.

Warnung beim Wechseln des AMI

Wenn Sie die Konfiguration von Volumes oder Sicherheitsgruppen ändern, die mit dem ausgewählten AMI verknüpft sind, und dann ein anderes AMI auswählen, wird ein Fenster geöffnet, in dem Sie gewarnt werden, dass einige Ihrer aktuellen Einstellungen geändert oder entfernt werden. Sie können die Änderungen an den Sicherheitsgruppen und Volumes überprüfen. Darüber hinaus können Sie entweder anzeigen, welche Volumes hinzugefügt und gelöscht werden oder nur die hinzugefügten Volumes anzeigen.

Instance-Typ

Der Instance-Typ definiert die Hardware-Konfiguration und Größe der Instance. Größere Instance-Typen haben mehr CPU und Arbeitsspeicher. Weitere Informationen finden Sie unter Amazon EC2 EC2-Instance-Typen.

- Wählen Sie unter Instance-Typ den Instance-Typ für die Instance aus.

Kostenloses Kontingent — Wenn Ihr AWS Konto weniger als 12 Monate alt ist, können Sie Amazon EC2 im Rahmen des kostenlosen Kontingents verwenden, indem Sie den Instance-Typ t2.micro auswählen (oder den Instance-Typ t3.micro in Regionen, in denen t2.micro nicht verfügbar ist). Wenn ein Instance-Typ unter dem kostenlosen Kontingent berechtigt ist, ist er als Free tier eligible (Kostenloses Kontingent berechtigt) gekennzeichnet. Weitere Informationen zu t2.micro und t3.micro finden Sie unter Burstable Performance Instances.

- Vergleichen von Instance-Typen: Sie können verschiedene Instance-Typen anhand der folgenden Attribute vergleichen: Anzahl der vCPUs, Architektur, Speichermenge (GiB), Speichertyp und Netzwerkleistung.
- Tipps einholen: Sie können Anleitungen und Vorschläge für Instance-Typen vom Amazon Q EC2 Instance Type Selector erhalten. Weitere Informationen finden Sie unter Empfehlungen für Instance-Typen für einen neuen Workload erhalten:.

Schlüsselpaar (Anmeldung)

Wählen Sie für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder wählen Sie Neues Schlüsselpaar erstellen, um ein neues zu erstellen. Weitere Informationen finden Sie unter Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances.

> **Important**
>
> Wenn Sie die Option Proceed without key pair (Not recommended) (Ohne Schlüsselpaar fortfahren (Nicht empfohlen)) auswählen, können Sie keine Verbindung zur Instance herstellen, es sei denn, Sie wählen ein AMI aus, das entsprechend konfiguriert ist, um Benutzern eine andere Anmeldemöglichkeit zu erlauben.

Network settings (Netzwerkeinstellungen)

Konfigurieren Sie die Netzwerkeinstellungen nach Bedarf.

- VPC: Wählen Sie eine vorhandene VPC für Ihre Instance. Sie können die Standard-VPC oder eine zuvor erstellte VPC wählen. Weitere Informationen finden Sie unter the section called “Virtual Private Clouds”.
- Subnetz: Sie können eine Instance in einem Subnetz starten, das einer Availability Zone, einer Local Zone, Wavelength-Zone oder einem Outpost zugeordnet ist.

Um die Instance in einer Availability Zone zu starten, wählen Sie das Subnetz aus, in dem die Instance gestartet werden soll. Um ein neues Subnetz zu erstellen, wählen Sie Create new subnet aus, um die Amazon VPC-Konsole aufzurufen. Wenn Sie fertig sind, kehren Sie zum Launch Instance Wizard zurück und wählen Sie das Symbol zum Aktualisieren, um Ihr Subnetz in die Liste zu laden.

Um die Instance in einem reinen IPv6-Subnetz zu starten, muss die Instance auf dem Nitro System erstellt werden.

Um die Instance in einer Local Zone zu starten, wählen Sie ein Subnetz aus, das Sie in der Local Zone erstellt haben.

Um eine Instance in einem Outpost zu starten, wählen Sie ein Subnetz in einer VPC aus, die Sie dem Outpost zugeordnet haben.

- Auto-assign Public IP: Legen Sie fest, ob Ihre Instance eine öffentliche IPv4-Adresse erhält. Instances in einem Standardsubnetz erhalten standardmäßig eine öffentliche IPv4-Adresse, Instances in einem nicht standardmäßigen Subnetz nicht. Sie können Enable oder Disable auswählen, um die Standardeinstellungen des Subnetzes zu überschreiben. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen.
- Firewall (Sicherheitsgruppen): Verwenden Sie eine Sicherheitsgruppe, um Firewallregeln für Ihre Instance zu definieren. Diese Regeln legen fest, welcher eingehende Netzwerkverkehr an Ihre Instance übertragen wird. Der gesamte übrige Datenverkehr wird ignoriert. Weitere Informationen zu Sicherheitsgruppen finden Sie unter Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances.

  Wenn Sie eine Netzwerkschnittstelle hinzufügen, müssen Sie dieselbe Sicherheitsgruppe in der Netzwerkschnittstelle angeben.

  Wählen oder erstellen Sie eine Sicherheitsgruppe wie folgt:

  - Um eine vorhandene Sicherheitsgruppe für Ihre VPC auszuwählen, wählen Sie Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und wählen Sie Ihre Sicherheitsgruppe unter Common security groups (Allgemeine Sicherheitsgruppen).
  - Um eine neue Sicherheitsgruppe für Ihre VPC zu erstellen, wählen Sie Create security group (Sicherheitsgruppe erstellen). Der Launch Instance Wizard definiert die Sicherheitsgruppe launch-wizard-xautomatisch und bietet die folgenden Kontrollkästchen zum schnellen Hinzufügen von Sicherheitsgruppenregeln:

(Linux) SSH-Verkehr zulassen von — Erstellt eine Regel für eingehenden Datenverkehr, die es Ihnen ermöglicht, über SSH (Port 22) eine Verbindung zu Ihrer Instance herzustellen.

(Windows) RDP-Verkehr zulassen von — Erstellt eine Regel für eingehenden Datenverkehr, die es Ihnen ermöglicht, über RDP (Port 3389) eine Verbindung zu Ihrer Instance herzustellen.

Geben Sie an, ob der Datenverkehr von Anywhere (beliebiger Ursprung), Custom (Benutzerdefiniert) oder My IP (Meine IP) stammt.

Allow HTTPs traffic from the internet (HTTP-Datenverkehr aus dem Internet zulassen) – Erstellt eine Regel für eingehenden Datenverkehr, die Port 443 (HTTPS) öffnet, um Internetdatenverkehr von einem beliebigen Ursprung zuzulassen. Wenn Ihre Instance ein Webserver sein wird, benötigen Sie diese Regel.

Allow HTTP traffic from the internet (HTTP-Datenverkehr aus dem Internet zulassen) – Erstellt eine Regel für eingehenden Datenverkehr, die Port 80 (HTTP) öffnet, um Internetdatenverkehr von einem beliebigen Ursprung zuzulassen. Wenn Ihre Instance ein Webserver sein wird, benötigen Sie diese Regel.

Sie können diese Regeln bearbeiten und Regeln gemäß Ihren Anforderungen hinzufügen.

Um eine Regel zu bearbeiten oder hinzuzufügen, wählen Sie Edit (Bearbeiten) (oben rechts). Um eine Regel hinzuzufügen, wählen Sie Sicherheitsgruppenregel hinzufügen aus. Wählen Sie unter Type (Typ) den Netzwerkverkehrstyp aus. Das Feld Protokoll wird automatisch mit dem Protokoll ausgefüllt, um es für Netzwerkverkehr zu öffnen. Wählen Sie unter Quelltyp einen Quelltyp aus. Damit der Launch Instance Wizard die öffentliche IP-Adresse Ihres Computers hinzufügen kann, wählen Sie My IP (Meine IP). Wenn Sie jedoch eine Verbindung über einen ISP oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen, müssen Sie den von Client-Computern verwendeten IP-Adressbereich herausfinden.

> **Warning**
>
> Regeln, die allen IP-Adressen (`0.0.0.0/0`) den Zugriff auf Ihre Instance über SSH oder RDP ermöglichen, sind akzeptabel, wenn Sie eine Test-Instance kurz starten und bald anhalten oder beenden, sind jedoch nicht für Produktionsumgebungen geeignet. Sie sollten nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre Instance autorisieren.

- Advanced network configuration (Erweiterte Netzwerkkonfiguration) – Nur verfügbar, wenn Sie ein Subnetz auswählen.

  Netzwerkschnittstelle

  - Device index (Geräteindex): Der Index der Netzwerkkarte. Die primäre Netzwerkschnittstelle muss dem Netzwerkkartenindex 0 zugewiesen sein. Einige Instance-Typen unterstützen mehrere Netzwerkkarten.
  - Network interface (Netzwerkschnittstelle): Wählen Sie New interface (Neue Schnittstelle), damit Amazon EC2 eine neue Schnittstelle erstellen kann oder wählen Sie eine vorhandene, verfügbare Netzwerkschnittstelle aus.
  - Description (Beschreibung): (Optional) Eine Beschreibung für die neue Netzwerkschnittstelle.
  - Subnet (Subnetz): Das Subnetz, in dem eine neue Netzwerkschnittstelle erstellt werden soll. Für die primäre Netzwerkschnittstelle (`eth0`) ist dies das Subnetz, in dem die Instance gestartet wird. Wenn Sie für `eth0` eine vorhandene Netzwerkschnittstelle eingeben, wird die Instance in dem Subnetz gestartet, in dem sich die Netzwerkschnittstelle befindet.
  - Security groups (Sicherheitsgruppen): Eine oder mehrere Sicherheitsgruppen in Ihrer VPC, der/denen die Netzwerkschnittstelle zugeordnet werden soll.
  - Primary IP (Primäre IP): Eine private IPv4-Adresse aus dem Adressbereich für Ihr Subnetz. Lassen Sie das Feld leer, damit Amazon EC2 für Sie eine private IPv4-Adresse auswählen kann.
  - Secondary IP (Sekundäre IP): Eine oder mehrere zusätzliche private IPv4-Adressen aus dem Bereich Ihres Subnetzes. Klicken Sie auf Manuelles Zuweisen und geben Sie eine IP-Adresse ein. Klicken Sie auf IP hinzufügen, um eine weitere IP-Adresse hinzuzufügen. Alternativ können Sie Automatisch zuweisen auswählen, um Amazon EC2 ein AMI auswählen zu lassen. Geben Sie dann einen Wert ein, um die Anzahl der hinzuzufügenden IP-Adressen anzugeben.
  - (Nur IPv6) IPv6 IPs: Eine IPv6-Adresse aus dem Adressbereich für Ihr Subnetz. Klicken Sie auf Manuelles Zuweisen und geben Sie eine IP-Adresse ein. Klicken Sie auf IP hinzufügen, um eine weitere IP-Adresse hinzuzufügen. Alternativ können Sie Automatisch zuweisen auswählen, um Amazon EC2 ein AMI auswählen zu lassen. Geben Sie dann einen Wert ein, um die Anzahl der hinzuzufügenden IP-Adressen anzugeben.
  - IPv4 Prefixes: Die IPv4-Präfixe für die Netzwerkschnittstelle.
  - IPv6 Prefixes: Die IPv6-Präfixe für die Netzwerkschnittstelle.
  - (Dual-Stack und nur IPv6) Primäre IPv6-IP zuweisen: (Optional) Wenn Sie eine Instance in einem Dual-Stack- oder nur IPv6-Subnetz starten, haben Sie die Möglichkeit, primäre IPv6-IP zuzuweisen. Durch die Zuweisung einer primären IPv6-Adresse können Sie eine Unterbrechung des Datenverkehrs zu Instances oder ENIs vermeiden. Wählen Sie Aktivieren, wenn diese

Instance davon abhängt, dass sich ihre IPv6-Adresse nicht ändert. Wenn Sie die Instance starten, AWS wird automatisch eine IPv6-Adresse, die der mit Ihrer Instance verbundenen ENI zugeordnet ist, als primäre IPv6-Adresse zugewiesen. Sobald Sie eine IPv6-GUA-Adresse als primäre IPv6-Adresse aktiviert haben, können Sie sie nicht mehr deaktivieren. Wenn Sie eine IPv6-GUA-Adresse als primäre IPv6-Adresse aktivieren, wird die erste IPv6-GUA zur primären IPv6-Adresse gemacht, bis die Instance beendet oder die Netzwerkschnittstelle getrennt wird. Wenn Ihrer Instance mehrere IPv6-Adressen mit einer angefügten ENI zugeordnet sind und Sie eine primäre IPv6-Adresse aktivieren, wird die erste IPv6-GUA-Adresse, die der ENI zugeordnet ist, zur primären IPv6-Adresse.

- Delete on termination (Bei Beenden löschen): Wählen Sie aus, ob die Netzwerkschnittstelle gelöscht werden soll, wenn die Instance gelöscht wird.
- Elastic Fabric Adapter: Gibt an, ob die Netzwerkschnittstelle ein Elastic Fabric Adapter ist. Weitere Informationen finden Sie unter Elastic Fabric Adapter.
- ENA Express: ENA Express basiert auf der SRD-Technologie (AWS Scalable Reliable Datagram). Die SRD-Technologie verwendet einen Paketverteilungsmechanismus, um die Last zu verteilen und Netzwerküberlastungen zu vermeiden. Durch die Aktivierung von ENA Express können unterstützte Instances zusätzlich zu regulärem TCP-Datenverkehr auch SRD für die Kommunikation verwenden (sofern möglich). Der Launch Instance Wizard enthält keine ENA-Express-Konfiguration für die Instance, es sei denn, Sie wählen in der Liste die Option Aktivieren oder Deaktivieren aus.
- ENA Express UDP: Wenn Sie ENA Express aktiviert haben, können Sie es optional für UDP-Datenverkehr verwenden. Der Launch Instance Wizard enthält keine ENA-Express-Konfiguration für die Instance, es sei denn, Sie wählen Aktivieren oder Deaktivieren aus.

Wählen Sie Netzwerkschnittstelle hinzufügen, um weitere Netzwerkschnittstellen hinzuzufügen. Zusätzliche Netzwerkschnittstellen können sich in einem anderen Subnetz derselben VPC oder in einem Subnetz in einer anderen VPC befinden, die Sie besitzen (sofern sich das Subnetz in derselben Availability Zone wie Ihre Instance befindet). Wenn Sie eine zusätzliche Netzwerkschnittstelle hinzufügen möchten, die sich in einem anderen VPC-Subnetz befindet, wird bei der Auswahl eines Subnetzes die Option Multi-VPC-Subnetze angezeigt. Wenn Sie ein Subnetz in einer anderen VPC auswählen, wird die Bezeichnung Multi-VPC neben der Netzwerkschnittstelle angezeigt, die Sie hinzugefügt haben. Dadurch können Sie VPC-übergreifend mehrfach vernetzte Instances mit unterschiedlichen Netzwerk- und Sicherheitskonfigurationen erstellen. Beachten Sie, dass Sie, wenn Sie eine zusätzliche ENI von einer anderen VPC anhängen, eine Sicherheitsgruppe für die ENI aus dieser VPC auswählen müssen.

Weitere Informationen finden Sie unter Elastic-Network-Schnittstelle. Wenn Sie mehr als eine Netzwerkschnittstelle angeben, kann Ihre Instance keine öffentliche IPv4-Adresse erhalten. Außerdem können Sie, wenn Sie für eth0 eine vorhandene Netzwerkschnittstelle angeben, die Subnetzeinstellung für öffentliche IPv4-Adressen nicht mithilfe von Auto-assign Public IP überschreiben. Weitere Informationen finden Sie unter Zuweisen einer öffentlichen IPv4-Adresse beim Start einer Instance.

Speicher konfigurieren

Die von Ihnen ausgewählte AMI beinhaltet ein oder mehrere Speicher-Volumes, einschließlich eines Root-Volumes. Sie können zusätzliche Volumes angeben, die an die Instance angehängt werden sollen.

Sie können die Ansicht Einfach oder Erweitert verwenden. Mit der einfachen Simple-Ansicht legen Sie die Größe und Art des Volumes fest. Um alle Volume-Parameter anzugeben, verwenden Sie die Ansicht Erweitert oben rechts auf der Karte.

In der erweiterten Ansicht können Sie jedes Volume wie folgt konfigurieren:

- Storage type (Speichertyp): Wählen Sie Amazon-EBS- oder Instance-Speicher-Volumes aus, um sie Ihrer Instance zuzuordnen. Die in der Liste verfügbaren Volume-Typen hängen von dem Instance-Typ ab, den Sie ausgewählt haben. Weitere Informationen finden Sie unter Amazon EC2-Instance-Speicher und Amazon EBS-Volumes.
- Device name (Gerätename): Wählen Sie aus der Liste verfügbarer Gerätenamen für das Volume einen Eintrag aus.
- Snapshot: Wählen Sie den Snapshot aus, von dem das Volume wiederhergestellt werden soll. Sie können nach verfügbaren freigegebenen und öffentlichen Snapshots suchen, indem Sie Text in das Feld Snapshot eingeben.
- Größe (GiB): Sie können für EBS-Volumes eine Speichergröße angeben. Wenn Sie ein AMI und eine Instance ausgewählt haben, die im kostenlosen Kontingent enthalten sind, dürfen Sie den Grenzwert von 30 GiB Gesamtspeicher nicht überschreiten, um innerhalb des kostenlosen Kontingents zu bleiben.
- Volume Type (Volume-Typ): Wählen Sie für die EBS-Volumes einen Volume-Typ aus. Weitere Informationen finden Sie unter Amazon EBS-Volumetypen im Amazon EBS-Benutzerhandbuch.
- IOPS: Wenn Sie einen Provisioned IOPS SSD-Volume-Typ ausgewählt haben, können Sie die Zahl der I/O-Vorgänge pro Sekunde (IOPS) eingeben, die das Volume unterstützen kann.

- Delete on termination (Bei Beendigung löschen): Wählen Sie für Amazon-EBS-Volumes Ja, um das Volume zu löschen, wenn die Instance beendet wird oder wählen Sie Nein, um das Volume beizubehalten. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.
- Encrypted (Verschlüsselt): Wenn der Instance-Typ die EBS-Verschlüsselung unterstützt, können Sie Ja auswählen, um die Verschlüsselung für das Volume zu aktivieren. Wenn Sie für diese Region die standardmäßige Verschlüsselung aktiviert haben, wird der Standard-CMK für Sie ausgewählt. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung im Amazon EBS-Benutzerhandbuch.
- KMS key (KMS-Schlüssel): Wenn Sie Yes (Ja) für Encrypted (Verschlüsselt) ausgewählt haben, müssen Sie einen kundenverwalteten Schlüssel zum Verschlüsseln des Volumes auswählen. Wenn die für diese Region die standardmäßige Verschlüsselung aktiviert haben, wird der Standard-CMK für Sie ausgewählt. Sie können einen anderen Schlüssel auswählen oder den ARN eines Kundenverwaltungsschlüssels angeben, den Sie erstellt haben.
- Dateisysteme: Stellen Sie ein Amazon-EFS- oder Amazon-FSx-Dateisystem in der Instance bereit. Weitere Informationen zum Bereitstellen eines Amazon-EFS-Dateisystems finden Sie unter Verwenden Sie Amazon EFS mit Linux-Instances. Weitere Informationen zum Bereitstellen eines Amazon-FSx-Dateisystems finden Sie unter Verwenden von Amazon FSx mit Amazon EC2.

Erweiterte Details

Erweitern Sie für Advanced details (Erweiterte Details) den Bereich zur Ansicht der Felder und geben Sie zusätzliche Parameter für die Instance an.

- Kaufoption: Wählen Sie Request Spot Instances (Spot-Instances anfordern), um Spot-Instances zum Spot-Preis anzufordern, der auf den On-Demand-Preis begrenzt ist, und wählen Sie Customize (Anpassen), um die Standardeinstellungen für Spot-Instances zu ändern. Sie können Ihren Höchstpreis festlegen (nicht empfohlen) und den Anforderungstyp, die Anforderungsdauer und das Unterbrechungsverhalten ändern. Wenn Sie keine Spot-Instance anfordern, startet Amazon EC2 standardmäßig eine On-Demand-Instance. Weitere Informationen finden Sie unter Erstellt eine Spot-Instance-Anforderung.
- Domain-Join-Verzeichnis: Wählen Sie das AWS Directory Service Verzeichnis (Domain) aus, zu dem Ihre Instance nach dem Start hinzugefügt wird. Wenn Sie eine Domain auswählen, müssen Sie eine IAM Rolle mit den erforderlichen Berechtigungen auswählen. Weitere Informationen zum Domänenbeitritt zu Linux-Instances finden Sie unter Nahtloses Verbinden einer Linux EC2-Instance mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis. Weitere Informationen zum Domänenbeitritt

von Windows-Instances finden Sie unter Nahtloses Verbinden einer Windows EC2-Instance mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis.

- IAM-Instanzprofil: Wählen Sie ein AWS Identity and Access Management (IAM-) Instanzprofil aus, das der Instance zugeordnet werden soll. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.
- Hostname type (Hostnamentyp): Wählen Sie aus, ob der Hostname des Gastbetriebssystems der Instance der Ressourcenname oder der IP-Name sein soll. Weitere Informationen finden Sie unter Hostnamentypen für Amazon-EC2-Instances.
- DNS Hostname (DNS-Hostname): Bestimmt, ob die DNS-Abfragen an den Ressourcennamen oder den IP-Namen (je nach der Auswahl für Hostname type (Hostnamentyp)) mit der IPv4-Adresse (A-Datensatz), der IPv6-Adresse (AAAA-Datensatz) oder beidem antworten. Weitere Informationen finden Sie unter Hostnamentypen für Amazon-EC2-Instances.
- Shutdown behavior: Wählen Sie aus, ob die Instance beim Herunterfahren angehalten oder beendet werden soll. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.
- Stop - Hibernate behavior (Stopp – Verhalten im Ruhezustand): Um den Ruhezustand zu aktivieren, wählen Sie Enable (Aktivieren). Dieses Feld ist nur verfügbar, wenn Ihre Instance die Voraussetzungen für den Ruhezustand erfüllt. Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand.
- Termination protection (Beendigungsschutz): Um ein versehentliches Beenden zu verhindern, wählen Sie Aktivieren. Weitere Informationen finden Sie unter Aktivieren des Beendigungsschutzes.
- Stop protection (Stoppschutz): Um ein versehentliches Anhalten zu verhindern, wählen Sie Enable (Aktivieren). Weitere Informationen finden Sie unter Aktivieren des Stopp-Schutzes.
- Detaillierte CloudWatch Überwachung: Wählen Sie Aktivieren, um die detaillierte Überwachung Ihrer Instance mithilfe von Amazon zu aktivieren CloudWatch. Es fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.
- Elastische GPU: Amazon Elastic Graphics hat am 8. Januar 2024 das Ende der Lebensdauer erreicht. Für Workloads, die Grafikbeschleunigung erfordern, empfehlen wir die Verwendung von Amazon EC2 G4ad-, G4dn- oder G5-Instances.
- Elastic inference (Elastic Inference): Ein Elastic Inference-Accelerator, der Ihrer EC2-CPU-Instance zugewiesen werden soll. Weitere Informationen finden Sie unter Arbeiten mit Amazon Elastic Inference im Amazon Elastic Inference Developer-Handbuch.

> **Note**
>
> Ab 15. April 2023 AWS wird Amazon Elastic Inference (EI) keine Neukunden mehr in Amazon Elastic Inference (EI) einbinden und Bestandskunden dabei helfen, ihre Workloads auf Optionen umzustellen, die ein besseres Preis und eine bessere Leistung bieten. Nach dem 15. April 2023 können Neukunden keine Instances mit Amazon EI-Beschleunigern in Amazon SageMaker, Amazon ECS oder Amazon EC2 starten. Kunden, die Amazon EI in den letzten 30 Tagen mindestens einmal genutzt haben, gelten jedoch als aktuelle Kunden und können den Service weiterhin nutzen.

- Guthabenspezifikation: Wählen Sie Unbegrenzt aus, damit Anwendungen so lange wie nötig über die Baseline hinaus laufen können. Dieses Feld gilt nur für T-Instances. Es können zusätzliche Gebühren anfallen. Weitere Informationen finden Sie unter Burstable Performance Instances.
- Placement group name: Geben Sie eine Platzierungsgruppe an, in der die Instance gestartet werden soll. Wählen Sie eine vorhandene Platzierungsgruppe aus oder erstellen Sie eine neue. Nicht alle Instance-Typen unterstützen das Starten einer Instance in einer Platzierungsgruppe. Weitere Informationen finden Sie unter Placement-Gruppen.
- EBS-optimierte Instance: Eine Amazon-EBS-optimierte Instance verwendet einen optimierten Konfigurations-Stack und bietet zusätzliche, dedizierte Kapazität für Amazon EBS I/O. Wenn der Instance-Typ dieses Feature unterstützt, wählen Sie Aktivieren, um sie zu aktivieren. Es fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter the section called “EBS-Optimierung”.
- Capacity Reservation (Kapazitätsreservierung): Geben Sie an, ob die Instance in einer beliebigen offenen Kapazitätsreservierung (Offen), einer bestimmten Kapazitätsreservierung (Ziel nach ID) oder einer Kapazitätsreservierungsgruppe (Ziel nach Gruppe) gestartet werden soll. Um anzugeben, dass keine Kapazitätsreservierung verwendet werden soll, wählen Sie None (Keine) aus. Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.
- Tenancy: Wählen Sie aus, ob Ihre Instance auf einer gemeinsam genutzten (Shared), isolierten oder dedizierten (Dedicated) Hardware oder auf einem dedizierten Host Dedicated Host (Dedicated host) ausgeführt werden soll. Wenn Sie die Instance auf einem Dedicated Host starten möchten, können Sie angeben, ob die Instance in einer Hostressourcengruppe gestartet werden soll oder ob Sie eine bestimmte Dedicated Host verwenden möchten. Es können zusätzliche Gebühren anfallen. Weitere Informationen finden Sie unter Dedicated Instances und Dedicated Hosts.

- RAM disk ID (RAM-Datenträgerkennung): (Nur gültig für Paravirtual-AMIS (PV-AMIs). Wählen Sie eine RAM-Festplatte für die Instance. Wenn Sie einen Kernel ausgewählt haben, müssen Sie möglicherweise eine bestimmte RAM-Disk mit den Treibern auswählen, um ihn zu unterstützen.
- Kernel ID (Kernel-ID: (Nur gültig für Paravirtual-AMIs (PV-AMIs). Wählen Sie ein Kernel für die Instance.
- Nitro Enclaves: Mit dieser Funktion können Sie aus Amazon-EC2-Instances isolierte Ausführungsumgebungen namens Enklaven erstellen. Wählen Sie Aktivieren aus, um die Instance für AWS Nitro Enclaves zu aktivieren. Weitere Informationen finden Sie unter Was ist AWS Nitro Enclaves? im AWS Nitro Enclaves-Benutzerhandbuch.
- License configurations (Lizenzkonfigurationen): Sie können Instances für die angegebene Lizenzkonfiguration starten, um die Lizenznutzung nachzuverfolgen. Weitere Informationen finden Sie unter Erstellen einer Lizenzkonfiguration im Benutzerhandbuch zu AWS License Manager.
- Metadata accessible (Metadaten zugänglich): Sie können den Zugriff auf die Instance-Metadaten aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- IPv6-Endpunkt für Metadaten: Sie können der Instance ermöglichen, die IMDS-IPv6-Adresse zum Abrufen von Instanz-Metadaten zu verwenden. `[fd00:ec2::254]` Diese Option ist nur verfügbar, wenn Sie Instances, die auf dem AWS Nitro-System basieren, in einem IPv6-unterstützten Subnetz starten (Dual-Stack oder nur IPv6). Weitere Informationen zum Abrufen von Instance-Metadaten finden Sie unter Abrufen von Instance-Metadaten.
- Metadata version (Metadatenversion): Wenn Sie den Zugriff auf die Instance-Metadaten aktivieren, können Sie festlegen, dass die Verwendung von Instance-Metadatenservice Version 2 beim Anfordern von Instance-Metadaten erforderlich ist. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- Metadata response hop limit (Metadatenantwort-Hop-Limit): Wenn Sie Instance-Metadaten aktivieren, können Sie die zulässige Anzahl von Netzwerk-Hops für das Metadaten-Token festlegen. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- Allow tags in metadata (Tags in Metadaten erlauben): Wenn Sie Enable (Aktivieren) auswählen, erlaubt die Instance den Zugriff auf alle ihre Tags aus ihren Metadaten. Wenn kein Wert angegeben wird, ist der Zugriff auf die Tags in Instance-Metadaten standardmäßig nicht erlaubt. Weitere Informationen finden Sie unter Zulassen des Zugriffs auf Tags in Instance-Metadaten.
- User data: Sie können Benutzerdaten so festlegen, dass eine Instance während des Starts konfiguriert wird oder dass ein Konfigurationsskript ausgeführt wird. Weitere Informationen zu Benutzerdaten für Linux-Instances finden Sie unter. Führen Sie beim Start Befehle auf Ihrer

Amazon EC2 EC2-Instance aus Weitere Informationen zu Benutzerdaten für Windows-Instanzen finden Sie unterSo verarbeitet Amazon EC2 Benutzerdaten für Windows-Instances.

Übersicht

Verwenden Sie den Bereich Zusammenfassung, um die Anzahl der zu startenden Instances anzugeben, Ihre Instance-Konfiguration zu überprüfen und Ihre Instances zu starten.

- Number of instances: Geben Sie die Anzahl der Instances ein, die gestartet werden sollen. Alle Instances werden mit derselben Konfiguration gestartet.

> **Tip**
>
> Um sicherzustellen, dass Instances schneller gestartet werden, unterteilen Sie große Anforderungen in kleinere Batches. Erstellen Sie beispielsweise fünf separate Startanforderungen für jeweils 100 Instances anstelle von einer Startanforderung für 500 Instances.

- (Optional) Damit sichergestellt wird, dass Sie stets die richtige Zahl an Instances haben, um den Bedarf Ihrer Anwendung zu verarbeiten (wenn Sie mehr als eine Instance angeben), können Sie die Option consider EC2 Auto Scaling (EC2-Auto-Scaling berücksichtigen) auswählen, um eine Startvorlage und eine Auto-Scaling-Gruppe zu erstellen. Auto Scaling skaliert die Anzahl der Instances in der Gruppe entsprechend Ihren Spezifikationen. Weitere Informationen hierzu finden Sie unter Amazon EC2 Auto Scaling-Benutzerhandbuch.

> **Note**
>
> Wenn eine Instance, die sich in einer Auto Scaling-Gruppe befindet, von Amazon EC2 Auto Scaling als fehlerhaft markiert wird, wird die Instance automatisch für den Austausch geplant, wobei sie beendet und eine andere gestartet wird, und Sie verlieren Ihre Daten in der ursprünglichen Instance. Eine Instance wird als fehlerhaft markiert, wenn Sie die Instance beenden oder neu starten oder wenn ein anderes Ereignis die Instance als fehlerhaft markiert. Weitere Informationen finden Sie unter Zustandsprüfungen für Instances in einer Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

- Überprüfen Sie die Details Ihrer Instance und nehmen Sie ggf. Änderungen vor. Sie können direkt zu einem Abschnitt navigieren, indem Sie den entsprechenden Link im Bereich Zusammenfassung auswählen.
- Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Instance starten aus.

  Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

  (Optional) Sie können eine Abrechnungswarnung für die Instance erstellen. Wählen Sie auf dem Bestätigungsbildschirm unter Next Steps (Nächste Schritte) die Option Create billing alerts (Gebührenlimit-Warnungen erstellen) aus und befolgen Sie die Anweisungen. Gebührenlimit-Warnungen können auch nach dem Start der Instance erstellt werden. Weitere Informationen finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Einen Abrechnungsalarm erstellen, um Ihre geschätzten AWS Gebühren zu überwachen.

Starten einer Instance mit dem alten Launch Instance Wizard

Sie können eine Instance nur dann mit dem alten Launch Instance Wizard starten, wenn Ihre Region das alte Starterlebnis unterstützt. Der Launch Instance Wizard gibt alle Startparameter an, die zum Starten einer Instance erforderlich sind. Wenn der Launch Instance Wizard einen Standardwert bereitstellt, können Sie den Standardwert akzeptieren oder einen eigenen Wert angeben. Um eine Instance zu starten, müssen Sie ein AMI und ein Schlüsselpaar angeben.

Informationen zur Verwendung des neuen Launch Instance Wizard finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

> **Important**
>
> Wenn Sie eine Instance starten, die nicht vom kostenlosen AWS -Kontingent abgedeckt ist, fallen für die Zeit, in der die Instance ausgeführt wird, Gebühren an, selbst wenn sie nicht genutzt wird.

Schritte für das Starten einer Instance

- Initiieren des Instance-Starts
- Schritt 1: Auswählen eines Amazon Machine Images (AMI)
- Schritt 2: Auswählen eines Instance-Typs

- Schritt 3: Konfigurieren der Instance-Details
- Schritt 4: Hinzufügen von Speicher
- Schritt 5: Hinzufügen von Tags (Markierungen)
- Schritt 6: Konfigurieren einer Sicherheitsgruppe
- Schritt 7: Prüfen des Instance-Starts und Auswahl des Schlüsselpaars

Initiieren des Instance-Starts

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Auf der Navigationsleiste oben im Bildschirm wird die aktuelle Region angezeigt (beispielsweise US East (Ohio)). Wählen Sie eine Region für die Instance aus, die Ihre Anforderungen erfüllt. Die Auswahl ist wichtig, da nur bestimmte Amazon EC2-Ressourcen zwischen Regionen geteilt werden können. Weitere Informationen finden Sie unter Ressourcenstandorte.
3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.

Schritt 1: Auswählen eines Amazon Machine Images (AMI)

Wenn Sie eine Instance starten, müssen Sie eine Konfiguration auswählen, die als Amazon Machine Image (AMI) bezeichnet wird. Ein AMI enthält die Informationen, die zum Erstellen einer neuen Instance erforderlich sind. Ein AMI kann beispielsweise die Software enthalten, die für die Funktion als Webserver erforderlich ist, z. B. Linux, Apache und Ihre Website.

Wenn Sie eine Instance starten, können Sie entweder ein AMI aus der Liste auswählen oder einen Systems Manager-Parameter auswählen, der auf eine AMI-ID verweist. Weitere Informationen finden Sie unter the section called “Finden Sie ein AMI mithilfe eines Systems Manager Manager-Parameters”.

Verwenden Sie auf der Seite Choose an Amazon Machine Image (AMI) (Wählen Sie ein Amazon Machine Image (AMI) aus) eine von zwei Optionen, um ein AMI zu wählen. Entweder durchsuchen Sie die Liste der AMIs oder durch den Systems Manager-Parameter.

Über Suchen in der Liste der AMIs

1. Wählen Sie im linken Bereich den zu verwendenden AMI-Typ aus:

Schnellstart

Eine Auswahl beliebter AMIs, mit denen Sie schnell anfangen können. Um ein AMI auszuwählen, das im kostenlosen Kontingent enthalten ist, wählen Sie im linken Bereich die Option Free tier only aus. Diese AMIs sind mit Free tier eligible gekennzeichnet.

My AMIs

Die privaten AMIs, die Sie besitzen oder private AMIs, die für Sie freigegeben wurden Um mit Ihnen geteilte AMIs anzuzeigen, wählen Sie Shared with me (Mit mir geteilt) im linken Fensterbereich.

AWS Marketplace

Ein Online-Shop, in dem Sie Software kaufen können, die darauf läuft AWS, einschließlich AMIs. Weitere Informationen zum Starten einer Instance vom AWS Marketplace finden Sie unterStarten Sie eine AWS Marketplace Instanz.

Community AMIs

Die AMIs, die AWS Community-Mitglieder anderen zur Nutzung zur Verfügung gestellt haben. Um die Liste der AMIs nach Betriebssystem zu filtern, wählen Sie unter Operating system das entsprechende Kontrollkästchen aus. Sie können außerdem nach Architektur und Root-Gerätetyp filtern.

2. (Linux-Instances) Überprüfen Sie den Root-Gerätetyp, der für jedes AMI aufgeführt ist. Achten Sie hierbei darauf, welche AMIs den Typ aufweisen, den Sie benötigen, entweder `ebs` (gestützt durch Amazon EBS) oder `instance-store` (gestützt durch Instance-Speicher). Weitere Informationen finden Sie unter Speicher für das Root-Gerät.
3. Prüfen Sie, welcher Typ unter Virtualization type für die einzelnen AMIs aufgeführt ist. Achten Sie hierbei darauf, welche AMIs den Typ aufweisen, den Sie benötigen, entweder `hvm` oder `paravirtual`. Manche Instance-Typen benötigen beispielsweise HVM. Weitere Informationen zu Linux-Virtualisierungstypen finden Sie unterAMI-Virtualisierungstypen.
4. Prüfen Sie den für jedes AMI aufgelisteten Startmodus. Achten Sie hierbei darauf, welche AMIs den Startmodus aufweisen, den Sie benötigen, entweder `legacy-bios` oder `uefi`. Weitere Informationen finden Sie unter Amazon EC2 EC2-Startmodi.
5. Wählen Sie ein AMI aus, das Ihren Anforderungen entspricht, und klicken Sie auf Select.

Über den Systems Manager-Parameter

1. Wählen Sie Search by Systems Manager parameter (Suchen nach Systems Manager-Parameter) (oben rechts).
2. Wählen Sie für Systems Manager-Parameter einen Parameter aus. Die entsprechende AMI-ID erscheint neben Currently resolves to (Gegenwärtig aufgelöst nach).
3. Wählen Sie Search (Suchen) aus. Die AMIs, die der AMI-ID entsprechen, erscheinen in der Liste.
4. Wählen Sie die AMI aus der Liste und wählen Sie Select (Auswählen).

Schritt 2: Auswählen eines Instance-Typs

Wählen Sie auf der Seite Choose an Instance Type (Einen Instance-Typ auswählen) die Hardware-Konfiguration und Größe der zu startenden Instance aus. Größere Instance-Typen haben mehr CPU und Arbeitsspeicher. Weitere Informationen finden Sie unter Amazon EC2-Instance-Typen.

Um für das kostenlose Kontingent berechtigt zu bleiben, wählen Sie den Instance-Typ t2.micro (oder den Instance-Typ t3.micro in Regionen, in denen t2.micro nicht verfügbar ist). Wenn ein Instance-Typ unter dem kostenlosen Kontingent berechtigt ist, ist er als Free tier eligible (Kostenloses Kontingent berechtigt) gekennzeichnet. Weitere Informationen zu t2.micro und t3.micro finden Sie unter Burstable Performance Instances.

Standardmäßig zeigt der Assistent Instance-Typen der aktuellen Generation an und wählt basierend auf dem von Ihnen ausgewählten AMI den ersten verfügbaren Instance-Typ aus. Um Instance-Typen früherer Generationen anzuzeigen, wählen Sie in der Filterliste All generations aus.

> **Note**
>
> Um eine Instance zu Testzwecken schnell einzurichten, können Sie Review and Launch auswählen, um die standardmäßigen Konfigurationseinstellungen zu akzeptieren und Ihre Instance zu starten. Andernfalls wählen Sie Next: Configure Instance Details aus, um Ihre Instance weiter zu konfigurieren.

Schritt 3: Konfigurieren der Instance-Details

Ändern Sie auf der Seite Configure Instance Details die folgenden Einstellungen nach Bedarf (erweitern Sie Advanced Details, um alle Einstellungen anzuzeigen). Wählen Sie dann Next: Add Storage aus:

- Number of instances: Geben Sie die Anzahl der Instances ein, die gestartet werden sollen.

> **Tip**
>
> Um sicherzustellen, dass Instances schneller gestartet werden, unterteilen Sie große Anforderungen in kleinere Batches. Erstellen Sie beispielsweise fünf separate Startanforderungen für jeweils 100 Instances anstelle von einer Startanforderung für 500 Instances.

- (Optional) Damit sichergestellt wird, dass Sie die richtige Zahl an Instances haben, um den Bedarf Ihre Anwendung zu verarbeiten, können Sie die Option Launch into Auto Scaling Group auswählen, um eine Startkonfiguration und eine Auto Scaling-Gruppe zu erstellen. Auto Scaling skaliert die Anzahl der Instances in der Gruppe entsprechend Ihren Spezifikationen. Weitere Informationen hierzu finden Sie unter Amazon EC2 Auto Scaling-Benutzerhandbuch.

> **Note**
>
> Wenn eine Instance, die sich in einer Auto Scaling-Gruppe befindet, von Amazon EC2 Auto Scaling als fehlerhaft markiert wird, wird die Instance automatisch für den Austausch geplant, wobei sie beendet und eine andere gestartet wird, und Sie verlieren Ihre Daten in der ursprünglichen Instance. Eine Instance wird als fehlerhaft markiert, wenn Sie die Instance beenden oder neu starten oder wenn ein anderes Ereignis die Instance als fehlerhaft markiert. Weitere Informationen finden Sie unter Zustandsprüfungen für Auto Scaling-Instances im Amazon EC2 Auto Scaling-Benutzerhandbuch.

- Purchasing option: Wählen Sie Request Spot instances (Spot-Instances anfordern) aus, um eine Spot-Instance zu starten. Dieses fügt Optionen dieser Seite hinzu und löscht sie wieder daraus. Sie können optional Ihren Höchstpreis festlegen (nicht empfohlen) und optional den Anforderungstyp, das Unterbrechungsverhalten und die Anforderungsgültigkeit ändern. Weitere Informationen finden Sie unter Erstellt eine Spot-Instance-Anforderung.
- Network (Netzwerk): Wählen Sie die VPC aus oder klicken Sie zum Erstellen einer neuen VPC auf Create new VPC (Neue VPC erstellen), um zur Amazon-VPC-Konsole zu gelangen. Wenn Sie

fertig sind, kehren Sie zum Launch Instance Wizard zurück und wählen Sie Aktualisieren aus, um die VPC in die Liste zu laden.

- Subnetz: Sie können eine Instance in einem Subnetz starten, das einer Availability Zone, einer Local Zone, Wavelength-Zone oder einem Outpost zugeordnet ist.

  Um die Instance in einer Availability Zone zu starten, wählen Sie das Subnetz aus, in dem die Instance gestartet werden soll. Sie können Keine Präferenz auswählen, um ein Standardsubnetz in einer beliebigen Availability Zone AWS auswählen zu lassen. Um ein neues Subnetz zu erstellen, wählen Sie Create new subnet aus, um die Amazon VPC-Konsole aufzurufen. Wenn Sie fertig sind, kehren Sie zum Assistenten zurück und wählen Sie Refresh aus, um das Subnetz in die Liste zu laden.

  Um die Instance in einer Local Zone zu starten, wählen Sie ein Subnetz aus, das Sie in der Local Zone erstellt haben.

  Um eine Instance in einem Outpost zu starten, wählen Sie ein Subnetz in einer VPC aus, die Sie einem Outpost zugeordnet haben.
- Auto-assign Public IP: Legen Sie fest, ob Ihre Instance eine öffentliche IPv4-Adresse erhält. Instances in einem Standardsubnetz erhalten standardmäßig eine öffentliche IPv4-Adresse, Instances in einem nicht standardmäßigen Subnetz nicht. Sie können Enable oder Disable auswählen, um die Standardeinstellungen des Subnetzes zu überschreiben. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen.
- Auto-assign IPv6 IP: Geben Sie an, ob Ihre Instance eine IPv6-Adresse aus dem Bereich des Subnetzes erhält. Wählen Sie Enable oder Disable aus, um die Standardeinstellungen des Subnetzes zu überschreiben. Diese Option ist nur verfügbar, wenn Sie Ihrer VPC und Ihrem Subnetz einen IPv6-CIDR-Block zugeordnet haben. Weitere Informationen finden Sie unter Hinzufügen eines IPv6-CIDR-Blocks zu Ihrer VPC im Amazon-VPC-Benutzerhandbuch.
- Hostname type (Hostnamentyp): Wählen Sie aus, ob der Hostname des Gastbetriebssystems der Instance der Ressourcenname oder der IP-Name sein soll. Weitere Informationen finden Sie unter Hostnamentypen für Amazon-EC2-Instances.
- DNS Hostname (DNS-Hostname): Bestimmt, ob die DNS-Abfragen an den Ressourcennamen oder den IP-Namen (je nach der Auswahl für Hostname type (Hostnamentyp)) mit der IPv4-Adresse (A-Datensatz), der IPv6-Adresse (AAAA-Datensatz) oder beidem antworten. Weitere Informationen finden Sie unter Hostnamentypen für Amazon-EC2-Instances.
- Domänenbeitrittsverzeichnis: Wählen Sie das AWS Directory Service Verzeichnis (Domain) aus, zu dem Ihre Instance nach dem Start hinzugefügt wird. Wenn Sie eine Domain auswählen, müssen

Sie eine IAM Rolle mit den erforderlichen Berechtigungen auswählen. Weitere Informationen zum Domänenbeitritt zu Linux-Instances finden Sie unter Nahtloses Verbinden einer Linux EC2-Instance mit Ihrem AWS verwalteten Microsoft AD-Verzeichnis. Weitere Informationen zum Domänenbeitritt zu Windows-Instances Nahtloser Beitritt zu einer Windows EC2-Instance.

- Placement group: Durch die Platzierungsgruppe wird die Platzierungsstrategie Ihrer Instances festgelegt. Wählen Sie eine vorhandene Platzierungsgruppe aus oder erstellen Sie eine neue. Diese Option ist nur verfügbar, wenn Sie einen Instance-Typ ausgewählt haben, der Placement-Gruppen unterstützt. Weitere Informationen finden Sie unter Placement-Gruppen.
- Kapazitätsreservierung: Geben Sie an, ob die Instance in der freigegebenen Kapazität, einer open Kapazitätsreservierung, einer bestimmten Kapazitätsreservierung oder einer Kapazitätsreservierung-Gruppe gestartet werden soll. Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.
- IAM-Rolle: Wählen Sie eine AWS Identity and Access Management (IAM-) Rolle aus, die der Instance zugeordnet werden soll. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.
- CPU options (CPU-Optionen): Wählen Sie Specify CPU options (CPU-Optionen angeben) aus, um eine benutzerdefinierte Anzahl von vCPUs beim Start festzulegen. Legen Sie die Anzahl der CPU-Kerne und -Threads pro Kern fest. Weitere Informationen finden Sie unter CPU-Optionen optimieren.
- Shutdown behavior: Wählen Sie aus, ob die Instance beim Herunterfahren angehalten oder beendet werden soll. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.
- Stop - Hibernate behavior (Stopp – Ruhezustandsverhalten): Aktivieren Sie dieses Kontrollkästchen, um den Ruhezustand zu aktivieren. Diese Option ist nur verfügbar, wenn die Instance die Voraussetzungen für den Ruhezustand erfüllt. Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand.
- Enable termination protection (Terminierungsschutz aktivieren): Um ein versehentliches Beenden zu verhindern, aktivieren Sie dieses Kontrollkästchen. Weitere Informationen finden Sie unter Aktivieren des Beendigungsschutzes.
- Enable stop protection (Anhalteschutz aktivieren): Um ein versehentliches Anhalten zu verhindern, aktivieren Sie dieses Kontrollkästchen. Weitere Informationen finden Sie unter Aktivieren des Stopp-Schutzes.
- Überwachung: Wählen Sie dieses Kontrollkästchen, um die detaillierte Überwachung Ihrer Instance mithilfe von Amazon zu aktivieren CloudWatch. Es fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.

- EBS-optimized instance (EBS-optimierte Instance): Eine Amazon EBS-optimierte Instance verwendet einen optimierten Konfigurations-Stack und bietet zusätzliche dedizierte Kapazität für Amazon EBS-I/O. Unterstützt der Instance-Typ dieses Feature, aktivieren Sie dieses Kontrollkästchen, um die Funktion zu verwenden. Es fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter Verwenden von Amazon EBS-optimierten Instances.
- Tenancy: Wenn Sie Ihre Instance in einer VPC starten, können Sie die Instance auf isolierter, dedizierter Hardware (Dedicated) oder auf einem dedizierten Host (Dedicated host) ausführen. Es können zusätzliche Gebühren anfallen. Weitere Informationen finden Sie unter Dedicated Instances und Dedicated Hosts.
- T2/T3 Unlimited: Markieren Sie dieses Kontrollkästchen, um es Anwendungen zu ermöglichen, die Leistung zu steigern und die Baseline so lange wie nötig zu überschreiten. Es können zusätzliche Gebühren anfallen. Weitere Informationen finden Sie unter Burstable Performance Instances.
- File systems (Dateisysteme): Um ein neues Dateisystem für das Mounten Ihrer Instance zu erstellen, wählen Sie Create new file system (Neues Dateisystem erstellen), geben Sie einen Namen für das neue Dateisystem ein und wählen Sie dann Create (Erstellen). Das Dateisystem wird mit Quick Create Amazon EFS erstellt, das die vom Service empfohlenen Einstellungen anwendet. Die Sicherheitsgruppen, die erforderlich sind, um den Zugriff auf das Dateisystem zu ermöglichen, werden automatisch erstellt und an die Instance und die Mount-Ziele des Dateisystems angehängt. Sie können auch wählen, die erforderlichen Sicherheitsgruppen manuell zu erstellen und anzuhängen. Um ein oder mehrere vorhandene Amazon EFS-Dateisysteme in Ihre Instance zu mounten, wählen Sie Add file system (Dateisystem hinzufügen) und wählen Sie dann die zu mountenden Dateisysteme und die zu verwendenden Mount-Punkte aus. Weitere Informationen finden Sie unter Verwenden Sie Amazon EFS mit Linux-Instances.
- Network interfaces: Wenn Sie ein spezielles Subnetz ausgewählt haben, können Sie bis zu zwei Netzwerkschnittstellen für Ihre Instance angeben:
  - Wählen Sie unter Netzwerkschnittstelle die Option Neue Netzwerkschnittstelle aus, um eine neue Schnittstelle AWS erstellen zu können, oder wählen Sie eine vorhandene, verfügbare Netzwerkschnittstelle aus.
  - Geben Sie für Primäre IP eine private IPv4-Adresse aus dem Bereich Ihres Subnetzes ein, oder lassen Sie Auto-Assign stehen, damit AWS Sie eine private IPv4-Adresse auswählen können.
  - Wählen Sie für Secondary IP addresses die Option Add IP aus, um der ausgewählten Netzwerkschnittstelle mehr als eine private IPv4-Adresse zuzuweisen.
  - (Nur IPv6) Wählen Sie für IPv6-IPs die Option IP hinzufügen und geben Sie eine IPv6-Adresse aus dem Bereich des Subnetzes ein, oder lassen Sie die automatische Zuweisung stehen, damit Sie eine für Sie auswählen können. AWS

  - Network Card Index (Netzwerkkartenindex): Der Index der Netzwerkkarte. Die primäre Netzwerkschnittstelle muss dem Netzwerkkartenindex 0 zugewiesen sein. Einige Instance-Typen unterstützen mehrere Netzwerkkarten.
  - Wählen Sie Add Device aus, um eine sekundäre Netzwerkschnittstelle hinzuzufügen. Eine sekundäre Netzwerkschnittstelle kann sich in einem anderen Subnetz der VPC befinden, vorausgesetzt, es befindet sich in derselben Availability Zone wie Ihre Instance.

  Weitere Informationen finden Sie unter Elastic-Network-Schnittstelle. Wenn Sie mehr als eine Netzwerkschnittstelle angeben, kann Ihre Instance keine öffentliche IPv4-Adresse erhalten. Außerdem können Sie, wenn Sie für eth0 eine vorhandene Netzwerkschnittstelle angeben, die Subnetzeinstellung für öffentliche IPv4-Adressen nicht mithilfe von Auto-assign Public IP überschreiben. Weitere Informationen finden Sie unter Zuweisen einer öffentlichen IPv4-Adresse beim Start einer Instance.

- Kernel ID: (Nur gültig für PV-AMIs (Paravirtual)) Wählen Sie Use default aus, es sei denn, Sie möchten einen speziellen Kernel verwenden.
- RAM disk ID: (Nur gültig für PV-AMIs (Paravirtual)) Wählen Sie Use default aus, es sei denn, Sie möchten einen bestimmten RAM-Datenträger verwenden. Wenn Sie einen Kernel ausgewählt haben, müssen Sie möglicherweise einen bestimmten RAM-Datenträger mit den Treibern auswählen, die ihn unterstützen.
- Enclave: Wählen Sie Aktivieren aus, um die Instanz für Nitro Enclaves zu aktivieren. AWS Weitere Informationen finden Sie unter Was ist Nitro Enclaves? AWS im AWS Nitro Enclaves-Benutzerhandbuch.
- Metadatenzugriff: Sie können den Zugriff auf den Instance Metadata Service (IMDS) aktivieren oder deaktivieren. Weitere Informationen finden Sie unter IMDSv2 verwenden.
- IPv6-Endpunkt für Metadaten: Sie können der Instance ermöglichen, die IMDS-IPv6-Adresse zum Abrufen von Instanz-Metadaten zu verwenden. `[fd00:ec2::254]` Diese Option ist nur verfügbar, wenn Sie Instances, die auf dem AWS Nitro-System basieren, in einem IPv6-unterstützten Subnetz starten (Dual-Stack oder nur IPv6). Weitere Informationen zum Abrufen von Instance-Metadaten finden Sie unter Abrufen von Instance-Metadaten.
- Metadatenversion: Wenn Sie den Zugriff auf den IMDS aktivieren, können Sie festlegen, dass die Verwendung von Instance-Metadatenservice Version 2 beim Anfordern von Instance-Metadaten erforderlich ist. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.

- Metadaten-Token-Antwort-Hop-Limit: Wenn Sie den IMDS aktivieren, können Sie die zulässige Anzahl von Netzwerk-Hops für das Metadaten-Token festlegen. Weitere Informationen finden Sie unter IMDSv2 verwenden.
- User data: Sie können Benutzerdaten so festlegen, dass eine Instance während des Starts konfiguriert wird oder dass ein Konfigurationsskript ausgeführt wird. Um eine Datei anzufügen, wählen Sie die Option As file aus und gehen Sie zu der anzufügenden Datei.

Schritt 4: Hinzufügen von Speicher

Die von Ihnen ausgewählte AMI beinhaltet ein oder mehrere Speicher-Volumes, einschließlich eines Root-Gerät-Volumes. Auf der Seite Add Storage (Speicher hinzufügen) können Sie durch Auswahl von Add New Volume (Neues Volume hinzufügen) zusätzliche Volumes angeben, die der Instance zugeordnet werden. Konfigurieren Sie die einzelnen Volumes wie folgt und wählen Sie anschließend Next: Add Tags (Weiter: Tags (Markierungen) hinzufügen) aus.

- Type: Wählen Sie Instance-Speicher- oder Amazon EBS-Volumes aus, die mit Ihrer Instance verknüpft werden. Die in der Liste verfügbaren Volume-Typen hängen von dem Instance-Typ ab, den Sie ausgewählt haben. Weitere Informationen finden Sie unter Amazon EC2-Instance-Speicher und Amazon EBS-Volumes.
- Device: Wählen Sie aus der Liste verfügbarer Gerätenamen für das Volume einen Eintrag aus.
- Snapshot: Geben Sie den Namen oder die ID des Snapshots ein, von dem oder der ein Volume wiederhergestellt wird. Sie können auch nach verfügbaren geteilten und öffentlichen Snapshots suchen, indem Sie Text in das Feld Snapshot eingeben. Bei den Snapshot-Beschreibungen muss die Groß- und Kleinschreibung beachtet werden.
- Size (Größe): Sie können für EBS-Volumes eine Speichergröße angeben. Auch wenn Sie ein AMI und eine Instance ausgewählt haben, die im kostenlosen Kontingent enthalten sind, dürfen Sie den Grenzwert von 30 GiB Gesamtspeicher nicht überschreiten, um innerhalb des kostenlosen Kontingents zu bleiben.
- Volume Type (Volume-Typ): Sie wählen für EBS-Volumes einen Volume-Typ aus. Weitere Informationen finden Sie unter Amazon EBS-Volumetypen im Amazon EBS-Benutzerhandbuch.
- IOPS: Wenn Sie einen Provisioned IOPS SSD-Volume-Typ ausgewählt haben, können Sie die Zahl der I/O-Vorgänge pro Sekunde (IOPS) eingeben, die das Volume unterstützen kann.
- Delete on Termination: Aktivieren Sie bei Amazon EBS-Volumes dieses Kontrollkästchen, um das Volume zu löschen, wenn die Instance beendet ist. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.

- Encrypted (Verschlüsselt): Wenn der Instance-Typ die EBS-Verschlüsselung unterstützt, können Sie den Verschlüsselungsstatus des Volumes angeben. Wenn die für diese Region die standardmäßige Verschlüsselung aktiviert haben, wird der Standard-CMK für Sie ausgewählt. Sie können einen anderen Schlüssel auswählen oder die Verschlüsselung deaktivieren. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung im Amazon EBS-Benutzerhandbuch.

Schritt 5: Hinzufügen von Tags (Markierungen)

Legen Sie auf der Seite Add Tags die Tags (Markierungen) fest, indem Sie die Schlüssel- und Wert-Kombinationen angeben. Sie können die Instance, die Volumes oder beides markieren. Bei Spot-Instances können Sie nur die Spot-Instance-Anforderung mit Tags (Markierungen) versehen. Klicken Sie auf Add another Tag, um Ihren Ressourcen mehrere Tags (Markierungen) hinzuzufügen. Wählen Sie Next: Configure Security Group, wenn Sie bereit sind.

Schritt 6: Konfigurieren einer Sicherheitsgruppe

Verwenden Sie auf der Seite Configure Security Group eine Sicherheitsgruppe, um Firewall-Regeln für Ihre Instance zu definieren. Diese Regeln legen fest, welcher eingehende Netzwerkverkehr an Ihre Instance übertragen wird. Der gesamte übrige Datenverkehr wird ignoriert. (Weitere Informationen zu Sicherheitsgruppen finden Sie unter Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances.) Gehen Sie folgendermaßen vor, um eine Sicherheitsgruppe auszuwählen oder zu erstellen. Klicken Sie anschließend auf Review and Launch.

- Um eine vorhandene Sicherheitsgruppe zu wählen, wählen Sie Select an existing security group und dann Ihre Sicherheitsgruppe. Sie können die Regeln einer vorhandenen Sicherheitsgruppe nicht bearbeiten. Sie können diese jedoch zu einer neuen Gruppe kopieren, indem Sie Copy to new (Zu neu kopieren) auswählen. Sie können dann Regeln hinzufügen, wie im nächsten Schritt beschrieben.
- Um eine neue Sicherheitsgruppe zu erstellen, wählen Sie Create a new security group. Der Assistent definiert automatisch die Sicherheitsgruppe launch-wizard- x und erstellt eine Regel für eingehenden Datenverkehr, mit der Sie eine Verbindung zu Ihrer Instance herstellen können. Linux-Instances verwenden eine eingehende Regel für SSH (Port 22) und Windows-Instances verwenden eine eingehende Regel für RDP (Port 3389).
- Sie können Regeln gemäß Ihren Anforderungen hinzufügen. Wenn Ihre Instance beispielsweise ein Webserver ist, öffnen Sie die Ports 80 (HTTP) und 443 (HTTPS), um Internetdatenverkehr zuzulassen.

Um eine Regel hinzuzufügen, klicken Sie auf Add Rule, wählen Sie das Protokoll für das Öffnen für Netzwerk-Datenverkehr aus und legen Sie dann die Quelle fest. Wählen Sie My IP aus der Liste Source aus, damit der Assistent die öffentliche IP-Adresse Ihres Computers hinzufügt. Wenn Sie jedoch eine Verbindung über einen ISP oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen, müssen Sie den von Client-Computern verwendeten IP-Adressbereich herausfinden.

> **Warning**
>
> Für diese kurze Übung sind Regeln akzeptabel, die allen IP-Adressen (`0.0.0.0/0`) erlauben, über SSH oder RDP auf Ihre Instance zuzugreifen, für Produktionsumgebung ist dies jedoch unsicher. Sie sollten nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre Instance autorisieren.

Schritt 7: Prüfen des Instance-Starts und Auswahl des Schlüsselpaars

Prüfen Sie auf der Seite Review Instance Launch die Details Ihrer Instance und nehmen Sie notwendige Änderungen vor, indem Sie den entsprechenden Edit-Link auswählen.

Sobald Sie bereit sind, wählen Sie Launch aus.

Im Dialogfeld Select an existing key pair or create a new key pair (Ein bestehendes Schlüsselpaar wählen oder ein neues Schlüsselpaar erstellen) können Sie ein bestehendes Schlüsselpaar wählen oder ein neues erstellen. Klicken Sie beispielsweise auf Choose an existing key pair und wählen Sie dann das Schlüsselpaar aus, das Sie beim Einrichten erstellt haben. Weitere Informationen finden Sie unter Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances.

> **Important**
>
> Wenn Sie die Option Proceed without key pair auswählen, können Sie keine Verbindung zur Instance herstellen, es sei denn, Sie wählen ein AMI aus, das so konfiguriert ist, dass Benutzern eine andere Anmeldemöglichkeit erlaubt ist.

Zum Starten Ihrer Instance aktivieren Sie das Bestätigungskontrollkästchen und wählen Sie dann Launch Instances aus.

(Optional) Sie können einen Alarm für eine Statusprüfung für die Instance erstellen (möglicherweise fallen zusätzliche Gebühren an). Wählen Sie auf dem Bestätigungsbildschirm Create status check

alarms aus und folgen Sie den Anweisungen. Alarme für Statusprüfung können auch nach dem Start der Instance erstellt werden. Weitere Informationen finden Sie unter Erstellen und Bearbeiten von Statusprüfungsalarmen.

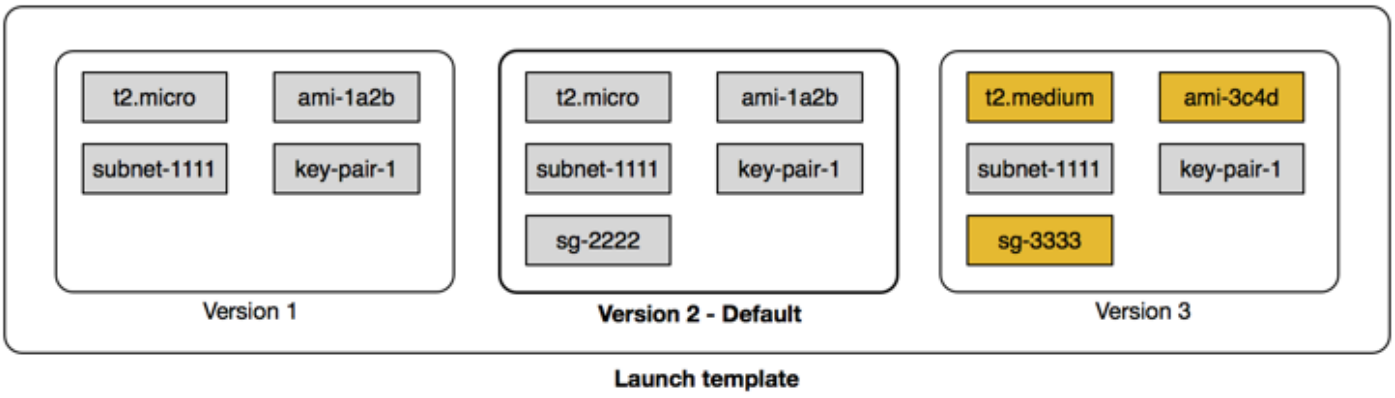
Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Starten einer Instance über eine Startvorlage

Sie können eine Startvorlage verwenden, um Instance-Startparameter zu speichern, sodass Sie sie nicht bei jedem Start einer Instance angeben müssen. Sie können beispielsweise eine Startvorlage mit der AMI-ID, dem Instance-Typ und den Netzwerkeinstellungen erstellen, die Sie normalerweise zum Starten von Instances verwenden. Wenn Sie eine Instance mit der Amazon EC2 EC2-Konsole, einem AWS SDK oder einem Befehlszeilentool starten, können Sie die Startvorlage angeben, anstatt die Parameter erneut einzugeben.

Sie können für jede Startvorlage eine oder mehrere nummerierte Startvorlagenversionen erstellen. Jede Version kann unterschiedliche Startparameter besitzen. Wenn Sie eine Instance über eine Startvorlage starten, können Sie eine beliebige Version der Startvorlage verwenden. Wenn Sie keine Version angeben, wird die Standardversion verwendet. Sie können eine beliebige Version der Startvorlage als Standardvorlage festlegen — standardmäßig ist dies die erste Version der Startvorlage.

Im folgenden Diagramm ist eine Startvorlage mit drei Versionen dargestellt. Die erste Version gibt den Instancetyp, die AMI-ID, das Subnetz und das Schlüsselpaar an, mit denen die Instance geladen werden soll. Die zweite Version basiert auf der ersten Version und gibt zudem eine Sicherheitsgruppe für die Instance an. Die dritte Version verwendet für einige der Parameter andere Werte. Version 2 wird als Standardversion festgelegt. Wenn über diese Startvorlage eine Instance gestartet werden würde, würden die Startparameter von Version 2 verwendet werden, sofern keine andere Version angegeben wurde.



Inhalt

Einschränkungen der Startvorlage

Die folgenden Regeln gelten für Startvorlagen und Startvorlagenversionen:

- Kontingente — Um die Kontingente für Ihre Startvorlagen und Startvorlagenversionen anzuzeigen, öffnen Sie die Service Quotas Quotas-Konsole oder verwenden Sie den list-service-quotas AWS CLI Befehl. Jedes AWS Konto kann bis zu 5.000 Startvorlagen pro Region und bis zu 10.000 Versionen pro Startvorlage enthalten. Ihre Konten können je nach Alter und Nutzungsverlauf über unterschiedliche Kontingente verfügen.
- Parameter sind optional – Startvorlagenparameter sind optional. Sie müssen jedoch sicherstellen, dass Ihre Anforderung zum Launchen einer Instance alle erforderlichen Parameter enthält. Wenn Ihre Startvorlage z. B. keine AMI-ID enthält, müssen Sie sowohl die Startvorlage als auch eine AMI-ID eingeben, wenn Sie eine Instance starten.
- Parameter nicht validiert – Die Parameter der Startvorlage werden nicht vollständig validiert, wenn Sie die Startvorlage erstellen. Wenn Sie falsche Werte für Parameter angeben oder keine unterstützten Parameterkombinationen verwenden, können keine Instances unter Verwendung dieser Startvorlage gestartet werden. Achten Sie darauf, die richtigen Werte für die Parameter anzugeben und unterstützte Parameter-Kombinationen zu verwenden. Um beispielsweise eine Instance in einer Platzierungsgruppe zu starten, müssen Sie einen unterstützten Instance-Typ angeben.
- Tags – Sie können eine Startvorlage, jedoch nicht die Version einer Startvorlage markieren.
- Unveränderlich – Startvorlagen sind unveränderlich. Um eine Startvorlage zu ändern, müssen Sie eine neue Version der Startvorlage erstellen.
- Versionsnummern – Die Startvorlagenversionen werden in der Reihenfolge nummeriert, in der sie erstellt werden. Wenn Sie eine Startvorlagenversion erstellen, können Sie die Versionsnummer nicht selbst angeben.

Steuern des Zugriffs auf Startvorlagen mit IAM-Berechtigungen

Mithilfe von IAM-Berechtigungen können Sie steuern, welche Aktionen Benutzer für Startvorlagen ausführen können, z. B. Startvorlagen anzeigen, erstellen oder löschen.

Wenn Sie Benutzern die Erlaubnis erteilen, Startvorlagen und Startvorlagenversionen zu erstellen, können Sie die Ressourcen, die sie in einer Startvorlage angeben können, nicht mithilfe von Berechtigungen auf Ressourcenebene einschränken. Stellen Sie daher sicher, dass Sie nur den entsprechenden Administratoren Berechtigungen zum Erstellen von Startvorlagen und Startvorlagenversionen gewähren.

Sie müssen jedem, der eine Startvorlage verwendet, die erforderlichen Berechtigungen zum Erstellen und Zugreifen auf die in der Startvorlage angegebenen Ressourcen gewähren. Beispielsweise:

- Um eine Instance von einem gemeinsam genutzten privaten Amazon Machine Image (AMI) aus zu starten, muss der Benutzer über eine Startberechtigung für das AMI verfügen.
- Um EBS-Volumes mit Tags aus vorhandenen Snapshots zu erstellen, muss der Benutzer über Lesezugriff auf die Snapshots sowie über Berechtigungen zum Erstellen und Markieren von Volumes verfügen.

Inhalt

ec2: Vorlage CreateLaunch

Um eine Startvorlage in der Konsole oder mithilfe der APIs zu erstellen, muss der Prinzipal über die `ec2:CreateLaunchTemplate`-Berechtigung in einer IAM-Richtlinie verfügen. Verwenden Sie nach Möglichkeit Tags, um den Zugriff auf die Startvorlagen in Ihrem Konto zu steuern.

Beispielsweise gewährt die folgende IAM-Richtlinienanweisung dem Prinzipal nur dann die Berechtigung, Startvorlagen zu erstellen, wenn die Vorlage das angegebene Tag verwendet (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForCreatingTaggedLaunchTemplates",
    "Action": "ec2:CreateLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Prinzipale, die Schlüssel erstellen, benötigen möglicherweise einige verwandte Berechtigungen, wie beispielsweise:

- ec2: CreateTags — Um der Startvorlage während des `CreateLaunchTemplate` Vorgangs Tags hinzuzufügen, muss der `CreateLaunchTemplate` Aufrufer über die `ec2:CreateTags` entsprechende Berechtigung in einer IAM-Richtlinie verfügen.
- ec2: RunInstances — Um EC2-Instances von der Startvorlage aus zu starten, die sie erstellt haben, muss der Principal auch über die `ec2:RunInstances` entsprechende Berechtigung in einer IAM-Richtlinie verfügen.

Bei Aktionen zur Ressourcenerstellung, die Tags anwenden, müssen Benutzer über `ec2:CreateTags`-Berechtigungen verfügen. Die folgende IAM-Richtlinienanweisung verwendet den Bedingungsschlüssel `ec2:CreateAction`, um Benutzern das Erstellen von Tags nur im Kontext von `CreateLaunchTemplate` zu ermöglichen. Die Benutzer können keine vorhandenen Startvorlagen oder andere Ressourcen kennzeichnen. Weitere Informationen finden Sie unter Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.

```
{
    "Sid": "IAMPolicyForTaggingLaunchTemplatesOnCreation",
    "Action": "ec2:CreateTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateLaunchTemplate"
        }
    }
```

```
}
```

Der IAM-Benutzer, der eine Startvorlage erstellt, verfügt nicht automatisch über die Berechtigung, die von ihm erstellte Startvorlage zu verwenden. Wie jeder andere Prinzipal muss der Ersteller der Startvorlage eine Berechtigung über eine IAM-Richtlinie erhalten. Wenn ein IAM-Benutzer eine EC2-Instance über eine Startvorlage starten möchte, muss er über die `ec2:RunInstances`-Berechtigung verfügen. Beim Gewähren dieser Berechtigungen können Sie festlegen, dass Benutzer nur Startvorlagen mit bestimmten Tags oder bestimmten IDs verwenden können. Sie können auch das AMI und andere Ressourcen steuern, auf die jeder, der Startvorlagen verwendet, beim Starten von Instances verweisen und diese verwenden kann, indem Sie Berechtigungen auf Ressourcenebene für den `RunInstances`-Aufruf angeben. Beispiele für Richtlinien finden Sie unter Startvorlagen.

ec2: Vorlagen DescribeLaunch

Um Startvorlagen im Konto aufzulisten, muss der Prinzipal über die `ec2:DescribeLaunchTemplates`-Berechtigung in einer IAM-Richtlinie verfügen. Da `Describe`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen, müssen sie Sie ohne Bedingungen angeben, und der Wert des Ressourcenelements in der Richtlinie muss `"*"` sein.

Beispielsweise gewährt die folgende IAM-Richtlinienanweisung dem Prinzipal die Berechtigung, alle Startvorlagen im Konto aufzulisten.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplates",
    "Action": "ec2:DescribeLaunchTemplates",
    "Effect": "Allow",
    "Resource": "*"
}
```

ec2: DescribeLaunch TemplateVersions

Prinzipale, die Startvorlagen aufrufen, sollten auch über die `ec2:DescribeLaunchTemplateVersions`-Berechtigung verfügen, den gesamten Satz von Attributen abzurufen, aus denen die Startvorlagen bestehen.

Um Startvorlagenversionen im Konto aufzulisten, muss der Prinzipal über die `ec2:DescribeLaunchTemplateVersions`-Berechtigung in einer IAM-Richtlinie verfügen. Da `Describe`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen, müssen sie Sie ohne Bedingungen angeben, und der Wert des Ressourcenelements in der Richtlinie muss `"*"` sein.

Beispielsweise gewährt die folgende IAM-Richtlinienanweisung dem Prinzipal die Berechtigung, alle Startvorlagenversionen im Konto aufzulisten.

```
{
    "Sid": "IAMPolicyForDescribingLaunchTemplateVersions",
    "Effect": "Allow",
    "Action": "ec2:DescribeLaunchTemplateVersions",
    "Resource": "*"
}
```

ec2: Vorlage DeleteLaunch

> **Important**
>
> Seien Sie vorsichtig, wenn Sie Prinzipalen die Berechtigung zum Löschen einer Ressource gewähren. Das Löschen einer Startvorlage kann zu einem Fehler in einer AWS Ressource führen, die auf der Startvorlage basiert.

Um eine Startvorlage zu löschen muss der Prinzipal über die `ec2:DeleteLaunchTemplate`-Berechtigung in einer IAM-Richtlinie verfügen. Wann immer möglich, verwenden Sie Bedingungsschlüssel, um die Berechtigungen einzuschränken.

Die folgende IAM-Richtlinienanweisung gewährt dem Prinzipal beispielsweise nur dann die Berechtigung, Startvorlagen zu löschen, wenn die Vorlage das angegebene Tag verwendet (*purpose*=*testing*).

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplates",
    "Action": "ec2:DeleteLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/purpose": "testing"
        }
    }
}
```

Alternativ können Sie ARNs verwenden, um die Startvorlage zu identifizieren, auf die die IAM-Richtlinie angewendet wird.

Eine Startvorlage verfügt über den folgenden ARN.

```
"Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d310e"
```

Sie können mehrere ARNs angeben, indem Sie sie in eine Liste einschließen, oder Sie können einen `Resource`-Wert von `"*"` ohne das `Condition`-Element angeben, damit der Prinzipal alle Startvorlagen im Konto löschen kann.

Steuern von Berechtigungen für Versionsverwaltung

Vertrauenswürdigen Administratoren können Sie Zugriff zum Erstellen und Löschen von Versionen einer Startvorlage sowie zum Ändern der Standardversion einer Startvorlage gewähren, indem Sie IAM-Richtlinien ähnlich den folgenden Beispielen verwenden.

Important

Seien Sie vorsichtig, wenn Sie Principals die Erlaubnis erteilen, Startvorlagenversionen zu erstellen oder Startvorlagen zu ändern.

- Wenn Sie eine Startvorlagenversion erstellen, wirken Sie sich auf alle AWS Ressourcen aus, die es Amazon EC2 ermöglichen, Instances in Ihrem Namen mit der `Latest` Version zu starten.
- Wenn Sie eine Startvorlage ändern, können Sie die Version ändern `Default` und sich somit auf alle AWS Ressourcen auswirken, die es Amazon EC2 ermöglichen, Instances in Ihrem Namen mit dieser modifizierten Version zu starten.

Sie müssen auch vorsichtig mit AWS Ressourcen umgehen, die mit der Vorlagenversion interagieren `Latest` oder diese `Default` starten, wie EC2-Flotte und Spot-Flotte. Wenn für `Latest` oder `Default` eine andere Startvorlagenversion verwendet wird, überprüft Amazon EC2 die Benutzerberechtigungen nicht erneut auf auszuführende Aktionen, wenn neue Instances gestartet werden, um die Zielkapazität der Flotte zu erfüllen, da keine Benutzerinteraktion mit der AWS -Ressource erfolgt. Indem einem Benutzer die Berechtigung zum Aufrufen der APIs `CreateLaunchTemplateVersion` und `ModifyLaunchTemplate` gewährt wird, wird dem Benutzer effektiv auch die `iam:PassRole`-Berechtigung gewährt, wenn er die Flotte auf eine andere Startvorlagenversion verweist, die ein Instance-Profil (einen Container für eine IAM-Rolle) enthält. Dies bedeutet, dass ein Benutzer potenziell eine Startvorlage aktualisieren kann, um eine IAM-Rolle an eine Instance zu übergeben, auch wenn er nicht über die

entsprechende `iam:PassRole`-Berechtigung verfügt. Sie können dieses Risiko kontrollieren, indem Sie bei der Vergabe von Berechtigungen für die Erstellung und Verwaltung von Startvorlagenversionen vorsichtig vorgehen.

ec2: CreateLaunchTemplateVersion

Um eine neue Version einer Startvorlage zu erstellen, muss der Prinzipal über die `ec2:CreateLaunchTemplateVersion`-Berechtigung für die Startvorlage in einer IAM-Richtlinie verfügen.

Die folgende IAM-Richtlinienerklärung gewährt dem Prinzipal beispielsweise nur dann die Berechtigung, Startvorlagenversionen zu erstellen, wenn die Version das angegebene Tag verwendet (*`environment`*=*`production`*). Alternativ können Sie eine oder mehrere Startvorlagen-ARNs angeben, oder Sie können einen `Resource`-Wert von `"*"` ohne das `Condition`-Element angeben, damit der Prinzipal Versionen jeder Startvorlage im Konto erstellen kann.

```
{
    "Sid": "IAMPolicyForCreatingLaunchTemplateVersions",
    "Action": "ec2:CreateLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2: DeleteLaunch TemplateVersion

Important

Wie immer sollten Sie Vorsicht walten lassen, wenn Sie Prinzipalen die Berechtigung zum Löschen einer Ressource erteilen. Das Löschen einer Version der Startvorlage kann zu einem Fehler in einer AWS Ressource führen, die auf der Version der Startvorlage basiert.

Um eine neue Version einer Startvorlagenversion zu erstellen, muss der Prinzipal über die `ec2:DeleteLaunchTemplateVersion`-Berechtigung für die Startvorlage in einer IAM-Richtlinie verfügen.

Die folgende IAM-Richtlinienerklärung gewährt dem Prinzipal beispielsweise nur dann die Berechtigung, Startvorlagenversionen zu löschen, wenn die Version das angegebene Tag verwendet (*`environment`*=*`production`*). Alternativ können Sie eine oder mehrere Startvorlagen-ARNs angeben, oder Sie können einen `Resource`-Wert von `"*"` ohne das `Condition`-Element angeben, damit der Prinzipal Versionen jeder Startvorlage im Konto löschen kann.

```
{
    "Sid": "IAMPolicyForDeletingLaunchTemplateVersions",
    "Action": "ec2:DeleteLaunchTemplateVersion",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

ec2: ModifyLaunchTemplate

Um die mit einer Startvorlage zugeordnete `Default`-Version zu ändern, muss der Prinzipal über die `ec2:ModifyLaunchTemplate`-Berechtigung für die Startvorlage in einer IAM-Richtlinie verfügen.

Die folgende IAM-Richtlinienerklärung gewährt dem Prinzipal beispielsweise nur dann die Berechtigung, Startvorlagen zu ändern, wenn die Vorlage das angegebene Tag verwendet (*`environment`*=*`production`*). Alternativ können Sie eine oder mehrere Startvorlagen-ARNs angeben, oder Sie können einen `Resource`-Wert von `"*"` ohne das `Condition`-Element angeben, damit der Prinzipal jede Startvorlage im Konto ändern kann.

```
{
    "Sid": "IAMPolicyForModifyingLaunchTemplates",
    "Action": "ec2:ModifyLaunchTemplate",
    "Effect": "Allow",
    "Resource": "*",
    "Condition": {
```

```
        "StringEquals": {
            "aws:ResourceTag/environment": "production"
        }
    }
}
```

Steuern des Zugriffs auf Tags in Startvorlagen

Sie können Bedingungsschlüssel verwenden, um Tagging-Berechtigungen einzuschränken, wenn es sich bei der Ressource um eine Startvorlage handelt. Die folgende IAM-Richtlinie erlaubt beispielsweise nur das Entfernen des Tags mit dem *temporary*-Schlüssel aus Startvorlagen im angegebenen Konto und in der angegebenen Region.

```
{
    "Sid": "IAMPolicyForDeletingTagsOnLaunchTemplates",
    "Action": "ec2:DeleteTags",
    "Effect": "Allow",
    "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
    "Condition": {
        "ForAllValues:StringEquals": {
            "aws:TagKeys": ["temporary"]
        }
    }
}
```

Weitere Informationen zu Bedingungsschlüsseln, mit denen Sie die Tag-Schlüssel und -Werte steuern können, die auf Amazon-EC2-Ressourcen angewendet werden können, finden Sie unter Kontrollieren des Zugriffs auf bestimmte Tags (Markierungen).

Verwenden der Startvorlagen für das Starten von Instances

Sie können festlegen, dass Benutzer Instances nur über eine Startvorlage starten können und dass sie nur eine bestimmte Startvorlage verwenden dürfen. Sie können auch festlegen, wer Startvorlagen und Versionen von Startvorlagen erstellen, ändern, beschreiben und löschen darf.

Verwenden von Startvorlagen zum Steuern von Startparametern

Eine Startvorlage kann alle oder einige der Parameter zum Starten einer Instance enthalten. Wenn Sie eine Instance über eine Startvorlage starten, können Sie Parameter außer Kraft setzen, die in der Startvorlage angegeben werden. Sie können auch zusätzliche Parameter angeben, die nicht in der Startvorlage enthalten sind.

> **Note**
>
> Sie können während des Starts keine Startvorlagenparameter entfernen (Sie können beispielsweise keinen Nullwert für den Parameter angeben). Um einen Parameter zu entfernen, erstellen Sie eine neue Version der Startvorlage ohne den Parameter und starten Sie die Instance mit dieser Version.

Zum Starten von Instances müssen Benutzer über die Berechtigung zur Verwendung der `ec2:RunInstances`-Aktion verfügen. Benutzer müssen außerdem über Berechtigungen zum Erstellen oder Verwenden der Ressourcen verfügen, die mit der Instance erstellt oder ihr zugewiesen werden. Sie können für die Aktion `ec2:RunInstances` Berechtigungen auf Ressourcenebene verwenden, um die Startparameter zu steuern, die die Benutzer festlegen können. Alternativ können Sie Benutzern gestatten, eine Instance unter Nutzung einer Startvorlage zu starten. Auf diese Weise können Sie Startparameter über eine Startvorlage anstatt über eine IAM-Richtlinie verwalten und eine Startvorlage als Autorisierungsmethode für das Starten von Instances einsetzen. Sie können z. B. festlegen, dass Benutzer Instances nur über eine Startvorlage starten und dass sie nur eine bestimmte Startvorlage verwenden können. Sie können auch steuern, welche Startparameter Benutzer in der Startvorlage außer Kraft setzen dürfen. Beispiele für Richtlinien finden Sie unter Startvorlagen.

Steuern der Nutzung von Startvorlagen

Standardmäßig sind -Benutzer nicht zum Arbeiten mit Startvorlagen berechtigt. Sie können eine Richtlinie erstellen, über die Benutzer Berechtigungen zum Erstellen, Ändern, Beschreiben und Löschen von Startvorlagen und Startvorlagenversionen erhalten. Sie können auf einige Startvorlagen-Aktionen auch Berechtigungen auf Ressourcenebene anwenden, mit denen Sie steuern können, welche Ressourcen Benutzer für diese Aktionen nutzen können. Weitere Informationen erhalten Sie in den folgenden Beispielrichtlinien: Beispiel: Arbeiten mit Startvorlagen.

Überlegen Sie sorgfältig, wenn Sie Benutzern Berechtigungen zur Verwendung der Aktionen `ec2:CreateLaunchTemplate` und `ec2:CreateLaunchTemplateVersion` erteilen. Mit Berechtigungen auf Ressourcenebene können Sie nicht steuern, welche Ressourcen Benutzer in der Startvorlage angeben können. Um einzuschränken, welche Ressourcen zum Starten einer Instance verwendet werden, achten Sie darauf, nur die betreffenden Administratoren zum Erstellen von Startvorlagen und Startvorlagenversionen zu berechtigen.

Wichtige Sicherheitsaspekte bei der Verwendung von Startvorlagen mit EC2-Flotte oder -Spot-Flotte

Zur Verwendung von Startvorlagen müssen Sie Ihren Benutzern auch Berechtigungen zum Erstellen, Ändern, Beschreiben und Löschen von Startvorlagen und Startvorlagenversionen erteilen. Sie können steuern, wer Startvorlagen und Startvorlagenversionen erstellen kann, indem Sie den Zugriff auf die Aktionen `ec2:CreateLaunchTemplate` und `ec2:CreateLaunchTemplateVersion` steuern. Sie können auch steuern, wer Startvorlagen ändern kann, indem Sie den Zugriff auf die Aktion `ec2:ModifyLaunchTemplate` steuern.

> **Important**
>
> Wenn eine EC2-Flotte oder Spot-Flotte so konfiguriert ist, dass sie die aktuelle oder standardmäßige Startvorlagenversion verwendet, weiß die Flotte nicht, ob die aktuelle Version oder die Standardversion später geändert werden, sodass sie auf eine andere Startvorlagenversion verweisen. Wenn eine andere Version der Startvorlage als aktuelle Version oder Standardversion verwendet wird, überprüft Amazon EC2 die Berechtigungen für auszuführende Aktionen nicht erneut, wenn neue Instances gestartet werden, um die Zielkapazität der Flotte zu erreichen. Dies ist ein wichtiger Aspekt bei der Erteilung von Berechtigungen für die Erstellung und Verwaltung von Startvorlagenversionen, insbesondere bei der Aktion `ec2:ModifyLaunchTemplate`, die es einem Benutzer ermöglicht, die Standardversion der Startvorlage zu ändern.

Wenn einem Benutzer die Berechtigung erteilt wird, die EC2-Aktionen für die Startvorlagen-APIs zu verwenden, erhält der Benutzer effektiv auch die `iam:PassRole`-Berechtigung, wenn eine EC2-Flotte oder -Spot-Flotte erstellt oder aktualisiert wird, um auf eine andere Startvorlagenversion zu verweisen, die ein Instance-Profil enthält (einen Container für eine IAM-Rolle). Dies bedeutet, dass ein Benutzer potenziell eine Startvorlage aktualisieren kann, um eine IAM-Rolle an eine Instance zu übergeben, auch wenn er nicht über die entsprechende `iam:PassRole`-Berechtigung verfügt. Weitere Informationen und ein Beispiel für eine IAM-Richtlinie finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

Weitere Informationen finden Sie unter Steuern der Nutzung von Startvorlagen und Beispiel: Arbeiten mit Startvorlagen.

Erstellen einer Startvorlage

Erstellen Sie eine Startvorlage mit von Ihnen definierten Parametern, oder verwenden Sie eine vorhandene Startvorlage oder eine Instanz als Grundlage für eine neue Startvorlage.

Aufgaben

- Erstellen Sie eine Startvorlage aus Parametern
- Erstellen einer Startvorlage anhand einer vorhandenen Startvorlage
- Erstellen einer Startvorlage aus einer Instance
- Verwenden eines Systems-Manager-Parameters anstelle einer AMI-ID

Erstellen Sie eine Startvorlage aus Parametern

Um eine Launchvorlage zu erstellen, müssen Sie den Namen der Launchvorlage und mindestens einen Instance-Konfigurationsparameter angeben.

Anweisungen für die Konsole

Um eine Startvorlage mit der Konsole zu erstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates (Startvorlagen) und dann Create launch template (Startvorlage erstellen) aus.
3. Die Parameter der Startvorlage sind gruppiert. Einzelheiten zu den einzelnen Gruppen finden Sie in den folgenden Abschnitten.
4. Verwenden Sie den Bereich „Zusammenfassung“, um die Konfiguration Ihrer Startvorlage zu überprüfen. Sie können zu einem beliebigen Abschnitt navigieren, indem Sie den entsprechenden Link auswählen und dann die erforderlichen Änderungen vornehmen.
5. Wenn Sie bereit sind, Ihre Launchvorlage zu erstellen, wählen Sie Create launch template (Launchvorlage erstellen) aus.

Name, Beschreibung und Tags der Startvorlage

1. Geben Sie für Launch template name (Startvorlagenname) einen aussagekräftigen Namen für die Startvorlage ein.
2. Geben Sie unter Template version description (Beschreibung der Vorlagenversion) eine kurze Beschreibung dieser Version der Startvorlage ein.

3. Um die Startvorlage bei der Erstellung zu markieren, erweitern SieTemplate tags (Vorlagen-Tags) und wählen Sie Add tag (Tag hinzufügen) aus. Geben Sie dann einen Tag-Schlüssel und ein Wert-Paar ein. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.

   > **Note**
   >
   > Um die Ressourcen zu markieren, die beim Start einer Instance erstellt werden, müssen Sie die Tags unter Resource tags (Ressourcen-Tags) angeben. Weitere Informationen finden Sie unter Ressourcen-Tags.

Anwendungs- und Betriebssystem-Images (Amazon Machine Image)

Ein Amazon Machine Image (AMI) enthält die Informationen, die zum Starten einer Instance erforderlich sind. Ein AMI kann beispielsweise die Software enthalten, die für die Funktion als Webserver erforderlich ist, z. B. Linux, Apache und Ihre Website.

Sie finden wie folgt ein passendes AMI. Bei jeder Option zum Auffinden eines AMIs können Sie Cancel (Abbrechen) (oben rechts) auswählen, um zur Launchvorlage zurückzukehren, ohne ein AMI auszuwählen.

Suchleiste

Um alle verfügbaren AMIs zu durchsuchen, geben Sie ein Schlüsselwort in die AMI-Suchleiste ein und drücken Sie dann die Eingabetaste. Wählen Sie Select (Auswählen) zum Auswählen des AMI aus.

Kürzlich gestartet

Die AMIs, die Sie kürzlich verwendet haben.

Wählen Sie Kürzlich gestartet oder Derzeit verwendet aus und wählen Sie dann unter Amazon Machine Image (AMI) ein AMI.

My AMIs

Die privaten AMIs, die Sie besitzen oder private AMIs, die für Sie freigegeben wurden

Klicken Sie auf Im Besitz von mir oder Mit mir geteilt und wählen Sie dann unter Amazon Machine Image (AMI) ein AMI aus.

Schnellstart

AMIs sind nach Betriebssystem (OS) gruppiert, damit Sie loslegen können.

Wählen Sie zuerst das benötigte Betriebssystem und dann unter Amazon Machine Image (AMI) ein AMI aus. Um ein AMI auszuwählen, das für das kostenlose Kontingent berechtigt ist, vergewissern Sie sich, dass das AMI als Für kostenloses Kontingent berechtigt markiert ist.

Durchsuchen Sie weitere AMIs

Wählen Sie Weitere AMIs durchsuchen aus, um den vollständigen AMI-Katalog zu durchsuchen.

- Um alle verfügbaren AMIs zu durchsuchen, geben Sie ein Schlüsselwort in die Suchleiste ein und drücken Sie dann die Eingabetaste.
- Um mit einem Systems-Manager-Parameter nach einem AMI zu suchen, wählen Sie die Pfeilschaltfläche rechts neben der Suchleiste und dann Search by Systems Manager parameter (Nach Systems-Manager-Parameter suchen) aus. Weitere Informationen finden Sie unter Finden Sie ein AMI mithilfe eines Systems Manager Manager-Parameters.
- Um einen Systems-Manager-Parameter anzugeben, der beim Start einer Instance aus der Startvorlage in ein AMI aufgelöst wird, wählen Sie die Pfeilschaltfläche rechts neben der Suchleiste und dann Benutzerdefinierten Wert/Systems-Manager-Parameter angeben aus. Weitere Informationen finden Sie unter Verwenden eines Systems-Manager-Parameters anstelle einer AMI-ID.
- Um nach Kategorie zu suchen, wählen Sie Schnellstart-AMIs, Meine AMIs, AWS Marketplace - AMIs oder Community-AMIs aus.

  Das AWS Marketplace ist ein Online-Shop, in dem Sie Software kaufen können, die darauf läuft AWS, einschließlich AMIs. Weitere Informationen zum Starten einer Instance vom AWS Marketplace finden Sie unterStarten Sie eine AWS Marketplace Instanz. In Community-AMIs finden Sie AMIs, die AWS Community-Mitglieder anderen zur Nutzung zur Verfügung gestellt haben. AMIs von Amazon oder einem verifizierten Partner sind mit Verifizierter Anbieter gekennzeichnet.
- Um die Liste der AMIs zu filtern, aktivieren Sie ein oder mehrere Kontrollkästchen unter Ergebnisse verfeinern auf der linken Seite des Bildschirms. Die Filteroptionen unterscheiden sich in Abhängigkeit von der ausgewählten Suchkategorie.
- Prüfen Sie, welcher Root device type für die einzelnen AMIs aufgeführt ist. Achten Sie darauf, welche AMIs den benötigten Typ aufweisen: entweder ebs (unterstützt von Amazon EBS) oder instance-store (unterstützt durch Instance-Speicher). Weitere Informationen finden Sie unter Speicher für das Root-Gerät.

- Prüfen Sie, welcher Typ unter Virtualization type für die einzelnen AMIs aufgeführt ist. Achten Sie darauf, welche AMIs den benötigten Typ aufweisen: entweder hvm oder paravirtual. Manche Instance-Typen benötigen beispielsweise HVM. Weitere Informationen finden Sie unter AMI-Virtualisierungstypen.
- Prüfen Sie den für jedes AMI aufgelisteten Startmodus. Achten Sie darauf, welche AMIs den benötigten Startmodus aufweisen: entweder legacy-bios, uefi oder uefi-preferred. Weitere Informationen finden Sie unter Amazon EC2 EC2-Startmodi.
- Wählen Sie ein AMI aus, das Ihren Anforderungen entspricht, und klicken Sie auf Select.

Instance-Typ

Der Instance-Typ definiert die Hardware-Konfiguration und Größe der Instance. Größere Instance-Typen haben mehr CPU und Arbeitsspeicher. Weitere Informationen finden Sie unter Amazon EC2 EC2-Instance-Typen.

Für Instance type (Instance-Typ) können Sie entweder einen Instance-Typ auswählen oder Sie können Instance-Attribute angeben und Amazon EC2 die Instance-Typen mit diesen Attributen identifizieren lassen.

> **Note**
>
> Die Angabe von Instance-Attributen wird nur unterstützt, wenn Auto-Scaling-Gruppen, EC2-Flottte und Spot-Flotte zum Starten von Instances verwendet werden. Weitere Informationen finden Sie unter Erstellen einer Auto-Scaling-Gruppe mithilfe der attributbasierten Instance-Typauswahl, Attributbasierte Auswahl von Instance-Typen für EC2-Flotte und Attributbasierte Auswahl von Instance-Typen für Spot-Flotte.
> Wenn Sie die Startvorlage im Launch-Instance-Assistenten oder mit der RunInstancesAPI verwenden möchten, müssen Sie einen Instance-Typ auswählen.

- Instance type (Instance-Typ): Vergewissern Sie sich, dass der Instance-Typ mit dem von Ihnen angegebenen AMI kompatibel ist. Weitere Informationen finden Sie unter Amazon EC2-Instance-Typen.
- Vergleichen von Instance-Typen: Sie können verschiedene Instance-Typen anhand der folgenden Attribute vergleichen: Anzahl der vCPUs, Architektur, Speichermenge (GiB), Speichertyp und Netzwerkleistung.

- Tipps einholen: Sie können Anleitungen und Vorschläge für Instance-Typen vom Amazon Q EC2 Instance Type Selector erhalten. Weitere Informationen finden Sie unter Empfehlungen für Instance-Typen für einen neuen Workload erhalten:.
- Erweitert: Um Instance-Attribute anzugeben und Amazon EC2 die Instance-Typen mit diesen Attributen identifizieren zu lassen, wählen Sie Erweitert und dann Instance-Typ-Attribute angeben.
  - Anzahl vCPUs: Geben Sie die minimale und maximale Anzahl der vCPUs für Ihre Rechenanforderungen ein. Um keine Limits anzugeben, geben Sie einen Mindestwert von **0** ein und lassen Sie den Höchstwert leer.
  - Speichermenge (MiB): Geben Sie in MiB den minimalen und maximalen Arbeitsspeicher für Ihre Rechenanforderungen ein. Um keine Limits anzugeben, geben Sie einen Mindestwert von **0** ein und lassen Sie den Höchstwert leer.
  - Erweitern Sie Optionale Instance-Typattribute und wählen Sie Attribut hinzufügen aus, um Ihre Rechenanforderungen detaillierter auszudrücken. Informationen zu den einzelnen Attributen finden Sie unter InstanceRequirementsAnfrage in der Amazon EC2 API-Referenz.
  - Resultierende Instance-Typen: Sie können eine Vorschau der Instance-Typen anzeigen, die den angegebenen Attributen entsprechen. Um Instance-Typen auszuschließen, wählen Sie Attribut hinzufügen aus und wählen Sie in der Liste Attribut die Option Ausgeschlossene Instance-Typen. Wählen Sie aus der Liste Attributwert die auszuschließenden Instance-Typen aus.

Schlüsselpaar (Anmeldung)

Das Schlüsselpaar für die Instance.

Wählen Sie für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder wählen Sie Neues Schlüsselpaar erstellen, um ein neues zu erstellen. Weitere Informationen finden Sie unter Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances.

Network settings (Netzwerkeinstellungen)

Konfigurieren Sie die Netzwerkeinstellungen nach Bedarf.

- Subnetz: Sie können eine Instance in einem Subnetz starten, das einer Availability Zone, einer Local Zone, Wavelength-Zone oder einem Outpost zugeordnet ist.

  Um die Instance in einer Availability Zone zu starten, wählen Sie das Subnetz aus, in dem die Instance gestartet werden soll. Um ein neues Subnetz zu erstellen, wählen Sie Create new subnet aus, um die Amazon VPC-Konsole aufzurufen. Wenn Sie fertig sind, kehren Sie zum Assistenten zurück und wählen Sie das Symbol „Aktualisieren“, um Ihr Subnetz in die Liste zu laden.

Um die Instance in einer Local Zone zu starten, wählen Sie ein Subnetz aus, das Sie in der Local Zone erstellt haben.

Um eine Instance in einem Outpost zu starten, wählen Sie ein Subnetz in einer VPC aus, die Sie dem Outpost zugeordnet haben.

- Firewall (security groups) (Firewal (Sicherheitsgruppen)): Verwenden Sie eine oder mehrere Sicherheitsgruppen, um Firewall-Regeln für Ihre Instance zu definieren. Diese Regeln legen fest, welcher eingehende Netzwerkverkehr an Ihre Instance übertragen wird. Der gesamte übrige Datenverkehr wird ignoriert. Weitere Informationen zu Sicherheitsgruppen finden Sie unter Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances.

  Wenn Sie eine Netzwerkschnittstelle hinzufügen, müssen Sie dieselben Sicherheitsgruppen in der Netzwerkschnittstelle angeben.

  Wählen oder erstellen Sie eine Sicherheitsgruppe wie folgt:

  - Um eine vorhandene Sicherheitsgruppe auszuwählen, wählen Sie Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und wählen Sie Ihre Sicherheitsgruppe unter Common security groups (Allgemeine Sicherheitsgruppen).
  - Um eine neue Sicherheitsgruppe zu erstellen, wählen Sie Create a new security group (Sicherheitsgruppe erstellen).

    Sie können Regeln gemäß Ihren Anforderungen hinzufügen. Wenn Ihre Instance beispielsweise ein Webserver ist, öffnen Sie die Ports 80 (HTTP) und 443 (HTTPS), um den Internetdatenverkehr zu erlauben.

    Um eine Regel hinzuzufügen, wählen Sie Sicherheitsgruppenregel hinzufügen aus. Wählen Sie unter Type (Typ) den Netzwerkverkehrstyp aus. Das Feld Protokoll wird automatisch mit dem Protokoll ausgefüllt, um es für Netzwerkverkehr zu öffnen. Wählen Sie unter Quelltyp einen Quelltyp aus. Damit die Launchvorlage die öffentliche IP-Adresse Ihres Computers hinzufügen kann, wählen Sie My IP (Meine IP) aus. Wenn Sie jedoch eine Verbindung über einen ISP oder hinter Ihrer Firewall ohne statische IP-Adresse herstellen, müssen Sie den von Client-Computern verwendeten IP-Adressbereich herausfinden.

    > **Warning**
    >
    > Regeln, die allen IP-Adressen (`0.0.0.0/0`) den Zugriff auf Ihre Instance über SSH oder RDP ermöglichen, sind akzeptabel, wenn Sie eine Test-Instance kurz starten und bald

anhalten oder beenden, sind jedoch nicht für Produktionsumgebungen geeignet. Sie sollten nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre Instance autorisieren.

- Advanced network configuration (Erweiterte Netzwerkkonfiguration)

  Netzwerkschnittstelle

  - Device (Gerät): Die Gerätenummer für die Netzwerkschnittstelle, z. B. `eth0` für die primäre Netzwerkschnittstelle. Wenn Sie das Feld leer lassen, erstellt AWS die primäre Netzwerkschnittstelle.
  - Network interface (Netzwerkschnittstelle): Wählen Sie New interface (Neue Schnittstelle), damit Amazon EC2 eine neue Schnittstelle erstellen kann oder wählen Sie eine vorhandene, verfügbare Netzwerkschnittstelle aus.
  - Description (Beschreibung): (Optional) Eine Beschreibung für die neue Netzwerkschnittstelle.
  - Subnet (Subnetz): Das Subnetz, in dem eine neue Netzwerkschnittstelle erstellt werden soll. Für die primäre Netzwerkschnittstelle (`eth0`) ist dies das Subnetz, in dem die Instance gestartet wird. Wenn Sie für `eth0` eine vorhandene Netzwerkschnittstelle eingeben, wird die Instance in dem Subnetz gestartet, in dem sich die Netzwerkschnittstelle befindet.
  - Security groups (Sicherheitsgruppen): Eine oder mehrere Sicherheitsgruppen in Ihrer VPC, der/denen die Netzwerkschnittstelle zugeordnet werden soll.
  - Auto-assign Public IP (Öffentliche IP automatisch zuordnen): Legen Sie fest, ob Ihre Instance eine öffentliche IPv4-Adresse erhält. Instances in einem Standardsubnetz erhalten standardmäßig eine öffentliche IPv4-Adresse, Instances in einem nicht standardmäßigen Subnetz nicht. Sie können Enable oder Disable auswählen, um die Standardeinstellungen des Subnetzes zu überschreiben. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen.
  - Primary IP (Primäre IP): Eine private IPv4-Adresse aus dem Adressbereich für Ihr Subnetz. Lassen Sie das Feld leer, damit Amazon EC2 für Sie eine private IPv4-Adresse auswählen kann.
  - Secondary IP (Sekundäre IP): Eine oder mehrere zusätzliche private IPv4-Adressen aus dem Bereich Ihres Subnetzes. Klicken Sie auf Manuelles Zuweisen und geben Sie eine IP-Adresse ein. Klicken Sie auf IP hinzufügen, um eine weitere IP-Adresse hinzuzufügen. Alternativ können Sie Automatisch zuweisen auswählen, um Amazon EC2 ein AMI auswählen zu lassen. Geben Sie dann einen Wert ein, um die Anzahl der hinzuzufügenden IP-Adressen anzugeben.
  - (Nur IPv6) IPv6 IPs: Eine IPv6-Adresse aus dem Adressbereich für Ihr Subnetz. Klicken Sie auf Manuelles Zuweisen und geben Sie eine IP-Adresse ein. Klicken Sie auf IP hinzufügen, um eine weitere IP-Adresse hinzuzufügen. Alternativ können Sie Automatisch zuweisen auswählen, um

Amazon EC2 ein AMI auswählen zu lassen. Geben Sie dann einen Wert ein, um die Anzahl der hinzuzufügenden IP-Adressen anzugeben.

- IPv4 Prefixes: Die IPv4-Präfixe für die Netzwerkschnittstelle.
- IPv6 Prefixes: Die IPv6-Präfixe für die Netzwerkschnittstelle.
- (Optional) Primäre IPv6-IP zuweisen: Wenn Sie eine Instance in einem Dual-Stack- oder Nur-IPv6-Subnetz starten, haben Sie die Möglichkeit, primäre IPv6-IP zuzuweisen. Durch die Zuweisung einer primären IPv6-Adresse können Sie eine Unterbrechung des Datenverkehrs zu Instances oder ENIs vermeiden. Wählen Sie Aktivieren, wenn diese Instance davon abhängt, dass sich ihre IPv6-Adresse nicht ändert. Wenn Sie die Instance starten, AWS wird automatisch eine IPv6-Adresse, die der mit Ihrer Instance verbundenen ENI zugeordnet ist, als primäre IPv6-Adresse zugewiesen. Sobald Sie eine IPv6-GUA-Adresse als primäre IPv6-Adresse aktiviert haben, können Sie sie nicht mehr deaktivieren. Wenn Sie eine IPv6-GUA-Adresse als primäre IPv6-Adresse aktivieren, wird die erste IPv6-GUA zur primären IPv6-Adresse gemacht, bis die Instance beendet oder die Netzwerkschnittstelle getrennt wird. Wenn Ihrer Instance mehrere IPv6-Adressen mit einer angefügten ENI zugeordnet sind und Sie eine primäre IPv6-Adresse aktivieren, wird die erste IPv6-GUA-Adresse, die der ENI zugeordnet ist, zur primären IPv6-Adresse.
- Delete on termination (Bei Beenden löschen): Wählen Sie aus, ob die Netzwerkschnittstelle gelöscht werden soll, wenn die Instance gelöscht wird.
- Elastic Fabric Adapter: Gibt an, ob die Netzwerkschnittstelle ein Elastic Fabric Adapter ist. Weitere Informationen finden Sie unter the section called “Elastic Fabric Adapter”.
- Network card index (Netzwerkkarten-Index): Der Index der Netzwerkkarte. Die primäre Netzwerkschnittstelle muss dem Netzwerkkartenindex 0 zugewiesen sein. Einige Instance-Typen unterstützen mehrere Netzwerkkarten.
- ENA Express: ENA Express basiert auf der SRD-Technologie (AWS Scalable Reliable Datagram). Die SRD-Technologie verwendet einen Paketverteilungsmechanismus, um die Last zu verteilen und Netzwerküberlastungen zu vermeiden. Durch die Aktivierung von ENA Express können unterstützte Instances zusätzlich zu regulärem TCP-Datenverkehr auch SRD für die Kommunikation verwenden (sofern möglich). Die Startvorlage enthält keine ENA Express-Konfiguration für die Instance, es sei denn, Sie wählen Aktivieren oder Deaktivieren aus.
- ENA Express UDP: Wenn Sie ENA Express aktiviert haben, können Sie es optional für UDP-Datenverkehr verwenden. Die Startvorlage enthält keine ENA Express-Konfiguration für die Instance, es sei denn, Sie wählen Aktivieren oder Deaktivieren aus.

Wählen Sie Add network interface (Netzwerkschnittstelle hinzufügen) aus, um weitere Netzwerkschnittstellen hinzuzufügen. Die Anzahl der Netzwerkschnittstellen, die Sie hinzufügen können, hängt von der Anzahl ab, die vom ausgewählten Instance-Typ unterstützt wird. Zusätzliche Netzwerkschnittstellen können sich in einem anderen Subnetz derselben VPC oder in einem Subnetz in einer anderen VPC befinden, die Sie besitzen (sofern sich das Subnetz in derselben Availability Zone wie Ihre Instance befindet). Wenn Sie ein Subnetz in einer anderen VPC auswählen, wird die Bezeichnung Multi-VPC neben der Netzwerkschnittstelle angezeigt, die Sie hinzugefügt haben. Dadurch können Sie VPC-übergreifend mehrfach vernetzte Instances mit unterschiedlichen Netzwerk- und Sicherheitskonfigurationen erstellen. Beachten Sie, dass Sie, wenn Sie eine zusätzliche ENI von einer anderen VPC anhängen, eine Sicherheitsgruppe für die ENI aus dieser VPC auswählen müssen.

Weitere Informationen finden Sie unter Elastic-Network-Schnittstelle. Wenn Sie mehr als eine Netzwerkschnittstelle angeben, kann Ihre Instance keine öffentliche IPv4-Adresse erhalten. Außerdem können Sie, wenn Sie für eth0 eine vorhandene Netzwerkschnittstelle angeben, die Subnetzeinstellung für öffentliche IPv4-Adressen nicht mithilfe von Auto-assign Public IP überschreiben. Weitere Informationen finden Sie unter Zuweisen einer öffentlichen IPv4-Adresse beim Start einer Instance.

Speicher konfigurieren

Wenn Sie ein AMI für die Launchvorlage angeben, enthält das AMI ein oder mehrere Speicher-Volumes, einschließlich des Root-Volumes (Volume 1 (AMI Root)). Sie können zusätzliche Volumes angeben, die an die Instance angehängt werden sollen.

Sie können die Ansicht Einfach oder Erweitert verwenden. Mit der einfachen Ansicht legen Sie die Größe und Art des Volumes fest. Um alle Volume-Parameter anzugeben, verwenden Sie die Ansicht Erweitert oben rechts auf der Karte.

Um ein neues Volume hinzuzufügen, wählen Sie Add new volume (Neues Volume hinzufügen).

In der erweiterten Ansicht können Sie jedes Volume wie folgt konfigurieren:

- Storage type (Speichertyp): Der Typ des Volumes (EBS oder flüchtig), das Ihrer Instance zugeordnet werden soll. Der Volume-Typ Instance-Speicher (flüchtig) ist nur verfügbar, wenn Sie einen Instance-Typ auswählen, der ihn unterstützt. Weitere Informationen finden Sie unter Amazon EC2-Instance-Speicher und Amazon EBS-Volumes.

- Device name (Gerätename): Wählen Sie aus der Liste verfügbarer Gerätenamen für das Volume einen Eintrag aus.
- Snapshot: Wählen Sie den Snapshot aus, von dem das Volume erstellt werden soll. Sie können nach verfügbaren freigegebenen und öffentlichen Snapshots suchen, indem Sie Text in das Feld Snapshot eingeben.
- Größe (GiB): Sie können für EBS-Volumes eine Speichergröße angeben. Wenn Sie ein AMI und eine Instance ausgewählt haben, die im kostenlosen Kontingent enthalten sind, dürfen Sie den Grenzwert von 30 GiB Gesamtspeicher nicht überschreiten, um innerhalb des kostenlosen Kontingents zu bleiben.
- Volume Type (Volume-Typ): Wählen Sie für die EBS-Volumes einen Volume-Typ aus. Weitere Informationen finden Sie unter Amazon EBS-Volumetypen im Amazon EBS-Benutzerhandbuch.
- IOPS: Wenn Sie einen Volume des Typs Bereitgestellte IOPS-SSD (`io1` und `io2`) oder Universelle SSD (`gp3`) ausgewählt haben, können Sie die Anzahl der I/O-Operationen pro Sekunde (IOPS) eingeben, die das Volume unterstützen kann. Dies ist für io1-, io2- und gp3-Volumes erforderlich. Wird bei gp2-, st1-, sc1- oder Standard-Volumes nicht unterstützt. Wenn Sie diesen Parameter für die Startvorlage weglassen, müssen Sie einen Wert dafür angeben, wenn Sie eine Instance über die Startvorlage starten.
- Delete on termination (Bei Beendigung löschen): Wählen Sie für Amazon-EBS-Volumes Ja, um das Volume zu löschen, wenn die Instance beendet wird oder wählen Sie Nein, um das Volume beizubehalten. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.
- Encrypted (Verschlüsselt): Wenn der Instance-Typ die EBS-Verschlüsselung unterstützt, können Sie Ja auswählen, um die Verschlüsselung für das Volume zu aktivieren. Wenn Sie für diese Region die standardmäßige Verschlüsselung aktiviert haben, wird der Standard-CMK für Sie ausgewählt. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung im Amazon EBS-Benutzerhandbuch.
- KMS key (KMS-Schlüssel): Wenn Sie Yes (Ja) für Encrypted (Verschlüsselt) ausgewählt haben, müssen Sie einen kundenverwalteten Schlüssel zum Verschlüsseln des Volumes auswählen. Wenn die für diese Region die standardmäßige Verschlüsselung aktiviert haben, wird der Standard-CMK für Sie ausgewählt. Sie können einen anderen Schlüssel auswählen oder den ARN eines Kundenverwaltungsschlüssels angeben, den Sie erstellt haben.

Ressourcen-Tags

Um die Ressourcen zu markieren, die beim Start einer Instance erstellt werden, wählen Sie unterResource tags (Ressourcen-Tags) Add tag (Tag hinzufügen)aus, und geben Sie dann einen Tag-Schlüssel und ein Wert-Paar ein. Geben Sie unter Resource types (Ressourcentypen) die Ressourcen an, die bei der Erstellung markiert werden sollen. Sie können den gleichen Tag für alle Ressourcen spezifizieren oder verschiedene Tags für verschiedene Ressourcen angeben. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.

Sie können Tags für die folgenden Ressourcen angeben, die erstellt werden, wenn eine Startvorlage verwendet wird:

- Instances
- Datenträger
- Spot-Instance-Anforderungen
- Netzwerkschnittstellen

> **Note**
>
> Um die Startvorlage selbst zu markieren, müssen Sie die Tags unter Template tags (Vorlagen-Tags) angeben. Weitere Informationen finden Sie unter Name, Beschreibung und Tags der Startvorlage.

Erweiterte Details

Erweitern Sie für Advanced details (Erweiterte Details) den Bereich zur Ansicht der Felder und geben Sie zusätzliche Parameter für die Instance an.

- Kaufoption: Wählen Sie Request Spot Instances (Spot-Instances anfordern), um Spot-Instances zum Spot-Preis anzufordern, der auf den On-Demand-Preis begrenzt ist, und wählen Sie Customize (Anpassen), um die Standardeinstellungen für Spot-Instances zu ändern. Sie können Ihren Höchstpreis festlegen (nicht empfohlen) und den Anforderungstyp, die Anforderungsdauer und das Unterbrechungsverhalten ändern. Wenn Sie keine Spot-Instance anfordern, startet EC2 standardmäßig eine On-Demand-Instance. Weitere Informationen finden Sie unter Spot-Instances.
- IAM instance profile (IAM-Instance-Profil): Wählen Sie ein AWS Identity and Access Management -Instance-Profil (IAM), das der Instance zugeordnet werden soll. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.

- Hostname type (Hostnamentyp): Wählen Sie aus, ob der Hostname des Gastbetriebssystems der Instance der Ressourcenname oder der IP-Name sein soll. Weitere Informationen finden Sie unter Hostnamentypen für Amazon-EC2-Instances.
- DNS Hostname (DNS-Hostname): Bestimmt, ob die DNS-Abfragen an den Ressourcennamen oder den IP-Namen (je nach der Auswahl für Hostname type (Hostnamentyp)) mit der IPv4-Adresse (A-Datensatz), der IPv6-Adresse (AAAA-Datensatz) oder beidem antworten. Weitere Informationen finden Sie unter Hostnamentypen für Amazon-EC2-Instances.
- Shutdown behavior: Wählen Sie aus, ob die Instance beim Herunterfahren angehalten oder beendet werden soll. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.
- Stop - Hibernate behavior (Stopp – Verhalten im Ruhezustand): Um den Ruhezustand zu aktivieren, wählen Sie Enable (Aktivieren). Dieses Feld ist nur für Instances gültig, die die Voraussetzungen für den Ruhezustand erfüllen. Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand.
- Termination protection (Beendigungsschutz): Um ein versehentliches Beenden zu verhindern, wählen Sie Aktivieren. Weitere Informationen finden Sie unter Aktivieren des Beendigungsschutzes.
- Stop protection (Stoppschutz): Um ein versehentliches Anhalten zu verhindern, wählen Sie Enable (Aktivieren). Weitere Informationen finden Sie unter Aktivieren des Stopp-Schutzes.
- Detaillierte CloudWatch Überwachung: Wählen Sie Aktivieren, um eine detaillierte Überwachung der Instance mithilfe von Amazon zu aktivieren CloudWatch. Es fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.
- Elastische GPU: Amazon Elastic Graphics hat am 8. Januar 2024 das Ende der Lebensdauer erreicht. Für Workloads, die Grafikbeschleunigung erfordern, empfehlen wir die Verwendung von Amazon EC2 G4ad-, G4dn- oder G5-Instances.
- Elastic inference (Elastic Inference): Ein Elastic Inference-Accelerator, der Ihrer EC2-CPU-Instance zugewiesen werden soll. Weitere Informationen finden Sie unter Arbeiten mit Amazon Elastic Inference im Amazon Elastic Inference Developer-Handbuch.

> **Note**
>
> Ab 15. April 2023 AWS wird Amazon Elastic Inference (EI) keine Neukunden mehr in Amazon Elastic Inference (EI) einbinden und Bestandskunden dabei helfen, ihre Workloads auf Optionen umzustellen, die ein besseres Preis und eine bessere Leistung bieten. Nach dem 15. April 2023 können Neukunden keine Instances mit Amazon EI-Beschleunigern in

Amazon SageMaker, Amazon ECS oder Amazon EC2 starten. Kunden, die Amazon EI in den letzten 30 Tagen mindestens einmal genutzt haben, gelten jedoch als aktuelle Kunden und können den Service weiterhin nutzen.

- Guthabenspezifikation: Wählen Sie Unbegrenzt aus, damit Anwendungen so lange wie nötig über die Baseline hinaus laufen können. Dieses Feld gilt nur für T-Instances. Es können zusätzliche Gebühren anfallen. Weitere Informationen finden Sie unter Burstable Performance Instances.
- Placement group name: Geben Sie eine Platzierungsgruppe an, in der die Instance gestartet werden soll. Wählen Sie eine vorhandene Platzierungsgruppe aus oder erstellen Sie eine neue. Nicht alle Instance-Typen können in einer Platzierungsgruppe gestartet werden. Weitere Informationen finden Sie unter Placement-Gruppen.
- EBS-optimized instance (EBS-optimierte Instance): Wählen Sie Enable (Aktivieren) aus, um zusätzliche, dedizierte Kapazität für Amazon-EBS-I/O bereitzustellen. Nicht alle Instance-Typen unterstützen dieses Feature. Es fallen zusätzliche Gebühren an. Weitere Informationen finden Sie unter the section called “EBS-Optimierung”.
- Capacity Reservation (Kapazitätsreservierung): Geben Sie an, ob die Instance in einer beliebigen offenen Kapazitätsreservierung (Offen), einer bestimmten Kapazitätsreservierung (Ziel nach ID) oder einer Kapazitätsreservierungsgruppe (Ziel nach Gruppe) gestartet werden soll. Um anzugeben, dass keine Kapazitätsreservierung verwendet werden soll, wählen Sie None (Keine) aus. Weitere Informationen finden Sie unter Starten von Instances in einer bestehenden Kapazitätsreservierung.
- Tenancy: Wählen Sie aus, ob Ihre Instance auf einer gemeinsam genutzten (Shared), isolierten oder dedizierten (Dedicated) Hardware oder auf einem dedizierten Host Dedicated Host (Dedicated host) ausgeführt werden soll. Wenn Sie die Instance auf einem Dedicated Host starten möchten, können Sie angeben, ob die Instance in einer Hostressourcengruppe gestartet werden soll oder ob Sie eine bestimmte Dedicated Host verwenden möchten. Es können zusätzliche Gebühren anfallen. Weitere Informationen finden Sie unter Dedicated Instances und Dedicated Hosts.
- RAM disk ID (RAM-Datenträgerkennung): (Nur gültig für Paravirtual-AMIS (PV-AMIs). Wählen Sie eine RAM-Festplatte für die Instance. Wenn Sie einen Kernel ausgewählt haben, müssen Sie möglicherweise eine bestimmte RAM-Disk mit den Treibern auswählen, um ihn zu unterstützen.
- Kernel ID (Kernel-ID: (Nur gültig für Paravirtual-AMIs (PV-AMIs). Wählen Sie ein Kernel für die Instance.
- Nitro Enclaves: Mit dieser Funktion können Sie aus Amazon-EC2-Instances isolierte Ausführungsumgebungen namens Enklaven erstellen. Wählen Sie Enable (Aktivieren) aus, um

die Instance für AWS Nitro Enclaves zu aktivieren. Weitere Informationen finden Sie unter Was ist AWS Nitro Enclaves? im AWS -Nitro-Enclaves-Benutzerhandbuch.

- License configurations (Lizenzkonfigurationen): Sie können Instances für die angegebene Lizenzkonfiguration starten, um die Lizenznutzung nachzuverfolgen. Weitere Informationen finden Sie unter Erstellen einer Lizenzkonfiguration im Benutzerhandbuch zu AWS License Manager.
- Specify CPU options (CPU-Optionen angeben): Wählen Sie Specify CPU options (CPU-Optionen angeben) aus, um eine benutzerdefinierte Anzahl von vCPUs beim Launchen festzulegen. Legen Sie die Anzahl der CPU-Kerne und -Threads pro Kern fest. Weitere Informationen finden Sie unter CPU-Optionen optimieren.
- IPv6-Endpunkt mit Metadaten: Sie können der Instance ermöglichen, die IMDS-IPv6-Adresse `[fd00:ec2::254]` zum Abrufen von Instance-Metadaten zu verwenden. Diese Option ist nur verfügbar, wenn Sie Instances, die auf dem AWS Nitro-System basieren, in einem IPv6-unterstützten Subnetz starten (Dual-Stack oder nur IPv6). Weitere Informationen finden Sie unter Abrufen von Instance-Metadaten.
- Metadatenzugriff: Sie können den Zugriff auf den IMDS aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- Metadatenversion: Wenn Sie den Zugriff auf den IMDS aktivieren, können Sie festlegen, dass die Verwendung von Instance-Metadatenservice Version 2 beim Anfordern von Instance-Metadaten erforderlich ist. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- Metadatenantwort-Hop-Limit: Wenn Sie den IMDS aktivieren, können Sie die zulässige Anzahl von Netzwerk-Hops für das Metadaten-Token festlegen. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.
- Allow tags in metadata (Tags in Metadaten zulassen): Wenn Sie Enable (Aktivieren) auswählen, erlaubt die Instance den Zugriff auf alle ihre Instance-Tags aus ihren Metadaten. Wenn Sie diese Einstellung nicht in die Vorlage aufnehmen, ist der Zugriff auf die Tags in Instance-Metadaten standardmäßig nicht erlaubt. Weitere Informationen finden Sie unter Zulassen des Zugriffs auf Tags in Instance-Metadaten.
- User data: Sie können Benutzerdaten so festlegen, dass eine Instance während des Starts konfiguriert wird oder dass ein Konfigurationsskript ausgeführt wird. Weitere Informationen finden Sie unter Führen Sie beim Start Befehle auf Ihrer Amazon EC2 EC2-Instance aus.

AWS CLI Beispiel

Im folgenden Beispiel wird der Befehl create-launch-template verwendet, um eine Startvorlage mit dem angegebenen Namen und der angegebenen Instanzkonfiguration zu erstellen.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --version-description WebVersion1 \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Im Folgenden finden Sie ein JSON-Beispiel, das die Startvorlagendaten für die Instanzkonfiguration angibt. Speichern Sie den JSON-Code in einer Datei und nehmen Sie ihn in den `--launch-template-data` Parameter auf, wie im Beispielbefehl gezeigt.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r4.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":2
    }
}
```

Es folgt eine Beispielausgabe.

```
{
    "LaunchTemplate": {
```

```
        "LatestVersionNumber": 1,
        "LaunchTemplateId": "lt-01238c059e3466abc",
        "LaunchTemplateName": "TemplateForWebServer",
        "DefaultVersionNumber": 1,
        "CreatedBy": "arn:aws:iam::123456789012:root",
        "CreateTime": "2017-11-27T09:13:24.000Z"
    }
}
```

AWS Tools for Windows PowerShell Beispiel

Im folgenden Beispiel wird das New-EC2LaunchTemplateCmdlet verwendet, um eine Startvorlage mit dem angegebenen Namen und der Instanzkonfiguration zu erstellen.

```
$launchTemplateData = [Amazon.EC2.Model.RequestLaunchTemplateData]@{
    ImageId = 'ami-8c1be5f6'
    InstanceType = 'r4.4xlarge'
    NetworkInterfaces = @(
        [Amazon.EC2.Model.LaunchTemplateInstanceNetworkInterfaceSpecificationRequest]@{
            AssociatePublicIpAddress = $true
            DeviceIndex = 0
            Ipv6AddressCount = 1
            SubnetId = 'subnet-7b16de0c'
        }
    )
    TagSpecifications = @(
        [Amazon.EC2.Model.LaunchTemplateTagSpecificationRequest]@{
            ResourceType = 'instance'
            Tags = [Amazon.EC2.Model.Tag]@{
                Key = 'Name'
                Value = 'webserver'
            }
        }
    )
    CpuOptions = [Amazon.EC2.Model.LaunchTemplateCpuOptionsRequest]@{
        CoreCount = 4
        ThreadsPerCore = 2
    }
}
$tagSpecificationData = [Amazon.EC2.Model.TagSpecification]@{
    ResourceType = 'launch-template'
    Tags = [Amazon.EC2.Model.Tag]@{
        Key = 'purpose'
```

```
        Value = 'production'
    }
}
New-EC2LaunchTemplate -LaunchTemplateName 'TemplateForWebServer' -VersionDescription
 'WebVersion1' -LaunchTemplateData $launchTemplateData -TagSpecification
 $tagSpecificationData
```

Es folgt eine Beispielausgabe.

```
CreatedBy            : arn:aws:iam::123456789012:root
CreateTime           : 9/19/2023 16:57:55
DefaultVersionNumber : 1
LatestVersionNumber  : 1
LaunchTemplateId     : lt-01238c059eEXAMPLE
LaunchTemplateName   : TemplateForWebServer
Tags                 : {purpose}
```

Erstellen einer Startvorlage anhand einer vorhandenen Startvorlage

Sie können eine vorhandene Startvorlage klonen und dann die Parameter anpassen, um eine neue Startvorlage zu erstellen. Dies ist jedoch nur möglich, wenn Sie die Amazon EC2 EC2-Konsole verwenden. Das Klonen einer Vorlage AWS CLI wird nicht unterstützt.

Console

So erstellen Sie eine Startvorlage anhand einer vorhandenen Startvorlage

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates (Startvorlagen) und dann Create launch template (Startvorlage erstellen) aus.
3. Geben Sie für Launch template name (Startvorlagenname) einen aussagekräftigen Namen für die Startvorlage ein.
4. Geben Sie unter Template version description (Beschreibung der Vorlagenversion) eine kurze Beschreibung dieser Version der Startvorlage ein.
5. Um die Startvorlage bei der Erstellung mit einem Tag (Markierung) zu markieren, erweitern Sie Template Tags (Vorlagen-Tag (Markierung)), wählen Add Tags (Tags (Markierung) hinzufügen) aus und geben Sie dann ein Tag (Markierung)-Schlüssel-/Wert-Paar ein.
6. Erweitern Sie Source template (Quellvorlage). Wählen Sie in Launch template name (Name der Startvorlage) die Startvorlage aus, auf der die neue Startvorlage basieren soll.

7. Wählen Sie für Source template version die Version der Startvorlage aus, auf der die neue Startvorlage basieren soll.
8. Passen Sie alle Startparameter wie erforderlich an und wählen Sie Create launch template (Startvorlage erstellen).

Erstellen einer Startvorlage aus einer Instance

Console

So erstellen Sie eine Startvorlage aus einer Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und anschließend Aktionen, Eine Vorlage aus einer Instance erstellen aus.
4. Geben Sie einen Namen, eine Beschreibung und Tag (Markierung) an und passen Sie die Startparameter wie erforderlich an.

> **Note**
>
> Erstellen Sie eine Startvorlage aus einer Instance, so sind die ID- und IP-Adresse der Netzwerkschnittstelle der Instance in der Vorlage nicht enthalten.

5. Wählen Sie Create launch template.

AWS CLI

Sie können die verwenden AWS CLI , um eine Startvorlage aus einer vorhandenen Instance zu erstellen, indem Sie zuerst die Startvorlagendaten von einer Instance abrufen und dann mithilfe der Startvorlagendaten eine Startvorlage erstellen.

So erhalten Sie Startvorlagendaten von einer Instance

- Verwenden Sie den Befehl get-launch-template-data und geben Sie die Instance-ID an. Sie können die Ausgabe als Basis zum Erstellen einer neuen Startvorlage oder einer neuen Version der Startvorlage verwenden. Die Ausgabe umfasst standardmäßig ein `LaunchTemplateData`-Objekt der obersten Ebene, das nicht in den Daten der

Startvorlage angegeben werden kann. Verwenden Sie die Option `--query`, um dieses Objekt auszuschließen.

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData"
```

Es folgt eine Beispielausgabe.

```
    {
        "Monitoring": {},
        "ImageId": "ami-8c1be5f6",
        "BlockDeviceMappings": [
            {
                "DeviceName": "/dev/xvda",
                "Ebs": {
                    "DeleteOnTermination": true
                }
            }
        ],
        "EbsOptimized": false,
        "Placement": {
            "Tenancy": "default",
            "GroupName": "",
            "AvailabilityZone": "us-east-1a"
        },
        "InstanceType": "t2.micro",
        "NetworkInterfaces": [
            {
                "Description": "",
                "NetworkInterfaceId": "eni-35306abc",
                "PrivateIpAddresses": [
                    {
                        "Primary": true,
                        "PrivateIpAddress": "10.0.0.72"
                    }
                ],
                "SubnetId": "subnet-7b16de0c",
                "Groups": [
                    "sg-7c227019"
                ],
                "Ipv6Addresses": [
```

```
                {
                    "Ipv6Address": "2001:db8:1234:1a00::123"
                }
            ],
            "PrivateIpAddress": "10.0.0.72"
        }
    ]
}
```

Sie können die Ausgabe direkt in eine Datei schreiben, z. B.:

```
aws ec2 get-launch-template-data \
    --instance-id i-0123d646e8048babc \
    --query "LaunchTemplateData" >> instance-data.json
```

So erstellen Sie eine Startvorlage mithilfe von Startvorlagendaten

- Verwenden Sie den Befehl create-launch-template, um eine Startvorlage mit der Ausgabe des vorherigen Verfahrens zu erstellen. Weitere Informationen zum Erstellen einer Startvorlage mithilfe von finden Sie unterErstellen Sie eine Startvorlage aus Parametern. AWS CLI

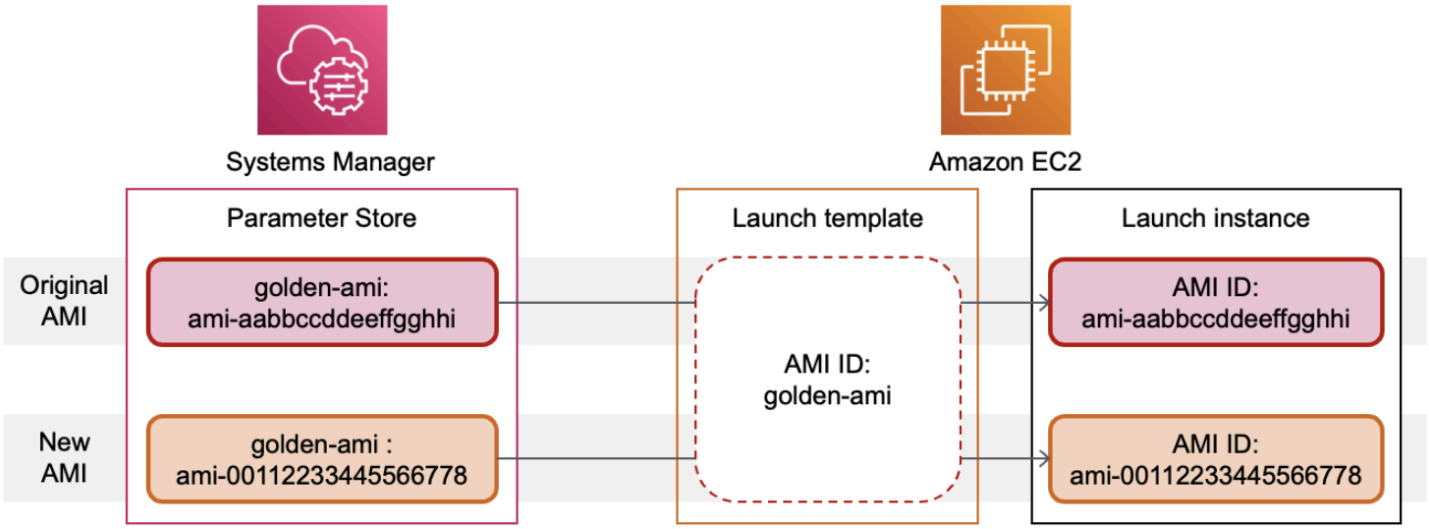
Verwenden eines Systems-Manager-Parameters anstelle einer AMI-ID

Sie können anstelle einer AMI-ID in Ihren Startvorlagen auch einen AWS Systems Manager -Parameter angeben. Wenn sich die AMI-ID ändert, können Sie die AMI-ID an einem Ort aktualisieren, indem Sie den Systems-Manager-Parameter im Systems-Manager-Parameterspeicher aktualisieren. Parameter können auch mit anderen geteilt werden AWS-Konten. Sie können AMI-Parameter zentral in einem Konto speichern und verwalten und sie mit jedem anderen Konto teilen, das sie referenzieren muss. Mithilfe eines Systems-Manager-Parameters können alle Ihre Startvorlagen in einer einzigen Aktion aktualisiert werden.

Ein Systems-Manager-Parameter ist ein benutzerdefiniertes Schlüssel-Wert-Paar, das Sie im Systems-Manager-Parameterspeicher erstellen. Der Parameterspeicher bietet einen zentralen Ort zum Speichern Ihrer Anwendungskonfigurationswerte. Weitere Informationen finden Sie unter AWS Systems Manager -Parameterspeicher im Benutzerhandbuch für AWS Systems Manager .

Im folgenden Diagramm wird der `golden-ami`-Parameter zuerst dem ursprünglichen AMI `ami-aabbccddeeffgghhi` im Parameterspeicher zugeordnet. In der Startvorlage lautet der Wert für die

AMI-ID `golden-ami`. Wenn eine Instance mit dieser Startvorlage gestartet wird, wird die AMI-ID zu `ami-aabbccddeeffgghhi` aufgelöst. Später wird das AMI aktualisiert, was zu einer neuen AMI-ID führt. Im Parameter Store wird der `golden-ami`-Parameter dem neuen `ami-00112233445566778` zugeordnet. Die Startvorlage bleibt unverändert. Wenn eine Instance mit dieser Startvorlage gestartet wird, wird die AMI-ID in das neue `ami-00112233445566778` aufgelöst.



Systems-Manager-Parameterformat für AMI-IDs

Startvorlagen erfordern, dass benutzerdefinierte Systems-Manager-Parameter das folgende Format einhalten, wenn sie anstelle einer AMI-ID verwendet werden:

- Parametertyp: `String`
- Parameterdatentyp: `aws:ec2:image` – Dadurch wird sichergestellt, dass der Parameterspeicher überprüft, ob der von Ihnen eingegebene Wert das richtige Format für eine AMI-ID hat.

Weitere Informationen zum Erstellen eines gültigen Parameters für eine AMI-ID finden Sie unter Erstellen von Systems-Manager-Parametern im AWS Systems Manager -Benutzerhandbuch.

Systems-Manager-Parameterformat in Startvorlagen

Um einen Systems-Manager-Parameter anstelle einer AMI-ID in einer Startvorlage zu verwenden, müssen Sie beim Angeben des Parameters in der Startvorlage eines der folgenden Formate verwenden:

Um auf einen öffentlichen Parameter zu verweisen:

- `resolve:ssm:`*`public-parameter`*

Um auf einen Parameter zu verweisen, der im selben Konto gespeichert ist:

- `resolve:ssm:parameter-name`
- `resolve:ssm:parameter-name:version-number` – Die Versionsnummer selbst ist eine Standardbezeichnung
- `resolve:ssm:parameter-name:label`

Um auf einen Parameter zu verweisen, der von einem anderen gemeinsam genutzt wird AWS-Konto:

- `resolve:ssm:parameter-ARN`
- `resolve:ssm:parameter-ARN:version-number`
- `resolve:ssm:parameter-ARN:label`

Parameter-Versionen

Systems-Manager-Parameter sind versionierte Ressourcen. Wenn Sie einen Parameter aktualisieren, erstellen Sie neue, aufeinander folgende Versionen des Parameters. Systems Manager unterstützt Parameterbezeichnungen, die Sie bestimmten Versionen eines Parameters zuordnen können.

Der `golden-ami`-Parameter kann beispielsweise drei Versionen haben: `1`, `2` und `3`. Sie können eine Parameterbezeichnung `beta` erstellen, die Version 2 zugeordnet ist, und eine Parameterbezeichnung `prod`, die Version `3` zugeordnet ist.

In einer Startvorlage können Sie Version 3 des `golden-ami`-Parameters angeben, indem Sie eines der folgenden Formate verwenden:

- `resolve:ssm:golden-ami:3`
- `resolve:ssm:golden-ami:prod`

Die Angabe der Version oder Bezeichnung ist optional. Wenn keine Version oder Bezeichnung angegeben ist, wird die neueste Version des Parameters verwendet.

Angeben eines Systems-Manager-Parameters in einer Startvorlage

Sie können einen Systems-Manager-Parameter in einer Startvorlage anstelle einer AMI-ID angeben, wenn Sie eine Startvorlage oder eine neue Version einer Startvorlage erstellen.

Console

So geben Sie einen Systems-Manager-Parameter in einer Startvorlage an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates (Startvorlagen) und dann Create launch template (Startvorlage erstellen) aus.
3. Geben Sie für Launch template name (Startvorlagenname) einen aussagekräftigen Namen für die Startvorlage ein.
4. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) die Option Browse more AMIs (Weitere AMIs durchsuchen) aus.
5. Wählen Sie die Pfeiltaste rechts neben der Suchleiste und wählen Sie dann Benutzerdefinierten Wert/Systems-Manager-Parameter angeben aus.
6. Gehen Sie im Dialogfeld Benutzerdefinierten Wert oder Systems-Manager-Parameter angeben wie folgt vor:

   a. Geben Sie für AMI-ID oder Systems-Manager-Parameterzeichenfolge den Systems-Manager-Parameternamen in einem der folgenden Formate ein:

      Um auf einen öffentlichen Parameter zu verweisen:

      - **resolve:ssm:*public-parameter***

      Um auf einen Parameter zu verweisen, der im selben Konto gespeichert ist:

      - **resolve:ssm:*parameter-name***
      - **resolve:ssm:*parameter-name*:*version-number***
      - **resolve:ssm:*parameter-name*:*label***

      Um auf einen Parameter zu verweisen, der von einem anderen gemeinsam genutzt wird AWS-Konto:

      - **resolve:ssm:*parameter-ARN***
      - **resolve:ssm:*parameter-ARN*:*version-number***
      - **resolve:ssm:*parameter-ARN*:*label***

b. Wählen Sie Speichern.

7. Geben Sie nach Bedarf weitere Startvorlagenparameter an und wählen Sie dann Startvorlage erstellen aus.

Weitere Informationen finden Sie unter Erstellen Sie eine Startvorlage aus Parametern.

AWS CLI

So geben Sie einen Systems-Manager-Parameter in einer Startvorlage an

- Verwenden Sie zum Erstellen der Startvorlage den create-launch-template-Befehl. Um das zu verwendende AMI anzugeben, geben Sie den Systems-Manager-Parameternamen in einem der folgenden Formate ein:

  Um auf einen öffentlichen Parameter zu verweisen:

  - **resolve:ssm:*public-parameter***

  Um auf einen Parameter zu verweisen, der im selben Konto gespeichert ist:

  - **resolve:ssm:*parameter-name***
  - **resolve:ssm:*parameter-name*:*version-number***
  - **resolve:ssm:*parameter-name*:*label***

  Um auf einen Parameter zu verweisen, der von einem anderen gemeinsam genutzt wird AWS-Konto:

  - **resolve:ssm:*parameter-ARN***
  - **resolve:ssm:*parameter-ARN*:*version-number***
  - **resolve:ssm:*parameter-ARN*:*label***

  Das folgende Beispiel erstellt eine Startvorlage, die Folgendes festlegt:

  - Ein Name für die Startvorlage (*TemplateForWebServer*)
  - Ein Tag für die Launchvorlage (*purpose*=*production*)
  - Die Daten für die Instance-Konfiguration, die in einer JSON-Datei angegeben sind:

- Das zu verwendende AMI (`resolve:ssm:golden-ami`)
- Der zu startende Instance-Typ (*m5.4xlarge*)
- Ein Tag für die Instance (*Name*=*webserver*)

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForWebServer \
    --tag-specifications 'ResourceType=launch-
template,Tags=[{Key=purpose,Value=production}]' \
    --launch-template-data file://template-data.json
```

Im Folgenden finden Sie eine Beispiel-JSON-Datei, die die Launchvorlagen-Daten für die Instance-Konfiguration enthält. Der Wert für `ImageId` ist der Systems-Manager-Parametername, der im erforderlichen Format `resolve:ssm:golden-ami` eingegeben wird.

```
{"LaunchTemplateData": {
    "ImageId": "resolve:ssm:golden-ami",
    "InstanceType": "m5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }]
  }
}
```

Stellen Sie sicher, dass eine Startvorlage die richtige AMI-ID erhält

Um den Systems Manager Manager-Parameter in die tatsächliche AMI-ID aufzulösen

Verwenden Sie den Befehl describe-launch-template-versions und fügen Sie den Parameter hinzu. `--resolve-alias`

```
aws ec2 describe-launch-template-versions \
    --launch-template-name my-launch-template \
    --versions $Default \
```

```
    --resolve-alias
```

Die Antwort enthält die AMI-ID für`ImageId`. Wenn in diesem Beispiel eine Instance mit dieser Startvorlage gestartet wird, wird die AMI-ID wie folgt aufgelöst. `ami-0ac394d6a3example`

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-089c023a30example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2022-12-28T19:52:27.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Bob",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0ac394d6a3example",
                "InstanceType": "t3.micro",
            }
        }
    ]
}
```

Zugehörige Ressourcen

Weitere Informationen zur Arbeit mit Systems Manager Manager-Parametern finden Sie in den folgenden Referenzmaterialien in der Systems Manager Manager-Dokumentation.

- Informationen zum Nachschlagen der öffentlichen AMI-Parameter, die von Amazon EC2 unterstützt werden, finden Sie unter Öffentliche AMI-Parameter aufrufen.
- Informationen zur gemeinsamen Nutzung von Parametern mit anderen AWS Konten oder über AWS Organizations finden Sie unter Arbeiten mit gemeinsam genutzten Parametern.
- Informationen zur Überwachung, ob Ihre Parameter erfolgreich erstellt wurden, finden Sie unter Native Parameterunterstützung für Amazon Machine Image IDs.

Einschränkungen

- Derzeit unterstützen EC2-Flotten und Spot-Flotten nicht die Verwendung einer Startvorlage, bei der ein Systems-Manager-Parameter anstelle einer AMI-ID angegeben ist. Wenn Sie für EC2-Flotten und Spot-Flotten ein AMI in der Startvorlage angeben, müssen Sie die AMI-ID angeben.

- Amazon EC2 Auto Scaling bietet weitere Einschränkungen. Weitere Informationen finden Sie unter Verwenden von AWS Systems Manager Parametern anstelle von AMI-IDs in Startvorlagen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Ändern einer Startvorlage (Verwalten von Startvorlagenversionen)

Startvorlagen sind unveränderlich; nach der Erstellung einer Startvorlage können Sie sie nicht ändern. Stattdessen können Sie eine neue Version der Startvorlage erstellen, die alle erforderlichen Änderungen enthält.

Sie können verschiedene Versionen einer Startvorlage erstellen, die Standardversion festlegen, eine Startvorlagenversion beschreiben und nicht mehr benötigte Versionen löschen.

Aufgaben

- Erstellen einer Startvorlagenversion
- Festlegen einer Standardversion der Startvorlage
- Beschreiben einer Startvorlagenversion
- Löschen einer Startvorlagenversion

Erstellen einer Startvorlagenversion

Wenn Sie eine Startvorlagenversion erstellen, können Sie neue Startparameter angeben oder eine vorhandene Version als Grundlage für die neue Version verwenden. Weitere Informationen zu den Startparametern finden Sie unter Erstellen einer Startvorlage.

Console

So erstellen Sie eine Startvorlagenversion

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie eine Startvorlage aus, und wählen Sie dann Actions (Aktionen), Modify template (Create new version) ((Vorlage ändern) (Neue Version erstellen)).
4. Geben Sie unter Template version description (Beschreibung der Vorlagenversion) eine Beschreibung für diese Version der Startvorlage ein.

5. (Optional) Erweitern Sie die Source template (Quellvorlage) und wählen Sie eine Version der Startvorlage aus, die als Basis für die neue Version der Startvorlage dienen soll. Die neue Startvorlagenversion erbt die Startparameter von dieser Startvorlagenversion.
6. Ändern Sie die Startparameter nach Bedarf und wählen Sie Create launch template (Startvorlage erstellen).

AWS CLI

So erstellen Sie eine Startvorlagenversion

- Verwenden Sie den Befehl create-launch-template-version. Sie können eine Quellversion angeben, auf der die neue Version basieren soll. Die neue Startvorlagenversion erbt die Startparameter von dieser Startvorlagenversion und Sie können mit `--launch-template-data` Parameter überschreiben. Das folgende Beispiel erstellt eine neue Version, die auf Version 1 der Startvorlage basiert und eine andere AMI-ID angibt.

```
aws ec2 create-launch-template-version \
    --launch-template-id lt-0abcd290751193123 \
    --version-description WebVersion2 \
    --source-version 1 \
    --launch-template-data "ImageId=ami-c998b6b2"
```

Festlegen einer Standardversion der Startvorlage

Sie können die Standardversion für die Startvorlage festlegen. Wenn Sie eine Instance über eine Startvorlage starten, ohne eine Version anzugeben, wird die Instance unter Verwendung der Parameter der Standardversion gestartet.

Console

So legen Sie eine Standardversion der Startvorlage fest

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie die Startvorlage und anschließend Actions (Aktionen), Set default version (Standardversion festlegen) aus.

4. Wählen Sie unter Template version (Vorlagenversion) die Versionsnummer aus, die als Standardversion festgelegt werden soll, und wählen Sie Set as default version (Als Standardversion festlegen).

AWS CLI

So legen Sie eine Standardversion der Startvorlage fest

- Verwenden Sie den Befehl modify-launch-template und geben Sie die Version an, die Sie als Standard festlegen möchten.

```
aws ec2 modify-launch-template \
    --launch-template-id lt-0abcd290751193123 \
    --default-version 2
```

Beschreiben einer Startvorlagenversion

Über die Konsole können Sie alle Versionen der ausgewählten Startvorlage anzeigen oder eine Liste der Startvorlagen abrufen, deren neueste Version oder Standardversion mit einer bestimmten Versionsnummer übereinstimmt. Mithilfe von können Sie alle Versionen, einzelne Versionen oder eine Reihe von Versionen einer bestimmten Startvorlage beschreiben. AWS CLI Sie können auch alle aktuellen Versionen oder alle Standardversionen aller Startvorlagen in Ihrem Konto beschreiben.

Console

So beschreiben Sie eine Startvorlagenversion

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Sie können eine Version einer bestimmten Startvorlage anzeigen oder eine Liste der Startvorlagen abrufen, deren neueste Version oder Standardversion mit einer bestimmten Versionsnummer übereinstimmt.
   - So zeigen Sie eine Version einer Startvorlage an: Wählen Sie die Startvorlage aus. Wählen Sie auf der Registerkarte Versionen unter Version eine Version aus, um deren Details anzuzeigen.

- So rufen Sie eine Liste aller Startvorlagen ab, deren neueste Version mit einer bestimmten Versionsnummer übereinstimmt: Wählen Sie in der Suchleiste die Option Aktuelle Version aus und wählen Sie dann eine Versionsnummer aus.
- So rufen Sie eine Liste aller Startvorlagen ab, deren Standardversion mit einer bestimmten Versionsnummer übereinstimmt: Wählen Sie in der Suchleiste die Option Standardversion aus und wählen Sie dann eine Versionsnummer aus.

AWS CLI

So beschreiben Sie eine Startvorlagenversion

- Verwenden Sie den Befehl describe-launch-template-versions und geben Sie die Versionsnummern an. Im folgenden Beispiel werden die Versionen *1* und *3* angegeben.

```
aws ec2 describe-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1 3
```

So beschreiben Sie die neuesten und standardmäßigen Versionen der Startvorlagen in Ihrem Konto

- Verwenden Sie den Befehl describe-launch-template-versions und geben Sie `$Latest`, `$Default` oder beide an. Sie müssen die Startvorlagen-ID und den Namen in dem Aufruf weglassen. Sie können keine Versionsnummern angeben.

```
aws ec2 describe-launch-template-versions \
    --versions "$Latest,$Default"
```

Löschen einer Startvorlagenversion

Wenn eine Startvorlagenversion nicht mehr benötigt wird, können Sie sie löschen.

Überlegungen

- Sie können die Versionsnummer nach dem Löschen nicht mehr ersetzen.

- Sie können die Standardversion der Startvorlage nicht löschen. Sie müssen zunächst eine andere Version als Standard zuweisen. Wenn die Standardversion die einzige Version für die Startvorlage ist, müssen Sie die gesamte Startvorlage löschen.
- Bei Verwendung der Konsole können Sie jeweils eine Startvorlagenversion löschen. Wenn Sie die verwenden AWS CLI, können Sie bis zu 200 Versionen der Startvorlage in einer einzigen Anfrage löschen. Um mehr als 200 Versionen in einer einzigen Anfrage zu löschen, können Sie die Startvorlage löschen, wodurch auch alle zugehörigen Versionen gelöscht werden.

Console

So löschen Sie eine Startvorlagenversion

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie die Startvorlage und anschließend Actions (Aktionen), Delete template version (Vorlagenversion löschen) aus.
4. Wählen Sie die zu löschende Version aus und wählen Sie Delete (Löschen).

AWS CLI

So löschen Sie eine Startvorlagenversion

- Verwenden Sie den Befehl delete-launch-template-versions und geben Sie die zu löschenden Versionsnummern an. Wenn Sie die verwenden, können Sie bis zu 200 Startvorlagenversionen in einer einzigen Anfrage löschen.

```
aws ec2 delete-launch-template-versions \
    --launch-template-id lt-0abcd290751193123 \
    --versions 1
```

Löschen einer Startvorlage

Wenn eine Startvorlage nicht mehr benötigt wird, können Sie sie löschen. Beim Löschen einer Startvorlage werden alle ihre Versionen gelöscht. Informationen zum Löschen einer bestimmten Version einer Startvorlage finden Sie unter Löschen einer Startvorlagenversion.

Wenn Sie eine Startvorlage löschen, wirkt sich das nicht auf Instances aus, die Sie über die Startvorlage gestartet haben.

Console

So löschen Sie eine Startvorlage

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie die Startvorlage und anschließend Actions (Aktionen), Delete template (Vorlage löschen) aus.
4. Geben Sie **`Delete`** ein, um das Löschen zu bestätigen, und wählen Sie dann Löschen.

AWS CLI

So löschen Sie eine Startvorlage

- Verwenden Sie den AWS CLI-Befehl delete-launch-template und geben Sie die Startvorlage an.

```
aws ec2 delete-launch-template --launch-template-id lt-01238c059e3466abc
```

Starten von Instances über eine Startvorlage

Startvorlagen werden von mehreren Instance-Startservices unterstützt. In diesem Thema wird beschrieben, wie Sie eine Startvorlage verwenden, wenn Sie eine Instance mithilfe des EC2 Launch Instance Wizard, Amazon EC2 Auto Scaling, der EC2-Flotte und der Spot-Flotte starten.

Themen

- Starten einer Instance über eine Startvorlage
- Verwenden von Startvorlagen mit Amazon EC2 Auto Scaling
- Verwenden von Startvorlagen mit EC2-Flotte
- Verwenden von Startvorlagen mit Spot-Flotte

Starten einer Instance über eine Startvorlage

Sie können die Parameter in einer Startvorlage zum Starten einer Instance verwenden. Sie haben die Möglichkeit, Startparameter außer Kraft zu setzen oder hinzuzufügen, bevor Sie die Instance starten.

Zu Instances, die über eine Startvorlage gestartet werden, werden automatisch zwei Tags mit den Schlüsseln `aws:ec2launchtemplate:id` und `aws:ec2launchtemplate:version` zugewiesen. Diese Tags (Markierungen) können nicht entfernt oder bearbeitet werden.

Console

So starten Sie eine Instance über eine Startvorlage mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates aus.
3. Wählen Sie die Startvorlage und anschließend Actions (Aktionen), Launch instance from template (Instance aus Vorlage starten) aus.
4. Wählen Sie unter Source template version (Quellvorlagenversion) die zu verwendende Startvorlagenversion aus.
5. Geben Sie unter Number of instances (Anzahl der Instances) die Anzahl der Instances an, die gestartet werden sollen.
6. (Optional) Sie können Startvorlagen-Parameter übersteuern oder hinzufügen, indem Sie im Bereich Instance details Parameter ändern und hinzufügen.
7. Wählen Sie Launch instance from template.

AWS CLI

So starten Sie eine Instance über eine Startvorlage mithilfe der AWS CLI

- Geben Sie mit dem Befehl run-instances den Parameter `--launch-template` an. Optional können Sie die zu verwendende Startvorlagenversion angeben. Wenn Sie keine Version angeben, wird die Standardversion verwendet.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123,Version=1
```

- Um einen Parameter der Startvorlage zu übersteuern, geben Sie den Parameter im Befehl run-instances an. Das folgende Beispiel übersteuert den Instance-Typ, der in der Startvorlage angegeben wird (sofern zutreffend).

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --instance-type t2.small
```

- Wenn Sie einen verschachtelten Parameter angeben, der Teil einer komplexen Struktur ist, wird die Instance wie in der Startvorlage angegeben mittels der komplexen Struktur sowie aller zusätzlichen von Ihnen angegebenen verschachtelten Parameter gestartet.

  Im folgenden Beispiel wird die Instance mit dem Tag (Markierung) *Owner*=*TeamA* sowie allen anderen Tags (Markierungen), die in der Startvorlage angegeben werden, gestartet. Wenn in der Startvorlage ein Tag (Markierung) mit dem Schlüssel *Owner* vorhanden ist, wird der Wert durch *TeamA* ersetzt.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --tag-specifications "ResourceType=instance,Tags=[{Key=Owner,Value=TeamA}]"
```

  Im folgenden Beispiel wird die Instance mit einem Volume mit dem Gerätenamen */dev/xvdb* sowie beliebigen anderen Blockgerät-Zuweisungen gestartet, die in der Startvorlage angegeben werden. Wenn in der Startvorlage ein für */dev/xvdb* definiertes Volume vorhanden ist, werden dessen Werte durch die angegebenen Werte ersetzt.

```
aws ec2 run-instances \
    --launch-template LaunchTemplateId=lt-0abcd290751193123 \
    --block-device-mappings "DeviceName=/dev/
xvdb,Ebs={VolumeSize=20,VolumeType=gp2}"
```

Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

PowerShell

So starten Sie eine Instance über eine Startvorlage mithilfe der AWS Tools for PowerShell

- Verwenden Sie den New-EC2InstanceBefehl und geben Sie den `-LaunchTemplate` Parameter an. Optional können Sie die zu verwendende Startvorlagenversion angeben. Wenn Sie keine Version angeben, wird die Standardversion verwendet.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Um einen Startvorlagenparameter zu überschreiben, geben Sie den Parameter im New-EC2InstanceBefehl an. Das folgende Beispiel übersteuert den Instance-Typ, der in der Startvorlage angegeben wird (sofern zutreffend).

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
)
```

- Wenn Sie einen verschachtelten Parameter angeben, der Teil einer komplexen Struktur ist, wird die Instance wie in der Startvorlage angegeben mittels der komplexen Struktur sowie aller zusätzlichen von Ihnen angegebenen verschachtelten Parameter gestartet.

  Im folgenden Beispiel wird die Instance mit dem Tag (Markierung) *Owner*=*TeamA* sowie allen anderen Tags (Markierungen), die in der Startvorlage angegeben werden, gestartet. Wenn in der Startvorlage ein Tag (Markierung) mit dem Schlüssel *Owner* vorhanden ist, wird der Wert durch *TeamA* ersetzt.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
        }
) `
    -TagSpecification (
        New-Object -TypeName Amazon.EC2.Model.TagSpecification -Property @{
            ResourceType = 'instance';
            Tags         = @(
                @{key = "Owner"; value = "TeamA" },
                @{key = "Department"; value = "Operations" }
            )
        }
)
```

Im folgenden Beispiel wird die Instance mit einem Volume mit dem Gerätenamen */dev/xvdb* sowie beliebigen anderen Blockgerät-Zuweisungen gestartet, die in der Startvorlage angegeben werden. Wenn in der Startvorlage ein für */dev/xvdb* definiertes Volume vorhanden ist, werden dessen Werte durch die angegebenen Werte ersetzt.

```
Import-Module AWS.Tools.EC2
New-EC2Instance `
    -InstanceType t4g.small  `
    -LaunchTemplate (
        New-Object -TypeName Amazon.EC2.Model.LaunchTemplateSpecification -
Property @{
            LaunchTemplateId = 'lt-0abcd290751193123';
            Version          = '4'
    }
) `
    -BlockDeviceMapping  (
        New-Object -TypeName Amazon.EC2.Model.BlockDeviceMapping -Property @{
            DeviceName = '/dev/xvdb';
            EBS        = (
                New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property @{
                    VolumeSize = 25;
```

```
                    VolumeType = 'gp3'
                }
            )
        }
)
```

Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Verwenden von Startvorlagen mit Amazon EC2 Auto Scaling

Sie können eine Auto Scaling-Gruppe erstellen und eine Startvorlage zur Verwendung für die Gruppe angeben. Wenn Amazon EC2 Auto Scaling Instances in der Auto Scaling-Gruppe startet, verwendet es die in der zugeordneten Startvorlage definierten Startparameter. Weitere Informationen finden Sie unter Erstellen einer Startvorlage für eine Auto Scaling Scaling-Gruppe und Erstellen einer Startvorlage mit erweiterten Einstellungen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Bevor Sie eine Auto Scaling-Gruppe mit einer Startvorlage erstellen können, müssen Sie eine Startvorlage erstellen, die alle für das Starten einer Instance in einer Auto Scaling-Gruppe erforderlichen Parameter enthält, z. B. die ID des AMI. Die Konsole bietet Anleitungen zur Erstellung einer Vorlage, die Sie mit Amazon EC2 Auto Scaling verwenden können.

So erstellen Sie eine Startvorlage für die Verwendung mit Auto Scaling mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Launch Templates (Startvorlagen) und dann Create launch template (Startvorlage erstellen) aus.
3. Geben Sie für Launch template name (Startvorlagenname) einen aussagekräftigen Namen für die Startvorlage ein.
4. Geben Sie unter Template version description (Beschreibung der Vorlagenversion) eine kurze Beschreibung dieser Version der Startvorlage ein.
5. Aktivieren Sie das Kontrollkästchen unter Auto Scaling guidance (Auto-Scaling-Anleitung), damit Amazon EC2 beim Erstellen einer Vorlage für die Verwendung mit Auto Scaling eine hilfreiche Anleitung bereitstellt.
6. Ändern Sie die Startparameter nach Bedarf. Da Sie die Auto Scaling-Anleitung ausgewählt haben, sind einige Felder erforderlich und einige Felder sind nicht verfügbar. Informationen

zur Konfiguration der Startparameter für Amazon EC2 Auto Scaling finden Sie unter Erstellen einer Startvorlage für eine Auto Scaling Scaling-Gruppe und Erstellen einer Startvorlage mit erweiterten Einstellungen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

7. Wählen Sie Startvorlage erstellen.
8. (Optional) Um eine Auto-Scaling-Gruppe mit dieser Startvorlage zu erstellen, wählen Sie in der Seite Next steps (Nächste Schritte) die Option Create Auto Scaling group (Auto-Scaling-Gruppe erstellen) aus.

Beispiele, die zeigen, wie Sie Startvorlagen mit verschiedenen Parameterkombinationen erstellen können, finden Sie unter Beispiele für die Erstellung und Verwaltung von Startvorlagen mit dem AWS Command Line Interface (AWS CLI) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch. AWS CLI

Um eine Auto Scaling Scaling-Gruppe mit einer Startvorlage zu erstellen oder zu aktualisieren, verwenden Sie den AWS CLI

- Geben Sie mit dem Befehl create-auto-scaling-group oder update-auto-scaling-group den Parameter `--launch-template` an.

Weitere Informationen zum Erstellen oder Aktualisieren einer Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage finden Sie in den folgenden Themen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

- Auto Scaling Scaling-Gruppen mithilfe von Startvorlagen erstellen
- Eine Auto Scaling Scaling-Gruppe aktualisieren

Verwenden von Startvorlagen mit EC2-Flotte

Sie können eine EC2-Flotte-Anforderung erstellen und eine Startvorlage in der Instance-Konfiguration angeben. Wenn Amazon EC2 die EC2-Flotte-Anforderung erfüllt, verwendet es die in der zugeordneten Startvorlage definierten Startparameter. Sie können einige der Parameter überschreiben, die in der Startvorlage angegeben werden.

Weitere Informationen finden Sie unter Erstellen einer EC2-Flotte.

Um eine EC2-Flotte mit einer Startvorlage zu erstellen, verwenden Sie AWS CLI

- Verwenden Sie den Befehl create-fleet. Geben Sie mit dem Parameter `--launch-template-configs` die Startvorlage und alle Überschreibungen für die Startvorlage an.

Verwenden von Startvorlagen mit Spot-Flotte

Sie können eine Spot-Flotten-Anforderung erstellen und eine Startvorlage in der Instance-Konfiguration angeben. Wenn Amazon EC2 die Spot-Flotten-Anforderung erfüllt, verwendet es die in der zugeordneten Startvorlage definierten Startparameter. Sie können einige der Parameter überschreiben, die in der Startvorlage angegeben werden.

Weitere Informationen finden Sie unter Erstellen eine Spot-Flotten-Anforderung.

So erstellen Sie eine Spot-Flotten-Anforderung mit einer Startvorlage über die Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Spot-Instances anfordern aus.
4. Wählen Sie unter Launch parameters (Startparameter) die Option Use a launch template (Eine Startvorlage verwenden) aus.
5. Wählen Sie unter Launch template (Startvorlage) eine Startvorlage und dann im Feld auf der rechten Seite die Version der Startvorlage aus.
6. Konfigurieren Sie Ihre Spot-Flotte, indem Sie verschiedene Optionen auf diesem Bildschirm auswählen. Weitere Informationen zu diesen Optionen finden Sie unter Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole).
7. Wenn Sie bereit sind, Ihre Spot-Flotte zu erstellen, klicken Sie auf Launch (Starten).

Um eine Spot-Flotte-Anfrage mit einer Startvorlage zu erstellen, verwenden Sie den AWS CLI

- Verwenden Sie den Befehl request-spot-fleet. Geben Sie mit dem Parameter `LaunchTemplateConfigs` die Startvorlage und alle Überschreibungen für die Startvorlage an.

Starten einer Instance mit den Parametern einer vorhandenen Instance

Die Amazon-EC2-Konsole stellt eine Mehr wie diese starten-Option bereit, mit der Sie eine aktuelle Instance als Grundlage verwenden können, um andere Instances zu starten. Mit dieser Option

werden automatisch bestimmte Konfigurationsdetails der ausgewählten Instance in den Amazon EC2 Launch Instance Wizard eingegeben.

Überlegungen

- Wir klonen Ihre Instances nicht, sondern replizieren nur einige der Konfigurationsdetails. Um eine Kopie Ihrer Instance zu erstellen, erstellen Sie zuerst ein AMI davon und starten Sie dann weitere Instance über das AMI. Erstellen Sie eine Startvorlage, um sicherzustellen, dass Sie Ihre Instances mit denselben Startdetails starten.
- Die aktuelle Instance muss sich im Status `running` befinden.

Details kopiert

Die folgenden Konfigurationsdetails werden von der ausgewählten Instance in den Launch Instance Wizard kopiert:

- AMI-ID
- Instance-Typ
- Availability Zone oder die VPC und das Subnetz, in der bzw. dem sich die ausgewählte Instance befindet
- Öffentliche IPv4-Adresse. Wenn die ausgewählte Instance aktuell eine öffentliche IPv4-Adresse hat, erhält die neue Instance eine öffentliche IPv4-Adresse – unabhängig von der Standardeinstellung für die öffentliche IPv4-Adresse der ausgewählten Instance. Weitere Informationen über öffentliche IPv4-Adressen finden Sie unter Öffentliche IPv4-Adressen.
- Platzierungsgruppe, falls zutreffend
- Die der Instance zugeordnete IAM-Rolle, falls zutreffend
- Einstellung des Beendigungsverhaltens (Anhalten oder Beenden)
- Einstellung des Beendigungsschutzes ("true" oder "false")
- CloudWatch Überwachung (aktiviert oder deaktiviert)
- Amazon EBS-Optimierungseinstellung ("true" oder "false")
- Tenancy-Einstellung beim Start in einer VPC (geteilt oder dediziert)
- Kernel-ID und RAM-Datenträger-ID, falls zutreffend
- Benutzerdaten, falls angegeben
- Der Instance zugeordnete Tags (Markierungen), falls zutreffend
- Der Instance zugeordnete Sicherheitsgruppen

- [Windows-Instanzen] Zuordnungsinformationen. Wenn die ausgewählte Instance einer Konfigurationsdatei zugeordnet ist, wird dieselbe Datei automatisch der neuen Instance zugeordnet. Wenn die Konfigurationsdatei eine verbundene Domain-Konfiguration enthält, wird die neue Instance automatisch mit derselben Domain verknüpft. Weitere Informationen zum Beitritt zu einer Domain finden Sie unter Nahtloser Beitritt zu einer Windows-EC2-Instance im AWS Directory Service -Administratorhandbuch.

Details wurden nicht kopiert

Die folgenden Konfigurationsdetails werden nicht von der ausgewählten Instance kopiert. Stattdessen wendet der Assistent deren Standardeinstellungen oder Verhalten an:

- Anzahl der Netzwerkschnittstellen – Der Standard ist eine Netzwerkschnittstelle, und zwar die primäre Netzwerkschnittstelle (eth0).
- Speicher – Die Standardspeicherkonfiguration wird vom AMI und dem Instance-Typ bestimmt.

So starten Sie weitere Instances wie eine bestehende Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine Instance aus und dann Aktionen, Images und Vorlagen, Mehr von dieser Art starten.
4. Der Launch Instance Wizard wird geöffnet. Sie können alle notwendigen Änderungen an der Instance-Konfiguration vornehmen, indem Sie verschiedene Optionen auf diesem Bildschirm auswählen.

   Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Launch instance (Instance starten) aus.
5. Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Starten Sie eine AWS Marketplace Instanz

Mit dem Amazon EC2 EC2-Startassistenten können Sie ein Produkt abonnieren und eine Instance über das AMI des Produkts starten. AWS Marketplace Weitere Informationen zu gebührenpflichtigen

AMIs finden Sie unter Gebührenpflichtige AMIs. Um Ihr Abonnement nach dem Start zu beenden, beenden Sie zunächst alle Instances, die darin ausgeführt werden. Weitere Informationen finden Sie unter Verwalte deine AWS Marketplace Abonnements.

New console

Um eine Instance AWS Marketplace mithilfe des Startassistenten zu starten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.
3. (Optional) Geben Sie unter Name und Tags für Name einen beschreibenden Namen für Ihre Instance ein.
4. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) die Option Browse more AMIs (Weitere AMIs durchsuchen) und wählen Sie dann die Registerkarte AWS Marketplace AMIs (-AMIs) aus. Finden Sie eine passende AMI, indem Sie die Kategorien durchsuchen oder die Suchfunktion verwenden. Um ein Produkt auszuwählen, wählen Sie Select (Auswählen).
5. Es öffnet sich ein Fenster mit einer Übersicht über das von Ihnen ausgewählte Produkt. Sie können die Preisinformationen und andere vom Anbieter bereitgestellte Informationen anzeigen. Wenn Sie bereit sind, wählen Sie eine der folgenden Schaltflächen:

   - Beim Start der Instance abonnieren — Ihr Abonnement beginnt, wenn Sie Launch Instance wählen (in Schritt 10).
   - Jetzt abonnieren — Ihr Abonnement beginnt sofort. Während das Abonnement läuft, können Sie die Instanz konfigurieren, indem Sie mit den Schritten in diesem Verfahren fortfahren. Sollten Probleme mit den Kreditkarteninformationen bestehen, werden Sie zum Aktualisieren dieser aufgefordert.

   > **Note**
   >
   > Die Nutzung des Produkts wird Ihnen erst in Rechnung gestellt, wenn Sie eine Instance mit dem AMI gestartet haben. Beachten Sie die Preise für jeden unterstützten Instance-Typ, wenn Sie einen Instance-Typ auswählen. Für das Produkt können auch zusätzliche Steuern anfallen.

6. Wählen Sie unter Instance type (Instance-Typ) einen Instance Typ für Ihre Instance aus. Der Instance-Typ definiert die Hardware-Konfiguration und die Größe der zu startenden Instance.

7. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
8. Notieren Sie sich unter Network settings (Netzwerkeinstellungen), Firewall (security groups) (Firewall (Sicherheitsgruppen)) die neue Sicherheitsgruppe, die gemäß den Spezifikationen des Herstellers für das Produkt erstellt wurde. Die Sicherheitsgruppe kann Regeln enthalten, die allen IPv4-Adressen (`0.0.0.0/0`) den Zugriff auf SSH (Port 22) unter Linux oder RDP (Port 3389) unter Windows erlauben. Wir empfehlen, die Regeln anzupassen, sodass nur eine bestimmte Adresse bzw. ein bestimmter Adressbereich über diese Ports auf Ihre Instance zugreifen kann.
9. Sie können die anderen Felder auf dem Bildschirm verwenden, um Ihre Instance zu konfigurieren, Speicher und Tags hinzuzufügen. Weitere Informationen zu den verschiedenen Optionen, die Sie konfigurieren können, finden Sie unter Starten einer Instance mit definierten Parametern.
10. Überprüfen Sie im Bereich Summary (Zusammenfassung) unter Software Image (AMI) (Software-Image (AMI)) die Details des AMI, von dem Sie die Instance starten wollen. Überprüfen Sie auch die anderen Konfigurationsdetails, die Sie angegeben haben. Wenn Sie bereit sind, Ihre Instance zu starten, wählen Sie Instance starten aus.
11. Je nach abonniertem Produkt kann der Start der Instance ein paar Minuten oder länger dauern. Wenn Sie in Schritt 5 die Option Beim Instance-Start abonnieren ausgewählt haben, haben Sie zunächst das Produkt abonniert, bevor Ihre Instance gestartet werden kann. Sollten Probleme mit den Kreditkarteninformationen bestehen, werden Sie zum Aktualisieren dieser aufgefordert. Wenn die Bestätigungsseite für den Start angezeigt wird, wählen Sie View all instances (Alle Instances anzeigen), um zur Seite Instances zu gelangen.

   > **Note**
   >
   > Der Abonnementpreis wird Ihnen in Rechnung gestellt, solange sich Ihre Instance im `running`-Status befindet, auch wenn diese inaktiv ist. Wenn Ihre Instance angehalten wird, wird Ihnen möglicherweise weiterhin Speicherplatz in Rechnung gestellt.

12. Wenn sich die Instance im Zustand `running` befindet, können Sie eine Verbindung zu ihr herstellen. Wählen Sie dazu Ihre Instance in der Liste aus, wählen Sie Connect (Verbinden) und wählen Sie eine Verbindungsoption aus. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zur Linux-InstanceHerstellen einer Verbindung mit Ihrer -Windows-Instance.

> **Important**
>
> Überprüfen Sie die Nutzungsanweisungen des Anbieters sorgfältig, da Sie möglicherweise einen bestimmten Benutzernamen verwenden müssen, um eine Verbindung zu Ihrer Instance herzustellen. Weitere Informationen zum Zugriff auf Ihre Abonnementdetails finden Sie unter Verwalte deine AWS Marketplace Abonnements.

13. Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Old console

Um eine Instance AWS Marketplace mithilfe des Startassistenten zu starten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Amazon EC2-Dashboard Launch Instance (Instance starten) aus.
3. Wählen Sie auf der Seite Choose an Amazon Machine Image (AMI) (Auswählen eines Amazon Machine Image (AMI)) links die Kategorie AWS Marketplace aus. Suchen Sie in den Kategorien eine geeignete AMI oder verwenden Sie die Suchfunktion. Mit Select (Auswählen) wählen Sie das gewünschte Produkt aus.
4. In einem Dialogfeld wird eine Übersicht über das ausgewählte Produkt angezeigt. Sie können die Preisinformationen und andere vom Anbieter bereitgestellte Informationen anzeigen. Sobald Sie bereit sind, klicken Sie auf Continue (Fortfahren).

   > **Note**
   >
   > Ihnen wird die Verwendung des Produkts erst in Rechnung gestellt, wenn Sie eine Instance mit dem AMI starten. Achten Sie auf die Preise der einzelnen unterstützten Instance-Typen, denn auf der nächsten Seite des Assistenten werden Sie zur Auswahl eines Instance-Typs ausgewählt. Gegebenenfalls fallen zusätzliche Steuern für das Produkt an.

5. Wählen Sie auf der Seite Choose an Instance Type (Einen Instance-Typ auswählen) die Hardware-Konfiguration und Größe der zu startenden Instance aus. Wählen Sie danach Next: Configure Instance Details (Weiter: Instance-Details konfigurieren) aus.

6. Auf den nächsten Seiten des Assistenten können Sie Ihre Instance konfigurieren sowie Speicher und Tags (Markierungen) hinzufügen. Weitere Informationen zu den verschiedenen Konfigurationsoptionen finden Sie unter Starten einer Instance mit dem alten Launch Instance Wizard. Klicken Sie auf Weiter bis Sie zur Seite Configure Security Group gelangen.

   Der Assistent erstellt eine neue Sicherheitsgruppe gemäß den Produktspezifikationen des Anbieters. Die Sicherheitsgruppe enthält ggf. Regeln, die allen IPv4-Adressen (`0.0.0.0/0`) Zugriff auf SSH (Port 22) unter Linux oder RDP (Port 3389) unter Windows ermöglichen. Wir empfehlen, die Regeln anzupassen, sodass nur eine bestimmte Adresse bzw. ein bestimmter Adressbereich über diese Ports auf Ihre Instance zugreifen kann.

   Wählen Sie abschließend Review and Launch (Überprüfen und starten) aus.
7. Prüfen Sie auf der Seite Review Instance Launch (Überprüfen des Instance-Starts) die Details des AMI, in dem Sie die Instance starten, sowie die anderen Konfigurationsdetails, die Sie im Assistenten einrichten. Wählen Sie abschließend Launch (Starten) aus, um ein Schlüsselpaar auszuwählen oder zu erstellen und starten Sie die Instance.
8. Je nach abonniertem Produkt kann es ein paar Minuten dauern, bis die Instance gestartet wird. Bevor die Instance gestartet wird, wird zunächst das Abonnement durchgeführt. Sollten Probleme mit den Kreditkarteninformationen bestehen, werden Sie zum Aktualisieren dieser aufgefordert. Wenn die Start-Bestätigungsseite angezeigt wird, wählen Sie View Instances (Instances anzeigen) aus, um zur Instances-Seite zu wechseln.

   > **Note**
   >
   > Die Abonnementgebühren werden so lange in Rechnung gestellt wie die Instance ausgeführt wird (auch im Leerlauf). Wenn die Instance angehalten wird, fallen ggf. noch Gebühren für den Speicher an.
9. Wenn sich die Instance im Zustand `running` befindet, können Sie eine Verbindung zu ihr herstellen. Wählen Sie hierzu Ihre Instance aus der Liste aus und wählen Sie Connect (Verbinden) aus. Gehen Sie der Anleitung im Dialogfeld entsprechend vor. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zur Linux-InstanceHerstellen einer Verbindung mit Ihrer -Windows-Instance.

   > **Important**
   >
   > Prüfen Sie die Nutzungsinformationen des Anbieters sorgfältig, da Sie möglicherweise einen spezifischen Benutzernamen zum Anmelden an der Instance

benötigen. Weitere Informationen zum Zugriff auf die Abonnementdetails finden Sie unter Verwalte deine AWS Marketplace Abonnements.

10. Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Starten Sie eine AWS Marketplace AMI-Instanz mithilfe der API und CLI

Um Instances von AWS Marketplace Produkten aus zu starten, die die API oder die Befehlszeilentools verwenden, stellen Sie zunächst sicher, dass Sie das Produkt abonniert haben. Anschließend starten Sie eine Instance mit der AMI-ID des Produkts. Gehen Sie hierzu folgendermaßen vor:

Art	Dokumentation
AWS CLI	Verwenden Sie den run-instances-Befehl oder schlagen Sie unter folgendem Thema nach, um weitere Informationen zu erhalten: Starten einer Instance.
AWS Tools for Windows PowerShell	Verwenden Sie den New-EC2InstanceBefehl, oder lesen Sie das folgende Thema für weitere Informationen: Starten einer Amazon EC2 EC2-Instance mit Windows PowerShell
Abfrage-API	Verwenden Sie die RunInstancesAnfrage.

Beenden und starten Sie Amazon EC2 EC2-Instances

Sie können die Instance anhalten und erneut starten, wenn das Root-Gerät ein Amazon EBS-Volume ist. Wenn Sie eine Instance beenden, wird sie heruntergefahren. Wenn Sie eine Instance starten, wird sie in der Regel auf einen neuen zugrundeliegenden Host-Computer migriert und ihr wird eine neue öffentliche IPv4-Adresse zugewiesen.

Wenn Sie eine Instance anhalten, wird sie nicht gelöscht. Wenn Sie eine Instance nicht mehr benötigen, können Sie sie löschen. Weitere Informationen finden Sie unter Amazon EC2 EC2-Instances beenden. Informationen darüber wie Sie eine Instance in den Ruhezustand versetzen können, um den Inhalt des Instance-Speichers (RAM) zu speichern, finden Sie unter Versetzen

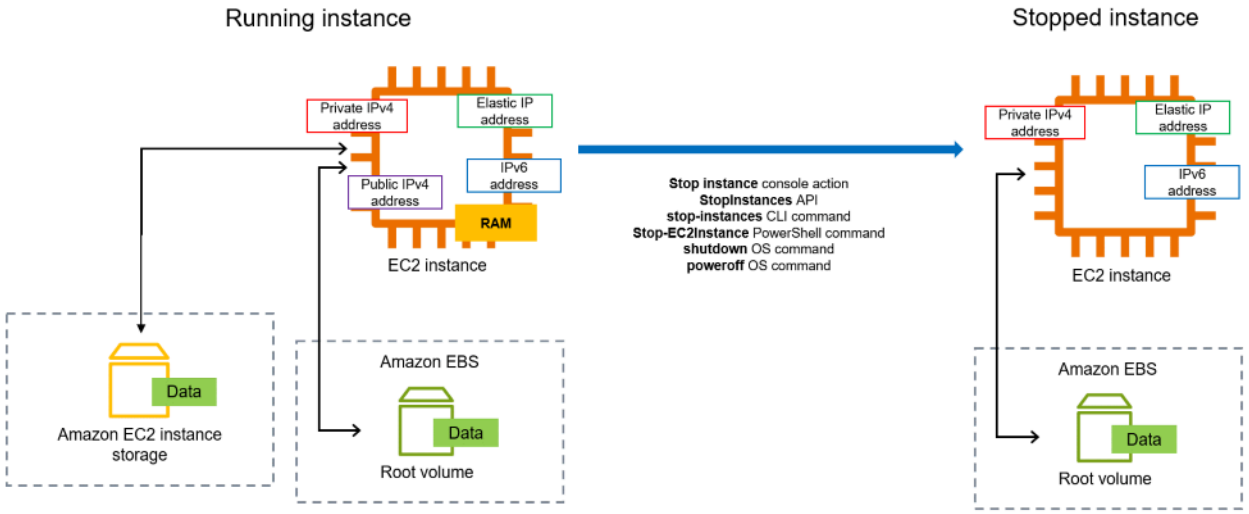
Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand. Informationen zu den Unterscheidungen zwischen den Aktionen des Instance-Lebenszyklus finden Sie unter Unterschiede zwischen Neustart, Anhalten, Ruhezustand und Beenden.

Inhalt

So funktioniert das Stoppen und Starten von Instanzen

Wenn Sie eine Instance beenden, werden Änderungen auf Betriebssystemebene der Instance registriert, einige Ressourcen gehen verloren und einige Ressourcen bleiben bestehen. Wenn Sie eine Instance starten, werden die Änderungen auf Instance-Ebene registriert.

Das folgende Diagramm zeigt, was verloren geht und was bestehen bleibt, wenn eine Amazon-EC2-Instance angehalten wird. Wenn eine Instance angehalten wird, verliert sie alle angeschlossenen Instance-Speicher-Volumes und die auf diesen Volumes gespeicherten Daten, die im Instance-RAM gespeicherten Daten und die zugewiesene öffentliche IPv4-Adresse, wenn der Instance keine elastische IP-Adresse zugeordnet ist. Eine Instance behält zugewiesene private IPv4-Adressen, der Instance zugeordnete Elastic-IP-Adressen, alle IPv6-Adressen sowie alle angefügten Amazon-EBS-Volumes und die Daten auf diesen Volumes.



Was geschieht, wenn Sie eine Instance anhalten?

Änderungen, die auf Betriebssystemebene registriert wurden

- Die API-Anfrage sendet ein Tastendruck-Ereignis an den Gast.
- Verschiedene Systemservices werden infolge des Tastendruck-Ereignisses gestoppt. Ein ordnungsgemäßes Herunterfahren wird durch das ACPI-Maustastendruck-Ereignis zum Herunterfahren vom Hypervisor ausgelöst.
- Das Herunterfahren des ACPI wird initiiert.
- Die Instance wird heruntergefahren, wenn ein ordnungsgemäßer Prozess dafür vorhanden ist. Die Zeit zum Herunterfahren des Betriebssystems kann nicht konfiguriert werden.
- Wenn das Instance-Betriebssystem nicht innerhalb weniger Minuten sauber heruntergefahren wird, wird ein Hard Shutdown durchgeführt.
- Die Instance wird nicht mehr ausgeführt.
- Der Instance-Status ändert sich zu `stopping` und dann zu `stopped`.
- [Auto Scaling] Wenn sich Ihre Instance in einer Auto-Scaling-Gruppe befindet, wenn sich die Instance in einem anderen Amazon-EC2-Status als `running` befindet oder wenn ihr Status für die Statusprüfungen `impaired` wird, betrachtet Amazon EC2 Auto Scaling die Instance als fehlerhaft und ersetzt sie. Weitere Informationen finden Sie unter Zustandsprüfungen für Auto Scaling-Instances im Amazon EC2 Auto Scaling-Benutzerhandbuch.
- [Windows-Instances] Wenn Sie eine Windows-Instance beenden und starten, führt der Launch-Agent Aufgaben auf der Instance aus, z. B. das Ändern der Laufwerksbuchstaben für alle angehängten Amazon EBS-Volumes. Weitere Informationen zu diesen Standardwerten und wie Sie sie ändern können, finden Sie unter. the section called “EC2Launch v2”

Verlorene Ressourcen

- Im Arbeitsspeicher gespeicherte Daten.
- Auf den Instance-Speicher-Volumes gespeicherte Daten.
- Die öffentliche IPv4-Adresse, die Amazon EC2 der Instance beim Start oder der Inbetriebnahme automatisch zugewiesen hat. Um eine öffentliche IPv4-Adresse beizubehalten, die sich nie ändert, können Sie Ihrer Instance eine Elastic-IP-Adresse zuordnen.

Ressourcen, die fortbestehen

- Alle angefügten Amazon-EBS-Volumes.
- Daten, die auf den angefügten Amazon-EBS-Volumes gespeichert sind.
- private IPv4-Adressen
- IPv6-Adressen
- elastische IP-Adressen, die der Instance zugeordnet sind Beachten Sie, dass Ihnen beim Anhalten der Instance die Gebühren für die zugeordneten Elastic-IP-Adressen in Rechnung gestellt werden.

Informationen darüber, was passiert, wenn Sie eine Mac-Instanz beenden, finden Sie unterthe section called “Stoppen und beenden Sie Ihre Mac-Instance”.

Was geschieht, wenn Sie eine Instance starten?

Auf Betriebssystemebene registrierte Änderungen

- In den meisten Fällen wird die Instance auf einen neuen zugrundeliegenden Host-Computer migriert (in einigen Fällen, z. B. wenn eine Instance einem Host in einer Dedicated- Host-Konfiguration zugewiesen wird, verbleibt sie jedoch auf dem aktuellen Host).
- Amazon EC2 weist der Instance eine neue öffentliche IPv4-Adresse zu, wenn die Instance so konfiguriert ist, dass sie eine öffentliche IPv4-Adresse erhält. Um eine öffentliche IPv4-Adresse beizubehalten, die sich nie ändert, können Sie Ihrer Instance eine Elastic-IP-Adresse zuordnen.

Testen der Reaktion der Anwendung auf Stopp und Start

Sie können AWS Fault Injection Service damit testen, wie Ihre Anwendung reagiert, wenn Ihre Instance gestoppt und gestartet wird. Weitere Informationen finden Sie im AWS Fault Injection Service -Benutzerhandbuch.

Kosten im Zusammenhang mit dem Stoppen und Starten der Instance

Die folgenden Kosten sind mit dem Anhalten und Starten einer Instance verbunden.

Anhalten – Sobald sich der Status einer Instance zu `shutting-down` oder `terminated` ändert, fallen für die Instance keine Gebühren mehr an. Für eine angehaltene Instance werden Ihnen keine Nutzungs- oder Datenübertragungsgebühren in Rechnung gestellt. Für die Speicherung von Amazon-EBS-Speichervolumes fallen Gebühren an.

Starten – Jedes Mal, wenn Sie eine angehaltene Instance starten, wird Ihnen mindestens eine Minute Nutzungsdauer in Rechnung gestellt. Nach einer Minute werden Ihnen nur die genutzten Sekunden in Rechnung gestellt. Wenn Sie beispielsweise eine Instance 20 Sekunden lang ausführen und sie dann anhalten, wird Ihnen eine Nutzungsminute in Rechnung gestellt. Wenn Sie eine Instance 3 Minuten und 40 Sekunden lang ausführen, werden Ihnen 3 Minuten und 40 Sekunden Nutzungsdauer in Rechnung gestellt.

Stoppen und starten Sie Ihre Instances manuell

Sie können Ihre Amazon EBS-gestützten Instances (Instances mit EBS-Root-Geräten) beenden und starten. Sie können Instances nicht mit dem Instance-Speicher-Root-Gerät beenden und starten.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Bevor Sie eine Instance beenden, stellen Sie sicher, dass Sie alle benötigten Daten von den Instance-Speicher-Volumes in einen persistenten Speicher wie Amazon EBS oder Amazon S3 kopiert haben.

Console

So beenden und starten Sie eine Amazon-EBS-gestützte Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Instances und dann die Instance aus.
3. Stellen Sie auf der Registerkarte Speicher sicher, dass der Root-Gerätetyp EBS ist. Andernfalls können Sie die Instanz nicht beenden.
4. Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten). Wenn diese Option deaktiviert ist, wurde die Instance entweder bereits angehalten oder das Root-Gerät ist ein Instance-Speicher-Volume.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus. Das Anhalten der Instance kann einige Minuten dauern.
6. Um eine angehaltene Instance zu starten, wählen Sie die Instance aus, und wählen Sie Instance-Status und anschließend Instance starten aus.
7. Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht.

8. Wenn Sie eine von Amazon EBS unterstützte Instance angehalten haben und diese im `stopping`-Status „hängen bleibt“, können Sie das Anhalten erzwingen. Weitere Informationen finden Sie unter Beheben von Problemen beim Anhalten Ihrer Instance.

Command line

Voraussetzungen

Stellen Sie sicher, dass das Root-Gerät der Instance ein EBS-Volume ist. Führen Sie beispielsweise den AWS CLI Befehl describe-instances aus und vergewissern Sie sich, dass dies nicht der Fall `RootDeviceType` ist`ebs`. `instance-store`

So beenden und starten Sie eine Amazon-EBS-gestützte Instance

Verwenden Sie einen der folgenden Befehle:

- AWS CLI – stop-instances und start-instances.
- AWS Tools for PowerShell— Stop-EC2Instanceund. Start-EC2Instance
- Betriebssystembefehle – Mit den Befehlen shutdown oder poweroff können Sie ein Herunterfahren einleiten. Wenn Sie einen Betriebssystembefehl verwenden, wird die Instance standardmäßig angehalten. Sie können das Verhalten stattdessen ändern, sodass sie beendet wird. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.

[Linux-Instanzen] Die Verwendung des halt Betriebssystembefehls von einer Instanz aus führt nicht zum Herunterfahren. Wenn Sie den Befehl halt verwenden, wird die Instance nicht angehalten. Stattdessen wird die CPU in den `HLT` versetzt, wodurch der CPU-Betrieb unterbrochen wird. Die Instance wird weiterhin ausgeführt.

Automatisches Anhalten und Starten Ihrer Instances

Sie können das Anhalten und Starten von Instances mit den folgenden Services automatisieren:

Instance Scheduler aktiviert AWS

Sie können Instance Scheduler on verwenden AWS , um das Starten und Stoppen von EC2-Instances zu automatisieren. Weitere Informationen finden Sie unter Wie verwende ich Instance

Scheduler, um EC2-Instances CloudFormation zu planen? Beachten Sie, dass zusätzliche Kosten anfallen.

AWS Lambda und eine EventBridge Amazon-Regel

Sie können Lambda und eine EventBridge Regel verwenden, um Ihre Instances nach einem Zeitplan zu beenden und zu starten. Weitere Informationen finden Sie unter Wie verwende ich Lambda, um Amazon EC2 EC2-Instances in regelmäßigen Abständen zu beenden und zu starten?

Amazon EC2 Auto Scaling

Um sicherzustellen, dass Sie die richtige Anzahl von Amazon-EC2-Instances zur Verfügung haben, um die Last für eine Anwendung zu bewältigen, erstellen Sie Auto-Scaling-Gruppen. Amazon EC2 Auto Scaling stellt sicher, dass Ihre Anwendung immer über die richtige Kapazität verfügt, um den Datenverkehr zu bewältigen, und spart Kosten, indem Instances nur dann gestartet werden, wenn sie benötigt werden. Beachten Sie, dass Amazon EC2 Auto Scaling nicht benötigte Instances nicht anhält, sondern beendet. Informationen zum Einrichten von Auto-Scaling-Gruppen finden Sie unter Erste Schritte mit Amazon EC2 Auto Scaling.

Alle ausgeführten und angehaltenen Instances suchen

Mit Amazon EC2 Global View finden Sie alle Ihre laufenden und gestoppten Instances AWS-Regionen auf einer einzigen Seite. Diese Funktion ist besonders nützlich für die Bestandsaufnahme und das Auffinden vergessener Instances. Informationen zur Verwendung von Global View finden Sie unter Amazon EC2 Global View.

Aktivieren Sie den Stopp-Schutz für Ihre Instance

Um zu verhindern, dass eine Instance versehentlich angehalten wird, können Sie einen Anhalte-Schutz für die Instance aktivieren. Der Stopp-Schutz schützt Ihre Instance auch vor versehentlichen Beendigungen.

Das `DisableApiStop` Attribut der Amazon EC2 `ModifyInstanceAttribute`EC2-API steuert, ob die Instance mithilfe der Amazon EC2 EC2-Konsole, der oder der AWS CLI Amazon EC2 EC2-API gestoppt werden kann. Sie können den Wert dieses Attributs beim Starten der Instance festlegen, während die Instance in Betrieb oder angehalten ist.

Überlegungen

- Die Aktivierung des Stopp-Schutzes verhindert nicht, dass Sie eine Instance versehentlich stoppen, indem Sie mit einem Betriebssystembefehl wie shutdown oder poweroff ein Herunterfahren der Instance einleiten.
- Die Aktivierung des Stopp-Schutzes AWS verhindert nicht, dass die Instance gestoppt wird, wenn es ein geplantes Ereignis zum Stoppen der Instance gibt.
- Das Aktivieren des Stopp-Schutzes hindert Amazon EC2 Auto Scaling nicht daran, eine Instance zu beenden, wenn die Instance fehlerbehaftet ist bzw. während Abskalierungs-Ereignissen. Sie können steuern, ob eine Auto-Scaling-Gruppe eine bestimmte Instance beim Abskalieren beenden kann, indem Sie den Instance-Skalierungsschutz verwenden.
- Der Stop-Schutz verhindert nicht nur, dass Ihre Instance versehentlich gestoppt wird, sondern auch, dass Ihre Instance versehentlich beendet wird AWS CLI, wenn Sie die Konsole oder die API verwenden. Es ändert jedoch nicht automatisch das `DisableApiTermination`-Attribut. Beachten Sie, dass, wenn das `DisableApiStop` Attribut auf gesetzt ist`false`, die `DisableApiTermination` Attributeinstellung bestimmt, ob die Instance mithilfe der Konsole oder der API beendet werden kann. AWS CLI Weitere Informationen finden Sie unter Amazon EC2 EC2-Instances beenden.
- Sie können den Stoppschutz nicht für Instance-Speicher-gestützte Instances aktivieren.
- Sie können den Stopp-Schutz nicht für Spot Instances aktivieren.
- Die Amazon-EC2-API folgt einem eventuellen Konsistenzmodell, wenn Sie den Stopp-Schutz aktivieren oder deaktivieren. Dies bedeutet, dass das Ergebnis der Ausführung von Befehlen zum Festlegen des Attributs Anhalte-Schutz möglicherweise nicht sofort für alle nachfolgenden Befehle, die Sie ausführen, sichtbar ist. Weitere Informationen finden Sie unter Eventual consistency im Amazon EC2 Developer Guide.

Schutzaufgaben anhalten

- Aktivieren des Stopp-Schutzes für eine Instance beim Starten
- Aktivieren des Stopp-Schutzes für eine laufende oder gestoppte Instance
- Deaktivieren des Stopp-Schutzes für eine laufende oder angehaltene Instance

Aktivieren des Stopp-Schutzes für eine Instance beim Starten

Sie können den Stopp-Schutz für eine Instance aktivieren, wenn Sie die Instance mithilfe einer der folgenden Methoden starten.

Console

So aktivieren Sie den Stopp-Schutz für eine Instance beim Starten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard Launch Instance (Instance starten) aus.
3. Konfigurieren Sie Ihre Instance im neuen Launch Instance Wizard.
4. Aktivieren Sie im Assistenten den Anhalte-Schutz, indem Sie unter Erweiterte Details die Option Aktivieren für Anhalte-Schutz auswählen.

AWS CLI

So aktivieren Sie den Stopp-Schutz für eine Instance beim Starten

Verwenden Sie den AWS CLI Befehl run-instances, um die Instance zu starten, und geben Sie den Parameter an. `disable-api-stop`

```
aws ec2 run-instances \
    --image-id ami-a1b2c3d4e5example \
    --instance-type t3.micro \
    --key-name MyKeyPair \
    --disable-api-stop \
    ...
```

Aktivieren des Stopp-Schutzes für eine laufende oder gestoppte Instance

Sie können den Stopp-Schutz für eine Instance aktivieren, wenn die Instance mithilfe einer der folgenden Methoden ausgeführt oder gestoppt wird.

Console

Aktivieren des Anhalte-Schutzes für eine laufende oder angehaltene Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus und wählen Sie dann Aktionen>Instance-Einstellungen>Anhalte-Schutz ändern.

4. Aktivieren Sie das Kontrollkästchen Enable (Aktivieren) und wählen Sie dann Save (Speichern) aus.

AWS CLI

Aktivieren des Anhalte-Schutzes für eine laufende oder angehaltene Instance

Verwenden Sie den Befehl AWS CLI modify-instance-attribute und geben Sie den Parameter an. `disable-api-stop`

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
    --disable-api-stop
```

Deaktivieren des Stopp-Schutzes für eine laufende oder angehaltene Instance

Sie können den Stopp-Schutz für eine laufende oder gestoppte Instance mit einer der folgenden Methoden deaktivieren.

Console

So deaktivieren Sie den Anhalte-Schutz für eine laufende oder angehaltene Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance und dann Actions (Aktionen) rechts oben, Instance Settings (Instance-Einstellungen), Change stop protection (Stopp-Schutz ändern).
4. Deaktivieren Sie das Kontrollkästchen Enable (Aktivieren) und wählen Sie dann Save (Speichern) aus.

AWS CLI

So deaktivieren Sie den Anhalte-Schutz für eine laufende oder angehaltene Instance

Verwenden Sie den Befehl AWS CLI modify-instance-attribute und geben Sie den Parameter an. `no-disable-api-stop`

```
aws ec2 modify-instance-attribute \
    --instance-id i-1234567890abcdef0 \
```

```
    --no-disable-api-stop
```

Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand

Wenn Sie eine Instance in den Ruhezustand versetzen, sendet Amazon EC2 an das Betriebssystem ein Signal, die Instance in den Ruhezustand zu versetzen ("suspend-to-disk"). Hierdurch wird der Inhalt des Instance-Arbeitsspeichers (RAM) auf dem Amazon-Elastic-Block-Store (Amazon EBS)-Stamm-Volume gespeichert. Amazon EC2 behält das EBS-Stamm-Volume der Instance und alle angefügten EBS-Daten-Volumen bei. Wenn Ihre Instance gestartet wird:

- Das EBS-Stamm-Volume wird in seinem vorherigen Zustand wiederhergestellt.
- Die RAM-Inhalte werden neu geladen.
- Die zuvor auf der Instance ausgeführten Prozesse werden fortgesetzt.
- Zuvor angefügte Daten-Volumes werden erneut angefügt und die Instance behält ihre Instance-ID bei.

Sie können eine Instance nur dann in den Ruhezustand versetzen, wenn sie für den Ruhezustand aktiviert ist und die Voraussetzungen für den Ruhezustand erfüllt.

Wenn das Bootstrapping und Erstellen des Arbeitsspeichers bei einer Instance sehr lange dauern, bevor sie voll produktiv ist, können Sie die Instance mithilfe des Ruhezustands vorbereiten. So bereiten Sie die Instance vor:

1. Starten Sie die Instance mit aktiviertem Ruhezustand.
2. Aktivieren Sie einen gewünschten Instance-Status.
3. Setzen Sie sie in den Ruhezustand, damit sie bereit ist, in den gewünschten Status wieder aufgenommen zu werden.

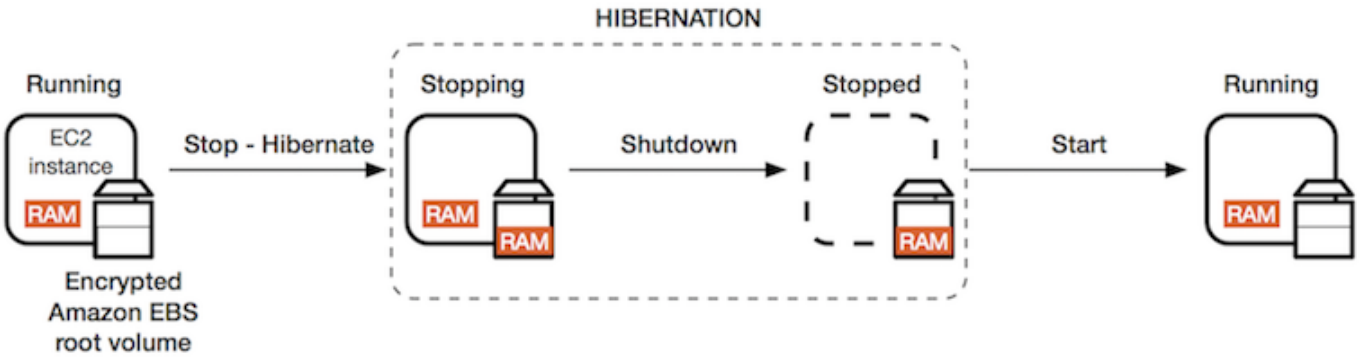
Die Instance-Nutzung für eine Instance im Ruhezustand, wenn sie sich im `stopped`-Staus befindet, oder für die Datenübertragung, wenn der Inhalt des RAM auf das EBS-Root-Volume übertragen wird, wird Ihnen nicht in Rechnung gestellt. Ihnen werden Gebühren für das Speichern aller EBS-Volumes berechnet, einschließlich für das Speichern der RAM-Inhalte.

Wenn Sie eine Instance nicht mehr benötigen, können Sie sie jederzeit beenden, auch wenn sie sich im Zustand `stopped` (Ruhezustand) befindet. Weitere Informationen finden Sie unter Amazon EC2 EC2-Instances beenden.

Inhalt

So funktioniert der Ruhezustand der Amazon EC2 EC2-Instance

Das folgende Diagramm zeigt einen grundlegenden Überblick über den Ruhezustand für EC2-Instances.



Was passiert, wenn Sie eine Instance in den Ruhezustand versetzen

Wenn Sie eine Instance in den Ruhezustand versetzen, passiert Folgendes:

- Die Instance wechselt in den Status `stopping`. Amazon EC2 gibt das Signal an das Betriebssystem weiter, um die Instance in den Ruhezustand zu versetzen ("suspend-to-disk"). Für den Ruhezustand werden alle Prozesse angehalten, der Inhalt des Instance-Arbeitsspeichers (RAM) wird auf dem EBS-Stamm-Volume gespeichert und dann wird die Instance regulär heruntergefahren.
- Nachdem die Instance vollständig heruntergefahren wurde, wechselt sie in den Zustand `stopped`.
- Alle EBS-Volumes bleiben der Instance angefügt und die Daten bleiben erhalten, auch der gespeicherte RAM-Inhalt.

- Alle Amazon EC2-Instance-Speicher-Volumes bleiben der Instance zugeordnet, die Daten auf den Instance-Speicher-Volumes gehen aber verloren.
- Während sich die Instance im Zustand `stopped` befindet, können Sie bestimmte Attribute der Instance wie Typ oder Größe ändern.
- In den meisten Fällen wird die Instance beim Start zu einem neuen Basis-Host-Computer migriert. Dies geschieht auch, wenn Sie eine Instance anhalten und starten.
- Wenn die Instance gestartet wird, wird die Instance hochgefahren und das Betriebssystem liest den Inhalt des RAM vom EBS-Root-Volume ein, bevor es Prozesse aufhebt, um den Status wiederherzustellen.
- Die Instance behält ihre privaten IPv4-Adressen sowie sämtliche IPv6-Adressen. Beim Start der Instance behält die Instance weiterhin ihre privaten IPv4-Adressen und alle IPv6-Adressen bei.
- Amazon EC2 gibt die öffentliche IPv4-Adresse frei. Beim Start der Instance weist Amazon EC2 der Instance eine neue öffentliche IPv4-Adresse zu.
- Die Instance behält die zugeordneten Elastic IP-Adressen bei. Für Elastic IP-Adressen, die einer Instance im Ruhezustand zugeordnet sind, fallen Gebühren an.

Informationen zum Unterschied zwischen Ruhezustand und Neustart, Anhalten und Beenden finden Sie unter Unterschiede zwischen Neustart, Anhalten, Ruhezustand und Beenden.

Einschränkungen

- Wenn Sie eine Instance in den Ruhezustand versetzen, gehen sämtliche Daten auf allen Instance-Speicher-Volumes verloren.
- (Linux-Instances) Sie können eine Linux-Instance mit mehr als 150 GB RAM nicht in den Ruhezustand versetzen.
- (Windows-Instanzen) Sie können eine Windows-Instanz, die über mehr als 16 GB RAM verfügt, nicht in den Ruhezustand versetzen.
- Wenn Sie einen Snapshot oder ein AMI aus einer Instance erstellen, die im Ruhezustand ist oder den Ruhezustand aktiviert hat, können Sie möglicherweise keine Verbindung mit einer neuen Instance herstellen, die aus dem AMI oder aus einem AMI, das aus dem Snapshot erstellt wurde, gestartet wird.
- (Nur Spot Instances) Wenn Amazon EC2 Ihre Spot Instance in den Ruhezustand versetzt, kann nur Amazon EC2 Ihre Instance fortsetzen. Wenn Sie Ihre Spot Instance in den Ruhezustand versetzen (vom Benutzer initiierter Ruhezustand), können Sie Ihre Instance fortsetzen. Eine Spot Instance im

Ruhezustand kann nur wieder aufgenommen werden, wenn Kapazität verfügbar ist und der Spot-Preis kleiner oder gleich Ihrem angegebenen Höchstpreis ist.

- Sie können eine Instance in den Ruhezustand versetzen, die sich in einer Auto Scaling-Gruppe befindet oder von Amazon ECS verwendet wird. Wenn sich die Instance in einer Auto Scaling-Gruppe befindet und Sie sie in den Ruhezustand versetzen möchten, kennzeichnet der Amazon EC2 Auto Scaling-Dienst die angehaltene Instance als fehlerhaft, beendet sie ggf. und startet eine Ersatz-Instance. Weitere Informationen finden Sie unter Zustandsprüfungen für Instances in einer Auto Scaling Scaling-Gruppe im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
- Sie können eine Instance, die für den Start im UEFI-Modus konfiguriert ist, nicht in den Ruhezustand versetzen, wenn UEFI Secure Boot aktiviert ist.
- Wenn Sie eine Instance in den Ruhezustand versetzen, die in eine Kapazitätsreservierung gestartet wurde, stellt das Kapazitätsreservierung nicht sicher, dass die Instance im Ruhezustand fortgesetzt werden kann, nachdem Sie versucht haben, sie zu starten.
- Sie können eine Instance, die einen Kernel unter 5.10 verwendet, nicht in den Ruhezustand versetzen, wenn der Federal Information Processing Standard (FIPS)-Modus aktiviert ist.
- Das Aufrechterhalten des Ruhezustands einer Instance für mehr als 60 Tagse wird nicht unterstützt. Wenn der Ruhezustand länger als 60 Tage beibehalten werden soll, müssen Sie die in den Ruhezustand versetzte Instance starten, anhalten und starten.
- Unsere Plattform wird regelmäßig mit Upgrades und Sicherheits-Patches aktualisiert, was zu Konflikten mit vorhandenen Instances im Ruhezustand führen kann. Sie werden über kritische Updates benachrichtigt, für die Instances im Ruhezustand gestartet werden müssen, damit die Instance heruntergefahren oder neu gestartet werden kann, um erforderliche Upgrades und Sicherheits-Patches anzuwenden.

Überlegungen zum Ruhezustand einer Spot Instance

- Wenn Sie Ihre Spot Instance in den Ruhezustand versetzen, können Sie sie neu starten, sofern Kapazität verfügbar ist und der Spot-Preis kleiner oder gleich Ihrem angegebenen Höchstpreis ist.
- Wenn Amazon EC2 Ihre Spot Instance in den Ruhezustand versetzt:
  - Nur Amazon EC2 kann Ihre Instance fortsetzen.
  - Amazon EC2 startet die in den Ruhezustand versetzte Spot Instance wieder, wenn Kapazität mit einem Spot-Preis verfügbar wird, der kleiner oder gleich Ihrem angegebenen Höchstpreis ist.
  - Bevor Amazon EC2 Ihre Spot Instance in den Ruhezustand versetzt, erhalten Sie zwei Minuten vor Beginn des Ruhezustands eine Unterbrechungsbenachrichtigung.

Weitere Informationen finden Sie unter Spot-Instance-Unterbrechungen.

- Es gibt mehrere Möglichkeiten, den Ruhezustand für eine Spot Instance zu aktivieren. Weitere Informationen finden Sie unter Festlegen des Unterbrechungsverhaltens.

Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance

Sie können die Unterstützung für den Ruhezustand für eine On-Demand-Instance oder eine Spot-Instance aktivieren, wenn Sie sie starten. Sie können den Ruhezustand für eine bestehende Instance nicht aktivieren, unabhängig davon, ob sie läuft oder gestoppt ist. Weitere Informationen finden Sie unter Aktivieren Sie den Ruhezustand der Instanz.

Anforderungen, um eine Instance in den Ruhezustand zu versetzen

- AWS-Regionen
- AMIs
- Instanzfamilien
- Instance-RAM-Größe
- Root-Volume-Typ
- Größe des Root-Volumes
- Verschlüsselung des Root-Volumes
- EBS-Volume-Typ
- Spot-Instance-Anforderungen

AWS-Regionen

Sie können den Ruhezustand für alle Instanzen verwenden. AWS-Regionen

AMIs

Sie müssen ein HVM-AMI verwenden, das den Ruhezustand unterstützt. Die folgenden AMIs unterstützen den Ruhezustand:

Linux-AMIs

- AL2023 AMI veröffentlicht 20.09.2023 oder später
- Amazon Linux 2 AMI ab 29.08.2019

- Amazon Linux AMI 2018.03, veröffentlicht ab 16.11.2018
- CentOS Version 8 AMI [1] (Zusätzliche Konfiguration ist erforderlich)
- Fedora Version 34 oder höher AMI [1] (Zusätzliche Konfiguration ist erforderlich)
- Red Hat Enterprise Linux (RHEL) 9 AMI [1] (Zusätzliche Konfiguration ist erforderlich)
- Red Hat Enterprise Linux (RHEL) 8 AMI [1] (Zusätzliche Konfiguration ist erforderlich)
- Ubuntu 22.04.2 LTS (Jammy Jellyfish) AMI mit einer Seriennummer ab 20230303 oder höher[2]
- Ubuntu 20.04 LTS (Focal Fossa) AMI mit einer Seriennummer ab 20210820 oder höher [2]
- Ubuntu 18.04 LTS (Bionic Beaver) AMI mit einer Seriennummer ab 20190722.1 oder höher [2] [4]
- Ubuntu 16.04 LTS (Xenial Xerus) AMI [2] [3] [4] (Zusätzliche Konfiguration ist erforderlich)

[1] Für CentOS, Fedora und Red Hat Enterprise Linux wird der Ruhezustand nur auf Nitro-basierten Instances unterstützt.

[2] Wir empfehlen, KASLR auf Instances mit Ubuntu 22.04.2 LTS (Jammy Jellyfish), Ubuntu 20.04 LTS (Focal Fossa), Ubuntu 18.04 LTS (Bionic Beaver) und Ubuntu 16.04 LTS (Xenial Xerus) zu deaktivieren. Weitere Informationen finden Sie unter Deaktivieren von KASLR auf einer Instance (nur Ubuntu).

[3] Für das Ubuntu 16.04 LTS (Xenial Xerus) AMI wird der Ruhezustand auf `t3.nano`-Instance-Typen nicht unterstützt. Es wird kein Patch zur Verfügung gestellt, da Ubuntu (Xenial Xerus) die Unterstützung im April 2021 beendet hat. Wenn Sie `t3.nano`-Instance-Typen nutzen möchten empfehlen wir, auf Ubuntu 22.04.2 LTS (Jammy Jellyfish) AMI, Ubuntu 20.04 LTS (Focal Fossa) AMI oder Ubuntu 18.04 LTS (Bionic Beaver) AMI upzugraden.

[4] Support für Ubuntu 18.04 LTS (Bionic Beaver) und Ubuntu 16.04 LTS (Xenial Xerus) hat das Ende ihrer Lebensdauer erreicht.

Informationen zum Konfigurieren eines eigenen AMI zum Unterstützen des Ruhezustands finden Sie unter Konfigurieren Sie ein Linux-AMI zur Unterstützung des Ruhezustands.

Die Unterstützung für andere Versionen von Ubuntu sowie für andere Betriebssysteme folgt in Kürze.

Windows-AMIs

- Windows Server 2022-AMI ab 13.09.2023

- Windows Server 2019-AMI ab 11.09.2019
- Windows Server 2016-AMI ab 11.09.2019
- Windows Server 2012 R2-AMI ab 11.09.2019
- Windows Server 2012-AMI ab 11.09.2019

Instanzfamilien

Sie müssen eine Instance-Familie verwenden, die den Ruhezustand unterstützt.

- Allgemeiner Zweck: M3, M4, M5, M5a, M5ad, M5d, M6i, M6id, M7i, M7i-Flex, T2, T3, T3a
- Für Berechnungen optimiert: C3, C4, C5, C5d, C6i, C6id, C7a, C7i, C7i-Flex
- Speicheroptimiert: R3, R4, R5, R5a, R5ad, R5d, R7a, R7i, R7iz
- Speicheroptimiert: I3, I3en

Nitro-Instances — Bare-Metal-Instances werden nicht unterstützt.

So zeigen Sie die verfügbaren Instance-Typen an, die den Ruhezustand in einer bestimmten Region unterstützen

Die verfügbaren Instance-Typen variieren je nach Region. Um die verfügbaren Instance-Typen anzuzeigen, für die der Ruhezustand in einer Region unterstützt wird, verwenden Sie den Befehl describe-instance-types mit dem Parameter `--region`. Fügen Sie den `--filters`-Parameter mit ein, um die Ergebnisse auf die Instance-Typen zu skalieren, die den Ruhezustand unterstützen, und den `--query`Parameter, um die Ausgabe auf den Wert von `InstanceType` zu skalieren.

```
aws ec2 describe-instance-types --filters Name=hibernation-supported,Values=true --
query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Beispielausgabe

```
c3.2xlarge
c3.4xlarge
c3.8xlarge
c3.large
c3.xlarge
c4.2xlarge
c4.4xlarge
```

```
c4.8xlarge
...
```

Instance-RAM-Größe

Linux-Instanzen — Sie müssen weniger als 150 GB groß sein.

Windows-Instanzen — Können bis zu 16 GB groß sein. Um eine T3- oder T3a-Windows-Instance in den Ruhezustand zu versetzen, empfehlen wir mindestens 1 GB RAM.

Root-Volume-Typ

Bei dem Root-Volume muss es sich um ein EBS-Volume handeln, nicht um ein Instance-Speicher-Volume.

Größe des Root-Volumes

Das Root-Volume muss groß genug sein, um den RAM-Inhalt zu speichern und Ihrer erwarteten Nutzung, z. B. dem Betriebssystem oder den Anwendungen, gerecht zu werden. Wenn Sie den Ruhezustand aktivieren, wird beim Starten Speicherplatz auf dem Stamm-Volume zugewiesen, um den RAM zu speichern.

Verschlüsselung des Root-Volumes

Das Root-Volume muss verschlüsselt werden, um den Schutz vertraulicher Inhalte zu gewährleisten, die sich im Ruhezustand im Arbeitsspeicher befinden. Wenn RAM-Daten auf das EBS-Stamm-Volume verschoben werden, werden sie immer verschlüsselt. Die Verschlüsselung des Stamm-Volumes wird beim Starten der Instance erzwungen.

Verwenden Sie eine der folgenden drei Optionen, um sicherzustellen, dass das Stammvolume ein verschlüsseltes EBS-Volume ist:

- Standardmäßige EBS-Verschlüsselung: Sie können die standardmäßige EBS-Verschlüsselung aktivieren, um sicherzustellen, dass alle neuen EBS-Volumes, die in Ihrem AWS -Konto erstellt wurden, verschlüsselt sind. Auf diese Weise können Sie den Ruhezustand für Ihre Instances aktivieren, ohne die Verschlüsselungsabsicht beim Instance-Start anzugeben. Weitere Informationen finden Sie unter Verschlüsselung standardmäßig aktivieren.
- EBS-Einzelschritt-Verschlüsselung: Sie können verschlüsselte EBS-gestützte EC2-Instances aus einem unverschlüsselten AMI starten und gleichzeitig den Ruhezustand aktivieren. Weitere Informationen finden Sie unter Verwenden der Verschlüsselung mit EBS-gestützten AMIs.

- Verschlüsseltes AMI: Sie können die EBS-Verschlüsselung unter Verwendung eines verschlüsselten AMI zum Starten Ihrer Instance aktivieren. Wenn Ihr AMI über kein verschlüsseltes Stamm-Snapshot verfügt, können Sie es auf ein neues AMI kopieren und Verschlüsselung anfordern. Weitere Informationen finden Sie unter Verschlüsseln eines unverschlüsselten Images während des Kopierens und Kopieren eines AMI.

EBS-Volume-Typ

Die EBS-Volumes müssen einen der folgenden EBS-Volumetypen verwenden:

- Allzweck-SSD (`gp2` und `gp3`)
- Bereitgestellte IOPS SSD (`io1` und `io2`)

Wenn Sie einen Volume-Typ Provisioned IOPS SSD wählen, müssen Sie das EBS-Volume mit den entsprechenden IOPS bereitstellen, um eine optimale Leistung für den Ruhezustand zu erzielen. Weitere Informationen finden Sie unter Amazon EBS-Volumetypen im Amazon EBS-Benutzerhandbuch.

Spot-Instance-Anforderungen

Für Spot-Instances gelten die folgenden Anforderungen:

- Der Spot Instance-Anfrage-Typ muss `persistent` sein.
- Sie können in der Spot-Instance-Anforderung keine Startgruppe angeben.

Konfigurieren Sie ein Linux-AMI zur Unterstützung des Ruhezustands

Die folgenden Linux-AMIs unterstützen den Ruhezustand, aber um eine Instance, die mit einem dieser AMIs gestartet wurde, in den Ruhezustand zu versetzen, ist eine zusätzliche Konfiguration erforderlich, bevor Sie die Instance in den Ruhezustand versetzen können.

Zusätzliche Konfigurationsschritte sind erforderlich für:

- Mindest-AMI für Amazon Linux 2, veröffentlicht am 29.08.2019 oder später
- Amazon Linux 2 veröffentlicht vor 29.08.2019
- Amazon Linux veröffentlicht vor 16.11.2018
- CentOS Version 8 oder neuer
- Fedora Version 34 oder höher

- Red Hat Enterprise Linux 8 oder 9
- Ubuntu 20.04 (Focal Fossa) veröffentlicht vor Seriennummer 20210820
- Ubuntu 18.04 (Bionic Beaver) veröffentlicht vor Seriennummer 20190722.1
- Ubuntu 16.04 (Xenial Xerus)

Weitere Informationen finden Sie unter Instance-Software auf Ihrer Amazon Linux 2-Instance aktualisieren.

Für die folgenden AMIs ist keine zusätzliche Konfiguration erforderlich, da sie bereits für die Unterstützung des Ruhezustands konfiguriert sind:

- AL2023 AMI veröffentlicht 20.09.2023 oder später
- Vollständiges Amazon-Linux-2-AMI, veröffentlicht am 29.08.2019 oder später
- Amazon Linux AMI 2018.03, veröffentlicht ab 16.11.2018
- Ubuntu 22.04.2 LTS (Jammy Jellyfish) AMI mit einer Seriennummer ab 20230303 oder höher
- Ubuntu 20.04 LTS (Focal Fossa) AMI mit einer Seriennummer ab 20210820 oder höher
- Ubuntu 18.04 LTS (Bionic Beaver) AMI mit einer Seriennummer ab 20190722.1 oder höher

Mindest-AMI für Amazon Linux 2, veröffentlicht am 29.08.2019 oder später

So konfigurieren Sie ein Mindest-AMI für Amazon Linux 2, das 2019.08.29 oder später veröffentlicht wurde, zur Unterstützung des Ruhezustands

1. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

2. Den Service neu starten.

```
[ec2-user ~]$ sudo systemctl start hibinit-agent
```

Amazon Linux 2 veröffentlicht vor 29.08.2019

So konfigurieren Sie ein Amazon-Linux-2-AMI vor 29.08.2019 zum Unterstützen des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.14.138-114.102` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

4. Überprüfen Sie, ob die Kernel-Version auf `4.14.138-114.102` oder höher aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

5. Halten Sie die Instance an und erstellen Sie ein AMI. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

Amazon Linux veröffentlicht vor 16.11.2018

So konfigurieren Sie ein Amazon Linux-AMI, veröffentlicht vor 16.11.2018, zum Unterstützen des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.14.77-70.59` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

3. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

4. Bestätigen Sie, dass die Kernel-Version auf `4.14.77-70.59` oder höher aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

5. Halten Sie die Instance an und erstellen Sie ein AMI. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

CentOS Version 8 oder neuer

So konfigurieren Sie ein AMI der CentOS Version 8 oder höher zur Unterstützung des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.18.0-305.7.1.el8_4.x86_64` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren Sie das EPEL-Repository (Fedora Extra Packages for Enterprise Linux).

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

3. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Aktivieren Sie den Ruhezustand des Agenten, um beim Booten zu starten.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

6. Bestätigen Sie, dass die Kernel-Version auf `4.18.0-305.7.1.el8_4.x86_64` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Fedora Version 34 oder höher

So konfigurieren Sie ein AMI der Fedora Version 34 oder höher zur Unterstützung des Ruhezustands

1. Aktualisieren Sie den Kernel auf `5.12.10-300.fc34.x86_64` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo dnf install ec2-hibinit-agent
```

3. Aktivieren Sie den Ruhezustand des Agenten, um beim Booten zu starten.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

4. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

5. Bestätigen Sie, dass die Kernel-Version auf `5.12.10-300.fc34.x86_64` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Red Hat Enterprise Linux 8 oder 9

So konfigurieren Sie ein AMI des Red Hat Enterprise Linux 8 oder 9 zur Unterstützung des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.18.0-305.7.1.el8_4.x86_64` oder höher.

```
[ec2-user ~]$ sudo yum update kernel
```

2. Installieren Sie das EPEL-Repository (Fedora Extra Packages for Enterprise Linux).

   RHEL-Version 8:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   RHEL-Version 9:

```
[ec2-user ~]$ sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

3. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo yum install ec2-hibinit-agent
```

4. Aktivieren Sie den Ruhezustand des Agenten, um beim Booten zu starten.

```
[ec2-user ~]$ sudo systemctl enable hibinit-agent.service
```

5. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

6. Bestätigen Sie, dass die Kernel-Version auf `4.18.0-305.7.1.el8_4.x86_64` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Ubuntu 20.04 (Focal Fossa) veröffentlicht vor Seriennummer 20210820

Ein Ubuntu 20.04 LTS (Focal Fossa)-AMI, das vor der Seriennummer 20210820 veröffentlicht wurde, für die Unterstützung der Ruhezustandsfunktion konfigurieren

1. Aktualisieren Sie die linux-aws-kernel Version auf `5.8.0-1038.40` oder höher und grub2 auf `2.04-1ubuntu26.13` oder später.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

3. Bestätigen Sie, dass die Kernel-Version auf `5.8.0-1038.40` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

4. Bestätigen Sie, dass die grub2-Version auf `2.04-1ubuntu26.13` oder eine neuere Version aktualisiert wurde.

```
[ec2-user ~]$ dpkg --list | grep grub2-common
```

Ubuntu 18.04 (Bionic Beaver) veröffentlicht vor Seriennummer 20190722.1

So konfigurieren Sie ein Ubuntu 18.04 LTS-AMI, das vor der Seriennummer 20190722.1 veröffentlicht wurde, um den Ruhezustand zu unterstützen

1. Aktualisieren Sie den Kernel auf `4.15.0-1044` oder höher.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt dist-upgrade
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

4. Bestätigen Sie, dass die Kernel-Version auf `4.15.0-1044` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Ubuntu 16.04 (Xenial Xerus)

Um Ubuntu 16.04 LTS für die Unterstützung des Ruhezustands zu konfigurieren, müssen Sie das linux-aws-hwe Kernel-Paket Version 4.15.0-1058-aws oder höher und den ec2-hibinit-Agenten installieren.

> **Important**
>
> Das Kernelpaket `linux-aws-hwe` wird von Canonical unterstützt. Die Standardunterstützung für Ubuntu 16.04 LTS endete im April 2021 und das Paket erhält keine regelmäßigen Updates mehr. Es wird jedoch zusätzliche Sicherheitsupdates erhalten, bis der erweiterte Sicherheitswartungs-Support 2024 endet. Weitere Informationen finden Sie unter Amazon EC2 Hibernation for Ubuntu 16.04 LTS now available im Canonical Ubuntu Blog. Es wird empfohlen, auf Ubuntu 20.04 LTS (Focal Fossa)-AMI oder Ubuntu 18.04 LTS (Bionic Beaver)-AMI upzugraden.

So konfigurieren Sie ein Ubuntu 16.04 LTS AMI zur Unterstützung des Ruhezustands

1. Aktualisieren Sie den Kernel auf `4.15.0-1058-aws` oder höher.

```
[ec2-user ~]$ sudo apt update
[ec2-user ~]$ sudo apt install linux-aws-hwe
```

2. Installieren des `ec2-hibinit-agent`-Paket aus den Repositories.

```
[ec2-user ~]$ sudo apt install ec2-hibinit-agent
```

3. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

4. Bestätigen Sie, dass die Kernel-Version auf `4.15.0-1058-aws` oder später aktualisiert wurde.

```
[ec2-user ~]$ uname -a
```

Ruhezustand für eine Amazon EC2 EC2-Instance aktivieren

Um eine Instance in den Ruhezustand zu setzen, müssen Sie sie zunächst beim Starten der Instance für den Ruhezustand aktivieren.

> **Important**
>
> Für einmal gestartete Instances kann der Ruhezustand nicht mehr aktiviert oder deaktiviert werden.

Themen

Aktivieren des Ruhezustands für On-Demand-Instances

Nutzen Sie eine der folgenden Methoden, um den Ruhezustand für Ihre On-Demand-Instances zu aktivieren.

New console

So aktivieren Sie den Ruhezustand für eine On-Demand-Instance

1. Folgen Sie den Anweisungen zum Starten einer Instance, aber starten Sie die Instance erst, nachdem Sie die folgenden Schritte zur Aktivierung des Ruhezustands ausgeführt haben.
2. Um den Ruhezustand zu aktivieren, konfigurieren Sie die folgenden Felder im Launch Instance Wizard:

   a. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) ein AMI aus, das den Ruhezustand unterstützt. Weitere Informationen finden Sie unter AMIs.

   b. Wählen Sie unter Instance type (Instance-Typ) einen unterstützten Instance-Typ aus. Weitere Informationen finden Sie unter Instanzfamilien.

   c. Wählen Sie unter Configure storage (Speicher konfigurieren) die Option Advanced (Erweitert) (rechts) und geben Sie die folgenden Informationen für das Root-Volume an:

      - Geben Sie unter Größe (GiB) die Größe des EBS-Stamm-Volumes ein. Das Volume muss groß genug sein, um den RAM-Inhalt zu speichern und der erwarteten Nutzung gerecht zu werden.
      - Wählen Sie unter Volume type (Volume-Typ) einen unterstützten EBS-Volume-Typ aus Allzweck-SSD (`gp2` und `gp3`) oder bereitgestellte IOPS-SSD (`io1` und `io2`).
      - Wählen Sie für Encrypted (Verschlüsselt) die Option Yes (Ja) aus. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, ist Ja ausgewählt.
      - Wählen Sie für KMS key (KMS-Schlüssel) den Verschlüsselungsschlüssel für das Volume. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, wird der Standard-Verschlüsselungsschlüssel ausgewählt.

      Weitere Informationen zu den Voraussetzungen für das Stamm-Volume finden Sie unter Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance.

d. Erweitern Sie Advanced details (Erweiterte Details) und wählen Sie für Stop – Hibernate behavior (Stopp – Ruhezustand) die Option Enable (Aktivieren) aus.

3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Old console

So aktivieren Sie den Ruhezustand für eine On-Demand-Instance

1. Folgen Sie dem Verfahren unter Starten einer Instance mit dem alten Launch Instance Wizard.
2. Wählen Sie auf der Seite Choose an Amazon Machine Image (AMI) (Amazon-System-Image (AMI) auswählen) ein AMI aus, das den Ruhezustand unterstützt. Weitere Informationen zu unterstützten AMIs finden Sie unter Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance.
3. Wählen Sie auf der Seite Choose an Instance Type (Instance-Typ auswählen) einen unterstützten Instance-Typ und anschließend Next: Configure Instance Details (Weiter: Instance-Details konfigurieren) aus. Weitere Informationen zu unterstützten Instance-Typen finden Sie unter Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance.
4. Aktivieren Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) unter Stop – Hibernate Behavior (Anhalten – Verhalten für Ruhezustand) das Kontrollkästchen Enable hibernation as an additional stop behavior (Ruhezustand als zusätzliches Verhalten beim Anhalten aktivieren).
5. Geben Sie auf der Seite Speicher hinzufügen für das Stamm-Volume die folgenden Informationen an:

   - Geben Sie unter Größe (GiB) die Größe des EBS-Stamm-Volumes ein. Das Volume muss groß genug sein, um den RAM-Inhalt zu speichern und der erwarteten Nutzung gerecht zu werden.
   - Wählen Sie unter Volume-Typ einen unterstützten EBS-Volume-Typ aus (Universal-SSD (`gp2` und `gp3`) oder Bereitgestellte IOPS-SSD (`io1` und `io2`).
   - Wählen Sie unter Verschlüsselung den Verschlüsselungsschlüssel für das Volume aus. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, wird der Standard-Verschlüsselungsschlüssel ausgewählt.

Weitere Informationen zu den Voraussetzungen für das Stamm-Volume finden Sie unter Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance.

6. Fahren Sie den Aufforderungen des Assistenten entsprechend fort. Wählen Sie nach dem Überprüfen Ihrer Optionen auf der Seite Review Instance Launch (Instance-Start überprüfen) die Option Launch (Starten). Weitere Informationen finden Sie unter Starten einer Instance mit dem alten Launch Instance Wizard.

AWS CLI

So aktivieren Sie den Ruhezustand für eine On-Demand-Instance

Starten Sie mit dem Befehl run-instances eine Instance. Geben Sie die EBS-Stamm-Volume-Parameter mithilfe des `--block-device-mappings file://mapping.json`-Parameters an und aktivieren Sie den Ruhezustand mithilfe des `--hibernation-options Configured=true`-Parameters.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type m5.large \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
```

Geben Sie in Folgendes a `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> Der Wert für `DeviceName` muss mit dem Namen des Stammgeräts übereinstimmen, der dem AMI zugeordnet ist. Um den Namen des Stammgeräts zu finden, verwenden Sie den Befehl describe-images.
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```
>
> Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, können Sie sie weglassen`"Encrypted": true`.

PowerShell

Um den Ruhezustand für eine On-Demand-Instance zu aktivieren, verwenden Sie AWS Tools for Windows PowerShell

Verwenden Sie den New-EC2InstanceBefehl, um eine Instance zu starten. Geben Sie das EBS-Stamm-Volume an, indem Sie zuerst die Blockgerät-Zuweisung definieren und sie dann mit dem `-BlockDeviceMappings`-Parameter dem Befehl hinzufügen. Aktivieren Sie den Ruhezustand mit dem Parameter `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
            -ImageId ami-0abcdef1234567890 `
            -InstanceType m5.large `
            -BlockDeviceMappings $ebs_encrypt `
            -HibernationOptions_Configured $true `
            -MinCount 1 `
            -MaxCount 1 `
            -KeyName MyKeyPair
```

> **Note**
>
> Der Wert für `DeviceName` muss mit dem Namen des Stammgeräts übereinstimmen, der dem AMI zugeordnet ist. Verwenden Sie den Get-EC2ImageBefehl, um den Namen des Root-Geräts zu ermitteln.
>
> ```
> Get-EC2Image -ImageId ami-0abcdef1234567890
> ```
>
> Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, können Sie sie bei der Zuordnung `Encrypted = $true` von Blockgeräten weglassen.

Aktivieren des Ruhezustands für Spot Instances

Nutzen Sie eine der folgenden Methoden, um den Ruhezustand für Ihre Spot Instances zu aktivieren. Weitere Informationen zum Ruhezustand einer Spot Instance bei einer Unterbrechung finden Sie unter Spot-Instance-Unterbrechungen.

Console

Sie können den Launch Instance Wizard in der Amazon-EC2-Konsole verwenden, um den Ruhezustand für eine Spot Instance zu aktivieren.

So aktivieren Sie den Ruhezustand für eine Spot Instance

1. Befolgen Sie das Verfahren zum Anfordern einer Spot Instance mithilfe des Launch Instance Wizard. Starten Sie die Instance jedoch erst, wenn Sie die folgenden Schritte zum Aktivieren des Ruhezustands ausgeführt haben.
2. Um den Ruhezustand zu aktivieren, konfigurieren Sie die folgenden Felder im Launch Instance Wizard:
   a. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) ein AMI aus, das den Ruhezustand unterstützt. Weitere Informationen finden Sie unter AMIs.
   b. Wählen Sie unter Instance type (Instance-Typ) einen unterstützten Instance-Typ aus. Weitere Informationen finden Sie unter Instanzfamilien.
   c. Wählen Sie unter Configure storage (Speicher konfigurieren) die Option Advanced (Erweitert) (rechts) und geben Sie die folgenden Informationen für das Root-Volume an:

- Geben Sie unter Größe (GiB) die Größe des EBS-Stamm-Volumes ein. Das Volume muss groß genug sein, um den RAM-Inhalt zu speichern und der erwarteten Nutzung gerecht zu werden.
- Wählen Sie unter Volume type (Volume-Typ) einen unterstützten EBS-Volume-Typ aus Allzweck-SSD (`gp2` und `gp3`) oder bereitgestellte IOPS-SSD (`io1` und `io2`).
- Wählen Sie für Encrypted (Verschlüsselt) die Option Yes (Ja) aus. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, ist Ja ausgewählt.
- Wählen Sie für KMS key (KMS-Schlüssel) den Verschlüsselungsschlüssel für das Volume. Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, wird der Standard-Verschlüsselungsschlüssel ausgewählt.

Weitere Informationen zu den Voraussetzungen für das Stamm-Volume finden Sie unter Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance.

d. Erweitern Sie Erweiterte Details und führen Sie zusätzlich zu den Feldern zum Konfigurieren einer Spot Instance folgende Schritte aus:

   i. Wählen Sie als Anforderungstyp die Option Persistent aus.

   ii. Wählen Sie für Verhalten bei Unterbrechungen die Option Ruhezustand aus. Alternativ können Sie für das Verhalten Anhalten – Ruhezustand die Option Aktivieren wählen. Beide Felder aktivieren den Ruhezustand auf Ihrer Spot Instance. Sie müssen nur eine davon konfigurieren.

3. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

AWS CLI

Sie können den Ruhezustand für eine Spot Instance mit dem vrun-instances Befehl AWS CLI aktivieren.

So aktivieren Sie den Ruhezustand für eine Spot Instance mit dem **`hibernation-options`**-Parameter

Starten Sie mit dem Befehl run-instances eine Spot Instance. Geben Sie die EBS-Stamm-Volume-Parameter mithilfe des `--block-device-mappings file://mapping.json`-

Parameters an und aktivieren Sie den Ruhezustand mithilfe des `--hibernation-options Configured=true`-Parameters. Der Anfrage-Typ (`SpotInstanceType`) der Spot Instance muss `persistent` sein.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c4.xlarge \
    --block-device-mappings file://mapping.json \
    --hibernation-options Configured=true \
    --count 1 \
    --key-name MyKeyPair
    --instance-market-options
        {
           "MarketType":"spot",
           "SpotOptions":{
              "MaxPrice":"1",
              "SpotInstanceType":"persistent"
            }
        }
```

Geben Sie die Parameter des EBS-Root-Volumes in `mapping.json` wie folgt an.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "VolumeSize": 30,
            "VolumeType": "gp2",
            "Encrypted": true
        }
    }
]
```

> **Note**
>
> Der Wert für `DeviceName` muss mit dem Namen des Stammgeräts übereinstimmen, der dem AMI zugeordnet ist. Um den Namen des Stammgeräts zu finden, verwenden Sie den Befehl describe-images.
>
> ```
> aws ec2 describe-images --image-id ami-0abcdef1234567890
> ```

Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, können Sie sie weglassen`"Encrypted": true`.

PowerShell

Um den Ruhezustand für eine Spot-Instance zu aktivieren, verwenden Sie AWS Tools for Windows PowerShell

Verwenden Sie den New-EC2InstanceBefehl, um eine Spot-Instance anzufordern. Geben Sie das EBS-Stamm-Volume an, indem Sie zuerst die Blockgerät-Zuweisung definieren und sie dann mit dem `-BlockDeviceMappings`-Parameter dem Befehl hinzufügen. Aktivieren Sie den Ruhezustand mit dem Parameter `-HibernationOptions_Configured $true`.

```
PS C:\> $ebs_encrypt = New-Object Amazon.EC2.Model.BlockDeviceMapping
PS C:\> $ebs_encrypt.DeviceName = "/dev/xvda"
PS C:\> $ebs_encrypt.Ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
PS C:\> $ebs_encrypt.Ebs.VolumeSize = 30
PS C:\> $ebs_encrypt.Ebs.VolumeType = "gp2"
PS C:\> $ebs_encrypt.Ebs.Encrypted = $true

PS C:\> New-EC2Instance `
              -ImageId ami-0abcdef1234567890 `
              -InstanceType m5.large `
              -BlockDeviceMappings $ebs_encrypt `
              -HibernationOptions_Configured $true `
              -MinCount 1 `
              -MaxCount 1 `
              -KeyName MyKeyPair `
              -InstanceMarketOption @(
                    MarketType = spot;
                    SpotOptions @{
                    MaxPrice = 1;
                    SpotInstanceType = persistent}
                 )
```

Note

Der Wert für `DeviceName` muss mit dem Namen des Stammgeräts übereinstimmen, der dem AMI zugeordnet ist. Verwenden Sie den Get-EC2ImageBefehl, um den Namen des Root-Geräts zu ermitteln.

```
Get-EC2Image -ImageId ami-0abcdef1234567890
```

Wenn Sie die Verschlüsselung in dieser AWS Region standardmäßig aktiviert haben, können Sie sie bei der Zuordnung `Encrypted = $true` von Blockgeräten weglassen.

Es gibt mehrere Möglichkeiten, den Ruhezustand für eine Spot Instance zu aktivieren. Weitere Informationen finden Sie unter Festlegen des Unterbrechungsverhaltens.

Anzeigen, ob eine Instance für den Ruhezustand aktiviert ist

Verwenden Sie die folgenden Anweisungen, um anzuzeigen, ob eine Instance für den Ruhezustand aktiviert ist.

Console

So zeigen Sie an, ob eine Instance für den Ruhezustand aktiviert ist

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und überprüfen Sie auf der Registerkarte Details im Bereich Instance-Details das Stop-Hibernate-Verhalten. Enabled (Aktiviert) gibt an, dass die Instance für den Ruhezustand aktiviert ist.

AWS CLI

So zeigen Sie an, ob eine Instance für den Ruhezustand aktiviert ist

Verwenden Sie den Befehl describe-instances und geben Sie den Parameter `--filters "Name=hibernation-options.configured,Values=true"` an, um die für den Ruhezustand aktivierten Instances zu filtern.

```
aws ec2 describe-instances \
    --filters "Name=hibernation-options.configured,Values=true"
```

Das folgende Feld in der Ausgabe gibt an, dass die Instance für den Ruhezustand aktiviert wurde.

```
"HibernationOptions": {
```

```
    "Configured": true
}
```

PowerShell

So zeigen Sie an, ob eine Instance mithilfe der AWS Tools for Windows PowerShell für den Ruhezustand aktiviert wurde

Verwenden Sie den Get-EC2InstanceBefehl und geben Sie den `-Filter @{ Name="hibernation-options.configured"; Value="true"}` Parameter an, um Instances zu filtern, die für den Ruhezustand aktiviert sind.

```
(Get-EC2Instance -Filter @{Name="hibernation-options.configured";
 Value="true"}).Instances
```

Die Ausgabe listet die EC2-Instances auf, für die der Ruhezustand aktiviert wurde.

Deaktivieren von KASLR auf einer Instance (nur Ubuntu)

Um den Ruhezustand auf einer neu gestarteten Instance mit Ubuntu 16.04 LTS (Xenial Xerus), Ubuntu 18.04 LTS (Bionic Beaver) mit Seriennummer 20190722.1 oder höher oder Ubuntu 20.04 LTS (Focal Fossa) mit Seriennummer 20210820 oder höher auszuführen, raten wir dazu, KASLR (Kernel Address Space Layout Randomization) zu deaktivieren. Unter Ubuntu 16.04 LTS, Ubuntu 18.04 LTS oder Ubuntu 20.04 LTS ist KASLR standardmäßig aktiviert

KASLR ist ein standardmäßiges Linux-Kernel-Sicherheitsfeature, die Sie dabei unterstützt, Risiken und Auswirkungen noch nicht erkannter Schwachstellen des Speicherzugriffs zu reduzieren, indem der Wert der Basisadresse des Kernels randomisiert wird. Wenn KASLR aktiviert ist, besteht die Möglichkeit, dass die Instance nicht mehr gestartet wird, nachdem sie in den Ruhezustand versetzt wurde.

Weitere Informationen über KASLR finden Sie unter Ubuntu-Features.

So deaktivieren Sie KASLR auf einer Instance, die mit Ubuntu gestartet wurde

1. Stellen Sie per SSH eine Verbindung mit Ihrer Instance her. Weitere Informationen finden Sie unter the section called “Herstellen einer Verbindung mit SSH über Linux oder macOS”.
2. Öffnen Sie die Datei `/etc/default/grub.d/50-cloudimg-settings.cfg` mit einem Editor Ihrer Wahl. Bearbeiten Sie die Zeile `GRUB_CMDLINE_LINUX_DEFAULT` so, dass die Option `nokaslr` an ihrem Ende angefügt wird wie im folgenden Beispiel veranschaulicht.

```
GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
 nvme_core.io_timeout=4294967295 nokaslr"
```

3. Speichern Sie die Datei und beenden Sie den Editor.
4. Führen Sie den folgenden Befehl aus, um die Grub-Konfiguration erneut zu erstellen.

```
[ec2-user ~]$ sudo update-grub
```

5. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

6. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass `nokaslr` hinzugefügt wurde.

```
[ec2-user ~]$ cat /proc/cmdline
```

   Die Befehlsausgabe sollte die Option `nokaslr` enthalten.

Eine Amazon EC2 EC2-Instance in den Ruhezustand versetzen

Sie können den Ruhezustand für eine On-Demand-Instance oder Spot Instance einleiten, wenn es sich bei der Instance um eine EBS-gestützte Instance handelt, sie für den Ruhezustand aktiviert ist und die Voraussetzungen für den Ruhezustand erfüllt. Wenn eine Instance nicht erfolgreich in den Ruhezustand versetzt werden kann, wird sie regulär heruntergefahren.

Console

So versetzen Sie eine Instance in den Ruhezustand

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine Instance und dann Instance state (Instance-Status), Hibernate instance (Instance in den Ruhezustand versetzen) aus. Falls Instance in Ruhezustand versetzen deaktiviert ist, wurde die Instance entweder bereits in den Ruhezustand versetzt oder angehalten oder sie kann nicht in den Ruhezustand versetzt werden. Weitere Informationen finden Sie unter Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance.

4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Hibernate (Ruhezustand). Das Versetzen der Instance in den Ruhezustand kann einige Minuten dauern. Der Instance-Status wechselt zuerst zu Stopping (Wird angehalten) und sobald der Ruhezustand erreicht wurde, ist der Zustand Stopped (Angehalten).

AWS CLI

So versetzen Sie eine EBS-gestützte Instance in den Ruhezustand

Verwenden Sie den Befehl stop-instances und geben Sie den Parameter `--hibernate` an.

```
aws ec2 stop-instances \
    --instance-ids i-1234567890abcdef0 \
    --hibernate
```

PowerShell

Um eine Instance mit dem in den Ruhezustand zu versetzen AWS Tools for Windows PowerShell

Verwenden Sie den Stop-EC2InstanceBefehl und geben Sie den `-Hibernate $true` Parameter an.

```
Stop-EC2Instance `
    -InstanceId i-1234567890abcdef0 `
    -Hibernate $true
```

Console

So zeigen Sie an, ob der Ruhezustand für eine Instance initiiert wurde

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und überprüfen Sie auf der Registerkarte Details im Abschnitt Instance-Details den Wert für Statusübergangsmeldung.

   Kunde. UserInitiatedRuhezustand: Der vom Benutzer initiierte Ruhezustand gibt an, dass Sie den Ruhezustand auf der On-Demand-Instance oder Spot-Instance initiiert haben.

AWS CLI

So zeigen Sie an, ob der Ruhezustand für eine Instance initiiert wurde

Verwenden Sie den Befehl describe-instances und geben Sie den Filter `state-reason-code` an, um die Instances anzuzeigen, bei denen der Ruhezustand initiiert wurde.

```
aws ec2 describe-instances \
    --filters "Name=state-reason-code,Values=Client.UserInitiatedHibernate"
```

Das folgende Feld in der Ausgabe gibt an, dass der Ruhezustand auf der On-Demand-Instance oder Spot Instance initiiert wurde.

```
"StateReason": {
    "Code": "Client.UserInitiatedHibernate"
}
```

PowerShell

So zeigen Sie an, ob der Ruhezustand bei einer Instance mithilfe der AWS Tools for Windows PowerShell initiiert wurde

Verwenden Sie den Get-EC2InstanceBefehl und geben Sie den `state-reason-code` Filter an, um die Instances zu sehen, auf denen der Ruhezustand initiiert wurde.

```
Get-EC2Instance `
    -Filter @{Name="state-reason-code";Value="Client.UserInitiatedHibernate"}
```

Die Ausgabe listet die EC2-Instances auf, für die der Ruhezustand initiiert wurde.

Starten Sie eine Amazon EC2 EC2-Instance im Ruhezustand

Sie können eine in den Ruhezustand versetzte Instance genauso wie eine angehaltene Instance starten.

> **Note**
>
> Wenn Amazon EC2 bei Spot Instances die Instance in den Ruhezustand versetzt hat, kann sie nur von Amazon EC2 wieder aufgenommen werden. Sie können eine in den Ruhezustand versetzte Spot Instance nur dann wieder aufnehmen, wenn Sie sie in den

Ruhezustand versetzt haben. Spot Instances können nur dann wieder aufgenommen werden, wenn Kapazität verfügbar ist und der Spot-Preis kleiner oder gleich Ihrem angegebenen Höchstpreis ist.

Console

So starten Sie eine in den Ruhezustand versetzte Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine in den Ruhezustand versetzte Instance und dann Instance state (Instance-Status), Start instance (Instance starten) aus. Es kann einige Minuten dauern, bis die Instance in den Zustand `running` übergeht. Während dieser Zeit zeigen die Statusprüfungen der Instance, dass sie sich in einem fehlerhaften Zustand befindet, bis sie gestartet wurde.

AWS CLI

So starten Sie eine in den Ruhezustand versetzte Instance

Verwenden Sie den Befehl start-instances.

```
aws ec2 start-instances \
    --instance-ids i-1234567890abcdef0
```

PowerShell

Um eine Instance im Ruhezustand mit dem AWS Tools for Windows PowerShell

Verwenden Sie den Start-EC2Instance-Befehl.

```
Start-EC2Instance `
    -InstanceId i-1234567890abcdef0
```

Problembehandlung für den Ruhezustand der Amazon EC2 EC2-Instance

Nutzen Sie diese Informationen für die Diagnose von Problemen, die beim Versetzen einer Instance in den Ruhezustand auftreten können.

Probleme mit dem Ruhezustand

Versetzen in den Ruhezustand direkt nach dem Starten ist nicht möglich

Wenn Sie eine Instance zu kurz nach dem Starten in den Ruhezustand versetzen möchten, wird eine Fehlermeldung angezeigt.

Sie müssen nach dem Start etwa zwei Minuten für Linux-Instances und etwa fünf Minuten für Windows-Instances warten, bevor Sie in den Ruhezustand wechseln.

Der Übergang von **`stopping`** zu **`stopped`** dauert zu lange und der Speicherzustand wird nach dem Starten nicht wiederhergestellt

Wenn es bei einer Instance, die in den Ruhezustand versetzt wird, zu lange dauert, um vom Zustand `stopping` in den Zustand `stopped` zu wechseln, und der Speicherzustand nach dem Starten nicht wiederhergestellt wird, kann dies ein Hinweis darauf sein, dass der Ruhezustand nicht richtig konfiguriert wurde.

Linux-Instanzen

Suchen Sie im Systemprotokoll der Instance nach Meldungen, die mit dem Ruhezustand in Zusammenhang stehen. Um das Systemprotokoll zu öffnen, stellen Sie eine Verbindung mit der Instance her oder verwenden Sie den Befehl get-console-output. Suchen Sie die Protokollzeilen zu `hibinit-agent`. Wenn die Protokollzeilen auf einen Fehler hinweisen oder fehlen, ist höchstwahrscheinlich ein Fehler beim Konfigurieren des Ruhezustands beim Start aufgetreten.

Die folgende Fehlermeldung gibt z. B. an, dass das Stamm-Volume der Instance nicht groß genug ist: `hibinit-agent: Insufficient disk space. Cannot create setup for hibernation. Please allocate a larger root device.`

Wenn die letzte Protokollzeile von `hibinit-agent` `hibinit-agent: Running: swapoff /swap` lautet, wurde der Ruhezustand erfolgreich konfiguriert.

Wenn Sie keine Protokolle zu diesen Prozessen sehen, unterstützt das AMI möglicherweise keinen Ruhezustand. Informationen zu unterstützten AMIs finden Sie unter Voraussetzungen für den Ruhezustand der Amazon EC2 EC2-Instance. Wenn Sie Ihr eigenes Linux-AMI verwendet haben, stellen Sie sicher, dass Sie die Anweisungen für befolgt habenKonfigurieren Sie ein Linux-AMI zur Unterstützung des Ruhezustands.

Windows Server 2016 und höher

Suchen Sie im EC2-Startprotokoll nach Meldungen zum Ruhezustand. Stellen Sie eine Verbindung zur Instance her, um das EC2-Startprotokoll (`C:\ProgramData\Amazon\EC2-Windows\Launch\Log\Ec2Launch.log`) in einem Texteditor zu öffnen. Wenn Sie EC2Launch v2 verwenden, öffnen Sie `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Windows blendet Dateien und Ordner unter `C:\ProgramData` standardmäßig aus. Um die EC2-Startverzeichnisse und -dateien anzuzeigen, müssen Sie den Pfad im Windows Explorer eingeben oder die Ordnereigenschaften so ändern, dass versteckte Dateien und Ordner angezeigt werden.

Suchen Sie die Protokollzeilen zum Ruhezustand. Wenn die Protokollzeilen auf einen Fehler hinweisen oder fehlen, ist höchstwahrscheinlich ein Fehler beim Konfigurieren des Ruhezustands beim Start aufgetreten.

Die folgende Meldung weist beispielsweise darauf hin, dass der Ruhezustand nicht konfiguriert werden konnte: `Message: Failed to enable hibernation.` Wenn die Fehlermeldung ASCII-Dezimalwerte enthält, können Sie die ASCII-Werte in Klartext konvertieren, um die vollständige Fehlermeldung zu lesen.

Wenn die Protokollzeile `HibernationEnabled: true` enthält, wurde der Ruhezustand erfolgreich konfiguriert.

Windows Server 2012 R2 und früher

Suchen Sie im EC2-Konfigurationsprotokoll nach Meldungen, die mit dem Ruhezustand in Zusammenhang stehen. Stellen Sie für den Zugriff auf das EC2-Konfigurationsprotokoll eine Verbindung zur Instance her und öffnen Sie die Datei `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` in einem Texteditor. Suchen Sie die

Protokollzeilen für `SetHibernateOnSleep`. Wenn die Protokollzeilen auf einen Fehler hinweisen oder fehlen, ist höchstwahrscheinlich ein Fehler beim Konfigurieren des Ruhezustands beim Start aufgetreten.

Die folgende Fehlermeldung gibt z. B. an, dass das Stamm-Volume der Instance nicht groß genug ist: `SetHibernateOnSleep: Failed to enable hibernation: Hibernation failed with the following error: There is not enough space on the disk.`

Wenn die Protokollzeile `SetHibernateOnSleep: HibernationEnabled: true` lautet, wurde der Ruhezustand erfolgreich konfiguriert.

Größe der Windows-Instanz

Wenn Sie eine T3- oder T3a-Windows-Instance mit weniger als 1 GB RAM verwenden, versuchen Sie, die Größe der Instance auf eine Instanz mit mindestens 1 GB RAM zu erhöhen.

Instance "blockiert" im Stopp-Zustand

Wenn Sie eine Instance in den Ruhezustand versetzt haben und sie im Zustand `stopping` "festhängt", können Sie das Anhalten erzwingen. Weitere Informationen finden Sie unter Beheben von Problemen beim Anhalten Ihrer Instance.

Spot Instance kann nicht unmittelbar nach dem Ruhezustand gestartet werden

Wenn Sie versuchen, eine Spot Instance zu starten, die innerhalb der letzten zwei Minuten in den Ruhezustand versetzt wurde, wird möglicherweise die folgende Fehlermeldung angezeigt:

`You failed to start the Spot Instance because the associated Spot Instance request is not in an appropriate state to support start.`

Warten Sie etwa zwei Minuten für Linux-Instances und etwa fünf Minuten für Windows-Instanzen und versuchen Sie dann erneut, die Instance zu starten.

Fehler beim Fortsetzen von Spot Instances

Wenn Ihre Spot Instance erfolgreich in den Ruhezustand versetzt wurde, aber nicht fortgesetzt werden konnte und stattdessen komplett neu gestartet wurde, sodass der Ruhezustand nicht erhalten bleibt, enthielten die Benutzerdaten möglicherweise das folgende Skript:

```
/usr/bin/enable-ec2-spot-hibernation
```

Entfernen Sie dieses Skript aus dem Feld Benutzerdaten in der Startvorlage und fordern Sie dann eine neue Spot Instance an.

Hinweis: Selbst wenn die Instance nicht fortgesetzt werden konnte und der Ruhezustand nicht erhalten geblieben ist, kann die Instance auf die gleiche Weise gestartet werden wie beim Starten mit dem Zustand `stopped`.

Durchführen eines Neustarts Ihrer Instance

Ein Neustart einer Instance entspricht einem Neustart des Betriebssystems. In den meisten Fällen dauert es nur wenige Minuten, um die Instance neu zu starten.

Wenn Sie eine Instance neu starten, wird Folgendes beibehalten:

- Öffentlicher DNS-Name (IPv4)
- Private IPv4-Adresse
- Öffentliche IPv4-Adresse
- IPv6-Adresse (falls zutreffend)
- Alle Daten auf den Instance-Speicher-Volumes

Im Gegensatz zum Anhalten und Starten der Instance beginnt mit dem erneuten Hochfahren einer Instance kein neuer Instance-Abrechnungszeitraum (mit einer minimalen 1-Minuten-Abrechnung).

Unter Umständen planen wir für Ihre Instance einen Neustart zu Wartungszwecken ein, z. B. zum Aufspielen von Updates, für die ein Neustart erforderlich ist. Es sind keine Maßnahmen Ihrerseits erforderlich. Wir empfehlen Ihnen, den Neustart zum vorgesehenen Zeitpunkt abzuwarten. Weitere Informationen finden Sie unter Geplante Ereignisse für Ihre Instances.

Wir empfehlen Ihnen, die Amazon EC2-Konsole, ein Befehlszeilenwerkzeug oder die Amazon EC2-API zum erneuten Starten Ihrer Instance zu verwenden, anstatt den Neustart-Befehl für das Betriebssystem auf Ihrer Instance auszuführen. Wenn Sie die Amazon EC2-Konsole, ein Befehlszeilen-Tool oder die Amazon EC2-API für den Neustart Ihrer Instance verwenden, führen wir einen harten Neustart aus, wenn die Instance nicht innerhalb weniger Minuten problemlos herunterfährt. Wenn Sie AWS CloudTrail verwenden, wird bei der Nutzung von Amazon EC2 für den Neustart Ihrer Instance auch ein API-Eintrag für den Zeitpunkt des Instance-Neustarts erstellt.

Windows-Instances

Wenn Windows auf Ihrer Instance Updates installiert, empfehlen wir, Ihre Instance nicht mithilfe der Amazon EC2-Konsole oder der Befehlszeile neu zu starten oder herunterzufahren, solange nicht alle Updates installiert sind. Wenn Sie die Amazon EC2-Konsole oder die Befehlszeile für den Neustart oder das Herunterfahren Ihrer Instance verwenden, besteht das Risiko, dass ein "harter" Neustart Ihrer Instance ausgeführt wird. Ein solcher harter Neustart während der Installation von Updates könnte Ihre Instance in einen instabilen Zustand versetzen.

Console

So führen Sie einen Neustart Ihrer Instance mit der Konsole durch

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und anschließend die Optionen Instance State (Instance-Status) und Reboot instance (Instance neu starten) aus.

   Alternativ können Sie die Instance auswählen und dann Actions (Aktionen), Manage instance state (Instance-Status verwalten). Wählen Sie auf dem sich öffnenden Bildschirm Reboot (Neustart) und dann Change state (Status ändern) aus.
4. Wählen Sie Reboot (Neu starten) aus, wenn Sie zum Bestätigen aufgefordert werden.

   Die Instance verbleibt im Status `running` (wird ausgeführt).

Command line

So starten Sie eine Instance neu

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- reboot-instances (AWS CLI)
- Restart-EC2Instance (AWS Tools for Windows PowerShell)

Experiment mit Fehlersimulation ausführen

Sie können AWS Fault Injection Service damit testen, wie Ihre Anwendung reagiert, wenn Ihre Instanz neu gestartet wird. Weitere Informationen finden Sie im AWS Fault Injection Service - Benutzerhandbuch.

Amazon EC2 EC2-Instances beenden

Wenn Sie Ihre Instance nicht mehr benötigen, können Sie sie löschen. Dies wird als Beenden Ihrer Instance bezeichnet. Sobald der Status einer Instance zu `shutting-down` oder `terminated` wechselt, fallen für diese Instance keine Gebühren mehr an.

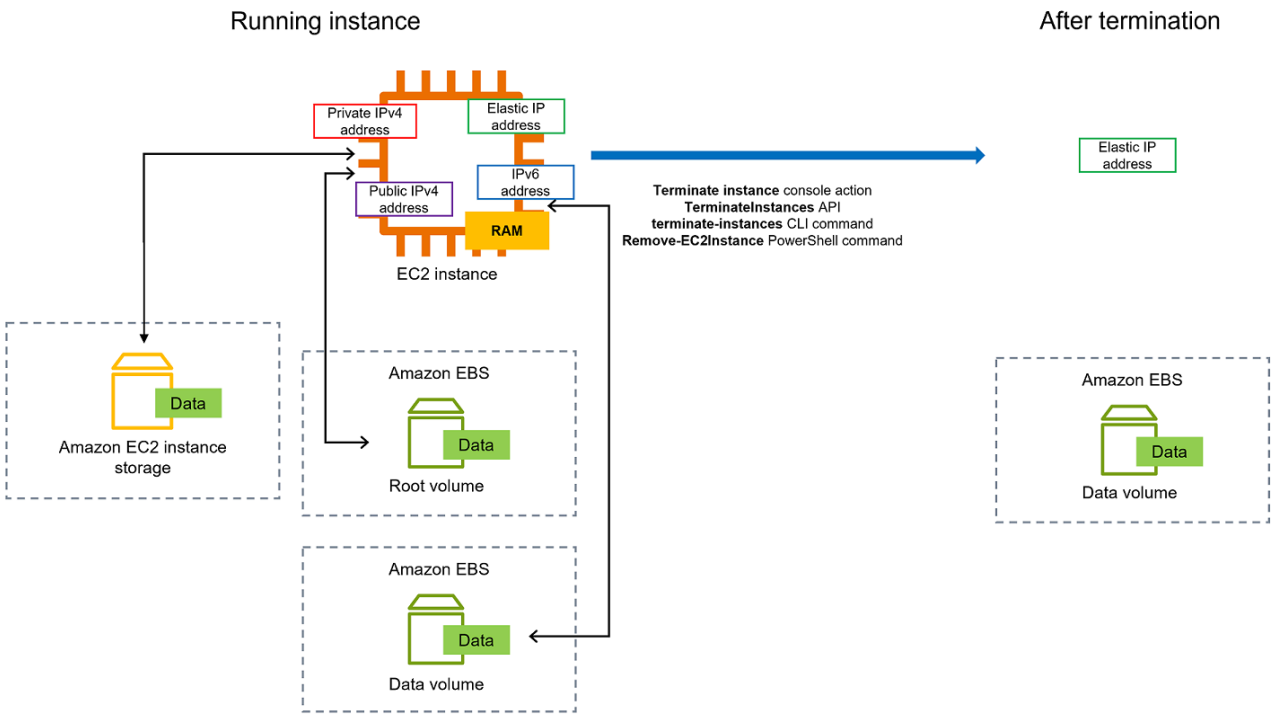
Sie können mit einer Instance keine Verbindung herstellen oder sie starten, nachdem Sie sie beendet haben. Sie können jedoch mit derselben AMI weitere Instances starten. Wenn Sie eine Instance lieber beenden oder in den Ruhezustand versetzen möchten, finden Sie weitere Informationen unter oder. Beenden und starten Sie Amazon EC2 EC2-Instances Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand Weitere Informationen finden Sie unter Unterschiede zwischen Neustart, Anhalten, Ruhezustand und Beenden.

Inhalt

So funktioniert das Kündigen einer Instanz

Wenn Sie eine Instance beenden, werden Änderungen auf Betriebssystemebene der Instance registriert, einige Ressourcen gehen verloren und einige Ressourcen bleiben bestehen.

Das folgende Diagramm zeigt, was verloren geht und was fortbesteht, wenn eine Amazon EC2 EC2-Instance beendet wird. Wenn eine Instance beendet wird, werden die Daten auf allen Instance-Speichervolumes und die im Instance-RAM gespeicherten Daten gelöscht. Alle Elastic IP-Adressen, die der Instance zugeordnet sind, werden getrennt. Bei Amazon EBS-Volumes und den Daten auf diesen Volumes hängt das Ergebnis von der Einstellung Löschen bei Kündigung für das Volume ab. Standardmäßig wird das Root-Volume gelöscht und die Datenvolumes bleiben erhalten.



Überlegungen

- Wird eine Instance beendet, werden die auf Instance-Speicher-Volumes befindlichen Daten, die mit der Instance verbunden sind, gelöscht.
- Root-Gerät-Volume für ein Amazon EBS werden standardmäßig gelöscht, wenn die Instance beendet wird. Allerdings bleiben jegliche weitere EBS-Volumes, die Sie beim Start anfügen oder jegliche EBS-Volumes, die Sie mit einer bestehenden Instance verbinden, fortbestehen, selbst nachdem Ihre Instance beendet wird. Weitere Informationen finden Sie unter Daten beim Beenden einer Instance aufbewahren.

> **Note**
>
> Für alle Volumes, die beim Beenden der Instance nicht gelöscht werden, fallen weiterhin Gebühren an.

- Um zu verhindern, dass eine Instance versehentlich von jemandem beendet wird, aktivieren Sie den Kündigungsschutz.
- Um zu kontrollieren, ob eine Instance beendet oder beendet wird, wenn das Herunterfahren von der Instance aus initiiert wird, ändern Sie das Verhalten beim Herunterfahren der Instance.

- Wenn Sie ein Skript zum Beenden der Instance ausführen, wird Ihre Instance möglicherweise fehlerhaft beendet, weil wir keine Möglichkeit haben, sicherzustellen, dass das Abschaltskript ausgeführt wird. Amazon EC2 versucht, eine Instance sauber herunterzufahren und alle Systemabschaltskripts auszuführen; jedoch können bestimmte Ereignisse (wie z. B. ein Hardware-Ausfall) die Ausführung dieser Systemabschaltskripts verhindern.

Was geschieht, wenn Sie eine Instance beenden

Auf Betriebssystemebene registrierte Änderungen

- Die API-Anfrage sendet ein Tastendruck-Ereignis an den Gast.
- Verschiedene Systemservices werden infolge des Tastendruck-Ereignisses gestoppt. Das ordnungsgemäße Herunterfahren des Systems erfolgt durch systemd (Linux) oder den Systemprozess (Windows). Ein ordnungsgemäßes Herunterfahren wird durch das ACPI-Maustastendruck-Ereignis zum Herunterfahren vom Hypervisor ausgelöst.
- Das Herunterfahren des ACPI wird initiiert.
- Die Instanz wird heruntergefahren, nachdem der Vorgang zum ordnungsgemäßen Herunterfahren beendet wurde. Die Zeit zum Herunterfahren des Betriebssystems kann nicht konfiguriert werden. Die Instance bleibt für eine kurze Zeit in der Konsole sichtbar, dann wird der Eintrag automatisch gelöscht.

Verlorene Ressourcen

- Daten, die auf einem Instance-Speicher-Volume gespeichert sind.
- Daten, die auf Root-Geräte-Volumes von Amazon EBS gespeichert sind, wenn das `DeleteOnTermination`-Attribut auf true festgelegt ist.

Ressourcen, die fortbestehen

- Daten, die auf zusätzlichen Amazon-EBS-Volumes gespeichert sind, die beim Start oder nach dem Start einer Instance angefügt wurden.

Reaktion der Anwendung auf die Beendigung der Instance testen

Sie können AWS Fault Injection Service damit testen, wie Ihre Anwendung reagiert, wenn Ihre Instance beendet wird. Weitere Informationen finden Sie im AWS Fault Injection Service - Benutzerhandbuch.

Beenden einer Instance

Sie können eine Instance jederzeit beenden.

Console

Um eine Instance mithilfe der Konsole zu beenden

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, und wählenSie Instance state (Instance-Status), Terminate instance (Instance beenden).
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.
5. Nachdem Sie eine Instance beendet haben, bleibt sie für kurze Zeit sichtbar und hat den Status`terminated`.

   Wenn die Kündigung fehlschlägt oder wenn eine beendete Instance länger als ein paar Stunden sichtbar ist, finden Sie weitere Informationen unterFortdauernde Anzeige einer beendeten Instance.

Command line

So beenden Sie Ihre Instance mittels Befehlszeile aus

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- terminate-instances (AWS CLI)
- Remove-EC2Instance (AWS Tools for Windows PowerShell)

Beheben von Problemen bei der Beendigung von Instances

Der Anforderer muss die Erlaubnis haben, anzurufen. `ec2:TerminateInstances` Weitere Informationen finden Sie unter Beispielrichtlinien für die Arbeit mit Instanzen.

Wenn Sie Ihre Instance beenden und eine andere Instance startet, haben Sie höchstwahrscheinlich die automatische Skalierung über ein Feature wie EC2-Flotte oder Amazon EC2 Auto Scaling konfiguriert. Weitere Informationen finden Sie unter Instances automatisch gestartet oder beendet.

Sie können eine Instance nicht beenden, wenn der Kündigungsschutz aktiviert ist. Weitere Informationen finden Sie unter Kündigungsschutz.

Wenn Ihre Instance länger als gewöhnlich im Status `shutting-down` bleibt, sollte sie durch automatisierte Prozesse innerhalb des Amazon EC2-Service bereinigt (beendet) werden. Weitere Informationen finden Sie unter Verzögertes Beenden einer Instance.

Aktivieren des Beendigungsschutzes

Um zu verhindern, dass Ihre Instance versehentlich beendet wird, können Sie den Beendigungsschutz für die Instance aktivieren. Das `DisableApiTermination` Attribut steuert, ob die Instance mit der AWS Management Console, AWS Command Line Interface (AWS CLI) oder API beendet werden kann. Standardmäßig ist der Kündigungsschutz für Ihre Instance deaktiviert, was bedeutet, dass Ihre Instance mit der AWS Management Console AWS CLI, oder API beendet werden kann. Sie können den Wert dieses Attributs festlegen, wenn Sie eine Instance starten, während die Instance ausgeführt wird oder während die Instance angehalten ist (für Amazon-EBS-gesicherte Instances).

Das `DisableApiTermination`-Attribut hindert Sie nicht daran, eine Instance zu beenden, indem Sie das Herunterfahren der Instance einleiten (mithilfe eines Betriebssystembefehls zum Herunterfahren des Systems), wenn das Attribut `InstanceInitiatedShutdownBehavior` festgelegt ist. Weitere Informationen finden Sie unter Ändern des durch die Instance initiierten Abschaltverhaltens.

Überlegungen

- Die Aktivierung des Kündigungsschutzes AWS verhindert nicht, dass die Instance beendet wird, wenn ein geplantes Ereignis zum Beenden der Instance stattfindet.
- Das Aktivieren des Stopp-Schutzes hindert Amazon EC2 Auto Scaling nicht daran, eine Instance zu beenden, wenn die Instance fehlerhaft ist bzw. während Abskalierungs-Ereignissen. Sie können

steuern, ob eine Auto-Scaling-Gruppe eine bestimmte Instance beim Abskalieren beenden kann, indem Sie den Instance-Skalierungsschutz verwenden. Sie können steuern, ob eine Auto-Scaling-Gruppe ungesunde Instances beenden kann, indem sie den ReplaceUnhealthy-Scaling-Prozess aussetzt.

- Sie können für Spot-Instances keinen Beendigungsschutz aktivieren.

Aktivieren des Beendigungsschutzes für eine Instance bei Startzeit

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard Launch Instance (Instance starten) und folgen Sie den Anweisungen im Assistenten.
3. Wählen Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) das Kontrollkästchen Enable termination protection (Beendigungsschutz aktivieren) aus.

Aktivieren des Beendigungsschutzes für eine laufende oder angehaltene Instance

1. Wählen Sie die Instance, wählen Sie Actions (Aktionen), Instance Settings (Instance-Einstellungen) und danach Change Termination Protection (Beendigungsschutz ändern) aus.
2. Wählen Sie Yes, Enable (Ja, Aktivieren).

Deaktivieren des Beendigungsschutzes für eine laufende oder angehaltene Instance

1. Wählen Sie die Instance, wählen Sie Actions (Aktionen), Instance Settings (Instance-Einstellungen) und danach Change Termination Protection (Beendigungsschutz ändern) aus.
2. Wählen Sie Yes, Disable (Ja, deaktivieren) aus.

Aktivieren oder Deaktivieren des Beendigungsschutzes mithilfe der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Beenden Sie mehrere Instances mit Kündigungsschutz

Wenn Sie mehrere Instances in mehreren Availability Zones in derselben Anfrage beenden und eine oder mehrere der angegebenen Instances für den Kündigungsschutz aktiviert sind, schlägt die Anfrage fehl und führt zu den folgenden Ergebnissen:

- Die angegebenen Instances, die sich in derselben Availability Zone wie die geschützte Instance befinden, werden nicht beendet.
- Die angegebenen Instances, die sich in verschiedenen Availability Zones befinden, in denen keine anderen angegebenen Instances geschützt sind, werden erfolgreich beendet.

Beispiel

Angenommen, Sie haben die folgenden vier Instances in zwei Availability Zones.

Instance	Availability Zone	Beendigungsschutz
Instanz 1	ALS	`Disabled`
Instanz 2		`Disabled`
Instanz 3	ALS B	`Enabled`
Instanz 4		`Disabled`

Wenn Sie versuchen, alle diese Instances in derselben Anforderung zu beenden, meldet die Anforderung einen Fehler mit den folgenden Ergebnissen:

- Instanz 1 und Instanz 2 wurden erfolgreich beendet, da keine der Instanzen für den Kündigungsschutz aktiviert ist.
- Instanz 3 und Instanz 4 können nicht beendet werden, da Instanz 3 für den Kündigungsschutz aktiviert ist.

Ändern des durch die Instance initiierten Abschaltverhaltens

Standardmäßig wird die Instance angehalten, wenn Sie ein Herunterfahren von einer Amazon-EBS-gesicherten Instance initiieren (z. B. mit den Befehlen shutdown oder poweroff). Durch das

Ändern von Attribut `InstanceInitiatedShutdownBehavior` können Sie dieses Verhalten für die Instance ändern, sodass sie anstatt dessen angehalten wird. Sie können dieses Attribut aktualisieren, während die Instance läuft oder angehalten ist.

Mit dem Befehl halt wird kein Herunterfahren initiiert. Wenn er verwendet wird, wird die Instance nicht beendet; stattdessen wird die CPU in HLT platziert und die Instance wird weiterhin ausgeführt.

> **Note**
>
> Das `InstanceInitiatedShutdownBehavior`-Attribut wird nur verwendet, wenn Sie das Betriebssystem der Instance selbst herunterfahren. Er gilt nicht, wenn Sie eine Instance über die `StopInstances`-API oder die Amazon-EC2-Konsole beenden.

Sie können das Attribut `InstanceInitiatedShutdownBehavior` mithilfe der Amazon EC2-Konsole oder der Befehlszeile ändern.

Console

Ändern des durch die Instance initiierten Abschaltverhaltens

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen, Verhalten beim Herunterfahren ändern.

   Unter Verhalten beim Herunterfahren wird das aktuelle Verhalten angezeigt.
5. Um das Verhalten zu ändern, wählen Sie Anhalten oder Beenden unter Beendigungsverhalten aus.
6. Wählen Sie Speichern.

Command line

Ändern des durch die Instance initiierten Abschaltverhaltens

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Daten beim Beenden einer Instance aufbewahren

Abhängig von Ihrem Anwendungsfall möchten Sie möglicherweise die Daten auf Ihrem Instance-Speicher-Volume oder Amazon-EBS-Volume beibehalten, wenn die Amazon-EC2-Instance beendet wird. Die Daten auf einem Instance-Speicher-Volume bleiben nicht erhalten, wenn eine Instance beendet wird. Wenn Sie die auf einem Instance-Speicher-Volume gespeicherten Daten über die Lebensdauer der Instance hinaus aufbewahren müssen, müssen Sie diese Daten manuell in einen persistenteren Speicher kopieren, z. B. ein Amazon-EBS-Volume, einen Amazon-S3-Bucket oder ein Amazon-EFS-Dateisystem. Weitere Informationen finden Sie unter Speicheroptionen für Ihre Amazon-EC2-Instances.

Für Daten in Amazon-EBS-Volumes verwendet Amazon EC2 den Wert des Attributs `DeleteOnTermination` für jedes angefügtes Amazon-EBS-Volume, um festzulegen, ob das Volume beibehalten oder gelöscht werden soll.

Der Standardwert für das Attribut `DeleteOnTermination`ist je nachdem, ob sich bei dem Volume um das Stammvolume der Instance oder um ein Nicht-Root-Volume handelt, das der Instance zugeordnet ist, verschieden.

Root-Volume

Wenn Sie eine Instance starten, ist das `DeleteOnTermination` Attribut für das Root-Volume einer Instance standardmäßig auf gesetzt`true`. Daher wird das Root-Volume einer Instance standardgemäß gelöscht, wenn die Instance beendet wird.

Nicht-Root-Volume

Wenn Sie einer Instance ein EBS-Volume hinzufügen, das kein Root-Volume ist, ist `DeleteOnTermination` das zugehörige Attribut standardmäßig auf gesetzt. `false` Standardgemäß werden deshalb diese Volumes beibehalten.

> **Note**
>
> Nach dem Beenden einer Instance können Sie einen Snapshot des beibehaltenen Volume erstellen oder es an eine andere Instance anhängen. Sie müssen ein Volume löschen, damit keine weiteren Gebühren anfallen.

Das Attribut `DeleteOnTermination` kann von dem Ersteller einer AMI sowie von der Person, die eine Instance startet, festgelegt werden. Wenn das Attribut vom Ersteller einer AMI oder von der Person geändert wird, die eine Instance startet, überschreibt die neue Einstellung die ursprüngliche AMI-Standardeinstellung. Wir empfehlen, die Standardeinstellung für das Attribut `DeleteOnTermination` zu überprüfen, nachdem Sie eine Instance mit einer AMI gestartet haben.

Um zu überprüfen, ob ein Amazon-EBS-Volume beim Beenden der Instance gelöscht wird, zeigen Sie die Details für das Volume im Detailbereich der Instance an. Scrollen Sie im Tab Speicher unter Blockgeräte nach rechts, um die Beim Beenden löschen-Einstellung für das Volume anzuzeigen.

- Bei Ja wird das Volume gelöscht, wenn die Instance beendet wird.
- Bei Nein wird das Volume nicht gelöscht, wenn die Instance beendet wird. Für alle Volumes, die beim Beenden der Instance nicht gelöscht werden, fallen weiterhin Gebühren an.

Ändern Sie das Root-Volume so, dass es beim Start erhalten bleibt

Mit der Konsole können Sie beim Starten einer Instance das Attribut `DeleteOnTermination` ändern. Zum Ändern dieses Attributs für eine laufende Instance müssen Sie die Befehlszeile verwenden.

Verwenden Sie eine der folgenden Methoden, um das Root-Volume so zu ändern, dass es beim Start bestehen bleibt.

Console

Ändern des Root-Volumes einer beizubehaltenden Instance beim Start mit einer Konsole

1. Folgen Sie den Anweisungen zum Starten einer Instance, aber starten Sie die Instance erst, nachdem Sie die folgenden Schritte durchgeführt haben, um das Root-Volume in persistent zu ändern.
2. Erweitern Sie unter Speicher (Volumes) die Informationen unter dem Root-Volume.
3. Wählen Sie für Beim Beenden löschen die Option Nein aus
4. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Command line

So ändern Sie das Root-Volume einer Instance so, dass es beim Start bestehen bleibt, indem Sie die Befehlszeile verwenden

Beim Starten einer EBS-backed Instance können Sie einen der folgenden Befehle zum Ändern des beizubehaltenden Root-Gerät-Volumes verwenden. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- run-instances (AWS CLI)
- New-EC2Instance (AWS Tools for Windows PowerShell)

Schließen Sie in den Blockgerät-Zuweisungen für die Volumes, die Sie beibehalten möchten, `--DeleteOnTermination` ein und geben Sie `false` an.

Um beispielsweise ein Volume beizubehalten, fügen Sie Ihrem `run-instances`-Befehl die folgende Option hinzu:

```
--block-device-mappings file://mapping.json
```

Geben Sie für `mapping.json` den Gerätenamen an, z. B. `/dev/sda1` oder `/dev/xvda`, und für `--DeleteOnTermination` geben Sie `false` an.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Ändern Sie das Root-Volume einer laufenden Instance so, dass es dauerhaft ist

Sie können einen der folgenden Befehle zum Ändern des Root-Gerät-Volumes einer beizubehaltenden EBS-backed Instance verwenden. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- modify-instance-attribute (AWS CLI)

- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Verwenden Sie z. B. den folgenden Befehl:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

Geben Sie für `mapping.json` den Gerätenamen an, z. B. `/dev/sda1` oder `/dev/xvda`, und für `--DeleteOnTermination` geben Sie `false` an.

```
[
  {
    "DeviceName": "device_name",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Ausmusterung einer Instance

Es ist geplant, dass eine Instanz außer Betrieb genommen wird, wenn ein AWS irreparabler Ausfall der zugrunde liegenden Hardware, die die Instanz hostet, festgestellt wird. Das Root-Gerät der Instanz bestimmt das Verhalten beim Außerbetriebnehmen der Instanz:

- Wenn das Root-Gerät Ihrer Instance ein Amazon EBS-Volume ist, wird die Instance angehalten und Sie können sie jederzeit neu starten. Durch das Starten einer gestoppten Instance wird diese auf eine neue Hardware migriert.
- Wenn es sich bei Ihrem Instance-Root-Gerät um ein Instance-Speicher-Volume handelt, wird die Instance beendet und kann nicht erneut verwendet werden.

Weitere Informationen zu den Instance-Ereignistypen finden Sie unter Geplante Ereignisse für Ihre Instances.

Inhalt

- Zu ergreifende Maßnahmen für vom Instance-Speicher gestützte Instances, die ausgemustert werden sollen

Ermitteln von Instances, die zur Ausmusterung vorgesehen sind

Wenn Ihre Instance ausgemustert werden soll, erhalten Sie vor dem Ereignis eine E-Mail mit der Instance-ID und dem Ausmusterungsdatum. Sie können auch über die Amazon EC2-Konsole oder die Befehlszeile prüfen, ob Instances, die zur Ausmusterung vorgesehen sind, vorhanden sind.

> **Important**
>
> Wenn eine Instance zur Ausmusterung vorgesehen ist, empfiehlt sich, so schnell wie möglich zu handeln, da die Instance möglicherweise nicht erreichbar ist. (Die E-Mail-Benachrichtigung, die Sie erhalten, lautet wie folgt: "Due to this degradation your instance could already be unreachable." ("Aufgrund dieser Degradierung könnte Ihre Instance bereits unerreichbar sein."). Weitere Informationen über die empfohlenen Maßnahmen, die Sie ergreifen sollten, finden Sie unter Check if your instance is reachable.

Möglichkeiten zum Ermitteln von Instances, die zur Ausmusterung vorgesehen sind

- E-Mail-Benachrichtigung
- Konsolen-Identifikation

E-Mail-Benachrichtigung

Wenn Ihre Instance ausgemustert werden soll, erhalten Sie vor dem Ereignis eine E-Mail mit der Instance-ID und dem Ausmusterungsdatum.

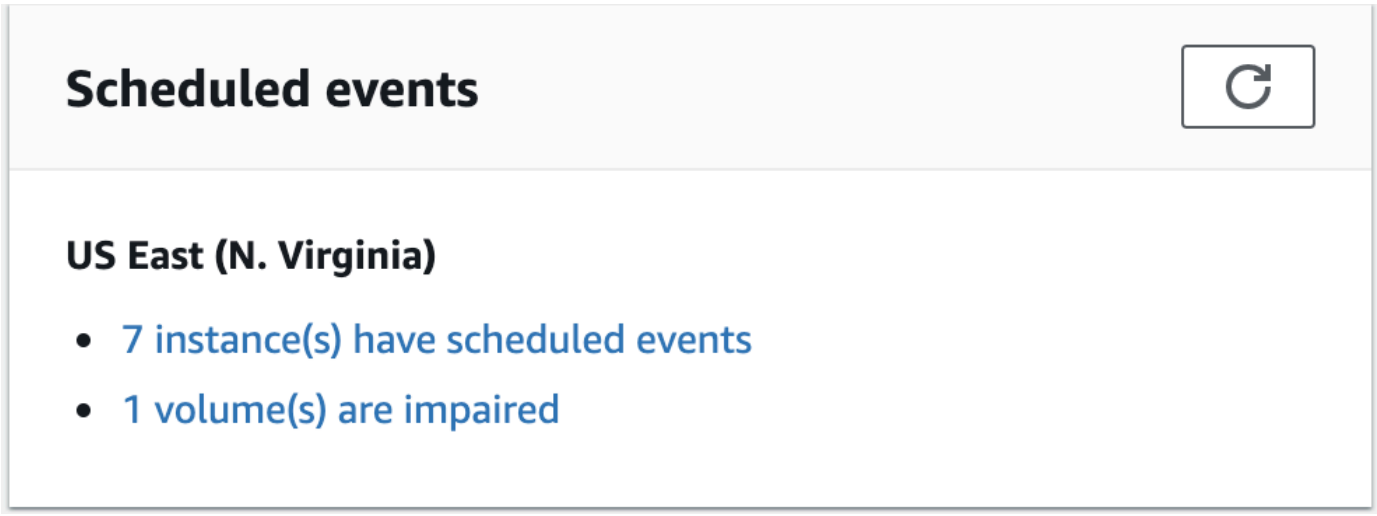
Die E-Mail wird an den primären Kontoinhaber und den Betriebskontakt gesendet. Weitere Informationen finden Sie unter Hinzufügen, Ändern oder Entfernen alternativer Kontakte im AWS Billing -Benutzerhandbuch.

Konsolen-Identifikation

Wenn Sie ein E-Mail-Konto verwenden, das Sie nicht regelmäßig auf Benachrichtigungen zu Instance-Ausmusterungen überprüfen, dann können Sie mit der Amazon EC2-Konsole oder der Befehlszeile ermitteln, ob für eine Ihrer Instances eine Ausmusterung geplant ist.

So ermitteln Sie Instances, die ausgemustert werden sollen, mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich EC2 Dashboard (EC2-Dashboard) aus. Unter Geplante Ereignisse werden die Ereignisse angezeigt, die Ihren Amazon EC2-Instances und -Volumes zugeordnet sind, sortiert nach Region.



3. Wenn eine Ihrer Instances mit einem geplanten Ereignis aufgeführt wird, klicken Sie auf den Link unter dem Namen der Region, um die Seite Events (Ereignisse) aufzurufen.
4. Auf der Seite Ereignisse werden alle Ressourcen aufgeführt, denen Ereignisse zugeordnet sind. Sie können die Instances, die ausgemustert werden sollen, anzeigen, indem Sie in der ersten Filterliste Instance resources (Instance-Ressourcen) und in der zweiten Filterliste Instance stop or retirement (Stoppen oder Ausmustern einer Instance) auswählen.
5. Wenn in den Filterergebnissen eine Instance angezeigt wird, die ausgemustert werden soll, wählen Sie sie aus und notieren Sie sich das Datum und die Uhrzeit, die im Feld Start time (Startzeit) im Detailbereich angezeigt wird. Das ist das Datum für die Ausmusterung Ihrer Instance.

So ermitteln Sie Instances, die ausgemustert werden sollen, mit der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-instance-status (AWS CLI)
- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)

Durchzuführende Maßnahmen für EBS-gestützte Instances, die ausgemustert werden sollen

Um die Daten in der zurückgezogenen Instance beizubehalten, können Sie eine der folgenden Aktionen ausführen. Sie sollten diese Aktion unbedingt vor dem Datum für die Ausmusterung Ihrer Instance ausführen, um unerwartete Ausfallzeiten und Datenverlust zu vermeiden.

Wenn Sie sich bei Linux-Instances nicht sicher sind, ob Ihre Instance von EBS oder einem Instance-Store unterstützt wird, finden Sie weitere Informationen unterErmitteln Sie den Root-Gerätetyp Ihrer Linux-Instance.

Überprüfen, ob Ihre Instance erreichbar ist

Wenn Sie benachrichtigt werden, dass Ihre Instance ausgemustert werden soll, empfiehlt es sich, so schnell wie möglich die folgenden Maßnahmen zu ergreifen:

- Überprüfen Sie, ob Ihre Instance erreichbar ist, indem Sie eine Verbindung zu Ihrer Instance herstellen oder an diese einen Ping senden.
- Wenn Ihre Instance erreichbar ist, sollten Sie planen, Ihre Instance zu einem geeigneten Zeitpunkt vor dem geplanten Ausmusterungsdatum zu stoppen/zu starten, wenn die Auswirkung minimal ist. Weitere Informationen zum Stoppen und Starten Ihrer Instance und darüber, was zu erwarten ist, wenn die Instance gestoppt wird (z. B. die Auswirkungen auf öffentliche, private und Elastic IP-Adressen, die Ihrer Instance zugeordnet sind) finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances. Beachten Sie, dass Daten auf Instance-Speicher-Volumes verloren gehen, wenn Sie die Instance stoppen und starten.
- Wenn Ihre Instance nicht erreichbar ist, sollten Sie sofort Maßnahmen ergreifen und einen Stop/Start durchführen, um Ihre Instance wiederherzustellen.
- Wenn Sie Ihre Instance beenden möchten, planen Sie dies auch so schnell wie möglich, damit keine weiteren Gebühren für die Instance anfallen.

Erstellen eines Backup Ihrer Instance

Erstellen Sie aus Ihrer Instance ein EBS-unterstütztes AMI, damit Sie ein Backup haben. Um die Datenintegrität zu gewährleisten, beenden Sie die Instance, bevor Sie das AMI erstellen. Sie können bis zum Datum für die geplante Ausmusterung warten, an dem die Instance gestoppt wird oder die Instance vorher selbst stoppen. Sie können die Instance jederzeit neu starten. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

Starten einer Ersatz-Instance

Nachdem Sie ein AMI von Ihrer Instance erstellt haben, können Sie das AMI verwenden, um eine Ersatz-Instance zu starten. Wählen Sie in der Amazon EC2-Konsole Ihr neues AMI aus und wählen Sie dann Aktionen, Start. Folgen Sie dem Assistenten, um Ihre Instance zu starten. Weitere Informationen zu den einzelnen Schritten des Assistenten finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Zu ergreifende Maßnahmen für vom Instance-Speicher gestützte Instances, die ausgemustert werden sollen

Um die Daten in der zurückgezogenen Instance beizubehalten, können Sie eine der folgenden Aktionen ausführen. Sie sollten diese Aktion unbedingt vor dem Datum für die Ausmusterung Ihrer Instance ausführen, um unerwartete Ausfallzeiten und Datenverlust zu vermeiden.

> **Warning**
>
> Wenn die Frist für die Ausmusterung Ihrer Instance Store-Backed Instance abgelaufen ist, wird diese beendet und Sie können sie bzw. die darin gespeicherten Daten nicht mehr wiederherstellen. Unabhängig von dem Root-Gerätetyp Ihrer Instance gehen die Daten auf Instance-Speicher-Volumes immer verloren, wenn die Instance ausgemustert wird, auch wenn die Volumes einer EBS-Backed Instance angefügt sind.

Überprüfen Sie, ob Ihre Instance erreichbar ist

Wenn Sie benachrichtigt werden, dass Ihre Instance ausgemustert werden soll, empfiehlt es sich, so schnell wie möglich die folgenden Maßnahmen zu ergreifen:

- Überprüfen Sie, ob Ihre Instance erreichbar ist, indem Sie eine Verbindung zu Ihrer Instance herstellen oder an diese einen Ping senden.
- Wenn Ihre Instance nicht erreichbar ist, kann wahrscheinlich nur sehr wenig getan werden, um Ihre Instance wiederherzustellen. Weitere Informationen finden Sie unterProblembehandlung bei unerreichbaren Instances. AWS beendet Ihre Instance am geplanten Auslaufdatum, sodass Sie bei einer Instance, die nicht erreichbar ist, die Instance sofort selbst beenden können.

Starten einer Ersatz-Instance

Erstellen Sie mithilfe der AMI-Tools, wie unter Erstellen einer Instance-Speicher-Backed Linux-AMI beschrieben, ein vom Instance-Speicher gestütztes AMI von Ihrer Instance. Wählen Sie in der Amazon EC2-Konsole Ihr neues AMI aus und wählen Sie dann Aktionen, Start. Folgen Sie dem Assistenten, um Ihre Instance zu starten. Weitere Informationen zu den einzelnen Schritten des Assistenten finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Konvertieren der Instance in eine EBS-gestützte Instance

Übertragen Sie Ihre Daten auf ein EBS-Volume, machen Sie einen Snapshot des Volumes und erstellen Sie dann ein AMI von dem Snapshot. Sie können eine Ersatz-Instance aus Ihrem neuen AMI starten. Weitere Informationen finden Sie unter Konvertieren Ihres Instance-Speicher-Backed AMI in ein Amazon EBS-gestütztes AMI.

Resilienz der Instanz

> **Important**
>
> Die folgenden Informationen beziehen sich auf die Konfiguration wiederherstellungsbezogener Funktionen auf fehlerfreien Instances. Wenn Sie derzeit Schwierigkeiten haben, auf Ihre Instance zuzugreifen, finden Sie weitere Informationen unter Problembehandlung bei EC2-Instances.

Falls festgestellt wird, dass AWS eine Instance aufgrund eines zugrunde liegenden Hardwareproblems nicht verfügbar ist, können Sie zwei Mechanismen konfigurieren, z. B. die Instance-Resilienz, mit der die Verfügbarkeit wiederhergestellt werden kann: vereinfachte automatische Wiederherstellung und CloudWatchaktionsbasierte Wiederherstellung von Amazon. Dieser Vorgang wird als Instanzwiederherstellung bezeichnet.

Mindestens ein Mechanismus muss im Voraus mit unterstützten Ressourcen konfiguriert oder aktiviert werden, damit der Instanzwiederherstellungsprozess stattfinden kann. Standardmäßig ist die vereinfachte automatische Wiederherstellung für unterstützte Instances aktiviert, wenn sie gestartet werden.

Themen

- Überblick über die Instanzwiederherstellung
- Alternativen zur Wiederherstellung von Instances
- Konfigurieren Sie die aktionsbasierte Wiederherstellung CloudWatch

- Konfigurieren Sie die vereinfachte automatische Wiederherstellung

Überblick über die Instanzwiederherstellung

Im Folgenden finden Sie Beispiele für zugrundeliegende Hardwareprobleme, die eine Instanzwiederherstellung erforderlich machen könnten:

- Verlust der Netzwerkverbindung
- Systemstromausfall
- Softwareprobleme auf dem physischen Host
- Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen

Eine wiederhergestellte Instanz ist identisch mit der ursprünglichen Instanz, einschließlich ihrer:

- Instance-ID
- Öffentliche, private und elastische IP-Adressen
- Instance-Metadaten
- Platzierungsgruppe
- Angehängte EBS-Volumes
- Availability Zone

Eine erfolgreiche Instance-Wiederherstellung wird der Instance als ungeplanter Neustart angezeigt. Mit anderen Worten, im flüchtigen Speicher gespeicherte Inhalte gehen verloren, Instance-Speicherdaten werden gelöscht und die Betriebszeit des Betriebssystems beginnt wieder bei Null.

Zum Schutz vor Datenverlust empfehlen wir, regelmäßig Backups wertvoller Daten zu erstellen. Weitere Informationen zu den bewährten Methoden für Sicherung und Wiederherstellung für Amazon EC2-Instances finden Sie unter Bewährte Methoden für Amazon EC2.

Alternativen zur Wiederherstellung von Instances

Die folgenden Alternativen zur Instanzwiederherstellung können in Betracht gezogen werden, wenn sie dem Anwendungsfall Ihrer Instances entsprechen.

Auto-Scaling-Gruppen

Sie können Auto Scaling Scaling-Gruppen verwenden, um eine Sammlung von Instances aus Gründen der Skalierung und Verfügbarkeit zu gruppieren. Falls eine Instance innerhalb einer Auto Scaling Scaling-Gruppe nicht verfügbar ist, wird die Instance automatisch durch die Auto Scaling Scaling-Gruppe ersetzt (nicht wiederhergestellt). Weitere Informationen finden Sie unter Was ist Amazon EC2 Auto Scaling? im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Amazon EBS Multi-Attach

Sie können Amazon EBS Multi-Attach für Ihre Instances so konfigurieren, dass mehrere Instances mit demselben EBS-Volume verbunden werden können. In Kombination mit geeigneter Software ermöglicht dies die Aktivierung von Clustering mit hoher Verfügbarkeit. Eine Beispielkonfiguration mit Linux-Instances finden Sie unter Clustered Storage Simplified: GFS2 on Amazon EBS Multi-Attach enabled volumes im Storage Blog. AWS

Konfigurieren Sie die aktionsbasierte Wiederherstellung CloudWatch

Important

- Die folgenden Informationen beziehen sich auf die Konfiguration wiederherstellungsbezogener Funktionen auf fehlerfreien Instanzen. Wenn Sie derzeit Schwierigkeiten haben, auf Ihre Instance zuzugreifen, finden Sie weitere Informationen unter Problembehandlung bei EC2-Instances.
- Damit Ihr Workload nach einer erfolgreichen Instance-Wiederherstellung ordnungsgemäß funktioniert, muss Ihre Instance booten und Datenverkehr akzeptieren, ohne dass manuelles Eingreifen erforderlich ist.

Sie können die CloudWatch aktionsbasierte Wiederherstellung von Amazon so konfigurieren, dass Wiederherstellungsaktionen zu CloudWatch Amazon-Alarmen hinzugefügt werden. CloudWatch Die aktionsbasierte Wiederherstellung funktioniert mit der `StatusCheckFailed_System` Metrik. CloudWatch Die aktionsbasierte to-the-minute Wiederherstellung bietet detaillierte Reaktionszeiten und Amazon Simple Notification Service (Amazon SNS) Benachrichtigungen über Wiederherstellungsaktionen und -ergebnisse. Diese Konfigurationsoptionen ermöglichen im Vergleich zur vereinfachten automatischen Wiederherstellung schnellere Wiederherstellungsversuche mit detaillierterer Kontrolle über die Reaktion auf Fehlschläge bei der Systemstatusprüfung. Weitere

Informationen zu den verfügbaren CloudWatch Optionen finden Sie unter Statuschecks für Ihre Instances.

Die CloudWatch aktionsbasierte Wiederherstellung von Amazon funktioniert nicht bei Serviceereignissen in der AWS Health Dashboard. Weitere Informationen finden Sie unter the section called “Behebung von Fehlern bei der CloudWatch aktionsbasierten Wiederherstellung”.

Themen

- Anforderungen und Einschränkungen für die CloudWatch aktionsbasierte Wiederherstellung
- Konfigurieren Sie CloudWatch die aktionsbasierte Wiederherstellung
- Behebung von Fehlern bei der CloudWatch aktionsbasierten Wiederherstellung

Anforderungen und Einschränkungen für die CloudWatch aktionsbasierte Wiederherstellung

CloudWatch Bei einer aktionsbasierten Wiederherstellung kann versucht werden, eine Instanz wiederherzustellen, wenn sie:

- Ist im `running` Bundesstaat. Weitere Informationen finden Sie unter the section called “Instance-Lebenszyklus”.
- Verwendet `default` (On-Demand) oder `dedicated` Instance-Tenancy. Weitere Informationen finden Sie unter the section called “Instance-Kaufoptionen”.
- Gehört zu einem Instance-Typ, für den Amazon EC2 Kapazität zur Verfügung hat. In einigen Situationen, wie z. B. bei erheblichen Ausfällen, ist nicht genügend Kapazität verfügbar, und einige Wiederherstellungsversuche können fehlschlagen.
- Verwendet keine `dedicated` Instance-Tenancy. Für Amazon EC2 Dedicated Hosts können Sie Dedicated Host Auto Recovery verwenden, um fehlerhafte Instances automatisch wiederherzustellen.
- Verwendet keinen Elastic Fabric-Adapter.
- Ist kein Mitglied einer Auto Scaling Scaling-Gruppe.
- Durchläuft derzeit kein geplantes Wartungsereignis.
- Verwendet einen der folgenden Instanztypen:
  - Universell: A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Für Berechnungen optimiert: C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7n | C7i | C7i-Flex

  - Speicheroptimiert: R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | u-3tb1 | u-6tb1 | u-9 tb1 | u-12 tb1 | u-18 tb1 | u-24 tb1 | u7i-12 tb | u7in-16 tb | u7in-16 tb | u7 7-in-24 TB | u7-in-32 TB | X1 | X1e | X2iZEN
  - Beschleunigtes Computing: G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
  - Hochleistungsrechnen: HPC6a | HPC7a | HPC7G
  - Metal-Instances: Jeder der oben genannten Typen mit der Metal-Instance-Größe.
- Hat Instance-Speicher-Volumes und verwendet einen der folgenden Instance-Typen: M3 | C3 | R3 | X1 | X1E | x2IDN | X2iEDN

> **Warning**
>
> - Daten auf Instance-Speicher-Volumes gehen verloren, wenn die Instance gestoppt wird. Weitere Informationen zum Stoppen einer Instance finden Sie unterthe section called “Instance stoppen und starten”.
> - Falls die Überprüfung des Systemstatus fehlschlägt, gehen die Daten, die dem Instance-Speicher und dem Blockgerät zugeordnet sind, möglicherweise verloren. Für diese Instance-Typen können Sie die Verwendung the section called “Aktivieren des Beendigungsschutzes” von in Betracht ziehen.
>
> Wir empfehlen Ihnen, regelmäßig Backups wertvoller Daten zu erstellen. Informationen zu den bewährten Methoden für Sicherung und Wiederherstellung für Amazon EC2 finden Sie unter Bewährte Methoden für Amazon EC2.

Sie können auch das AWS Management Console oder das verwenden AWS CLI , um die Instance-Typen anzuzeigen, die eine CloudWatch aktionsbasierte Wiederherstellung unterstützen.

Console

Um die Instance-Typen anzuzeigen, die Amazon CloudWatch Action Based Recovery unterstützen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Instance Types (Instance-Typen) aus.

3. Geben Sie in der Filterleiste Auto Recovery support: true (Unterstützung für automatische Wiederherstellung: wahr) ein. Alternativ können Sie den Filter auswählen, wenn Sie die Zeichen eingeben und der Filtername erscheint.

   In der Tabelle mit den Instance-Typen werden alle Instance-Typen angezeigt, die die CloudWatch aktionsbasierte Wiederherstellung von Amazon unterstützen.

AWS CLI

Um die Instance-Typen anzuzeigen, die Amazon CloudWatch Action Based Recovery unterstützen

Verwenden Sie den Befehl describe-instance-types.

```
aws ec2 describe-instance-types --filters Name=auto-recovery-supported,Values=true
--query "InstanceTypes[*].[InstanceType]" --output text | sort
```

Konfigurieren Sie CloudWatch die aktionsbasierte Wiederherstellung

CloudWatch Die aktionsbasierte Wiederherstellung funktioniert mit der `StatusCheckFailed_System` Metrik. CloudWatch Die aktionsbasierte Wiederherstellung wird über die CloudWatch Konsole konfiguriert. Informationen zur Einrichtung einer CloudWatch aktionsbasierten Wiederherstellung finden Sie unter Hinzufügen von Wiederherstellungsaktionen zu CloudWatch Alarmen im CloudWatch Amazon-Benutzerhandbuch.

Behebung von Fehlern bei der CloudWatch aktionsbasierten Wiederherstellung

Die folgenden Probleme können dazu führen, dass die Wiederherstellung Ihrer Instanz mit CloudWatch aktionsbasierter Wiederherstellung fehlschlägt:

- CloudWatch Die aktionsbasierte Wiederherstellung funktioniert nicht bei Serviceereignissen in der AWS Health Dashboard. Sie erhalten möglicherweise keine Benachrichtigungen zu Wiederherstellungsfehlern für solche Ereignisse. Die neuesten Informationen zur Serviceverfügbarkeit finden Sie auf der Seite zum Dienststatus.
- Es steht vorübergehend keine ausreichende Kapazität der Ersatz-Hardware zur Verfügung.
- Die Instanz hat die maximale tägliche Zulage für Wiederherstellungsversuche erreicht. Ihre Instance kann anschließend stillgelegt werden, wenn die automatische Wiederherstellung

fehlschlägt und als Ursache für das Nichtbestehen der ursprünglichen Systemstatusprüfung ein Leistungsabfall der Hardware ermittelt wurde.

Wenn die Systemstatusprüfung der Instance trotz mehrerer Wiederherstellungsversuche weiterhin fehlschlägt, finden Sie weitere Hinweise unter Problembehandlung bei Instanzen mit fehlgeschlagenen Statusprüfungen.

Konfigurieren Sie die vereinfachte automatische Wiederherstellung

> **Important**
>
> - Die folgenden Informationen beziehen sich auf die Konfiguration wiederherstellungsbezogener Funktionen auf fehlerfreien Instanzen. Wenn Sie derzeit Schwierigkeiten haben, auf Ihre Instance zuzugreifen, finden Sie weitere Informationen unter Problembehandlung bei EC2-Instances.
> - Damit Ihr Workload nach einer erfolgreichen Instance-Wiederherstellung ordnungsgemäß funktioniert, muss Ihre Instance booten und Datenverkehr akzeptieren, ohne dass manuelles Eingreifen erforderlich ist.

Standardmäßig überwacht die vereinfachte automatische Wiederherstellung alle unterstützten laufenden Instances. Falls bei der Überprüfung des Systemstatus ein Fehler festgestellt wird, versucht die vereinfachte automatische Wiederherstellung, die Instanz wieder in einen fehlerfreien Zustand zu versetzen. Die vereinfachte automatische Wiederherstellung funktioniert nicht bei Serviceereignissen in der AWS Health Dashboard. Weitere Informationen finden Sie unter the section called “Behebung von Fehlern bei der vereinfachten automatischen Wiederherstellung”.

Wenn ein vereinfachtes automatisches Wiederherstellungsereignis eintritt, erhalten Sie ein AWS Health Dashboard Ereignis. Informationen zum Konfigurieren von Benachrichtigungen für diese Ereignisse finden Sie unter Erste Schritte mit AWS-Benutzerbenachrichtigungen im AWS-Benutzerbenachrichtigungen Benutzerhandbuch. Mithilfe der EventBridge Amazon-Regeln können Sie mithilfe der folgenden Ereigniscodes auch vereinfachte automatische Wiederherstellungsereignisse überwachen:

- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_SUCCESS` — erfolgreiche Ereignisse
- `AWS_EC2_SIMPLIFIED_AUTO_RECOVERY_FAILURE` — fehlgeschlagene Ereignisse

Weitere Informationen finden Sie in den EventBridge Amazon-Regeln.

Themen

- Anforderungen und Einschränkungen für die vereinfachte automatische Wiederherstellung
- Konfigurieren Sie die vereinfachte automatische Wiederherstellung
- Behebung von Fehlern bei der vereinfachten automatischen Wiederherstellung

Anforderungen und Einschränkungen für die vereinfachte automatische Wiederherstellung

Die vereinfachte automatische Wiederherstellung versucht, eine Instanz wiederherzustellen, wenn sie:

- Ist im `running` Bundesstaat. Weitere Informationen finden Sie unter the section called “Instance-Lebenszyklus”.
- Verwendet `default` (On-Demand) oder `dedicated` Instance-Tenancy. Weitere Informationen finden Sie unter the section called “Instance-Kaufoptionen”.
- Gehört zu einem Instance-Typ, für den Amazon EC2 Kapazität zur Verfügung hat. In einigen Situationen, wie z. B. bei erheblichen Ausfällen, ist nicht genügend Kapazität verfügbar, und einige Wiederherstellungsversuche können fehlschlagen.
- Verwendet keine `dedicated` Instance-Tenancy. Für Amazon EC2 Dedicated Hosts können Sie Dedicated Host Auto Recovery verwenden, um fehlerhafte Instances automatisch wiederherzustellen.
- Verwendet keinen Elastic Fabric-Adapter.
- Ist keine `metal` Instanzgröße.
- Ist kein Mitglied einer Auto Scaling Scaling-Gruppe.
- Durchläuft derzeit kein geplantes Wartungsereignis.
- Hat keine Instance-Speicher-Volumes.
- Verwendet einen der folgenden Instance-Typen:
  - Universell: A1 | M3 | M4 | M5 | M5a | M5n | M5zn | M6a | M6g | M6i | M6in | M7a | M7g | M7i | M7i-flex | T1 | T2 | T3 | T3a | T4g
  - Für Berechnungen optimiert: C3 | C4 | C5 | C5a | C5n | C6a | C6g | C6gn | C6i | C6in | C7a | C7g | C7gn | C7n | C7i | C7i-Flex

- Speicheroptimiert: R3 | R4 | R5 | R5a | R5b | R5n | R6a | R6g | R6i | R6in | R7a | R7g | R7i | R7iz | u-3tb1 | u-6tb1 | u-9 tb1 | u-12 tb1 | u-18 tb1 | u-24 tb1 | u7i-12 tb | u7in-16 tb | u7in-16 tb | u7 7-in-24 TB | u7-in-32 TB | X1 | X1e | X2iZEN
- Beschleunigtes Computing: G3 | G3s | G5g | Inf1 | P2 | P3 | VT1
- Hochleistungsrechnen: HPC6a | HPC7a | HPC7G

⚠ Warning

- Daten auf Instance-Speicher-Volumes gehen verloren, wenn die Instance gestoppt wird. Weitere Informationen zum Stoppen einer Instance finden Sie unterthe section called “Instance stoppen und starten”.
- Falls die Überprüfung des Systemstatus fehlschlägt, gehen die Daten, die dem Instance-Speicher und dem Blockgerät zugeordnet sind, möglicherweise verloren. Für diese Instance-Typen können Sie die Verwendung the section called “Aktivieren des Beendigungsschutzes” von in Betracht ziehen.

Wir empfehlen Ihnen, regelmäßig Backups wertvoller Daten zu erstellen. Informationen zu den bewährten Methoden für Sicherung und Wiederherstellung für Amazon EC2 finden Sie unter Bewährte Methoden für Amazon EC2.

Konfigurieren Sie die vereinfachte automatische Wiederherstellung

Die vereinfachte automatische Wiederherstellung ist standardmäßig aktiviert, wenn Sie eine unterstützte Instanz starten. Sie können das automatische Wiederherstellungsverhalten so einstellen, dass es `disabled` während oder nach dem Start der Instance ausgeführt wird. Die `default` Konfiguration ermöglicht keine vereinfachte automatische Wiederherstellung für einen Instance-Typ, der nicht unterstützt wird.

Console

So deaktivieren Sie die vereinfachte automatische Wiederherstellung beim Starten der Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Launch instance (Instance starten) aus.

3. Wählen Sie im Abschnitt Advanced details (Erweiterte Details) bei Instance auto-recovery (Automatische Wiederherstellung der Instance) Disabled (Deaktiviert) aus.
4. Konfigurieren Sie die verbleibenden Instance-Starteinstellungen nach Bedarf und starten Sie dann die Instance.

So deaktivieren Sie die vereinfachte automatische Wiederherstellung für eine laufende oder angehaltene Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und dann Actions (Aktionen), Instance Settings (Instance-Einstellungen) und Change auto-recovery behavior (Verhalten der automatischen Wiederherstellung ändern).
4. Wählen Sie Off (Aus) und dann Save (Speichern) aus.

Automatisches Wiederherstellungsverhalten für laufende oder gestoppte Instance auf **`default`** festlegen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und dann Actions (Aktionen), Instance Settings (Instance-Einstellungen) und Change auto-recovery behavior (Verhalten der automatischen Wiederherstellung ändern).
4. Wählen Sie Standard (Ein) und dann Speichern.

AWS CLI

So deaktivieren Sie die vereinfachte automatische Wiederherstellung beim Launchen

Verwenden Sie den Befehl run-instances.

```
aws ec2 run-instances \
--image-id ami-1a2b3c4d \
--instance-type t2.micro \
--key-name MyKeyPair \
--maintenance-options AutoRecovery=Disabled \
```

```
  [...]
```

So deaktivieren Sie die vereinfachte automatische Wiederherstellung für eine laufende oder angehaltene Instance

Verwenden Sie den Befehl modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery disabled
```

Automatisches Wiederherstellungsverhalten für laufende oder gestoppte Instance auf **`default`** festlegen

Verwenden Sie den Befehl modify-instance-maintenance-options.

```
aws ec2 modify-instance-maintenance-options \
--instance-id i-0abcdef1234567890 \
--auto-recovery default
```

Behebung von Fehlern bei der vereinfachten automatischen Wiederherstellung

Die folgenden Probleme können dazu führen, dass die Wiederherstellung Ihrer Instance mit vereinfachter automatischer Wiederherstellung fehlschlägt:

- Die vereinfachte automatische Wiederherstellung funktioniert nicht bei Serviceereignissen in der AWS Health Dashboard. Sie erhalten möglicherweise keine Benachrichtigungen zu Wiederherstellungsfehlern für solche Ereignisse. Die neuesten Informationen zur Serviceverfügbarkeit finden Sie auf der Seite zum Dienststatus.
- Es steht vorübergehend keine ausreichende Kapazität der Ersatz-Hardware zur Verfügung.
- Die Instanz hat die maximale tägliche Zulage für Wiederherstellungsversuche erreicht. Ihre Instance kann anschließend stillgelegt werden, wenn die automatische Wiederherstellung fehlschlägt und als Ursache für das Nichtbestehen der ursprünglichen Systemstatusprüfung ein Leistungsabfall der Hardware ermittelt wurde.

Wenn die Systemstatusprüfung der Instance trotz mehrerer Wiederherstellungsversuche weiterhin fehlschlägt, finden Sie weitere Hinweise unter Problembehandlung bei Instanzen mit fehlgeschlagenen Statusprüfungen.

Arbeiten mit Instance-Metadaten

Instance-Metadaten sind Daten über eine Instance, mit denen Sie die ausgeführte Instance konfigurieren und verwalten können. Instance-Metadaten sind in Kategorien unterteilt (z. B. Hostname, Ereignisse und Sicherheitsgruppen).

Sie können Instance-Metadaten auch verwenden, um auf Benutzerdaten zuzugreifen, die Sie beim Start Ihrer Instance angegeben haben. Sie können beispielsweise Parameter für die Konfiguration Ihrer Instance angeben oder ein einfaches Skript einbinden. Sie können auch generische AMIs erstellen und Benutzerdaten verwenden, um die beim Start bereitgestellten Konfigurationsdateien zu ändern. Wenn Sie beispielsweise Webserver für verschiedene kleine Unternehmen betreiben, können sie alle dasselbe generische AMI verwenden und ihren Inhalt aus einem Amazon S3 S3-Bucket abrufen, den Sie beim Start in den Benutzerdaten angeben. Um jederzeit einen neuen Kunden hinzuzufügen, erstellen Sie einen Bucket für den Kunden, fügen Sie dessen Inhalt hinzu und starten Ihr AMI mit dem eindeutigen Bucket-Namen, der Ihrem Code in den Benutzerdaten zur Verfügung steht. Wenn Sie mehrere Instances mit demselben `RunInstances` Aufruf starten, sind die Benutzerdaten für alle Instances in dieser Reservierung verfügbar. Jede Instance, die Teil derselben Reservierung ist, hat eine eindeutige `ami-launch-index` Nummer, sodass Sie Code schreiben können, der steuert, was die Instances tun. Beispielsweise kann sich der erste Host selbst als ursprünglichen Knoten in einem Cluster auswählen. Ein detailliertes Beispiel für einen AMI-Start finden Sie unterLinux-Beispiel: AMI-Startindexwert.

EC2-Instances können außerdem dynamische Daten enthalten, z. B. ein Instance-Identitätsdokument, das beim Start der Instance generiert wird. Weitere Informationen finden Sie unter Kategorien von dynamischen Daten.

> **Important**
>
> Sie können nur innerhalb der Instance selbst auf Instance-Metadaten und Benutzerdaten zugreifen. Die Daten sind nicht durch Authentifizierungs- oder kryptografische Verfahren geschützt. Jeder, der direkten Zugriff auf die Instance hat, und möglicherweise auch jede Software, die auf der Instance läuft, kann deren Metadaten einsehen. Daher sollten Sie sensible Daten wie Passwörter oder langlebige Verschlüsselungscodes nicht als Benutzerdaten speichern.

Inhalt

- Konfigurieren der Instance-Metadaten-Optionen
- Abrufen von Instance-Metadaten
- Arbeiten mit Instance-Benutzerdaten
- Abrufen von dynamischen Daten
- Instance-Metadatenkategorien
- Linux-Beispiel: AMI-Startindexwert
- Instance-Identitätsdokumente
- Instance-Identitätsrollen

IMDSv2 verwenden

Sie können mit einer der folgenden Methoden auf Instance-Metadaten aus einer laufenden Instance zugreifen:

- Instance-Metadatenservice Version 1 (IMDSv1) – Ein Anfrage/Antwort-Verfahren
- Instance-Metadatenservice Version 2 (IMDSv2) – Ein sitzungsorientiertes Verfahren

Standardmäßig können Sie entweder IMDSv1 oder IMDSv2 oder beides verwenden.

Sie können den Instance Metadata Service (IMDS) auf jeder Instance so konfigurieren, dass lokaler Code oder Benutzer IMDSv2 verwenden müssen. Wenn Sie angeben, dass IMDSv2 verwendet werden muss, funktioniert IMDSv1 nicht mehr. Informationen darüber, wie Sie Ihre Instance für die Verwendung von IMDSv2 konfigurieren, finden Sie unter Konfigurieren der Instance-Metadaten-Optionen.

Die `PUT`- oder `GET`-Header sind für IMDSv2 eindeutig. Wenn diese Header in der Anfrage vorhanden sind, ist die Anfrage für IMDSv2 bestimmt. Wenn keine Header vorhanden sind, wird davon ausgegangen, dass die Anfrage für IMDSv1 bestimmt ist.

Einen ausführlichen Überblick über IMDSv2 finden Sie unter Erweitern Sie den EC2-Instance-Metadata-Service, um Abwehr von offenen Firewalls, Reverse-Proxys und SSRF-Schwachstellen mit Verbesserungen an EC2-Instance-Metadata-Service.

Informationen zum Abrufen von Instance-Metadaten finden Sie unter Abrufen von Instance-Metadaten.

Themen

- Funktionsweise von Instance-Metadatenservice Version 2
- Übergang zur Verwendung von Instance-Metadatenservice Version 2
- Verwenden eines unterstützten AWS -SDK

Funktionsweise von Instance-Metadatenservice Version 2

IMDSv2 verwendet sitzungsorientierte Anfragen. Bei sitzungsorientierten Anforderungen erstellen Sie ein Sitzungs-Token, das die Sitzungsdauer definiert, die mindestens eine Sekunde und maximal sechs Stunden betragen kann. Während der angegebenen Dauer können Sie dasselbe Sitzungs-Token für nachfolgende Anfragen verwenden. Nach Ablauf der angegebenen Dauer müssen Sie ein neues Sitzungs-Token erstellen, das Sie für zukünftige Anfragen verwenden können.

> **Note**
>
> In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des Instance Metadata Service (IMDS) verwendet: `169.254.169.254`. Wenn Sie Zeit Instance-Metadaten für EC2-Instances über die IPv6-Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6-Adresse verwenden: `[fd00:ec2::254]`. Die IPv6-Adresse des IMDS ist mit IMDSv2-Befehlen kompatibel. Auf die IPv6-Adresse kann nur auf Instances zugegriffen werden, die auf dem AWS Nitro-System basieren, und in einem IPv6-unterstützten Subnetz (Dual-Stack oder nur IPv6).

In den folgenden Beispielen werden ein Shell-Skript und IMDSv2 verwendet, um die Metadatenelemente der Instanz auf oberster Ebene abzurufen. Jedes Beispiel:

- Erstellt ein Sitzungs-Token mit einer Dauer von sechs Stunden (21 600 Sekunden) unter Verwendung der PUT-Anfrage.
- Speichert den Sitzungs-Token-Header in einer Variablen namens `TOKEN` (Linux-Instanzen) oder `token` (Windows-Instanzen)
- aFordert die Top-Level-Metadatenelemente über das Token an.

Linux-Beispiel

Sie können zwei separate Befehle ausführen oder kombinieren.

Separate Befehle

Generieren Sie zuerst ein Token mit dem folgenden Befehl.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"`
```

Verwenden Sie dann das Token, um mit dem folgenden Befehl Metadatenelemente der obersten Ebene zu generieren.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/
```

Kombinierte Befehle

Sie können das Token speichern und die Befehle kombinieren. Das folgende Beispiel kombiniert die beiden obigen Befehle und speichert den Sitzungs-Token-Header in einer Variablen namens TOKEN.

> **Note**
>
> Wenn beim Erstellen des Tokens anstelle eines gültigen Tokens ein Fehler auftritt, wird in der Variablen eine Fehlermeldung gespeichert, und der Befehl funktioniert nicht.

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-
ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

Nachdem Sie ein Token erstellt haben, können Sie es bis zum Ablauf wiederverwenden. Im folgenden Beispielbefehl, der die ID des AMIs abruft, mit dem die Instance gestartet wurde, wird das im vorherigen Beispiel in `$TOKEN` gespeicherte Token wiederverwendet.

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/ami-id
```

Windows-Beispiel

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -
Uri http://169.254.169.254/latest/meta-data/
```

Nachdem Sie ein Token erstellt haben, können Sie es bis zum Ablauf wiederverwenden. Im folgenden Beispielbefehl, der die ID des AMIs abruft, mit dem die Instance gestartet wurde, wird das im vorherigen Beispiel in `$token` gespeicherte Token wiederverwendet.

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} `
-Method GET -uri http://169.254.169.254/latest/meta-data/ami-id
```

Wenn Sie IMDSv2 zum Anfordern von Instance-Metadaten verwenden, muss die Anforderung Folgendes enthalten:

1. Verwenden Sie eine PUT-Anfrage, um eine Sitzung mit dem Instance-Metadaten-Service zu starten. Die PUT-Anfrage gibt ein Token zurück, das in nachfolgenden GET-Anfragen an den Instance-Metadaten-Service enthalten sein muss. Das Token wird für den Zugriff auf Metadaten mit IMDSv2 benötigt.
2. Nehmen Sie das Token GET in alle Anfragen an den IMDS auf. Wenn die Token-Verwendung auf `required` festgelegt ist, erhalten Anfragen ohne gültiges Token oder mit abgelaufenem Token einen `401 - Unauthorized`-HTTP-Fehlercode.
   - Das Token ist ein Instance-bezogener Schlüssel. Das Token ist in anderen EC2-Instances nicht gültig und wird abgelehnt, wenn Sie versuchen, es außerhalb der Instance zu verwenden, in der es erzeugt wurde.
   - Die PUT-Anfrage muss einen Header enthalten, der die Time To Live (TTL) für das Token in Sekunden bis zu maximal sechs Stunden (21 600 Sekunden) angibt. Das Token stellt eine logische Sitzung dar. Die TTL gibt die Gültigkeitsdauer des Token und damit die Dauer der Sitzung an.
   - Nachdem ein Token abgelaufen ist, müssen Sie eine neue Sitzung mit einem anderen PUT erstellen, um auf die Instance-Metadaten zuzugreifen.
   - Sie können auswählen, ob Sie ein Token wiederverwenden oder bei jeder Anforderung einen neues Token erstellen möchten. Für eine kleine Anzahl von Anfragen kann es einfacher sein, bei jedem Zugriff auf den IMDS ein Token zu generieren und sofort zu verwenden. Aus Effizienzgründen können Sie jedoch eine längere Dauer für das Token festlegen und es wiederverwenden, anstatt jedes Mal eine PUT-Anfrage stellen zu müssen, wenn Sie Instance-Metadaten anfordern müssen. Es gibt keine praktische Begrenzung der Anzahl der gleichzeitigen Tokens, die jeweils eine eigene Sitzung darstellen. IMDSv2 unterliegt jedoch

weiterhin den normalen IMDS-Verbindungs- und Drosselungsbeschränkungen. Weitere Informationen finden Sie unter Drosselung abfragen.

In IMDSv2 Instance-Metadatenanfragen sind HTTP `GET`- und `HEAD`-Methoden zulässig. `PUT`-Anfragen werden abgelehnt, wenn sie einen X-Forwarded-For-Header enthalten.

Standardmäßig hat die Antwort auf `PUT`-Anfragen auf IP-Protokollebene ein Antworthop-Limit (Time To Live) von 1. Wenn Sie ein größeres Hop-Limit benötigen, können Sie es mit dem Befehl AWS CLI modify-instance-metadata-options anpassen. Beispielsweise benötigen Sie möglicherweise eine größeres Hop-Limit für die Abwärtskompatibilität mit Container-Services, die auf der Instance ausgeführt werden. Weitere Informationen finden Sie unter Modifizieren von Instance-Metadatenoptionen für vorhandene Instances.

Übergang zur Verwendung von Instance-Metadatenservice Version 2

Wenn Sie die zu IMDSv2 migrieren, empfehlen wir Ihnen, die folgenden Tools und Wege zu verwenden.

Themen

- Tools zur Unterstützung beim Wechsel zu IMDSv2
- Empfohlener Weg zur Erzwingung von IMDSv2

Tools zur Unterstützung beim Wechsel zu IMDSv2

Wenn Ihre Software IMDSv1 verwendet, verwenden Sie die folgenden Tools, um Ihre Software für die Verwendung von IMDSv2 neu zu konfigurieren.

AWS Software

Die neuesten Versionen der AWS SDKs AWS CLI und unterstützen IMDSv2. Stellen Sie zur Verwendung von IMDSv2 sicher, dass Ihre EC2-Instances über die neuesten Versionen der CLI und der SDKs verfügen. Informationen zum Aktualisieren der CLI finden Sie unter Installieren, Aktualisieren und Deinstallieren von AWS CLI im AWS Command Line Interface - Benutzerhandbuch.

Alle Amazon Linux 2- und Amazon Linux 2023-Softwarepakete unterstützen IMDSv2. In Amazon Linux 2023 ist IMDSv1 standardmäßig deaktiviert.

Die minimalen AWS SDK-Versionen, die IMDSv2 unterstützen, finden Sie unter. Verwenden eines unterstützten AWS -SDK

IMDS-Paket-Analysator

Der IMDS-Paket-Analysator ist ein Open-Source-Tool, das IMDSv1-Aufrufe aus der Startphase Ihrer Instance identifiziert und protokolliert. Dies kann dazu beitragen, die Software zu identifizieren, die IMDSv1-Aufrufe auf EC2-Instances ausführt, sodass Sie genau bestimmen können, was Sie aktualisieren müssen, damit Ihre Instances IMDSv2 verwenden können. Sie können IMDS-Paket-Analysator von der Befehlszeile aus ausführen oder als Service installieren. Weitere Informationen finden Sie unter IMDS Packet Analyzer unter. GitHub

CloudWatch

IMDSv2 verwendet Token-gestützte Sitzungen, IMDSv1 hingegen nicht. Die `MetadataNoToken` CloudWatch Metrik verfolgt die Anzahl der Aufrufe des Instance Metadata Service (IMDS), die IMDSv1 verwenden. Indem Sie diese Metrik bis zum Wert Null nachverfolgen, können Sie feststellen, ob und wann Ihre Software auf IMDSv2 upgegradet wurde.

Nachdem Sie IMDSv1 deaktiviert haben, können Sie anhand der `MetadataNoTokenRejected` CloudWatch Metrik verfolgen, wie oft ein IMDSv1-Aufruf versucht und abgelehnt wurde. Indem Sie diese Metrik verfolgen, können Sie feststellen, ob Ihre Software aktualisiert werden muss, um IMDSv2 verwenden zu können.

Weitere Informationen finden Sie unter Instance-Metriken.

Aktualisierungen von EC2-APIs und -CLIs

Für neue Instances können Sie die RunInstancesAPI verwenden, um neue Instances zu starten, für die IMDSv2 erforderlich ist. Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances.

Für bestehende Instances können Sie die ModifyInstanceMetadataOptionsAPI verwenden, um die Verwendung von IMDSv2 vorzuschreiben. Weitere Informationen finden Sie unter Modifizieren von Instance-Metadatenoptionen für vorhandene Instances.

Um die Verwendung von IMDSv2 auf allen neuen Instances zu verlangen, die von Auto Scaling-Gruppen gestartet werden, können Ihre Auto Scaling-Gruppen entweder eine Startvorlage oder eine Startkonfiguration verwenden. Wenn Sie eine Startvorlage erstellen oder eine Startkonfiguration erstellen, müssen Sie die `MetadataOptions`-Parameter so konfigurieren, dass die Verwendung von IMDSv2 erforderlich ist. Die Auto-Scaling-Gruppe startet neue Instances mit der neuen Startvorlage oder Startkonfiguration, bestehende Instances sind davon

jedoch nicht betroffen. Für bestehende Instances in einer Auto Scaling Scaling-Gruppe können Sie die ModifyInstanceMetadataOptionsAPI verwenden, um die Verwendung von IMDSv2 für die vorhandenen Instances vorzuschreiben, oder Sie können die Instances beenden und die Auto Scaling Scaling-Gruppe startet neue Ersatz-Instances mit den Einstellungen der Instance-Metadaten-Optionen, die in der neuen Startvorlage oder Startkonfiguration definiert sind.

Verwenden eines AMI, das IMDSv2 standardmäßig konfiguriert

Beim Starten einer Instance können Sie sie automatisch so konfigurieren, dass sie standardmäßig IMDSv2 verwendet (der Parameter `HttpTokens` ist auf `required` eingestellt). Dazu starten Sie sie mit einem AMI, in dessen Konfiguration der Parameter `ImdsSupport` auf `v2.0` eingestellt ist. Sie können den `ImdsSupport`-Parameter auf `v2.0` festlegen, wenn Sie das AMI mit dem CLI-Befehl register-image registrieren, oder Sie können ein vorhandenes AMI ändern, indem Sie den CLI-Befehl modify-image-attribute verwenden. Weitere Informationen finden Sie unter Konfigurieren des AMI.

IAM-Richtlinien und SCPs

Sie können eine IAM-Richtlinie oder eine AWS Organizations Service Control Policy (SCP) verwenden, um Benutzer wie folgt zu kontrollieren:

- Eine Instance kann nicht über die RunInstancesAPI gestartet werden, es sei denn, die Instance ist für die Verwendung von IMDSv2 konfiguriert.
- Eine laufende Instanz kann nicht mithilfe der ModifyInstanceMetadataOptionsAPI geändert werden, um IMDSv1 erneut zu aktivieren.

Die IAM-Richtlinie oder die SCP muss die folgenden IAM-Bedingungsschlüssel enthalten:

- `ec2:MetadataHttpEndpoint`
- `ec2:MetadataHttpPutResponseHopLimit`
- `ec2:MetadataHttpTokens`

Wenn ein Parameter im API- oder CLI-Aufruf nicht dem Status entspricht, der in der Richtlinie mit dem Bedingungsschlüssel angegeben ist, schlägt der API- oder CLI-Aufruf mit der Antwort `UnauthorizedOperation` fehl.

Darüber hinaus können Sie eine zusätzliche Schutzebene auswählen, um die Änderung von IMDSv1 auf IMDSv2 zu erzwingen. Auf der Zugriffsverwaltungsebene können Sie in Bezug auf die APIs, die über EC2-Rollenanmeldedaten aufgerufen werden, einen neuen Bedingungsschlüssel entweder in IAM-Richtlinien oder in AWS Organizations Service Control Policies (SCPs) verwenden. Durch Verwendung des Bedingungsschlüssels `ec2:RoleDelivery` mit dem Wert

`2.0` in Ihren IAM-Richtlinien erhalten insbesondere API-Aufrufe mit Anmeldeinformationen von EC2-Rollen, die von IMDSv1 abgerufen wurden, die Antwort `UnauthorizedOperation`. Das Gleiche kann mit der von einer SCP erzwungenen Bedingung weiter gefasst werden. Dadurch wird sichergestellt, dass die über IMDSv1 gelieferten Anmeldeinformationen nicht tatsächlich für den Aufruf von APIs verwendet werden können, da alle API-Aufrufe, die nicht der angegebenen Bedingung entsprechen, einen `UnauthorizedOperation`-Fehler erhalten.

Beispiele für IAM-Richtlinien finden Sie unter Arbeiten mit Instance-Metadaten. Weitere Informationen zu SCPs finden Sie unter Service-Kontrollrichtlinien im Benutzerhandbuch von AWS Organizations .

Empfohlener Weg zur Erzwingung von IMDSv2

Mit den oben genannten Tools empfehlen wir Ihnen, diesen Pfad für den Wechsel zu IMDSv2 zu folgen.

Schritt 1: Zu Beginn

Aktualisieren Sie die SDKs, CLIs und Anwendungen, die Rollen-Anmeldeinformationen auf ihren EC2-Instances verwenden, auf IMDSv2-kompatible Versionen. Informationen zum Upgrade der CLI finden Sie unter Upgrade auf die neueste Version der AWS CLI im AWS Command Line Interface - Benutzerhandbuch.

Ändern Sie dann Ihre Software, die über die IMDSv2-Anfragen direkt auf Instance-Metadaten zugreift (mit anderen Worten, die kein SDK verwendet). Sie können den IMDS-Paket-Analysator verwenden, um die Software zu identifizieren, die Sie ändern müssen, um IMDSv2-Anfragen verwenden zu können.

Schritt 2: Verfolgen des Umstellungsfortschritts

Verfolgen Sie Ihren Umstellungsfortschritt anhand der Metrik. CloudWatch `MetadataNoToken` Diese Metrik zeigt die Anzahl der IMDSv1-Aufrufe des IMDS für Ihre Instances an. Weitere Informationen finden Sie unter Instance-Metriken.

Schritt 3: Wenn IMDSv1 nicht mehr genutzt wird

Wenn die CloudWatch Metrik keine IMDSv1-Nutzung `MetadataNoToken` verzeichnet, sind Ihre Instances bereit, vollständig auf IMDSv2 umgestellt zu werden. In dieser Phase können Sie Folgendes tun:

- Standardeinstellung für das Konto

Sie können festlegen, dass IMDSv2 als Standardkonto erforderlich ist. Wenn eine Instanz gestartet wird, wird die Instanzkonfiguration automatisch auf den Kontostandard gesetzt.

Gehen Sie wie folgt vor, um den Kontostandard festzulegen:

- Amazon EC2 EC2-Konsole: Stellen Sie im EC2-Dashboard unter Kontoattribute, Datenschutz und Sicherheit für IMDS-Standardeinstellungen den Instance-Metadatenservice auf Aktiviert und die Metadatenversion auf Nur V2 (Token erforderlich) ein. Weitere Informationen finden Sie unter Legen Sie IMDSv2 als Standard für das Konto fest.
- AWS CLI: Verwenden Sie den CLI-Befehl modify-instance-metadata-defaults und geben Sie und an. `--http-tokens required` `--http-put-response-hop-limit 2`

- Neue Instances

  Beim Starten einer neuen Instance haben Sie folgende Möglichkeiten:

  - Amazon-EC2-Konsole: Stellen Sie im Launch Instance Wizard die Option Zugriff auf Metadaten auf Aktiviert und die Option Metadatenversion auf (Nur V2 (Token erforderlich) ein. Weitere Informationen finden Sie unter Konfigurieren der Instance beim Start.
  - AWS CLI: Verwenden Sie den CLI-Befehl run-instances und geben Sie an, dass IMDSv2 erforderlich ist.

- Vorhandene Instances

  Bei vorhandenen Instances können Sie Folgendes tun:

  - Amazon-EC2-Konsole: Wählen Sie auf der Seite Instances Ihre Instance aus, wählen Sie Aktionen, Instance-Einstellungen, Instance-Metadatenoptionen ändern und für IMDSv2 die Option Erforderlich. Weitere Informationen finden Sie unter Erzwingen der Verwendung von IMDSv2.
  - AWS CLI: Geben Sie mit dem CLI-Befehl modify-instance-metadata-options an, dass nur IMDSv2 verwendet werden soll.

  Sie können die Instance-Metadatenoptionen auf laufenden Instances ändern, und Sie müssen die Instances nicht neu starten, nachdem Sie die Instance-Metadatenoptionen geändert haben.

Schritt 4: Überprüfen, dass alle Instances zu IMDSv2 gewechselt sind

Sie können überprüfen, ob irgendwelche Instances noch nicht so konfiguriert sind, dass sie die Verwendung von IMDSv2 erfordern, mit anderen Worten, bei denen IMDSv2 immer noch als `optional` konfiguriert ist. Wenn Instances immer noch als `optional` konfiguriert sind, können

Sie die Intance-Metadatenoptionen ändern, um IMDSv2 `required` zu machen, indem Sie den vorherigen Schritt 3 wiederholen.

Filtern Ihrer Instances:

- Amazon-EC2-Konsole: Auf der Seite Instances filtern Sie Ihre Instances mit Hilfe des Filters IMDSv2 = optional. Weitere Informationen zur Filterung erhalten Sie unter Filtern von Ressourcen mithilfe der Konsole. Sie können auch sehen, ob IMDSv2 für jede Instance erforderlich oder optional ist: Schalten Sie im Fenster Einstellungen auf IMDSv2 um, um die Spalte IMDSv2 zur Instance-Tabelle hinzuzufügen.
- AWS CLI: Verwenden Sie den CLI-Befehl describe-instances und filtern Sie wie folgt nach `metadata-options.http-tokens = optional`:

```
aws ec2 describe-instances --filters "Name=metadata-options.http-
tokens,Values=optional" --query "Reservations[*].Instances[*].[InstanceId]" --output
 text
```

Schritt 5: Wenn alle Instances zu IMDSv2 gewechselt sind

Die `ec2:MetadataHttpEndpoint` IAM-Bedingungsschlüssel `ec2:MetadataHttpTokensec2:MetadataHttpPutResponseHopLimit`, und können verwendet werden, um die Verwendung der APIs RunInstancesund der ModifyInstanceMetadataOptionsentsprechenden CLIs zu steuern. Wenn eine Richtlinie erstellt wird und ein Parameter im API-Aufruf nicht mit dem in der Richtlinie über den Bedingungsschlüssel angegebenen Status übereinstimmt, schlägt der API- oder CLI-Aufruf mit einer `Unauthorized0peration`-Antwort fehl. Beispiele für IAM-Richtlinien finden Sie unter Arbeiten mit Instance-Metadaten.

Darüber hinaus können Sie nach der Deaktivierung von IMDSv1 anhand der `MetadataNoTokenRejected` CloudWatch Metrik verfolgen, wie oft ein IMDSv1-Anruf versucht und abgelehnt wurde. Wenn Sie nach der Deaktivierung von IMDSv1 über Software verfügen, die nicht ordnungsgemäß funktioniert und die `MetadataNoTokenRejected` Metrik IMDSv1-Aufrufe aufzeichnet, muss diese Software wahrscheinlich aktualisiert werden, um IMDSv2 verwenden zu können.

Verwenden eines unterstützten AWS -SDK

Um IMDSv2 verwenden zu können, müssen Ihre EC2-Instances eine SDK-Version verwenden, die die Verwendung von IMDSv2 unterstützt. AWS Die neuesten Versionen aller SDKs unterstützen die Verwendung von IMDSv2 AWS .

> **Important**
>
> Wir empfehlen Ihnen, über die SDK-Versionen auf dem Laufenden zu bleiben, um über die neuesten Features, Sicherheitsupdates und zugrunde liegenden Abhängigkeiten informiert zu sein. Die fortgesetzte Verwendung einer nicht unterstützten SDK-Version wird nicht empfohlen und erfolgt nach Ihrem Ermessen. Weitere Informationen finden Sie in der Wartungsrichtlinie für AWS -SDKs und -Tools im AWS -Referenzhandbuch für SDKs und Tools.

Im Folgenden sind die Mindestversionen aufgeführt, die die Verwendung von IMDSv2 unterstützen:

- AWS CLI – 1.16.289
- AWS Tools for Windows PowerShell – 4.0.1.0
- AWS SDK for .NET – 3.3.634.1
- AWS SDK for C++ – 1.7.229
- AWS SDK for Go – 1.25.38
- AWS SDK for Go v2 — 0.19.0
- AWS SDK for Java – 1.11.678
- AWS SDK for Java 2.x – 2.10.21
- AWS SDK für JavaScript in Node.js — 2.722.0
- AWS SDK for PHP – 3.147.7
- AWS SDK für Python (Botocore) — 1.13.25
- AWS SDK for Python (Boto3) – 1.12.6
- AWS SDK for Ruby – 3.79.0

Konfigurieren der Instance-Metadaten-Optionen

Der Instanz-Metadatendienst (IMDS) wird lokal auf jeder EC2-Instance ausgeführt. Die Optionen für Instance-Metadaten beziehen sich auf eine Reihe von Konfigurationen, die den Zugriff und das Verhalten des IMDS auf einer EC2-Instance steuern.

Sie können die folgenden Optionen für Instance-Metadaten für jede Instance konfigurieren:

Dienst für Instanz-Metadaten (IMDS): | `enabled` `disabled`

Sie können den IMDS auf einer Instanz aktivieren oder deaktivieren. Wenn diese Option deaktiviert ist, können Sie oder ein anderer Code nicht auf die Instanz-Metadaten auf der Instanz zugreifen.

Das IMDS hat zwei Endpunkte auf einer Instance: IPv4 (`169.254.169.254`) und IPv6 (). `[fd00:ec2::254]` Wenn Sie das IMDS aktivieren, wird der IPv4-Endpunkt automatisch aktiviert. Wenn Sie den IPv6-Endpunkt aktivieren möchten, müssen Sie dies explizit tun.

IMDS IPv6-Endpunkt: | `enabled` `disabled`

Sie können den IPv6-IMDS-Endpunkt auf einer Instanz explizit aktivieren. Wenn der IPv6-Endpunkt aktiviert ist, bleibt der IPv4-Endpunkt aktiviert. Der IPv6-Endpunkt wird nur auf Instances unterstützt, die auf dem AWS Nitro-System basieren, und in einem IPv6-unterstützten Subnetz (Dual Stack oder nur IPv6).

Version der Metadaten: | `IMDSv1 or IMDSv2 (token optional)` `IMDSv2 only (token required)`

Bei der Anforderung von Instanz-Metadaten benötigen IMDSv2-Aufrufe ein Token. IMDSv1-Aufrufe benötigen kein Token. Sie können eine Instanz so konfigurieren, dass sie entweder IMDSv1- oder IMDSv2-Aufrufe (wobei ein Token optional ist) oder nur IMDSv2-Aufrufe erlaubt (für die ein Token erforderlich ist).

Limit für den Antwort-Hop für Metadaten: — `1` `64`

Das Hop-Limit ist die Anzahl der Netzwerk-Hops, die die PUT-Antwort ausführen darf. Sie können das Hop-Limit auf ein Minimum von `1` und ein Maximum von festlegen`64`. In einer Containerumgebung empfehlen wir, das Hop-Limit auf festzulegen`2`. Weitere Informationen finden Sie unter Überlegungen.

Zugriff auf Tags in Instanzmetadaten: `enabled` | `disabled`

Sie können den Zugriff auf die Tags der Instanz über die Metadaten einer Instanz aktivieren oder deaktivieren. Weitere Informationen finden Sie unter Arbeiten mit Instance-Tags in Instance-Metadaten.

Wo können die Optionen für Instanz-Metadaten konfiguriert werden

Die Optionen für Instanz-Metadaten können wie folgt auf verschiedenen Ebenen konfiguriert werden:

- Konto — Sie können Standardwerte für die Instanz-Metadatenoptionen auf Kontoebene für jede Option festlegen AWS-Region. Wenn eine Instance gestartet wird, werden die Optionen für die Instance-Metadaten automatisch auf die Werte auf Kontoebene festgelegt. Sie können diese Werte beim Start ändern. Standardwerte auf Kontoebene wirken sich nicht auf bestehende Instances aus.
- AMI — Sie können den `imds-support` Parameter auf festlegen, `v2.0` wenn Sie ein AMI registrieren oder ändern. Wenn eine Instance mit diesem AMI gestartet wird, wird die Version der Instance-Metadaten automatisch auf IMDSv2 und das Hop-Limit auf 2 gesetzt.
- Instance — Sie können alle Optionen für Instance-Metadaten einer Instance beim Start ändern und dabei die Standardeinstellungen außer Kraft setzen. Sie können die Optionen für Instance-Metadaten auch nach dem Start einer laufenden oder angehaltenen Instance ändern. Beachten Sie, dass Änderungen möglicherweise durch eine IAM- oder SCP-Richtlinie eingeschränkt werden.

Weitere Informationen finden Sie unter Konfigurieren von Instance-Metadatenoptionen für neue Instances und Modifizieren von Instance-Metadatenoptionen für vorhandene Instances.

Rangfolge der Optionen für Instanz-Metadaten

Der Wert für jede Instance-Metadatenoption wird beim Start der Instance in einer hierarchischen Rangfolge festgelegt. Die Hierarchie mit der höchsten Priorität an der Spitze sieht wie folgt aus:

- Priorität 1: Instanzkonfiguration beim Start — Werte können entweder in der Startvorlage oder in der Instanzkonfiguration angegeben werden. Alle hier angegebenen Werte haben Vorrang vor Werten, die auf Kontoebene oder im AMI angegeben wurden.
- Priorität 2: Kontoeinstellungen — Wenn beim Start der Instance kein Wert angegeben wird, wird er durch die Einstellungen auf Kontoebene bestimmt (die für jede Instanz festgelegt sind). AWS-Region Einstellungen auf Kontoebene enthalten entweder einen Wert für jede Metadatenoption oder geben an, dass überhaupt keine Präferenz ausgewählt wird.

- Priorität 3: AMI-Konfiguration — Wenn beim Start der Instanz oder auf Kontoebene kein Wert angegeben wird, wird er durch die AMI-Konfiguration bestimmt. Dies gilt nur für `HttpTokens` und `HttpPutResponseHopLimit`.

Jede Metadatenoption wird separat bewertet. Die Instance kann mit einer Mischung aus direkter Instance-Konfiguration, Standardeinstellungen auf Kontoebene und der Konfiguration aus dem AMI konfiguriert werden.

Sie können den Wert jeder Metadatenoption nach dem Start einer laufenden oder angehaltenen Instance ändern, sofern die Änderungen nicht durch eine IAM- oder SCP-Richtlinie eingeschränkt sind.

Ermitteln Sie Werte für Metadatenoptionen — Beispiel 1

In diesem Beispiel wird eine EC2-Instance in einer Region gestartet, für die `1` auf Kontoebene festgelegt `HttpPutResponseHopLimit` ist. Das angegebene AMI wurde auf `ImdsSupport` eingestellt`v2.0`. Beim Start werden keine Metadatenoptionen direkt auf der Instance angegeben. Die Instance wird mit den folgenden Metadatenoptionen gestartet:

```
"MetadataOptions": {
    ...
    "HttpTokens": "required",
    "HttpPutResponseHopLimit": 1,
    ...
```

Diese Werte wurden wie folgt bestimmt:

- Beim Start wurden keine Metadatenoptionen angegeben: Beim Start der Instance wurden weder in den Instance-Startparametern noch in der Startvorlage spezifische Werte für die Metadatenoptionen angegeben.
- Kontoeinstellungen haben als Nächstes Vorrang: Wenn beim Start keine spezifischen Werte angegeben wurden, haben die Einstellungen auf Kontoebene innerhalb der Region Vorrang. Das bedeutet, dass die auf Kontoebene konfigurierten Standardwerte angewendet werden. In diesem Fall `HttpPutResponseHopLimit` wurde der auf gesetzt`1`.
- AMI-Einstellungen haben letzten Vorrang: Wenn beim Start oder auf Kontoebene kein bestimmter Wert angegeben wurde `HttpTokens` (die Instance-Metadatenversion), wird die AMI-Einstellung angewendet. In diesem Fall wurde anhand der AMI-Einstellung `ImdsSupport: v2.0` festgelegt, dass dies auf eingestellt `HttpTokens` war`required`. Beachten Sie,

dass die AMI-Einstellung zwar für die Einstellung vorgesehen `ImdsSupport: v2.0` ist`HttpPutResponseHopLimit: 2`, sie jedoch durch die Einstellung auf Kontoebene, die höhere Priorität hat`HttpPutResponseHopLimit: 1`, außer Kraft gesetzt wurde.

Ermitteln Sie Werte für Metadatenoptionen — Beispiel 2

In diesem Beispiel wird die EC2-Instance mit den gleichen Einstellungen wie im vorherigen Beispiel 1 gestartet, allerdings mit der `HttpTokens` Einstellung `optional` direkt auf der Instance beim Start. Die Instance wird mit den folgenden Metadatenoptionen gestartet:

```
"MetadataOptions": {
    ...
    "HttpTokens": "optional",
    "HttpPutResponseHopLimit": 1,
    ...
```

Der Wert für `HttpPutResponseHopLimit` wird auf die gleiche Weise wie in Beispiel 1 bestimmt. Der Wert für `HttpTokens` wird jedoch wie folgt bestimmt: Metadatenoptionen, die beim Start auf der Instance konfiguriert wurden, haben Vorrang. Obwohl das AMI mit konfiguriert war `ImdsSupport: v2.0` (mit anderen Worten auf gesetzt `HttpTokens` ist`required`), hatte der Wert, der beim Start auf der Instance angegeben wurde (`HttpTokens`gesetzt auf`optional`), Vorrang.

Legen Sie die Version der Instance-Metadaten fest

Wenn eine Instanz gestartet wird, ist der Wert für die Version der Instanz-Metadaten entweder `IMDSv1 or IMDSv2 (token optional)` oder`IMDSv2 only (token required)`.

Beim Start der Instance können Sie den Wert für die Metadatenversion entweder manuell angeben oder den Standardwert verwenden. Wenn Sie den Wert manuell angeben, überschreibt er alle Standardwerte. Wenn Sie den Wert nicht manuell angeben möchten, wird er durch eine Kombination von Standardeinstellungen bestimmt, wie in der folgenden Tabelle beschrieben.

Die Tabelle zeigt, wie die Metadatenversion für eine Instance beim Start (angezeigt durch Resultierende Instance-Konfiguration in Spalte 4) durch die Einstellungen auf den verschiedenen Konfigurationsebenen bestimmt wird. Die Rangfolge erfolgt von links nach rechts, wobei die erste Spalte die höchste Priorität hat, und zwar wie folgt:

- Spalte 1: Startparameter — Stellt die Einstellung für die Instance dar, die Sie beim Start manuell angeben.

- Spalte 2: Standard auf Kontoebene — Stellt die Einstellung für das Konto dar.
- Spalte 3: AMI-Standard — Stellt die Einstellung auf dem AMI dar.

Startparameter	Standard auf Kontoebene	AMI-Standard	Resultierende Instanzkonfiguration
Nur V2 (Token erforderlich)	Keine Präferenz	Nur V2	Nur V2
Nur V2 (Token erforderlich)	Nur V2	Nur V2	Nur V2
Nur V2 (Token erforderlich)	V1 oder V2	Nur V2	Nur V2
V1 oder V2 (Token optional)	Keine Präferenz	Nur V2	V1 oder V2
V1 oder V2 (Token optional)	Nur V2	Nur V2	V1 oder V2
V1 oder V2 (Token optional)	V1 oder V2	Nur V2	V1 oder V2
Nicht gesetzt	Keine Präferenz	Nur V2	Nur V2
Nicht gesetzt	Nur V2	Nur V2	Nur V2
Nicht gesetzt	V1 oder V2	Nur V2	V1 oder V2
Nur V2 (Token erforderlich)	Keine Präferenz	Null	Nur V2
Nur V2 (Token erforderlich)	Nur V2	Null	Nur V2
Nur V2 (Token erforderlich)	V1 oder V2	Null	Nur V2

Startparameter	Standard auf Kontoebene	AMI-Standard	Resultierende Instanzkonfiguration
V1 oder V2 (Token optional)	Keine Präferenz	Null	V1 oder V2
V1 oder V2 (Token optional)	Nur V2	Null	V1 oder V2
V1 oder V2 (Token optional)	V1 oder V2	Null	V1 oder V2
Nicht gesetzt	Keine Präferenz	Null	V1 oder V2
Nicht gesetzt	Nur V2	Null	Nur V2
Nicht gesetzt	V1 oder V2	Null	V1 oder V2

Verwenden Sie IAM-Bedingungsschlüssel, um die Optionen für Instanz-Metadaten einzuschränken

Sie können IAM-Bedingungsschlüssel in einer IAM-Richtlinie oder einem SCP wie folgt verwenden:

- Zulassen, dass eine Instance nur gestartet wird, wenn sie so konfiguriert ist, dass sie die Verwendung von IMDSv2 erzwingt
- Beschränken der Anzahl der zulässigen Hops
- Deaktivieren des Zugriffs auf Instance-Metadaten

Aufgaben

- Konfigurieren von Instance-Metadatenoptionen für neue Instances
- Modifizieren von Instance-Metadatenoptionen für vorhandene Instances

> **Note**
>
> Sie sollten vorsichtig vorgehen und sorgfältige Tests durchführen, bevor Sie Änderungen vornehmen. Beachten Sie die folgenden Punkte:

- Wenn Sie die Verwendung von IMDSv2 erzwingen, werden Anwendungen oder Agenten, die IMDSv1 für Instance-Metadatenzugriffe verwenden, unterbrochen.
- Wenn Sie den gesamten Zugriff auf Instance-Metadaten deaktivieren, werden Anwendungen oder Agenten, die auf Instance-Metadaten angewiesen sind, den Zugriff auf die Funktion verlieren.
- Für IMDSv2 müssen Sie `/latest/api/token` beim Abrufen des Tokens nutzen.
- (Nur Windows) Wenn Ihre PowerShell Version älter als 4.0 ist, müssen Sie auf Windows Management Framework 4.0 aktualisieren, um die Verwendung von IMDSv2 zu erfordern.

Konfigurieren von Instance-Metadatenoptionen für neue Instances

Sie können die folgenden Optionen für Instanzmetadaten für neue Instanzen konfigurieren.

Optionen

- Erzwingen der Verwendung von IMDSv2
- Aktivieren Sie die IMDS-IPv4- und IPv6-Endpunkte
- Deaktivieren des Zugriffs auf Instance-Metadaten

Erzwingen der Verwendung von IMDSv2

Sie können die folgenden Methoden verwenden, um die Verwendung von IMDSv2 auf Ihren neuen Instanzen vorzuschreiben.

So machen Sie IMDSv2 erforderlich

- Legen Sie IMDSv2 als Standard für das Konto fest
- Konfigurieren der Instance beim Start
- Konfigurieren des AMI
- Verwenden einer IAM-Richtlinie

Legen Sie IMDSv2 als Standard für das Konto fest

Sie können die Standardversion für den Instanz-Metadatendienst (IMDS) jeweils auf Kontoebene festlegen. AWS-Region Das heißt, wenn Sie eine neue Instance starten, wird die Instanz-Metadatenversion automatisch auf den Standard auf Kontoebene gesetzt. Sie können den Wert

jedoch beim Start oder nach dem Start manuell überschreiben. Weitere Informationen darüber, wie sich Einstellungen auf Kontoebene und manuelle Überschreibungen auf eine Instance auswirken, finden Sie unter. Rangfolge der Optionen für Instanz-Metadaten

> **Note**
>
> Durch das Festlegen der Standardeinstellung auf Kontoebene werden bestehende Instanzen nicht zurückgesetzt. Wenn Sie beispielsweise den Standard auf Kontoebene auf IMDSv2 festlegen, sind alle vorhandenen Instanzen, die auf IMDSv1 festgelegt sind, nicht betroffen. Wenn Sie den Wert für bestehende Instances ändern möchten, müssen Sie den Wert für die Instances selbst manuell ändern.

Sie können den Kontostandard für die Instanz-Metadatenversion auf IMDSv2 festlegen, sodass alle neuen Instances beim Kontostart mit IMDSv2 erforderlich sind und IMDSv1 deaktiviert wird. Wenn Sie diesen Kontostandard verwenden, gelten beim Starten einer Instance die folgenden Standardwerte für die Instance:

- Konsole: Die Metadatenversion ist nur auf V2 festgelegt (Token erforderlich) und das Limit für den Metadaten-Response-Hop ist auf 2 festgelegt.
- AWS CLI: `HttpTokens` ist auf gesetzt `required` und `HttpPutResponseHopLimit` ist auf gesetzt2.

> **Note**
>
> Bevor Sie den Kontostandard auf IMDSv2 setzen, stellen Sie sicher, dass Ihre Instances nicht von IMDSv1 abhängig sind. Weitere Informationen finden Sie unter Empfohlener Weg zur Erzwingung von IMDSv2.

Console

Um IMDSv2 als Standard für das Konto für die angegebene Region festzulegen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Um das zu ändern AWS-Region, verwenden Sie die Regionsauswahl in der oberen rechten Ecke der Seite.

3. Wählen Sie im Navigationsbereich EC2 Dashboard (EC2-Dashboard) aus.
4. Wählen Sie unter Kontoattribute die Option Datenschutz und Sicherheit aus.
5. Wählen Sie neben IMDS-Standardeinstellungen die Option Verwalten aus.
6. Gehen Sie auf der Seite IMDS-Standardwerte verwalten wie folgt vor:

   a. Wählen Sie für Instance-Metadaten-Service die Option Aktiviert aus.
   b. Wählen Sie für Metadatenversion die Option Nur V2 (Token erforderlich) aus.
   c. Geben Sie für Metadata Response Hop Limit den Wert 2 an, wenn Ihre Instances Container hosten sollen. Wählen Sie andernfalls Keine Präferenz aus. Wenn keine Präferenz angegeben ist, wird der Wert beim Start standardmäßig auf 2 gesetzt, wenn das AMI IMDSv2 benötigt; andernfalls wird der Standardwert auf 1 gesetzt.
   d. Wählen Sie Aktualisieren.

AWS CLI

Um IMDSv2 als Standard für das Konto für die angegebene Region festzulegen

Verwenden Sie den Befehl modify-instance-metadata-defaults und geben Sie die Region an, in der die Einstellungen auf IMDS-Kontoebene geändert werden sollen. Schließen `--http-tokens` Sie die Einstellung auf ein und legen Sie fest, ob Ihre Instances Container `required` hosten werden. `--http-put-response-hop-limit` 2 Geben Sie andernfalls `-1` an, dass keine Präferenz angegeben werden soll. Wenn `-1` (keine Präferenz) angegeben ist, wird beim Start standardmäßig der Wert verwendet, 2 ob das AMI IMDSv2 benötigt; andernfalls ist der Standardwert. 1

```
aws ec2 modify-instance-metadata-defaults \
    --region us-east-1 \
    --http-tokens required \
    --http-put-response-hop-limit 2
```

Erwartete Ausgabe

```
{
    "Return": true
}
```

Um die Standardkontoeinstellungen für die Instance-Metadatenoptionen für die angegebene Region anzuzeigen

Verwenden Sie den get-instance-metadata-defaults Befehl und geben Sie die Region an.

```
aws ec2 get-instance-metadata-defaults --region us-east-1
```

Beispielausgabe

```
{
    "AccountLevel": {
        "HttpTokens": "required",
        "HttpPutResponseHopLimit": 2
    }
}
```

Konfigurieren der Instance beim Start

Wenn Sie eine Instance starten, können Sie sie so konfigurieren, dass die Verwendung von IMDSv2 erzwungen wird. Dazu konfigurieren Sie die folgenden Felder:

- Amazon-EC2-Konsole: Stellen Sie Metadata version (Metadatenversion) auf V2 only (token required) (Nur V2 (Token erforderlich)) ein.
- AWS CLI: Stellen Sie `HttpTokens` auf `required` ein.

Wenn Sie angeben, dass IMDSv2 erforderlich ist, müssen Sie auch den Endpunkt des Instance Metadata Service (IMDS) aktivieren, indem Sie Metadatazugriff auf Aktiviert (Konsole) oder `HttpEndpoint` auf `enabled` (AWS CLI) einstellen.

In einer Containerumgebung, in der IMDSv2 erforderlich ist, empfehlen wir, das Hop-Limit auf festzulegen. 2 Weitere Informationen finden Sie unter Überlegungen.

New console

So erzwingen Sie die Verwendung von IMDSv2 für eine neue Instance

- Wenn Sie eine neue Instance in der Amazon-EC2-Konsole starten, erweitern Sie Erweiterte Details wie folgt:
  - Für Metadaten zugänglich wählen Sie Aktiviert.
  - Wählen Sie für Metadatenversion die Option Nur V2 (Token erforderlich) aus.
  - (Container-Umgebung) Wählen Sie unter „Metadata Response Hop Limit“ den Wert 2 aus.

Weitere Informationen finden Sie unter Erweiterte Details.

Old console

So erzwingen Sie die Verwendung von IMDSv2 für eine neue Instance

- Wenn Sie eine neue Instance in der Amazon EC2-Konsole starten, wählen Sie auf der Seite Instance-Details konfigurieren die folgenden Optionen aus:
  - Wählen Sie unter Erweiterte Details für Metadaten verfügbar die Option Aktiviert aus.
  - Wählen Sie für Metadatenversion die Option V2 (Token erforderlich) aus.

Weitere Informationen finden Sie unter Schritt 3: Konfigurieren der Instance-Details.

AWS CLI

So erzwingen Sie die Verwendung von IMDSv2 für eine neue Instance

Im folgenden Beispiel für run-instances wird eine `c6i.large`-Instance gestartet, bei der `--metadata-options` auf `HttpTokens=required` gesetzt ist. Wenn Sie einen Wert für `HttpTokens` angeben, müssen Sie auch `HttpEndpoint` auf `enabled` einstellen. Da der sichere Token-Header für Anforderungen zum Abruf von Metadaten auf `required` eingestellt ist, muss die Instance beim Anfordern von Instance-Metadaten IMDSv2 verwenden.

Wenn in einer Container-Umgebung IMDSv2 erforderlich ist, empfehlen wir, das Hop-Limit auf with zu 2 setzen. `HttpPutResponseHopLimit=2`

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
 ...
    --metadata-options
 "HttpEndpoint=enabled,HttpTokens=required,HttpPutResponseHopLimit=2"
```

PowerShell

So erzwingen Sie die Verwendung von IMDSv2 für eine neue Instance

Das folgende New-EC2InstanceCmdlet-Beispiel startet eine `c6i.large` Instanz mit `MetadataOptions_HttpEndpoint` set to `enabled` und dem Parameter to.

`MetadataOptions_HttpTokens` `required` Wenn Sie einen Wert für `HttpTokens` angeben, müssen Sie auch `HttpEndpoint` auf `enabled` einstellen. Da der sichere Token-Header für Anforderungen zum Abruf von Metadaten auf `required` eingestellt ist, muss die Instance beim Anfordern von Instance-Metadaten IMDSv2 verwenden.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpTokens required
```

AWS CloudFormation

Informationen zum Angeben der Metadatenoptionen für eine Instance, die Sie verwenden AWS CloudFormation, finden Sie in der entsprechenden AWS::EC2::LaunchTemplate MetadataOptionsEigenschaft im AWS CloudFormation Benutzerhandbuch.

Konfigurieren des AMI

Wenn Sie ein neues AMI registrieren oder ein vorhandenes AMI ändern, können Sie den Parameter `imds-support` auf `v2.0` setzen. Bei Instances, die über dieses AMI gestartet werden, ist Metadata version (Metadatenversion) auf V2 only (token required) (Nur V2 (Token erforderlich)) (Konsole) oder `HttpTokens` auf `required` (AWS CLI) eingestellt. Mit diesen Einstellungen erzwingt die Instance die Verwendung von IMDSv2, wenn Instance-Metadaten angefordert werden.

Hinweis: Wenn Sie `imds-support` auf `v2.0` einstellen, wird bei Instances, die über dieses AMI gestartet werden, auch Metadata response hop limit (Limit für Metadaten-Antwort-Hop) (Konsole) oder `http-put-response-hop-limit` (AWS CLI) auf 2 eingestellt.

> **Important**
>
> Verwenden Sie diesen Parameter nur, wenn Ihre AMI-Software IMDSv2 unterstützt. Nachdem Sie den Wert auf `v2.0` gesetzt haben, können Sie das nicht mehr rückgängig machen. Die einzige Möglichkeit, Ihr AMI „zurückzusetzen“, besteht darin, ein neues AMI aus dem zugrunde liegenden Snapshot zu erstellen.

So konfigurieren Sie ein neues AMI für IMDSv2

Verwenden Sie eine der folgenden Methoden, um ein neues AMI für IMDSv2 zu konfigurieren.

AWS CLI

Das folgende register-image-Beispiel registriert ein AMI mit dem angegebenen Snapshot eines EBS-Stamm-Volumes als `/dev/xvda` des Geräts. Geben Sie `v2.0` für den `imds-support`-Parameter an, sodass von diesem AMI aus gestartete Instances erzwingen, dass beim Anfordern von Instance-Metadaten IMDSv2 verwendet wird.

```
aws ec2 register-image \
    --name my-image \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/
xvda,Ebs={SnapshotId=snap-0123456789example} \
    --architecture x86_64 \
    --imds-support v2.0
```

PowerShell

Das folgende Register-EC2ImageCmdlet-Beispiel registriert ein AMI, das den angegebenen Snapshot eines EBS-Root-Volumes als Gerät verwendet. `/dev/xvda` Geben Sie `v2.0` für den `ImdsSupport`-Parameter an, sodass von diesem AMI aus gestartete Instances erzwingen, dass beim Anfordern von Instance-Metadaten IMDSv2 verwendet wird.

```
Import-Module AWS.Tools.EC2  # Required for Amazon.EC2.Model object creation.
Register-EC2Image `
    -Name 'my-image' `
    -RootDeviceName /dev/xvda `
    -BlockDeviceMapping  (
    New-Object `
        -TypeName Amazon.EC2.Model.BlockDeviceMapping `
        -Property @{
        DeviceName = '/dev/xvda';
        EBS        = (New-Object -TypeName Amazon.EC2.Model.EbsBlockDevice -Property
 @{
                SnapshotId = 'snap-0123456789example';
                VolumeType = 'gp3'
                } )
        }  ) `
    -Architecture X86_64 `
    -ImdsSupport v2.0
```

So konfigurieren Sie ein bestehendes AMI für IMDSv2

Verwenden Sie eine der folgenden Methoden, um ein bereits vorhandenes AMI für IMDSv2 zu konfigurieren.

AWS CLI

Das folgende Beispiel für modify-image-attribute ändert ein vorhandenes AMI nur für IMDSv2. Geben Sie `v2.0` für den `imds-support`-Parameter an, sodass von diesem AMI aus gestartete Instances erzwingen, dass beim Anfordern von Instance-Metadaten IMDSv2 verwendet wird.

```
aws ec2 modify-image-attribute \
    --image-id ami-0123456789example \
    --imds-support v2.0
```

PowerShell

Das folgende Edit-EC2ImageAttributeCmdlet-Beispiel ändert ein vorhandenes AMI nur für IMDSv2. Geben Sie `v2.0` für den `imds-support`-Parameter an, sodass von diesem AMI aus gestartete Instances erzwingen, dass beim Anfordern von Instance-Metadaten IMDSv2 verwendet wird.

```
Edit-EC2ImageAttribute `
    -ImageId ami-0abcdef1234567890 `
    -ImdsSupport 'v2.0'
```

Verwenden einer IAM-Richtlinie

Sie können eine IAM-Richtlinie erstellen, die verhindert, dass Benutzer neue Instances starten, es sei denn, sie benötigen IMDSv2 auf der neuen Instance.

So erzwingen Sie die Verwendung von IMDSv2 auf allen neuen Instances mit einer IAM-Richtlinie

Um sicherzustellen, dass Benutzer beim Anfordern von Instance-Metadaten nur Instances starten können, die die Verwendung von IMDSv2 erfordern, können Sie angeben, dass die Bedingung für die Anforderung von IMDSv2 erfüllt sein muss, bevor eine Instance gestartet werden kann. Die IAM-Beispielrichtlinie finden Sie unter Arbeiten mit Instance-Metadaten.

Aktivieren Sie die IMDS-IPv4- und IPv6-Endpunkte

Das IMDS hat zwei Endpunkte auf einer Instanz: IPv4 () und IPv6 (). `169.254.169.254` `[fd00:ec2::254]` Wenn Sie das IMDS aktivieren, wird der IPv4-Endpunkt automatisch aktiviert.

Der IPv6-Endpunkt bleibt auch dann deaktiviert, wenn Sie eine Instance in einem reinen IPv6-Subnetz starten. Um den IPv6-Endpunkt zu aktivieren, müssen Sie dies explizit tun. Wenn Sie den IPv6-Endpunkt aktivieren, bleibt der IPv4-Endpunkt aktiviert.

Sie können den IPv6-Endpunkt beim Start der Instance oder danach aktivieren.

Anforderungen für die Aktivierung des IPv6-Endpunkts

- Der ausgewählte Instanztyp basiert auf dem AWS Nitro-System.
- Das ausgewählte Subnetz unterstützt IPv6, wobei es sich bei dem Subnetz entweder um ein Dual-Stack-Subnetz oder nur um IPv6 handelt.

Verwenden Sie eine der folgenden Methoden, um eine Instance mit aktiviertem IMDS-IPv6-Endpunkt zu starten.

New console

Um den IMDS-IPv6-Endpunkt beim Start der Instanz zu aktivieren

- Starten Sie die Instance in der Amazon-EC2-Konsole mit den folgenden Angaben unter Advanced details (Erweiterte Details):
  - Wählen Sie für Metadaten-IPv6-Endpunkt die Option Aktiviert aus.

Weitere Informationen finden Sie unter Erweiterte Details.

AWS CLI

Um den IMDS-IPv6-Endpunkt beim Instance-Start zu aktivieren

Das folgende run-instances-Beispiel startet eine `c6i.large`-Instance, wobei der IPv6-Endpunkt für den IMDS aktiviert ist. Um den IPv6-Endpunkt zu aktivieren, geben Sie für den Parameter `--metadata-options` den Wert `HttpProtocolIpv6=enabled` an. Wenn Sie einen Wert für `HttpProtocolIpv6` angeben, müssen Sie auch `HttpEndpoint` auf `enabled` einstellen.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=enabled,HttpProtocolIpv6=enabled"
```

PowerShell

Um den IMDS-IPv6-Endpunkt beim Instance-Start zu aktivieren

Das folgende New-EC2InstanceCmdlet-Beispiel startet eine `c6i.large` Instanz, bei der der IPv6-Endpunkt für das IMDS aktiviert ist. Legen Sie zum Aktivieren des IPv6-Endpunkts `MetadataOptions_HttpProtocolIpv6` auf `enabled` fest. Wenn Sie einen Wert für `MetadataOptions_HttpProtocolIpv6` angeben, müssen Sie auch `MetadataOptions_HttpEndpoint` auf `enabled` einstellen.

```
New-EC2Instance `
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint enabled `
    -MetadataOptions_HttpProtocolIpv6 enabled
```

Deaktivieren des Zugriffs auf Instance-Metadaten

Sie können den Zugriff auf die Instance-Metadaten deaktivieren, indem Sie den IMDS deaktivieren, wenn Sie eine Instance starten. Sie können den Zugriff später wieder aktivieren, indem Sie den IMDS erneut aktivieren. Weitere Informationen finden Sie unter Aktivieren des Zugriffs auf Instance-Metadaten.

Important

Sie können wählen, ob Sie den IMDS beim Start oder nach dem Start deaktivieren möchten. Wenn Sie den IMDS beim Start deaktivieren, funktioniert Folgendes möglicherweise nicht:

- Möglicherweise haben Sie keinen SSH-Zugriff auf Ihre Instance. Auf den `public-keys/0/openssh-key`, den öffentlichen SSH-Schlüssel Ihrer Instance, kann nicht zugegriffen werden, da der Schlüssel normalerweise über die EC2-Instance-Metadaten bereitgestellt und abgerufen wird.
- EC2-Benutzerdaten sind nicht verfügbar und werden beim Start der Instance nicht ausgeführt. EC2-Benutzerdaten werden auf dem IMDS gehostet. Wenn Sie den IMDS deaktivieren, deaktivieren Sie effektiv den Zugriff auf Benutzerdaten.

Sie können den IMDS nach dem Start wieder aktivieren, um auf diese Funktion zuzugreifen.

New console

So deaktivieren Sie den Zugriff auf Instance-Metadaten beim Start

- Starten Sie die Instance in der Amazon-EC2-Konsole mit den folgenden Angaben unter Advanced details (Erweiterte Details):
  - Für Metadaten zugänglich wählen Sie Deaktiviert.

Weitere Informationen finden Sie unter Erweiterte Details.

Old console

So deaktivieren Sie den Zugriff auf Instance-Metadaten beim Start

- Starten Sie die Instance in der Amazon-EC2-Konsole, wobei auf der Seite Configure Instance Details (Konfigurieren von Instance-Details) die folgende Option ausgewählt ist:
  - Wählen Sie unter Erweiterte Details für Metadaten verfügbar die Option Deaktiviert aus.

Weitere Informationen finden Sie unter Schritt 3: Konfigurieren der Instance-Details.

AWS CLI

So deaktivieren Sie den Zugriff auf Instance-Metadaten beim Start

Starten Sie die Instance, wobei `--metadata-options` auf `HttpEndpoint=disabled` eingestellt ist.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c6i.large \
    ...
    --metadata-options "HttpEndpoint=disabled"
```

PowerShell

So deaktivieren Sie den Zugriff auf Instance-Metadaten beim Start

Das folgende New-EC2InstanceCmdlet-Beispiel startet eine Instanz mit der Einstellung auf. `MetadataOptions_HttpEndpoint` `disabled`

```
New-EC2Instance `
```

```
    -ImageId ami-0abcdef1234567890 `
    -InstanceType c6i.large `
    -MetadataOptions_HttpEndpoint disabled
```

AWS CloudFormation

Informationen zum Angeben der Metadatenoptionen für eine Instanz, die Sie verwenden AWS CloudFormation, finden Sie in der AWS::EC2::LaunchTemplate MetadataOptionsentsprechenden Eigenschaft im AWS CloudFormation Benutzerhandbuch.

Modifizieren von Instance-Metadatenoptionen für vorhandene Instances

Sie können die Instance-Metadatenoptionen für vorhandene Instances ändern.

Sie können auch eine IAM-Richtlinie erstellen, die verhindert, dass Benutzer die Instance-Metadatenoptionen für vorhandene Instances ändern. Um zu kontrollieren, welche Benutzer die Optionen für Instanz-Metadaten ändern können, geben Sie eine Richtlinie an, die verhindert, dass alle Benutzer außer Benutzern mit einer bestimmten Rolle die ModifyInstanceMetadataOptionsAPI verwenden. Die IAM-Beispielrichtlinie finden Sie unter Arbeiten mit Instance-Metadaten.

Abfragen von Instance-Metadatenoptionen für vorhandene Instances

Sie können die Instance-Metadatenoptionen für Ihre vorhandenen Instances mit einer der folgenden Methoden abfragen.

Console

So fragen Sie die Instance-Metadaten-Optionen für eine bereits vorhandene Instance über die Konsole ab

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Überprüfen Sie die aktuellen Optionen für Instance-Metadaten im Dialogfeld „Optionen für Instance-Metadaten ändern“.

AWS CLI

Um die Instanz-Metadatenoptionen für eine bestehende Instanz abzufragen, verwenden Sie den AWS CLI

Verwenden Sie den CLI-Befehl describe-instances.

```
aws ec2 describe-instances \
    --instance-id i-1234567898abcdef0 \
    --query 'Reservations[].Instances[].MetadataOptions'
```

PowerShell

Um die Instanz-Metadatenoptionen für eine bestehende Instanz mit den Tools für abzufragen PowerShell

Verwenden Sie das Get-EC2InstanceCmdlet.

```
(Get-EC2Instance `
    -InstanceId i-1234567898abcdef0).Instances.MetadataOptions
```

Erzwingen der Verwendung von IMDSv2

Verwenden Sie eine der folgenden Methoden, um die Instance-Metadatenoptionen für eine bestehende Instance zu ändern, um zu erzwingen, dass beim Anfordern von Instance-Metadaten IMDSv2 verwendet wird. Wenn IMDSv2 erforderlich ist, kann IMDSv1 nicht verwendet werden.

> **Note**
>
> Bevor Sie verlangen, dass IMDSv2 verwendet wird, stellen Sie sicher, dass die Instanz keine IMDSv1-Aufrufe tätigt. Die `MetadataNoToken` CloudWatch Metrik verfolgt IMDSv1-Aufrufe. Wenn keine IMDSv1-Nutzung für eine Instance `MetadataNoToken` aufgezeichnet wird, ist die Instance bereit, IMDSv2 anzufordern.

Console

So erzwingen Sie die Verwendung von IMDSv2 auf einer vorhandenen Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Führen Sie im Dialogfeld Instance-Metadatenoptionen ändern Folgendes aus:
    a. Für den Instance-Metadatenservice wählen Sie die Option Aktivieren.
    b. Wählen Sie für IMDSv2 die Option Erforderlich aus.
    c. Wählen Sie Speichern.

AWS CLI

So erzwingen Sie die Verwendung von IMDSv2 auf einer vorhandenen Instance

Verwenden Sie den CLI-Befehl modify-instance-metadata-options und setzen Sie den Parameter `http-tokens` auf `required`. Wenn Sie einen Wert für `http-tokens` angeben, müssen Sie auch `http-endpoint` auf `enabled` einstellen.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens required \
    --http-endpoint enabled
```

PowerShell

So erzwingen Sie die Verwendung von IMDSv2 auf einer vorhandenen Instance

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den Parameter auf. `HttpTokens` `required` Wenn Sie einen Wert für `HttpTokens` angeben, müssen Sie auch `HttpEndpoint` auf `enabled` einstellen.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens required `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Die Verwendung von IMDSv1 wieder herstellen

Wenn IMDSv2 erforderlich ist, funktioniert IMDSv1 beim Anfordern von Instance-Metadaten nicht. Wenn IMDSv2 optional ist, funktionieren sowohl IMDSv2 als auch IMDSv1. Machen Sie IMDSv2 daher optional, um IMDSv1 wiederherzustellen, indem Sie eine der folgenden Methoden verwenden.

Console

So stellen Sie die Verwendung von IMDSv1 auf einer Instance wieder her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Führen Sie im Dialogfeld Instance-Metadatenoptionen ändern Folgendes aus:
   a. Vergewissern Sie sich, dass für den Instance-Metadatenservice die Option Aktivieren ausgewählt ist.
   b. Wählen Sie für IMDSv2 die Option Optional.
   c. Wählen Sie Speichern.

AWS CLI

So stellen Sie die Verwendung von IMDSv1 auf einer Instance wieder her

Sie können den CLI-Befehl modify-instance-metadata-options verwenden, wobei `http-tokens` auf `optional` gesetzt ist, um die Verwendung von IMDSv1 beim Anfordern von Instance-Metadaten wiederherzustellen.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-tokens optional \
    --http-endpoint enabled
```

PowerShell

So stellen Sie die Verwendung von IMDSv1 auf einer Instance wieder her

Sie können das Edit-EC2InstanceMetadataOptionCmdlet mit der `HttpTokens` Einstellung auf verwenden, `optional` um die Verwendung von IMDSv1 wiederherzustellen, wenn Instanzmetadaten angefordert werden.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpTokens optional `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Ändern des PUT-Antwort-Hop-Limits

Für bestehende Instances können Sie die Einstellungen für das PUT-Antwort-Hop-Limit ändern.

Derzeit unterstützen nur die AWS SDKs AWS CLI und die Änderung des PUT-Antwort-Hop-Limits.

AWS CLI

So ändern Sie das PUT-Antwort-Hop-Limit

Verwenden Sie den CLI-Befehl modify-instance-metadata-options und setzen Sie den Parameter `http-put-response-hop-limit` auf die gewünschte Anzahl von Hops. Im folgenden Beispiel wird das Hop-Limit auf 3 gesetzt. Beachten Sie, dass Sie beim Angeben eines Werts für `http-put-response-hop-limit` auch `http-endpoint` auf `enabled` setzen müssen.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-put-response-hop-limit 3 \
    --http-endpoint enabled
```

PowerShell

So ändern Sie das PUT-Antwort-Hop-Limit

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den `HttpPutResponseHopLimit` Parameter auf die erforderliche Anzahl von Hops. Im folgenden Beispiel wird das Hop-Limit auf 3 gesetzt. Beachten Sie, dass Sie beim Angeben eines Werts für `HttpPutResponseHopLimit` auch `HttpEndpoint` auf `enabled` setzen müssen.

```
(Edit-EC2InstanceMetadataOption `
```

```
    -InstanceId i-1234567898abcdef0 `
    -HttpPutResponseHopLimit 3 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Aktivieren Sie die IPv4- und IPv6-Endpunkte von IMDS

Das IMDS hat zwei Endpunkte auf einer Instanz: IPv4 () und IPv6 (). `169.254.169.254` `[fd00:ec2::254]` Wenn Sie das IMDS aktivieren, wird der IPv4-Endpunkt automatisch aktiviert. Der IPv6-Endpunkt bleibt auch dann deaktiviert, wenn Sie eine Instance in einem reinen IPv6-Subnetz starten. Um den IPv6-Endpunkt zu aktivieren, müssen Sie dies explizit tun. Wenn Sie den IPv6-Endpunkt aktivieren, bleibt der IPv4-Endpunkt aktiviert.

Sie können den IPv6-Endpunkt beim Start der Instance oder danach aktivieren.

Anforderungen für die Aktivierung des IPv6-Endpunkts

- Der ausgewählte Instanztyp basiert auf dem AWS Nitro-System.
- Das ausgewählte Subnetz unterstützt IPv6, wobei es sich bei dem Subnetz entweder um ein Dual-Stack-Subnetz oder nur um IPv6 handelt.

Derzeit unterstützen nur die AWS SDKs AWS CLI und die Aktivierung des IMDS-IPv6-Endpunkts nach dem Start der Instanz.

AWS CLI

Um den IMDS-IPv6-Endpunkt für Ihre Instance zu aktivieren

Verwenden Sie den CLI-Befehl modify-instance-metadata-options und setzen Sie den Parameter `http-protocol-ipv6` auf `enabled`. Beachten Sie, dass Sie beim Angeben eines Werts für `http-protocol-ipv6` auch `http-endpoint` auf `enabled` setzen müssen.

```
aws ec2 modify-instance-metadata-options \
 --instance-id i-1234567898abcdef0 \
 --http-protocol-ipv6 enabled \
 --http-endpoint enabled
```

PowerShell

Um den IMDS-IPv6-Endpunkt für Ihre Instance zu aktivieren

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den Parameter auf. `HttpProtocolIpv6` `enabled` Beachten Sie, dass Sie beim Angeben eines Werts für `HttpProtocolIpv6` auch `HttpEndpoint` auf `enabled` setzen müssen.

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpProtocolIpv6 enabled `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Aktivieren des Zugriffs auf Instance-Metadaten

Sie können den Zugriff auf Instance-Metadaten aktivieren, indem Sie den HTTP-Endpunkt des IMDS auf Ihrer Instance aktivieren, unabhängig davon, welche Version des IMDS Sie verwenden. Sie können diese Änderung jederzeit rückgängig machen, indem Sie den HTTP-Endpunkt deaktivieren.

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf Instance-Metadaten für eine Instance zu aktivieren.

Console

So aktivieren Sie den Zugriff auf Instance-Metadaten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Führen Sie im Dialogfeld Instance-Metadatenoptionen ändern Folgendes aus:
   a. Für den Instance-Metadatenservice wählen Sie die Option Aktivieren.
   b. Wählen Sie Speichern.

AWS CLI

So aktivieren Sie den Zugriff auf Instance-Metadaten

Verwenden Sie den CLI-Befehl modify-instance-metadata-options und setzen Sie den Parameter `http-endpoint` auf `enabled`.

```
aws ec2 modify-instance-metadata-options \
```

```
    --instance-id i-1234567898abcdef0 \
    --http-endpoint enabled
```

PowerShell

So aktivieren Sie den Zugriff auf Instance-Metadaten

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den Parameter auf. `HttpEndpoint` `enabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint enabled).InstanceMetadataOptions
```

Deaktivieren des Zugriffs auf Instance-Metadaten

Sie können den Zugriff auf Instance-Metadaten deaktivieren, indem Sie den HTTP-Endpunkt des IMDS auf Ihrer Instance deaktivieren, unabhängig davon, welche Version des IMDS Sie verwenden. Sie können diese Änderung jederzeit rückgängig machen, indem Sie den HTTP-Endpunkt aktivieren.

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf Instance-Metadaten für eine Instance zu deaktivieren.

Console

So deaktivieren Sie den Zugriff auf Instance-Metadaten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus.
4. Wählen Sie Aktionen, Instance-Einstellungen und Instance-Metadata-Optionen ändern.
5. Führen Sie im Dialogfeld Instance-Metadatenoptionen ändern Folgendes aus:
    a. Für den Instance-Metadatenservice entfernen Sie die Option Aktivieren.
    b. Wählen Sie Speichern.

AWS CLI

So deaktivieren Sie den Zugriff auf Instance-Metadaten

Verwenden Sie den CLI-Befehl modify-instance-metadata-options und setzen Sie den Parameter `http-endpoint` auf `disabled`.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-1234567898abcdef0 \
    --http-endpoint disabled
```

PowerShell

So deaktivieren Sie den Zugriff auf Instance-Metadaten

Verwenden Sie das Edit-EC2InstanceMetadataOptionCmdlet und setzen Sie den Parameter auf. `HttpEndpoint` `disabled`

```
(Edit-EC2InstanceMetadataOption `
    -InstanceId i-1234567898abcdef0 `
    -HttpEndpoint disabled).InstanceMetadataOptions
```

Abrufen von Instance-Metadaten

Da Ihre Instance-Metadaten von der ausgeführten Instance verfügbar sind, müssen Sie nicht die Amazon-EC2-Konsole oder die AWS CLI verwenden. Dies kann sehr hilfreich sein, wenn Sie ein Skript schreiben möchten, das in der Instance ausgeführt werden soll. So können Sie z. B. über die Instance-Metadaten auf die lokale IP-Adresse Ihrer Instance zugreifen, um die Verbindung zu einer externen Anwendung zu verwalten.

Instance-Metadaten werden in vier Kategorien unterteilt. Eine Beschreibung der einzelnen Instance-Metadatenkategorien finden Sie unter Instance-Metadatenkategorien.

Um alle Kategorien von Instance-Metadaten innerhalb einer laufenden Instance anzuzeigen, verwenden Sie die folgenden Pv4- oder IPv6-URIs.

IPv4

```
http://169.254.169.254/latest/meta-data/
```

IPv6

```
http://[fd00:ec2::254]/latest/meta-data/
```

Die IP-Adressen sind lokale Adressen (Link-local Addresses) und nur von der Instance aus gültig. Weitere Informationen finden Sie unter Link-lokale Adressen in diesem Benutzerhandbuch und unter Link-Local-Adresse auf Wikipedia.

> **Note**
>
> In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des IMDS verwendet: `169.254.169.254`. Wenn Sie Zeit Instance-Metadaten für EC2-Instances über die IPv6-Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6-Adresse verwenden: `[fd00:ec2::254]`. Die IPv6-Adresse des IMDS ist mit IMDSv2-Befehlen kompatibel. Auf die IPv6-Adresse kann nur auf Instances zugegriffen werden, die auf dem AWS Nitro-System basieren, und in einem IPv6-unterstützten Subnetz (Dual-Stack oder nur IPv6).

Das Befehlsformat ist unterschiedlich, je nachdem, ob Sie IMDSv1 oder IMDSv2 verwenden. Standardmäßig können Sie beide Versionen des IMDS verwenden. Um die Verwendung von IMDSv2 zu erzwingen, lesen Sie IMDSv2 verwenden.

Um Instanz-Metadaten auf Linux-Instances abzurufen

Sie können ein Tool wie cURL verwenden (wie im folgenden Beispiel).

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
```

Um Instanz-Metadaten auf Windows-Instanzen abzurufen

Sie können PowerShell Cmdlets verwenden, um den URI abzurufen. Wenn Sie beispielsweise Version 3.0 oder höher von ausführen PowerShell, verwenden Sie das folgende Cmdlet.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method GET -Uri http://169.254.169.254/latest/meta-data/
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
```

Wenn Sie es nicht verwenden möchten PowerShell, können Sie ein Drittanbieter-Tool wie GNU Wget oder cURL installieren.

> **Important**
>
> Wenn Sie ein Drittanbieter-Tool in einer Windows-Instance installieren, sollten Sie die zugehörige Dokumentation unbedingt sorgfältig lesen; die Methode für den HTTP-Aufruf sowie das Ausgabeformat können von dieser Dokumentation abweichen.

Kosten

Beachten Sie, dass für HTTP-Anfragen für den Abruf von Instance-Metadaten und Benutzerdaten keine Gebühren berechnet werden.

Überlegungen

Um Probleme beim Abrufen von Instance-Metadaten zu vermeiden, sollten Sie Folgendes beachten:

- In einer Container-Umgebung empfehlen wir, das Hop-Limit auf 2 festzulegen.

  Die AWS SDKs verwenden standardmäßig IMDSv2-Aufrufe. Wenn der IMDSv2-Anruf keine Antwort erhält, versucht das SDK den Anruf erneut und verwendet IMDSv1, falls er immer noch nicht erfolgreich ist. Dies kann zu einer Verzögerung führen, insbesondere in einer Container-Umgebung. Wenn in einer Containerumgebung das Hop-Limit 1 beträgt, wird die IMDSv2-Antwort nicht zurückgegeben, da das Gehen zum Container als zusätzlicher Netzwerk-Hop gilt. Um zu vermeiden, dass der Prozess auf IMDSv1 zurückfällt und somit die daraus resultierende

Verzögerung vermeiden, empfehlen wir, dass Sie die Hop-Grenze in einer Containerumgebung auf 2 setzen. Weitere Informationen finden Sie unter Konfigurieren der Instance-Metadaten-Optionen.

- (Nur Windows) Erstellen Sie benutzerdefinierte AMIs mit Windows Sysprep.

  Um sicherzustellen, dass IMDS funktioniert, wenn Sie eine Instance von einem benutzerdefinierten Windows-AMI aus starten, muss es sich bei dem AMI um ein standardisiertes Image handeln, das mit Windows Sysprep erstellt wurde. Andernfalls funktioniert der IMDS nicht. Weitere Informationen finden Sie unter. Erstellen Sie ein AMI mit Windows Sysprep
- Für IMDSv2 müssen Sie **`/latest/api/token`** beim Abrufen des Tokens nutzen.

  Das Ausgeben von PUT-Anfragen an einen beliebigen versionsspezifischen Pfad, beispielsweise `/2021-03-23/api/token`, führt dazu, dass der Metadatenservice 403-Verboten-Fehler zurückgibt. Dieses Verhalten ist beabsichtigt.
- Wenn IMDSv2 erforderlich ist, funktioniert IMDSv1 nicht.

  Sie können wie folgt überprüfen, ob IMDSv2 für eine Instance erforderlich ist: Wählen Sie die Instance aus, um deren Details anzuzeigen, und überprüfen Sie den Wert für IMDSv2. Der Wert lautet entweder Erforderlich (nur IMDSv2 kann verwendet werden) oder Optional (IMDSv2 und IMDSv1 können verwendet werden).

Antworten und Fehlermeldungen

Alle Instance-Metadaten werden als Text zurückgegeben (HTTP-Inhaltstyp `text/plain`).

Eine Anfrage für eine spezifische Metadatenressource gibt den entsprechenden Wert oder einen HTTP-Fehlercode `404 - Not Found` zurück, wenn die Ressource nicht verfügbar ist.

Eine Anfrage für eine allgemeine Metadatenressource (der URI endet auf „/”) gibt eine Liste der verfügbaren Ressourcen oder einen HTTP-Fehlercode `404 - Not Found` zurück, wenn keine entsprechenden Ressourcen vorhanden sind. Die Listenelemente stehen jeweils in einer eigenen Zeile, d. h. sie sind durch Zeilenvorschübe (ASCII 10) getrennt.

Für Anfragen, die mit Instance-Metadatenservice Version 2 gestellt werden, können die folgenden HTTP-Fehlercodes zurückgegeben werden:

- `400 - Missing or Invalid Parameters` – Die PUT-Anfrage ist nicht gültig.
- `401 - Unauthorized` – Die GET-Anfrage verwendet ein ungültiges Token. Die empfohlene Aktion ist das Erzeugen eines neuen Token.

- `403 - Forbidden` – Die Anfrage ist nicht zulässig oder der IMDS ist deaktiviert.

Beispiele für das Abrufen von Instance-Metadaten

Die folgenden Beispiele enthalten Befehle, die Sie auf einer Amazon EC2 EC2-Instance verwenden können. Das Befehlsformat ist für Linux- und Windows-Instances unterschiedlich.

Beispiele

- Abrufen der verfügbaren Versionen der Instance-Metadaten
- Anfordern der Top-Level-Metadatenelemente
- Rufen Sie die Werte für Metadatenelemente ab
- Abrufen der Liste der verfügbaren öffentlichen Schlüssel
- Anzeigen der Formate, in denen der öffentliche Schlüssel 0 verfügbar ist
- Anfordern des öffentlichen Schlüssels 0 (im OpenSSH-Schlüsselformat)
- Anfordern der Subnetz-ID für eine Instance
- Abrufen von Instance-Tags für eine Instance

Abrufen der verfügbaren Versionen der Instance-Metadaten

In diesem Beispiel werden die verfügbaren Versionen der Instance-Metadaten abgerufen. Jede Version bezieht sich auf einen Instance-Metadaten-Build, wenn neue Instance-Metadatenkategorien veröffentlicht wurden. Die Build-Versionen der Instance-Metadaten korrelieren nicht mit den Amazon-EC2-API-Versionen. Es stehen frühere Versionen zur Verfügung, für den Fall dass Skripte angewendet werden, die auf den Strukturen und Daten dieser früheren Versionen aufbauen.

> **Note**
>
> Um zu vermeiden, dass Sie Ihren Code jedes Mal aktualisieren müssen, wenn Amazon EC2 einen neuen Instance-Metadaten-Build veröffentlicht, empfehlen wir, `latest` im Pfad zu verwenden, nicht die Versionsnummer. Verwenden Sie zum Beispiel `latest` wie folgt: `curl http://169.254.169.254/latest/meta-data/ami-id`

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
```

```
2015-10-20
2016-04-19
...
latest
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/
1.0
2007-01-19
2007-03-01
2007-08-29
2007-10-10
```

```
2007-12-15
2008-02-01
2008-09-01
2009-04-04
2011-01-01
2011-05-01
2012-01-12
2014-02-25
2014-11-05
2015-10-20
2016-04-19
...
latest
```

Anfordern der Top-Level-Metadatenelemente

In diesem Beispiel werden die Metadaten-Elemente der obersten Ebene abgerufen. Weitere Informationen zu den Elementen in der Antwort finden Sie unterInstance-Metadatenkategorien.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
```

```
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
events/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-life-cycle
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/
ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
iam/
instance-action
instance-id
instance-type
local-hostname
local-ipv4
mac
metrics/
network/
```

```
placement/
profile
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/
```

Rufen Sie die Werte für Metadatenelemente ab

In diesen Beispielen werden die Werte einiger der Metadatenelemente der obersten Ebene abgerufen, die im vorherigen Beispiel abgerufen wurden. Die IMDSv2-Anfragen verwenden das gespeicherte Token, das im vorhergehenden Beispielbefehl erstellt wurde (vorausgesetzt, es ist nicht abgelaufen).

Linux

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-id
```

```
ami-0abcdef1234567890
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Windows

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/reservation-id
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/local-hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/ami-id
ami-0abcdef1234567890
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/reservation-
id
```

```
r-0efghijk987654321
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/local-
hostname
ip-10-251-50-12.ec2.internal
```

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
hostname
ec2-203-0-113-25.compute-1.amazonaws.com
```

Abrufen der Liste der verfügbaren öffentlichen Schlüssel

In diesem Beispiel wird die Liste der verfügbaren öffentlichen Schlüssel abgerufen.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/
0=my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/
0=my-public-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/
```

```
0=my-public-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/ 0=my-public-key
```

Anzeigen der Formate, in denen der öffentliche Schlüssel 0 verfügbar ist

In diesem Beispiel werden die Formate abgerufen, in denen der öffentliche Schlüssel 0 verfügbar ist.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/
openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/
openssh-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
openssh-key
```

Anfordern des öffentlichen Schlüssels 0 (im OpenSSH-Schlüsselformat)

In diesem Beispiel wird der öffentliche Schlüssel 0 abgerufen (im Format für OpenSSH-Schlüssel).

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
```

```
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/public-
keys/0/openssh-key
ssh-rsa MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
```

```
MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE my-public-key
```

Anfordern der Subnetz-ID für eine Instance

In diesem Beispiel wird eine Subnetz-ID für eine Instance vergeben.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/network/interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -
Method GET -Uri http://169.254.169.254/latest/meta-data/network/interfaces/
macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/network/
interfaces/macs/02:29:96:8f:6a:2d/subnet-id
subnet-be9b61d7
```

Abrufen von Instance-Tags für eine Instance

In den folgenden Beispielen sind für die Beispiel-Instance Tags zu Instance-Metadaten und die Instance-Tags `Name=MyInstance` und `Environment=Dev` aktiviert.

In diesem Beispiel sind alle Instance-Tag-Schlüssel für eine Instance vorhanden.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/tags/instance
Name
Environment
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

Im folgenden Beispiel wird der Wert des `Name`-Schlüssel, der im obigen Beispiel erhalten wurde, angegeben. Die IMDSv2-Anfrage verwendet das gespeicherte Token, das im vorhergehenden Beispielbefehl erstellt wurde (vorausgesetzt, es ist nicht abgelaufen).

IMDSv2

```
[ec2-user ~]$ curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/
latest/meta-data/tags/instance/Name
MyInstance
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

Windows

IMDSv2

```
PS C:\> $token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds"
 = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/instance
Name
Environment
```

Im folgenden Beispiel wird der Wert des `Name`-Schlüssel, der im obigen Beispiel erhalten wurde, angegeben. Die IMDSv2-Anfrage verwendet das gespeicherte Token, das im vorhergehenden Beispielbefehl erstellt wurde (vorausgesetzt, es ist nicht abgelaufen).

IMDSv2

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/tags/instance/Name
MyInstance
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/tags/
instance/Name
MyInstance
```

Drosselung abfragen

Wir drosseln die Abfragen an den IMDS pro Instance und begrenzen die Anzahl gleichzeitiger Verbindungen von einer Instance zum IMDS.

Wenn Sie das IMDS zum Abrufen von AWS Sicherheitsanmeldeinformationen verwenden, vermeiden Sie es, bei jeder Transaktion oder gleichzeitig von einer großen Anzahl von Threads oder Prozessen aus nach Anmeldeinformationen zu fragen, da dies zu einer Drosselung führen kann. Wir empfehlen stattdessen, die Anmeldeinformationen im Cache zu speichern, bis sie sich ihrer Ablaufzeit nähern. Weitere Informationen über die IAM-Rolle und die der Rolle zugeordneten Sicherheitsanmeldeinformationen finden Sie unter Abrufen von Sicherheitsanmeldeinformationen aus Instance-Metadaten.

Wenn es beim Zugriff auf den IMDS zu einer Drosselung kommt, versuchen Sie Ihre Abfrage mit einer exponentiellen Backoff-Strategie erneut.

Begrenzen des IMDS-Zugriffs

Sie können die Verwendung lokaler Firewall-Regeln in Betracht ziehen, um den Zugriff auf den IMDS für einige oder alle Prozesse zu deaktivieren.

> **Note**
>
> Bei Instances, die auf dem AWS Nitro-System basieren, kann das IMDS von Ihrem eigenen Netzwerk aus erreicht werden, wenn eine Netzwerk-Appliance innerhalb Ihrer VPC, z. B. ein virtueller Router, Pakete an die IMDS-Adresse weiterleitet und die standardmäßige Quell-/Zielprüfung für die Instance deaktiviert ist. Um zu verhindern, dass eine Quelle von außerhalb Ihrer VPC den IMDS erreicht, empfehlen wir Ihnen, die Konfiguration der Netzwerk-Appliance so zu ändern, dass Pakete mit der IPv4-Zieladresse des IMDS `169.254.169.254` und, falls Sie den IPv6-Endpunkt aktiviert haben, der IPv6-Adresse des IMDS verworfen werden. `[fd00:ec2::254]`

Linux

Verwendung von iptables zur Einschränkung des Zugriffs

Das folgende Beispiel verwendet Linux-iptables und sein `owner`-Modul, um zu verhindern, dass der Apache-Webserver (basierend auf seiner Standardinstallationsbenutzer-ID von `apache`) auf 169.254.169.254 zugreift. Es verwendet eine Verweigerungsregel, um alle Instance-Metadatenanfragen (ob IMDSv1 oder IMDSv2) von jedem Prozess abzulehnen, der als dieser Benutzer ausgeführt wird.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match owner
 --uid-owner apache --jump REJECT
```

Oder Sie können erwägen, nur bestimmten Benutzern oder Gruppen Zugriff zu gewähren, indem Sie Zulassungsregeln verwenden. Zulassungsregeln können aus Sicherheitssicht einfacher zu verwalten sein, da Sie eine Entscheidung darüber treffen müssen, welche Software Zugriff auf Instance-Metadaten benötigt. Wenn Sie Zulassungsregeln verwenden, ist es weniger wahrscheinlich, dass Sie Software versehentlich den Zugriff auf den Metadaten-Service erlauben (auf den sie nicht zugreifen soll), wenn Sie später die Software oder Konfiguration auf einer Instance ändern. Sie können außerdem Gruppen mit Zulassungsregeln kombinieren, sodass Sie Benutzer zu einer zugelassenen Gruppe hinzufügen und aus dieser entfernen können, ohne die Firewall-Regel ändern zu müssen.

Das folgende Beispiel verhindert den Zugriff auf den IMDS durch alle Prozesse, mit Ausnahme von Prozessen, die im Benutzerkonto `trustworthy-user` ausgeführt werden.

```
$ sudo iptables --append OUTPUT --proto tcp --destination 169.254.169.254 --match
 owner ! --uid-owner trustworthy-user --jump REJECT
```

> **Note**
>
> - Um lokale Firewall-Regeln zu verwenden, müssen Sie die vorhergehenden Beispielbefehle an Ihre Bedürfnisse anpassen.
> - Standardmäßig sind iptables-Regeln nicht über Systemneustarts hinweg persistent. Sie können durch die Verwendung von Betriebssystemfeatures, die hier nicht beschrieben werden, persistent gestaltet werden.

- Das iptables `owner`-Modul überprüft nur dann die Gruppenzugehörigkeit, wenn die Gruppe die Primärgruppe eines bestimmten lokalen Benutzers ist. Andere Gruppen werden nicht abgeglichen.

Verwendung von PF oder IPFW zur Einschränkung des Zugriffs

Wenn Sie FreeBSD oder OpenBSD verwenden, können Sie PF oder IPFW verwenden. Die folgenden Beispiele beschränken den Zugriff auf den IMDS auf den Root-Benutzer.

PF

```
$ block out inet proto tcp from any to 169.254.169.254
```

```
$ pass out inet proto tcp from any to 169.254.169.254 user root
```

IPFW

```
$ allow tcp from any to 169.254.169.254 uid root
```

```
$ deny tcp from any to 169.254.169.254
```

> **Note**
>
> Die Reihenfolge der PF- und IPFW-Befehle ist von Bedeutung. PF verwendet standardmäßig die letzte übereinstimmende Regel und IPFW die erste übereinstimmende Regel.

Windows

Verwenden der Windows-Firewall zur Zugriffsbeschränkung

Im folgenden PowerShell Beispiel wird die integrierte Windows-Firewall verwendet, um zu verhindern, dass der Internet Information Server-Webserver (basierend auf seiner standardmäßigen Installationsbenutzer-ID von) auf 169.254.169.254 zugreift. `NT AUTHORITY\IUSR` Es verwendet eine Verweigerungsregel, um alle Instance-Metadatenanfragen (ob IMDSv1 oder IMDSv2) von jedem Prozess abzulehnen, der als dieser Benutzer ausgeführt wird.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount ("NT
 AUTHORITY\IUSR")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $BlockPrincipalSDDL = "D:(A;;CC;;;$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service from IIS" -Action
 block -Direction out `
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $BlockPrincipalSDDL
```

Oder Sie können erwägen, nur bestimmten Benutzern oder Gruppen Zugriff zu gewähren, indem Sie Zulassungsregeln verwenden. Zulassungsregeln können aus Sicherheitssicht einfacher zu verwalten sein, da Sie eine Entscheidung darüber treffen müssen, welche Software Zugriff auf Instance-Metadaten benötigt. Wenn Sie Zulassungsregeln verwenden, ist es weniger wahrscheinlich, dass Sie Software versehentlich den Zugriff auf den Metadaten-Service erlauben (auf den sie nicht zugreifen soll), wenn Sie später die Software oder Konfiguration auf einer Instance ändern. Sie können außerdem Gruppen mit Zulassungsregeln kombinieren, sodass Sie Benutzer zu einer zugelassenen Gruppe hinzufügen und aus dieser entfernen können, ohne die Firewall-Regel ändern zu müssen.

Das folgende Beispiel verhindert den Zugriff auf Instance-Metadaten durch alle Prozesse, die als OS-Gruppe ausgeführt werden, die in der Variable `blockPrincipal` angegeben ist (in diesem Beispiel die Windows-Gruppe `Everyone`), mit Ausnahme der in `exceptionPrincipal` angegebenen Prozesse (in diesem Beispiel eine Gruppe namens `trustworthy-users`). Sie müssen für Prinzipale den Zugriff verweigern und ablehnen, da die Windows-Firewall im Gegensatz zur `! --uid-owner trustworthy-user`-Regel in Linux-iptables keinen Mechanismus zur Verfügung stellt, um nur einen bestimmten Prinzipal (Benutzer oder Gruppe) zuzulassen, indem alle anderen abgelehnt werden.

```
PS C:\> $blockPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("Everyone")
PS C:\> $BlockPrincipalSID =
 $blockPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $exceptionPrincipal = New-Object -TypeName System.Security.Principal.NTAccount
 ("trustworthy-users")
PS C:\> $ExceptionPrincipalSID =
 $exceptionPrincipal.Translate([System.Security.Principal.SecurityIdentifier]).Value
PS C:\> $PrincipalSDDL = "O:LSD:(D;;CC;;;$ExceptionPrincipalSID)(A;;CC;;;
$BlockPrincipalSID)"
PS C:\> New-NetFirewallRule -DisplayName "Block metadata service for
 $($blockPrincipal.Value), exception: $($exceptionPrincipal.Value)" -Action block -
Direction out `
```

```
-Protocol TCP -RemoteAddress 169.254.169.254 -LocalUser $PrincipalSDDL
```

> **Note**
>
> Um lokale Firewall-Regeln zu verwenden, müssen Sie die vorhergehenden Beispielbefehle an Ihre Bedürfnisse anpassen.

Verwenden von netsh-Regeln zur Zugriffsbeschränkung

Sie können erwägen, die gesamte Software mit `netsh`-Regeln zu blockieren. Diese sind jedoch viel weniger flexibel.

```
C:\> netsh advfirewall firewall add rule name="Block metadata service altogether"
 dir=out protocol=TCP remoteip=169.254.169.254 action=block
```

> **Note**
>
> - Um lokale Firewall-Regeln zu verwenden, müssen Sie die vorhergehenden Beispielbefehle an Ihre Bedürfnisse anpassen.
> - `netsh`-Regeln müssen von einer Eingabeaufforderung mit erhöhten Rechten aus festgelegt werden und können nicht so konfiguriert werden, dass sie bestimmte Prinzipale verweigern oder zulassen.

Arbeiten mit Instance-Benutzerdaten

Sie können Instance-Benutzerdaten verwenden, um Ihre Instances anzupassen. Wenn Sie eine Instance starten, können Sie Parameter oder Skripts als Benutzerdaten speichern. Alle Skripts in Benutzerdaten werden beim Start der Instance ausgeführt. Sie können Benutzerdaten als Instance-Attribut anzeigen. Sie können Benutzerdaten aus Ihrer Instance auch über den Instance Metadata Service (IMDS) anzeigen.

Überlegungen

- Benutzerdaten werden als Opaque-Daten behandelt: Was Sie eingeben, wird auch ausgegeben. Die Interpretation der Daten ist Aufgabe der Instance.

- Benutzerdaten müssen mit Base64 codiert werden. Die Amazon EC2-Konsole kann die base64-Codierung für Sie durchführen oder base64-codierte Eingaben entgegennehmen.
- Benutzerdaten sind auf 16 KB an Rohdaten, bevor diese base64-codiert werden, begrenzt. Die Länge einer Zeichenfolge n nach base64-Codierung ist ceil(n/3)*4.
- Benutzerdaten müssen base64-decodiert werden, wenn Sie sie abrufen. Wenn Sie die Daten über Instance-Metadaten oder die Konsole abrufen, werden sie automatisch für Sie dekodiert.
- Wenn Sie eine Instance anhalten, ihre Benutzerdaten ändern und die Instance wieder starten, werden die aktualisierten Benutzerdaten nicht automatisch ausgeführt, wenn Sie die Instance starten. Bei Windows-Instanzen können Sie Einstellungen so konfigurieren, dass aktualisierte Benutzerdatenskripts einmal ausgeführt werden, wenn Sie die Instanz starten oder bei jedem Neustart oder Start der Instanz.
- Benutzerdaten sind ein Instance-Attribut. Wenn Sie ein AMI auf der Grundlage einer Instance erstellen, sind die Instance-Benutzerdaten nicht im AMI enthalten.

Angeben von Instance-Benutzerdaten beim Start

Sie können Benutzerdaten angeben, wenn Sie eine Instance starten. Eine Anleitung für die Konsole finden Sie unter Angeben von Instance-Benutzerdaten beim Start. Ein Linux-Beispiel, das den verwendet AWS CLI, finden Sie unterthe section called “Benutzerdaten und die AWS CLI”. Ein Windows-Beispiel, das die Tools für Windows verwendet PowerShell, finden Sie unterthe section called “Benutzerdaten und die Tools für Windows PowerShell”.

Ändern von Instance-Benutzerdaten

Sie können Benutzerdaten für Instances mit einem EBS-Stamm-Volume ändern. Die Instances muss angehalten werden. Eine Anleitung für die Konsole finden Sie unter Anzeigen und Aktualisieren der Instance-Benutzerdaten. Ein Linux-Beispiel, das das verwendet AWS CLI, finden Sie unter modify-instance-attribute. Ein Windows-Beispiel, das die Tools für Windows verwendet, finden Sie unter. PowerShell the section called “Benutzerdaten und die Tools für Windows PowerShell”

Abrufen von Instance-Benutzerdaten aus Ihrer Instance

> **Note**
>
> In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des IMDS verwendet: `169.254.169.254`. Wenn Sie Zeit Instance-Metadaten für EC2-Instances über die IPv6-Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6-Adresse verwenden:

`[fd00:ec2::254]`. Die IPv6-Adresse des IMDS ist mit IMDSv2-Befehlen kompatibel. Auf die IPv6-Adresse kann nur auf Instances zugegriffen werden, die auf dem AWS Nitro-System basieren, und in einem IPv6-unterstützten Subnetz (Dual-Stack oder nur IPv6).

Verwenden Sie den folgenden URI, um Benutzerdaten aus einer Instance abzurufen.

```
http://169.254.169.254/latest/user-data
```

Eine Anfrage für Benutzerdaten geben die Daten unverändert zurück (Content-Type `application/octet-stream`). Wenn die Instance keine Benutzerdaten hat, gibt die Anfrage `404 - Not Found` zurück.

Dieses Beispiel gibt Benutzerdaten zurück, die als kommagetrennter Text angegeben wurden.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/user-data
```

```
1234,john,reboot,true | 4512,richard, | 173,,,
```

IMDSv1

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = Invoke-RestMethod
 -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} `
-Method PUT -Uri http://169.254.169.254/latest/api/token} -Method GET -uri
 http://169.254.169.254/latest/user-data
1234,john,reboot,true | 4512,richard, | 173,,,
```

Dieses Beispiel gibt Benutzerdaten zurück, die als Skript bereitgestellt wurden.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/user-
data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/user-data
#!/bin/bash
yum update -y
service httpd start
chkconfig httpd on
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-
seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/user-data
<powershell>
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Abrufen von Instance-Benutzerdaten von Ihrem Computer

Sie können Benutzerdaten für eine Instance von Ihrem eigenen Computer abrufen. Eine Anleitung für die Konsole finden Sie unter Anzeigen und Aktualisieren der Instance-Benutzerdaten. Ein Beispiel, das die verwendet, finden Sie unter. AWS CLIBenutzerdaten und die AWS CLI Ein Beispiel, das die Tools für Windows verwendet PowerShell, finden Sie unterBenutzerdaten und die Tools für Windows PowerShell.

Abrufen von dynamischen Daten

Um dynamische Daten aus einer laufenden Instance abzurufen, verwenden Sie die folgende URI.

```
http://169.254.169.254/latest/dynamic/
```

> **Note**
>
> In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des IMDS verwendet: `169.254.169.254`. Wenn Sie Zeit Instance-Metadaten für EC2-Instances über die IPv6-Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6-Adresse verwenden: `[fd00:ec2::254]`. Die IPv6-Adresse des IMDS ist mit IMDSv2-Befehlen kompatibel. Auf

die IPv6-Adresse kann nur auf Instances zugegriffen werden, die auf dem AWS Nitro-System basieren, und in einem IPv6-unterstützten Subnetz (Dual-Stack oder nur IPv6).

Dieses Beispiel zeigt, wie man die High-Level-Instance-Identitätskategorien abruft.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/dynamic/instance-identity/
rsa2048
pkcs7
document
signature
dsa2048
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/dynamic/instance-identity/
document
rsa2048
```

```
pkcs7
signature
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/dynamic/instance-
identity/
document
rsa2048
pkcs7
signature
```

Weitere Informationen zu dynamischen Daten und Beispiele dafür, wie sie abgerufen werden können, finden Sie unter Instance-Identitätsdokumente.

Instance-Metadatenkategorien

Instance-Metadaten werden in vier Kategorien unterteilt. Um Instance-Metadaten abzurufen, geben Sie die Kategorie in der Anfrage an, und die Metadaten werden in der Antwort zurückgegeben.

Wenn neue Kategorien veröffentlicht werden, wird ein neuer Instance-Metadaten-Build mit einer neuen Versionsnummer erstellt. In der folgenden Tabelle wird in der Spalte Version, als die Kategorie veröffentlicht wurde die Build-Version angegeben, als die Instance-Metadatenkategorie freigegeben wurde. Um zu vermeiden, dass Sie Ihren Code jedes Mal aktualisieren müssen, wenn Amazon EC2 einen neuen Instance-Metadaten-Build veröffentlicht, verwenden Sie `latest` in Ihren Metadaten-Anfragen, nicht die Versionsnummer. Weitere Informationen finden Sie unter Abrufen der verfügbaren Versionen der Instance-Metadaten.

Wenn Amazon EC2 eine neue Instance-Metadatenkategorie veröffentlicht, sind die Instance-Metadaten für die neue Kategorie möglicherweise nicht für vorhandene Instances verfügbar. Bei Instances, die auf dem Nitro-System erstellt wurden, können Sie Instance-Metadaten nur für die Kategorien abrufen, die beim Start verfügbar waren. Bei Instances mit dem Xen-Hypervisor können Sie die Instance stoppen und dann starten, um die für die Instance verfügbaren Kategorien zu aktualisieren.

In der folgenden Tabelle werden die Kategorien von Instance-Metadaten aufgeführt. Einige der Kategorienamen enthalten Platzhalter für Daten, die für Ihre Instance eindeutig sind.. *Mac* stellt beispielsweise die MAC-Adresse für die Netzwerkschnittstelle dar. Sie müssen die Platzhalter durch tatsächliche Werte ersetzen, wenn Sie die Instance-Metadaten abrufen.

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`ami-id`	Die für den Start der Instance verwendete AMI-ID	1,0
`ami-launch-index`	Wenn Sie mehrere Instances mit demselben `RunInstances` Aufruf starten, gibt dieser Wert die Startreihenfolge für jede Instance an. Der Wert für die zuerst gestartete Instance ist 0. Wenn Sie Instances mit Auto Scaling oder EC2-Flotte starten, ist dieser Wert immer 0.	1,0
`ami-manifest-path`	Der Pfad zu der AMI-Manif estdatei in Amazon S3. Wenn Sie für den Start der Instance ein Amazon EBS-Backed AMI verwendet haben, wird als Ergebnis ausgegebe `unknown`.	1,0
`ancestor-ami-ids`	Die AMI-IDs aller Instances, die für die Erstellung dieses AMIs gebündelt wurden. Dieser Wert ist nur vorhanden, wenn die AMI-Manifestdatei einen `ancestor-amis` -Schlüssel enthalten hat.	2007-10-10
`autoscaling/target-lifecycle-state`	Wert, der den Zielzustand des Auto-Scaling-Lebenszyklus anzeigt, in den eine Auto-Scaling-Instance übergeht. Wird verwendet , wenn die Instance nach dem 10. März 2022 in einen der Ziel-Lebe	15.07.2021

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
	nszyklusstatus wechselt. Mögliche Werte: `Detached` | `InService` | `Standby` | `Terminated` | `Warmed:Hibernated` | `Warmed:Running` | `Warmed:Stopped` | `Warmed:Terminated` . Siehe Abrufen des Zielleben szyklusstatus durch Instance-Metadaten im Benutzerhandbuch für Amazon EC2 Auto Scaling.	
`block-device-mapping/ami`	Das virtuelle Gerät, auf dem sich das Root- bzw. Boot-Dateisystem befindet	2007-12-15
`block-device-mapping/ebs` N	Die virtuellen Geräte, die mit einem Amazon EBS-Volume verknüpft sind. Amazon EBS-Volumes sind nur in Metadaten enthalten, wenn sie beim Starten der Instance – oder als die Instance zuletzt gestartet wurde – vorhanden waren. N zeigt dabei den Index für das Amazon EBS-Volume an (z. B. `ebs1` oder `ebs2`).	2007-12-15

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`block-device-mapping/ephemeral` N	Die virtuellen Geräte für alle Nicht-NVMe-Instance-Speicher-Volumes. N gibt den Index jedes Volumes an. Die Anzahl der Instance-Speicher-Volumes in der Blockgerät-Zuweisung entspricht möglicherweise nicht der tatsächlichen Anzahl der Instance-Speicher-Volumes für die Instance. Der Instance-Typ bestimmt die Anzahl der Instance-Speicher-Volumes, die für eine Instance verfügbar sind. Wenn die Anzahl der Instance-Speicher-Volumes in einer Blockgerät-Zuweisung die für eine Instance verfügbare Anzahl übersteigt, werden die überzähligen Instance-Speicher-Volumes ignoriert.	2007-12-15
`block-device-mapping/root`	Die virtuellen Laufwerke oder Partitionen, die den Root-Laufwerken oder Partitionen auf dem virtuellen Laufwerk zugeordnet sind, wobei das Root-Dateisystem (/ oder C:) der angegebenen Instance zugeordnet ist.	2007-12-15
`block-device-mapping/swap`	Die virtuellen Geräte, die mit `swap` verknüpft sind. Nicht immer vorhanden.	2007-12-15

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`elastic-gpus/associations/` *`elastic-gpu-id`*	Wenn eine Elastische GPU an die Instance angefügt ist, ist eine JSON-Zeichenkette mit Informationen über die Elastische GPU, einschließlich ihrer ID und Verbindungsinformationen enthalten.	30.11.2016
`elastic-inference/associations/` *`eia-id`*	Enthält eine JSON-Zeichenfolge mit Informationen zum Elastic Inference Accelerator einschließlich ID und Typ, wenn der Instance ein Elastic Interference Accelerator angefügt ist.	2018-11-29
`events/maintenance/history`	Enthält eine JSON-Zeichenfolge mit Informationen zu den Ereignissen, wenn es abgeschlossene oder abgebrochene Wartungsereignisse für die Instance gibt. Weitere Informationen finden Sie unter So zeigen Sie den Ereignisverlauf für abgeschlossene oder abgebrochene Ereignisse an.	2018-08-17
`events/maintenance/scheduled`	Enthält eine JSON-Zeichenfolge mit Informationen zu den Ereignissen, wenn es aktive Wartungsereignisse für die Instance gibt. Weitere Informationen finden Sie unter Anzeigen geplanter Ereignisse.	2018-08-17

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`events/recommendations/rebalance`	Die ungefähre Zeit in UTC, zu der die Empfehlungsbenachrichtigung des EC2-Instance-Neuausgleichs für die Instance ausgesendet wird. Das Folgende ist ein Beispiel für die Metadaten für diese Kategorie: `{"noticeTime": "2020-11-05T08:22:00Z"}` . Diese Kategorie ist erst verfügbar, nachdem die Benachrichtigung gesendet wurde. Weitere Informationen finden Sie unter Empfehlung zum Neuausgleich einer EC2-Instance.	27.10.2020
`hostname`	Wenn die EC2-Instance die IP-basierte Benennung (IPBN) verwendet, ist dies der private IPv4-DNS-Hostname der Instance. Wenn die EC2-Instance die ressourcenbasierte Benennung (RBN) verwendet, ist dies der RBN. Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0). Weitere Informationen zu IPBN und RBN finden Sie unter Hostnamentypen für Amazon-EC2-Instances.	1,0

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`iam/info`	Wenn der Instance eine IAM-Rolle zugeordnet ist, enthält es Informationen darüber, wann das Instanzprofil zuletzt aktualisiert wurde, einschließlich LastUpdated Datum und ID der Instanz. InstanceProfileArn InstanceProfile Andernfalls nicht vorhanden.	2012-01-12
`iam/security-credentials/role-name`	Wenn eine IAM-Rolle mit der Instance verknüpft ist, steht *`role-name`* für den Namen der Rolle; außerdem enthält *`role-name`* die temporären Sicherheitsanmeldeinformationen für die Rolle (weitere Informationen finden Sie unter Abrufen von Sicherheitsanmeldeinformationen aus Instance-Metadaten). Andernfalls nicht vorhanden.	2012-01-12
`identity-credentials/ec2/info`	Informationen zu den Anmeldeinformationen in `identity-credentials/ec2/security-credentials/ec2-instance` .	2018-05-23

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`identity-credentials/ec2/security-credentials/ec2-instance`	Anmeldeinformationen für die Instance-Identitätsrolle, die es der On-Instance-Software ermöglichen, sich selbst zu identifizieren AWS , um Funktionen wie EC2 Instance Connect und AWS Systems Manager Standard-Host-Management-Konfiguration zu unterstützen. An diese Anmeldeinformationen sind keine Richtlinien angehängt, sodass sie über keine zusätzlichen AWS API-Berechtigungen verfügen, die über die Identifizierung der Instance für die Funktion hinausgehen. AWS Weitere Informationen finden Sie unter Instance-Identitätsrollen.	2018-05-23
`instance-action`	Weist die Instance an, zur Vorbereitung einer Bündelung einen Neustart durchzuführen. Zulässige Werte: `none` | `shutdown` | `bundle-pending` .	2008-09-01
`instance-id`	Die ID dieser Instance	1,0
`instance-life-cycle`	Die Kaufoption dieser Instance. Weitere Informationen finden Sie unter Instance-Kaufoptionen.	01.10.2019

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`instance-type`	Der Typ der Instance. Weitere Informationen finden Sie unter Amazon EC2-Instance-Typen.	2007-08-29
`ipv6`	Die IPv6-Adresse der Instance. In Fällen, in denen mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dies auf die Netzwerkschnittstelle des eth0-Geräts (das Gerät, dessen Gerätenummer 0 ist) und die erste zugewiesene IPv6-Adresse. Wenn auf der Netzwerkschnittstelle keine IPv6-Adresse vorhanden ist [0], ist dieses Element nicht festgeleg t und führt zu einer HTTP-404-Antwort.	2021-01-03
`kernel-id`	Die ID des mit dieser Instance gestarteten Kernels (falls zutreffen d)	2008-02-01

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`local-hostname`	Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0). Wenn die EC2-Instance die IP-basierte Benennung (IPBN) verwendet, ist dies der private IPv4-DNS-Hostname der Instance. Wenn die EC2-Instance die ressourcenbasierte Benennung (RBN) verwendet, ist dies der RBN. Weitere Informationen zur Benennung von IPBN-, RBN- und EC2-Instances finden Sie unter Hostnamentypen für Amazon-EC2-Instances.	2007-01-19
`local-ipv4`	Die private IPv4-Adresse der Instance. Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0). Wenn es sich um eine reine IPv6-Instance handelt, wird dieses Element nicht festgelegt und führt zu einer HTTP-404-Antwort.	1,0

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`mac`	Die Media Access Control-Adresse (MAC) der Instance. Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0).	01.01.2011
`metrics/vhostmd`	Nicht mehr verfügbar.	2011-05-01
`network/interfaces/macs/mac/device-number`	Die eindeutige Gerätenummer, die mit dieser Schnittstelle verknüpft ist. Die Gerätenummer entspricht dem Gerätenamen; `device-number` 2 steht z. B. für das Gerät eth2. Diese Kategorie entspricht den Feldern `DeviceIndex` und `device-index` , die von der Amazon EC2 API und den EC2-Befehlen für die AWS CLI verwendet werden.	01.01.2011
`network/interfaces/macs/mac/interface-id`	Die ID der Netzwerkschnittstelle.	01.01.2011
`network/interfaces/macs/mac/ipv4-associations/public-ip`	Die privaten IPv4-Adressen, die mit jeder öffentlichen IP-Adresse verknüpft und dieser Netzwerkschnittstelle zugewiesen sind.	01.01.2011
`network/interfaces/macs/mac/ipv6s`	Die der Schnittstelle zugewiesenen IPv6-Adressen.	2016-06-30

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`network/interfaces/macs/mac/ipv6-prefix`	Das der Netzwerkschnittstelle zugewiesene IPv6-Präfix.	
`network/interfaces/macs/mac/local-hostname`	Der private IPv4-DNS-Hostname der Instance. Wenn mehrere Netzwerkschnittstellen vorhanden sind, bezieht sich dieser Wert auf das Gerät eth0 (das Gerät mit der Gerätenummer 0). Wenn es sich um eine reine IPv6-Instance handelt, ist dies der ressourcenbasierte Name. Weitere Informationen zu IPBN und RBN finden Sie unter Hostnamentypen für Amazon-EC2-Instances.	2007-01-19
`network/interfaces/macs/mac/local-ipv4s`	Die privaten IPv4-Adressen, die mit der Netzwerkschnittstelle verknüpft sind Wenn es sich um eine reine IPv6-Netzwerkschnittstelle handelt, wird dieses Element nicht festgelegt und führt zu einer HTTP-404-Antwort.	01.01.2011
`network/interfaces/macs/mac/mac`	Die MAC-Adresse der Instance	01.01.2011
`network/interfaces/macs/`*`mac`*`/network-card`	Der Index der Netzwerkkarte. Einige Instance-Typen unterstützen mehrere Netzwerkkarten.	01.11.2020

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`network/interfaces/macs/mac/owner-id`	Die ID des Eigentümers der Netzwerkschnittstelle. In Umgebungen mit mehreren Schnittstellen kann eine Schnittstelle von einem Drittanbieter wie Elastic Load Balancing zugewiesen werden. Der Datenverkehr auf einer Schnittstelle wird immer dem Eigentümer der Schnittstelle in Rechnung gestellt.	01.01.2011
`network/interfaces/macs/mac/public-hostname`	Der öffentliche DNS-Name (IPv4) der Schnittstelle. Diese Kategorie wird nur ausgegeben, wenn das Attribut `enableDnsHostnames` auf `true` gesetzt ist. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch. Wenn die Instance nur eine Public-IPv6-Adresse und keine Public-IPv4-Adresse hat, wird dieses Element nicht festgelegt und führt zu einer HTTP-404-Antwort.	01.01.2011
`network/interfaces/macs/mac/public-ipv4s`	Die öffentliche IP-Adresse oder die Elastic IP-Adressen, die dem Adapter zugeordnete sind. Es können mehrere IPv4-Adressen zu einer Instance gehören.	01.01.2011

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`network/interfaces/macs/mac/security-groups`	Sicherheitsgruppen, zu denen die Netzwerkschnittstelle gehört.	01.01.2011
`network/interfaces/macs/mac/security-group-ids`	Die IDs der Sicherheitsgruppen, zu denen die Netzwerkschnittstelle gehört.	01.01.2011
`network/interfaces/macs/mac/subnet-id`	Die ID für das Subnetz, in der sich die Schnittstelle befindet.	01.01.2011
`network/interfaces/macs/mac/subnet-ipv4-cidr-block`	Der IPv4-CIDR-Block für das Subnetz, in der sich die Schnittstelle befindet.	01.01.2011
`network/interfaces/macs/mac/subnet-ipv6-cidr-blocks`	Der IPv6-CIDR-Block für das Subnetz, in der sich die Schnittstelle befindet.	2016-06-30
`network/interfaces/macs/mac/vpc-id`	Die ID für die VPC, in der sich die Schnittstelle befindet.	01.01.2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-block`	Der primäre IPv4 CIDR-Block der VPC.	01.01.2011
`network/interfaces/macs/mac/vpc-ipv4-cidr-blocks`	Die IPv4 CIDR-Blöcke für die VPC	2016-06-30
`network/interfaces/macs/mac/vpc-ipv6-cidr-blocks`	Der IPv6-CIDR-Block für die VPC, in der sich die Schnittstelle befindet.	2016-06-30

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`placement/availability-zone`	Die Availability Zone, in der die Instance gestartet wurde	2008-02-01
`placement/availability-zone-id`	Die statische Availability Zone-ID, in der die Instance gestartet wird. Die Availability Zone-ID ist für alle Konten konsistent. Sie kann sich jedoch von der Availability Zone unterscheiden, die je nach Konto variieren kann.	01.10.2019
`placement/group-name`	Der Name der Platzierungsgruppe, in der die Instance gestartet wird.	24.08.2020
`placement/host-id`	Die ID des Hosts, auf dem die Instance gestartet wird. Gilt nur für Dedicated Hosts.	24.08.2020
`placement/partition-number`	Die Nummer der Partition, in der die Instance gestartet wird.	24.08.2020
`placement/region`	Die AWS Region, in der die Instance gestartet wird.	24.08.2020
`product-codes`	AWS Marketplace der Instance zugeordnete Produktcodes, falls vorhanden.	2007-03-01

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`public-hostname`	Das öffentliche DNS der Instance (IPv4). Diese Kategorie wird nur ausgegeben, wenn das Attribut `enableDnsHostnames` auf `true` gesetzt ist. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch. Wenn die Instance nur eine Public-IPv6-Adresse und keine Public-IPv4-Adresse hat, wird dieses Element nicht festgelegt und führt zu einer HTTP-404-Antwort.	2007-01-19
`public-ipv4`	Die öffentliche IPv4-Adresse. Wenn eine Elastic IP-Adresse mit der Instance verknüpft ist, ist der zurückgegebene Wert die Elastic IP-Adresse.	2007-01-19
`public-keys/0/openssh-key`	Der öffentliche Schlüssel. Nur verfügbar, wenn bei der Instance-Startzeit angegeben.	1,0
`ramdisk-id`	Die ID des RAM-Datenträgers, der beim Start angegeben wurde (falls zutreffend)	2007-10-10
`reservation-id`	Die ID der Reservierung	1,0

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`security-groups`	Die Namen der Sicherheitsgruppen für die Instance. Nach dem Start können Sie die Sicherheitsgruppen von Instances ändern. Diese Änderungen werden hier sowie unter network/interfaces/macs/*`mac`*/security-groups angezeigt.	1,0
`services/domain`	Die Domain für AWS Ressourcen für die Region.	2014-02-25
`services/partition`	Die Partition, in der sich die Ressource befindet. Für AWS Standardregionen lautet die Partition`aws`. Wenn Sie Ressourcen in anderen Partitionen haben, lautet die Partition `aws-`*`partitionname`* . Die Aufteilung der Ressourcen in der Region China (Peking) lautet beispielsweise `aws-cn`.	2015-10-20

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`spot/instance-action`	Die Aktion (in den Ruhezustand versetzen, anhalten oder beenden) sowie den ungefähren Zeitpunkt in UTC, an dem die Aktion ausgeführt wird. Dieses Element ist nur vorhanden, wenn die Spot-Instance für das Versetzen in den Ruhezustand, das Anhalten oder das Beenden markiert wurde. Weitere Informationen finden Sie unter instance-action.	15.11.2016
`spot/termination-time`	Die ungefähre Zeit in UTC, zu der das Betriebssystem für Ihre Spot-Instance das Signal zum Beenden empfängt. Dieses Element ist nur vorhanden und enthält einen Zeitwert (z. B. 2015-01-05T18:02:00Z), wenn die Spot-Instance von Amazon EC2 zum Beenden markiert wurde. Das Element für den Beendigungszeitpunkt enthält keinen Wert, wenn Sie die Spot-Instance selbst beenden. Weitere Informationen finden Sie unter termination-time.	2014-11-05

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`tags/instance`	Die Instance-Tags, die der Instance zugeordnet sind. Nur verfügbar, wenn Sie explizit Zugriff auf Tags in Instance-Metadaten zulassen. Weitere Informationen finden Sie unter Zulassen des Zugriffs auf Tags in Instance-Metadaten.	2021-03-23

Kategorien von dynamischen Daten

In der folgenden Tabelle werden die Kategorien von dynamischen Daten aufgeführt.

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`fws/instance-monitoring`	Wert, der angibt, ob der Kunde eine detaillierte einminütige Überwachung aktiviert hat. CloudWatch Zulässige Werte: `enabled | disabled`	2009-04-04
`instance-identity/document`	JSON-Wert mit Instance-Attributen, z. B. Instance-ID, private IP-Adresse, usw. Siehe Instance-Identitätsdokumente.	2009-04-04
`instance-identity/pkcs7`	Wird verwendet, um die Authentizität und den Inhalt des Dokuments mithilfe der Signatur zu überprüfen. Siehe Instance-Identitätsdokumente.	2009-04-04

Kategorie	Beschreibung	Version, als die Kategorie veröffentlicht wurde
`instance-identity/signature`	Die Daten können von Dritten verwendet werden, um den Ursprung und die Authentizität zu überprüfen. Siehe Instance-Identitätsdokumente.	2009-04-04

Linux-Beispiel: AMI-Startindexwert

Dieses Beispiel zeigt, wie Sie sowohl Benutzerdaten als auch Instanz-Metadaten verwenden können, um Ihre Linux-Instances zu konfigurieren.

> **Note**
>
> In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des IMDS verwendet: `169.254.169.254`. Wenn Sie Zeit Instance-Metadaten für EC2-Instances über die IPv6-Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6-Adresse verwenden: `[fd00:ec2::254]`. Die IPv6-Adresse des IMDS ist mit IMDSv2-Befehlen kompatibel. Auf die IPv6-Adresse kann nur auf Instances zugegriffen werden, die auf dem AWS Nitro-System basieren, und in einem IPv6-unterstützten Subnetz (Dual Stack oder nur IPv6).

Alice möchte vier Instances ihres bevorzugten Datenbank-AMI starten; die erste soll dabei als Master-Instance fungieren, die übrigen drei als Replikate. Beim Start der Instances möchte sie Benutzerdaten für die Replikationsstrategien der einzelnen Replikate hinzufügen. Sie weiß, dass diese Daten in allen vier Instances verwendet werden, d. h. sie muss die Benutzerdaten so strukturieren, dass jede Instance erkennt, welcher Teile für sie gedacht ist. Dies kann mithilfe des Instance-Metadatenwerts `ami-launch-index` erreicht werden; dieser ist für jede Instance eindeutig. Wenn sie mehrere Instances gleichzeitig startet, gibt das `ami-launch-index` die Reihenfolge an, in der die Instances gestartet wurden. Der Wert für die zuerst gestartete Instance ist `0`.

Hier sind die Benutzerdaten, die Alice erstellt hat.

```
replicate-every=1min | replicate-every=5min | replicate-every=10min
```

Die `replicate-every=1min`-Daten definieren die Konfiguration für das erste Replikat, `replicate-every=5min` definiert die Konfiguration für das zweite Replikat usw. Alice beschließt, diese Daten als ASCII-Zeichenfolge bereitzustellen; die Daten für die einzelnen Instances werden dabei durch ein Pipe-Symbol (`|`) voneinander getrennt.

Alice startet vier Instances mit dem Befehl run-instances unter Angabe der Benutzerdaten.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --count 4 \
    --instance-type t2.micro \
    --user-data "replicate-every=1min | replicate-every=5min | replicate-every=10min"
```

Nach dem Start sind in jeder Instance eine Kopie der Benutzerdaten und die folgenden Metadaten vorhanden:

- AMI-ID: ami-0abcdef1234567890
- Reservation ID: r-1234567890abcabc0
- Public keys: none
- Security group name: default
- Instance type: t2.micro

Für jede Instance sind aber auch bestimmte Metadaten vorhanden, die sich von denen der anderen unterscheiden.

Instance 1

Metadaten	Value
instance-id	i-1234567890abcdef0
ami-launch-index	0
public-hostname	ec2-203-0-113-25.compute-1.amazonaws.com
public-ipv4	67.202.51.223

Metadaten	Value
local-hostname	ip-10-251-50-12.ec2.internal
local-ipv4	10.251.50.35

Instance 2

Metadaten	Value
instance-id	i-0598c7d356eba48d7
ami-launch-index	1
public-hostname	ec2-67-202-51-224.compute-1.amazonaws.com
public-ipv4	67.202.51.224
local-hostname	ip-10-251-50-36.ec2.internal
local-ipv4	10.251.50.36

Instance 3

Metadaten	Value
instance-id	i-0ee992212549ce0e7
ami-launch-index	2
public-hostname	ec2-67-202-51-225.compute-1.amazonaws.com
public-ipv4	67.202.51.225
local-hostname	ip-10-251-50-37.ec2.internal
local-ipv4	10.251.50.37

Instance 4

Metadaten	Value
instance-id	i-1234567890abcdef0
ami-launch-index	3
public-hostname	ec2-67-202-51-226.compute-1.amazonaws.com
public-ipv4	67.202.51.226
local-hostname	ip-10-251-50-38.ec2.internal
local-ipv4	10.251.50.38

Alice mit dem Wert unter `ami-launch-index` bestimmen, welcher Teil der Benutzerdaten für eine bestimmte Instance anzuwenden ist.

1. Sie stellt eine Verbindung mit einer der Instances her und ruft den `ami-launch-index` für diese Instance ab, um sicherzustellen, dass es sich um eines der Replikate handelt:

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/meta-data/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

   Für die folgenden Schritte verwenden die IMDSv2-Anfragen das gespeicherte Token aus dem vorhergehenden IMDSv2-Befehl (vorausgesetzt, das Token ist nicht abgelaufen).

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/ami-launch-index
   2
   ```

2. Sie speichert das `ami-launch-index` als Variable.

IMDSv2

```
[ec2-user ~]$ ami_launch_index=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
 http://169.254.169.254/latest/meta-data/ami-launch-index`
```

IMDSv1

```
[ec2-user ~]$ ami_launch_index=`curl http://169.254.169.254/latest/meta-data/ami-
launch-index`
```

3. Sie speichert die Benutzerdaten als Variable.

   IMDSv2

   ```
   [ec2-user ~]$ user_data=`curl -H "X-aws-ec2-metadata-token: $TOKEN"
    http://169.254.169.254/latest/user-data`
   ```

   IMDSv1

   ```
   [ec2-user ~]$ user_data=`curl http://169.254.169.254/latest/user-data`
   ```

4. Schließlich verwendet Alice den Befehl cut, um den Teil der Benutzerdaten zu extrahieren, der für diese Instance gilt.

   IMDSv2

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

   IMDSv1

   ```
   [ec2-user ~]$ echo $user_data | cut -d"|" -f"$ami_launch_index"
   replicate-every=5min
   ```

Instance-Identitätsdokumente

Jede Instance, die Sie starten, hat ein Instance-Identitätsdokument, das Informationen über die Instance selbst liefert. Sie können die Attribute der Instance mit Instance-Identitätsdokument validieren.

Das Instance-Identitätsdokument wird generiert, wenn die Instance angehalten und gestartet, neu gestartet oder gelauncht wird. Das Instance-Identitätsdokument steht (im Klartext-JSON-Format) über den Instance Metadata Service (IMDS) bereit. Die IPv4-Adresse `169.254.169.254` ist eine lokale Adresse (Link-local address) und nur von der Instance aus gültig. Weitere Informationen finden Sie unter Link-local address in Wikipedia. Die IPv6-Adresse `[fd00:ec2::254]` ist eine lokale Adresse (Link-local address) und nur von der Instance aus gültig. Weitere Informationen finden Sie unter Eindeutige lokale Adresse auf Wikipedia.

> **Note**
>
> In den Beispielen in diesem Abschnitt wird die IPv4-Adresse des IMDS verwendet: `169.254.169.254`. Wenn Sie Zeit Instance-Metadaten für EC2-Instances über die IPv6-Adresse abrufen, stellen Sie sicher, dass Sie stattdessen die IPv6-Adresse verwenden: `[fd00:ec2::254]`. Die IPv6-Adresse des IMDS ist mit IMDSv2-Befehlen kompatibel. Auf die IPv6-Adresse kann nur auf Instances zugegriffen werden, die auf dem AWS Nitro-System basieren, und in einem IPv6-unterstützten Subnetz (Dual-Stack oder nur IPv6).

Sie können das Instance-Identitätsdokument jederzeit von einer laufenden Instance abrufen. Das Instance-Identitätsdokument-Plugin enthält die folgenden Informationen:

Daten	Beschreibung
`accountId`	Die ID des Kontos, das die Instance gestartet hat. AWS
`architecture`	Die Architektur des AMIs, das zum Starten der Instance verwendet wird (i386 | x86_64 | arm64).
`availabilityZone`	Die Availability Zone, in der die Instance ausgeführt wird.
`billingProducts`	Die Abrechnungsprodukte der Instance.
`devpayProductCodes`	Als veraltet gekennzeichnet.
`imageId`	Die ID des zum Start der Instance verwendeten AMI.
`instanceId`	Die ID der Instance.

Daten	Beschreibung
`instanceType`	Der Instance-Typ der Instance.
`kernelId`	Die ID des mit der Instance verknüpften Kernels, falls zutreffend.
`marketplaceProductCodes`	Der AWS Marketplace Produktcode des AMI, das zum Starten der Instance verwendet wurde.
`pendingTime`	Das Datum und die Uhrzeit, zu der die Instance gestartet wurde.
`privateIp`	Die private IPv4-Adresse der Instance.
`ramdiskId`	Die ID der mit der Instance verknüpften RAM-Disk, falls zutreffend.
`region`	Die Region, in der die Instance ausgeführt wird.
`version`	Die Version des Instance-Identitätsdokument-Formats.

Abrufen der Klartext-Instance-Identitätsdokument

So rufen Sie das Klartext-Instance-Identitätsdokument ab

Stellen Sie eine Verbindung zur Instance her und führen Sie den folgenden Befehl aus.

Linux

IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/dynamic/
instance-identity/document
```

IMDSv1

```
$ curl http://169.254.169.254/latest/dynamic/instance-identity/document
```

Windows

IMDSv2

```
PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
token).Content
```

```
PS C:\> (Invoke-WebRequest -Headers @{'X-aws-ec2-metadata-token' = $Token}
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content
```

IMDSv1

```
PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/dynamic/instance-identity/
document).Content
```

Es folgt eine Beispielausgabe.

```
{
    "devpayProductCodes" : null,
    "marketplaceProductCodes" : [ "1abc2defghijklm3nopqrs4tu" ],
    "availabilityZone" : "us-west-2b",
    "privateIp" : "10.158.112.84",
    "version" : "2017-09-30",
    "instanceId" : "i-1234567890abcdef0",
    "billingProducts" : null,
    "instanceType" : "t2.micro",
    "accountId" : "123456789012",
    "imageId" : "ami-5fb8c835",
    "pendingTime" : "2016-11-19T16:32:11Z",
    "architecture" : "x86_64",
    "kernelId" : null,
    "ramdiskId" : null,
    "region" : "us-west-2"
}
```

Verifizieren des Instance-Identitätsdokument

Wenn Sie beabsichtigen, den Inhalt des Instance-Identitätsdokument für einen wichtigen Zweck zu verwenden, sollten Sie den Inhalt und die Authentizität überprüfen, bevor Sie es verwenden.

Das Klartext-Instance-Identitätsdokument wird von drei gehashten und verschlüsselten Signaturen ergänzt. Sie können diese Signaturen verwenden, um die Herkunft und Authentizität des Instance-Identitätsdokument und der darin enthaltenen Informationen zu überprüfen. Die folgenden Signaturen werden bereitgestellt:

- Base64-kodierte Signatur—Dies ist ein Base64-kodierter SHA256-Hash des Instance-Identitätsdokument, der mit einem RSA-Schlüsselpaar verschlüsselt wird.
- PKCS7-Signatur—Dies ist ein SHA1-Hash des Instance-Identitätsdokument, der mit einem DSA-Schlüsselpaar verschlüsselt wird.
- RSA-2048-Signatur—Dies ist ein SHA256-Hash des Instance-Identitätsdokument, der mit einem RSA-2048-Schlüsselpaar verschlüsselt wird.

Jede Signatur ist an einem anderen Endpunkt in den Metadaten der Instance verfügbar. Sie können je nach Ihren Hashing- und Verschlüsselungsanforderungen eine beliebige dieser Signaturen verwenden. Um die Signaturen zu überprüfen, müssen Sie das entsprechende AWS öffentliche Zertifikat verwenden.

Die folgenden Themen enthalten detaillierte Schritte zur Validierung des Instance-Identitätsdokument unter Verwendung jeder Signatur.

- Verwenden der PKCS7-Signatur zum Überprüfen der Instance-Identitätsdokument
- Verwenden der base64-codierten Signatur zum Überprüfen der Instance-Identitätsdokument
- Verwenden der RSA-2048-Signatur zum Überprüfen der Instance-Identitätsdokument

Verwenden der PKCS7-Signatur zum Überprüfen der Instance-Identitätsdokument

In diesem Thema wird erklärt, wie Sie das Identitätsdokument der Instanz mithilfe der PKCS7-Signatur und des öffentlichen AWS DSA-Zertifikats verifizieren.

Linux-Instances

Um das Identitätsdokument der Instanz mithilfe der PKCS7-Signatur und des öffentlichen DSA-Zertifikats zu verifizieren AWS

1. Stellen Sie eine Verbindung zur Instance her.

2. Rufen Sie die PKCS7-Signatur aus den Metadaten der Instance ab und fügen Sie sie zu einer Datei namens `pkcs7` mit benötigter Kopf- und Fußzeile hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
   && TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/pkcs7 >> pkcs7 \
   && echo "" >> pkcs7 \
   && echo "-----END PKCS7-----" >> pkcs7
   ```

   IMDSv1

   ```
   $ echo "-----BEGIN PKCS7-----" >> pkcs7 \
   && curl -s http://169.254.169.254/latest/dynamic/instance-identity/pkcs7
    >> pkcs7 \
   && echo "" >> pkcs7 \
   && echo "-----END PKCS7-----" >> pkcs7
   ```

3. Suchen Sie das öffentliche DSA-Zertifikat für Ihre Region in AWS öffentliche Zertifikate und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate` ein.

4. Verwenden Sie den Befehl OpenSSL smime, um die Signatur zu überprüfen. Fügen Sie die Option `-verify` ein, um anzugeben, dass die Signatur verifiziert werden muss, und die Option `-noverify`, um anzugeben, dass das Zertifikat nicht verifiziert werden muss.

   ```
   $ openssl smime -verify -in pkcs7 -inform PEM -certfile certificate -noverify | tee
    document
   ```

   Wenn die Signatur gültig ist, wird die Meldung `Verification successful` angezeigt.

   Der Befehl schreibt außerdem den Inhalt des Instance-Identitätsdokuments in eine neue Datei namens `document`. Mit den folgenden Befehlen können Sie den Inhalt des Instance-Identitätsdokuments aus den Instance-Metadaten mit dem Inhalt dieser Datei vergleichen.

   ```
   $ openssl dgst -sha256 < document
   ```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Wenn die Signatur nicht verifiziert werden kann, wenden Sie sich an AWS Support.

Windows-Instances

Voraussetzungen

Dieses Verfahren erfordert die `System.Security` Microsoft .NET Core-Klasse. Führen Sie den folgenden Befehl aus, um die Klasse zu Ihrer PowerShell Sitzung hinzuzufügen.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Der Befehl fügt die Klasse nur der aktuellen PowerShell Sitzung hinzu. Wenn Sie eine neue Sitzung starten, müssen Sie den Befehl erneut ausführen.

Um das Identitätsdokument der Instanz mithilfe der PKCS7-Signatur und des öffentlichen AWS DSA-Zertifikats zu überprüfen

1. Stellen Sie eine Verbindung zur Instance her.
2. Rufen Sie die PKCS7-Signatur aus den Metadaten der Instance ab, konvertieren Sie sie in ein Byte-Array und fügen Sie sie an eine Variable namens `$Signature` an. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/pkcs7).Content)
   ```

IMDSv1

```
PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/pkcs7).Content)
```

3. Rufen Sie das Klartext-Identitätsdokument der Instance aus den Instance-Metadaten ab, konvertieren Sie es in ein Byte-Array und fügen Sie es zu einer Variablen namens `$Document` hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
   ```

4. Suchen Sie das öffentliche DSA-Zertifikat für Ihre Region in AWS öffentliche Zertifikate und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate.pem` ein.
5. Extrahieren Sie das Zertifikat aus der Zertifikatsdatei und speichern Sie es in einer Variablen mit dem Namen `$Store`.

   ```
   PS C:\> $Store =
    [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
   Path certificate.pem)))
   ```

6. Überprüfen Sie die Signatur.

   ```
   PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
   ```

   ```
   PS C:\> $SignatureDocument.Decode($Signature)
   ```

   ```
   PS C:\> $SignatureDocument.CheckSignature($Store, $true)
   ```

Wenn die Signatur gültig ist, gibt der Befehl keine Ausgabe zurück. Wenn die Signatur nicht verifiziert werden kann, gibt der Befehl zurüc `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Wenn Ihre Signatur nicht verifiziert werden kann, wenden Sie sich an AWS Support.

7. Validieren Sie den Inhalt des Instance-Identitätsdokuments.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Wenn der Inhalt des Identitätsdokuments der Instance gültig ist, gibt der Befehl `True` zurück. Wenn das Identitätsdokument der Instance nicht validiert werden kann, wenden Sie sich an AWS Support.

Verwenden der base64-codierten Signatur zum Überprüfen der Instance-Identitätsdokument

In diesem Thema wird erklärt, wie das Identitätsdokument der Instanz mithilfe der Base64-codierten Signatur und des öffentlichen RSA-Zertifikats verifiziert wird. AWS

Linux-Instances

Um das Identitätsdokument der Instanz mithilfe der Base64-codierten Signatur und des öffentlichen RSA-Zertifikats zu validieren AWS

1. Stellen Sie eine Verbindung zur Instance her.
2. Rufen Sie die base64-kodierte Signatur aus den Metadaten der Instance ab, konvertieren Sie sie in ein Binärformat und fügen Sie sie zu einer Datei namens `signature` hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

```
$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/signature | base64 -d >> signature
```

IMDSv1

```
$ curl -s http://169.254.169.254/latest/dynamic/instance-identity/signature |
 base64 -d >> signature
```

3. Rufen Sie die Klartext-Instance-Identitätsdokument aus den Metadaten der Instance ab und fügen Sie sie zu einer Datei mit dem Namen `document` hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   $ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
   metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   dynamic/instance-identity/document >> document
   ```

   IMDSv1

   ```
   $ curl -s http://169.254.169.254/latest/dynamic/instance-identity/document
    >> document
   ```

4. Suchen Sie das öffentliche RSA-Zertifikat für Ihre Region in AWS öffentliche Zertifikate und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate` ein.
5. Extrahieren Sie den öffentlichen Schlüssel aus dem öffentlichen AWS RSA-Zertifikat und speichern Sie ihn in einer Datei mit dem Namen. `key`

   ```
   $ openssl x509 -pubkey -noout -in certificate >> key
   ```

6. Verwenden Sie den Befehl OpenSSL dgst, um die Instance-Identitätsdokument zu überprüfen.

   ```
   $ openssl dgst -sha256 -verify key -signature signature document
   ```

   Wenn die Signatur gültig ist, wird die Meldung `Verification successful` angezeigt.

   Der Befehl schreibt außerdem den Inhalt des Instance-Identitätsdokuments in eine neue Datei namens `document`. Mit den folgenden Befehlen können Sie den Inhalt des Instance-Identitätsdokuments aus den Instance-Metadaten mit dem Inhalt dieser Datei vergleichen.

   ```
   $ openssl dgst -sha256 < document
   ```

```
$ curl -s -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/document | openssl dgst -sha256
```

Wenn die Signatur nicht verifiziert werden kann, wenden Sie sich an AWS Support.

Windows-Instances

Um das Identitätsdokument der Instanz mithilfe der Base64-codierten Signatur und des öffentlichen RSA-Zertifikats zu validieren AWS

1. Stellen Sie eine Verbindung zur Instance her.
2. Rufen Sie die base64-kodierte Signatur aus den Metadaten der Instance ab, konvertieren Sie sie in ein Byte-Array und fügen Sie sie der Variablen mit dem Namen `$Signature` hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/signature).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/signature).Content)
   ```

3. Rufen Sie das Klartext-Identitätsdokument der Instance aus den Instance-Metadaten ab, konvertieren Sie es in ein Byte-Array und fügen Sie es zu einer Variablen namens `$Document` hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

IMDSv2

```
PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
 @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
instance-identity/document).Content)
```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Suchen Sie das öffentliche RSA-Zertifikat für Ihre Region in AWS öffentliche Zertifikate und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate.pem` ein.
5. Überprüfen Sie das Instance-Identitätsdokument.

```
PS C:\> [Security.Cryptography.X509Certificates.X509Certificate2]::new((Resolve-
Path certificate.pem)).PublicKey.Key.VerifyData($Document, 'SHA256', $Signature)
```

Wenn die Signatur gültig ist, gibt der Befehl `True` zurück. Wenn die Signatur nicht verifiziert werden kann, wenden Sie sich an AWS Support.

Verwenden der RSA-2048-Signatur zum Überprüfen der Instance-Identitätsdokument

In diesem Thema wird erklärt, wie Sie das Identitätsdokument der Instanz mithilfe der RSA-2048-Signatur und des öffentlichen RSA-2048-Zertifikats verifizieren. AWS

Linux-Instances

Um das Identitätsdokument der Instanz mithilfe der RSA-2048-Signatur und des öffentlichen RSA-2048-Zertifikats zu verifizieren AWS

1. Stellen Sie eine Verbindung zur Instance her.
2. Rufen Sie die RSA-2048-Signatur aus den Metadaten der Instance ab und fügen Sie sie zusammen mit der notwendigen Kopf- und Fußzeile zu einer Datei namens `rsa2048` hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

IMDSv2

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
&& TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
dynamic/instance-identity/rsa2048 >> rsa2048 \
&& echo "" >> rsa2048 \
&& echo "-----END PKCS7-----" >> rsa2048
```

IMDSv1

```
$ echo "-----BEGIN PKCS7-----" >> rsa2048 \
&& curl -s http://169.254.169.254/latest/dynamic/instance-identity/rsa2048
 >> rsa2048 \
&& echo "" >> rsa2048 \
&& echo "-----END PKCS7-----" >> rsa2048
```

3. Suchen Sie das öffentliche RSA-2048-Zertifikat für Ihre Region in AWS öffentliche Zertifikate und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate` ein.
4. Verwenden Sie den Befehl OpenSSL smime, um die Signatur zu überprüfen. Fügen Sie die Option `-verify` ein, um anzugeben, dass die Signatur verifiziert werden muss, und die Option `-noverify`, um anzugeben, dass das Zertifikat nicht verifiziert werden muss.

   ```
   $ openssl smime -verify -in rsa2048 -inform PEM -certfile certificate -noverify |
    tee document
   ```

   Wenn die Signatur gültig ist, wird die Meldung `Verification successful` angezeigt. Wenn die Signatur nicht verifiziert werden kann, wenden Sie sich an AWS Support.

Windows-Instances

Voraussetzungen

Dieses Verfahren erfordert die `System.Security` Microsoft .NET Core-Klasse. Führen Sie den folgenden Befehl aus, um die Klasse zu Ihrer PowerShell Sitzung hinzuzufügen.

```
PS C:\> Add-Type -AssemblyName System.Security
```

> **Note**
>
> Der Befehl fügt die Klasse nur der aktuellen PowerShell Sitzung hinzu. Wenn Sie eine neue Sitzung starten, müssen Sie den Befehl erneut ausführen.

Um das Identitätsdokument der Instanz mithilfe der RSA-2048-Signatur und des öffentlichen RSA-2048-Zertifikats AWS zu überprüfen

1. Stellen Sie eine Verbindung zur Instance her.
2. Rufen Sie die RSA-2048-Signatur aus den Metadaten der Instance ab, konvertieren Sie sie in ein Byte-Array und fügen Sie sie an eine Variable namens `$Signature` an. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> [string]$token = (Invoke-WebRequest -Method Put -Headers @{'X-aws-
   ec2-metadata-token-ttl-seconds' = '21600'} http://169.254.169.254/latest/api/
   token).Content
   ```

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/rsa2048).Content)
   ```

   IMDSv1

   ```
   PS C:\> $Signature = [Convert]::FromBase64String((Invoke-WebRequest
    http://169.254.169.254/latest/dynamic/instance-identity/rsa2048).Content)
   ```

3. Rufen Sie das Klartext-Identitätsdokument der Instance aus den Instance-Metadaten ab, konvertieren Sie es in ein Byte-Array und fügen Sie es zu einer Variablen namens `$Document` hinzu. Verwenden Sie je nach der von der Instance verwendeten IMDS-Version einen der folgenden Befehle.

   IMDSv2

   ```
   PS C:\> $Document = [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest -Headers
    @{'X-aws-ec2-metadata-token' = $Token} http://169.254.169.254/latest/dynamic/
   instance-identity/document).Content)
   ```

IMDSv1

```
PS C:\> $Document =  [Text.Encoding]::UTF8.GetBytes((Invoke-WebRequest
 http://169.254.169.254/latest/dynamic/instance-identity/document).Content)
```

4. Suchen Sie das öffentliche RSA-2048-Zertifikat für Ihre Region in AWS öffentliche Zertifikate und fügen Sie den Inhalt in eine neue Datei mit dem Namen `certificate.pem` ein.
5. Extrahieren Sie das Zertifikat aus der Zertifikatsdatei und speichern Sie es in einer Variablen mit dem Namen `$Store`.

```
PS C:\> $Store =
 [Security.Cryptography.X509Certificates.X509Certificate2Collection]::new([Security.Cryptog
Path certificate.pem)))
```

6. Überprüfen Sie die Signatur.

```
PS C:\> $SignatureDocument = [Security.Cryptography.Pkcs.SignedCms]::new()
```

```
PS C:\> $SignatureDocument.Decode($Signature)
```

```
PS C:\> $SignatureDocument.CheckSignature($Store, $true)
```

Wenn die Signatur gültig ist, gibt der Befehl keine Ausgabe zurück. Wenn die Signatur nicht verifiziert werden kann, gibt der Befehl zurüc `Exception calling "CheckSignature" with "2" argument(s): "Cannot find the original signer`. Wenn Ihre Signatur nicht verifiziert werden kann, wenden Sie sich an AWS Support.

7. Validieren Sie den Inhalt des Instance-Identitätsdokuments.

```
PS C:
\> [Linq.Enumerable]::SequenceEqual($SignatureDocument.ContentInfo.Content, $Document)
```

Wenn der Inhalt des Identitätsdokuments der Instance gültig ist, gibt der Befehl `True` zurück. Wenn das Identitätsdokument der Instance nicht validiert werden kann, wenden Sie sich an AWS Support.

AWS öffentliche Zertifikate

Die folgenden AWS öffentlichen Zertifikate können verwendet werden, um den Inhalt des Instanzidentitätsdokuments einer Instanz zu überprüfen, wie in den folgenden Themen beschrieben:

- Überprüfung mittels PKCS7-Signatur
- Überprüfung mittels base64-codierter Signatur
- Überprüfung mittels RSA-2048-Signatur

Stellen Sie sicher, dass Sie das richtige Zertifikat für Ihre Region und das von Ihnen verwendete Überprüfungsverfahren verwenden. Wenn Sie die PKCS7-Signatur verifizieren, verwenden Sie das DSA-Zertifikat. Wenn Sie die base6-codierte Signatur verifizieren, verwenden Sie das RSA-Zertifikat. Wenn Sie die RSA-2048-Signatur verifizieren, verwenden Sie das RSA-2048-Zertifikat.

Erweitern Sie unten jede Region, um die regionsspezifischen Zertifikate anzuzeigen.

USA Ost (Ohio) – us-east-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUVJTc+hOU+8Gk3JlqsX438Dk5c58wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MTE0OVoXDTI5MDQyODE3MTE0OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUVJTc+hOU
+8Gk3JlqsX438Dk5c58wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAywJQaVNWJqW0R0T0xVOSoN1GLk9x9kKEuN67RN9CLin4dA97qa7Mr5W4P
FZ6vnh5CjOhQBRXV9xJUeYSdqVItNAUFK/fEzDdjf1nUfPlQ3OJ49u6CV01NoJ9m
usvY9kWcV46dqn2bk2MyfTTgvmeqP8fiMRPxxnVRkSzlldP5Fg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM07oeX4xevdMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA2MTAx
MjU4MThaGA8yMTk1MTExNDEyNTgxOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA6v6kGMnRmFDLxBEqXzP4npnL65OO0kmQ7w8YXQygSdmNIoScGSU5wfh9
mZdcvCxCdxgALFsFqPvH8fqiE9ttI0fEfuZvHOs8wUsIdKr0Zz0MjSx3cik4tKET
ch0EKfMnzKOgDBavraCDeX1rUDU0Rg7HFqNAOry3uqDmnqtk00XC9GenS3z/7ebJ
fIBEPAam5oYMVFpX6M6St77WdNE8wEU8SuerQughiMVx9kMB07imeVHBiELbMQ0N
lwSWRL/61fA02keGSTfSp/0m3u+lesf2VwVFhqIJs+JbsEscPxOkIRlzy8mGd/JV
ONb/DQpTedzUKLgXbw7KtO3HTG9iXQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU2CTGYE5fTjx7gQXzdZSGPEWAJY4wgY4GA1UdIwSBhjCBg4AU2CTG
YE5fTjx7gQXzdZSGPEWAJY6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM07oeX4xevdMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANdqkIpVypr2PveqUsAKke1wKCOSuw1UmH9k
xX1/VRoHbrI/UznrXtPQOPMmHA2LKSTedwsJuorUn3cFH6qNs8ixBDrl8pZwfKOY
```

```
IBJcTFBbI1xBEFkZoO3wczzo5+8vPQ60RVqAaYb+iCa1HFJpccC3Ovajfa4GRdNb
n6FYnluIcDbmpcQePoVQwX7W3oOYLB1QLN7fE6H1j4TBIsFdO3OuKzmaifQlwLYt
DVxVCNDabpOr6Uozd5ASm4ihPPoEoKo7Ilp0fOT6fZ41U2xWA4+HF/89UoygZSo7
K+cQ90xGxJ+gmlYbLFR5rbJOLfjrgDAb2ogbFy8LzHo2ZtSe60M=
-----END CERTIFICATE-----
```

USA Ost (Virginia) – us-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUE1y2NIKCU+Rg4uu4u32koG9QEYIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MzQwMVoXDTI5MDQyODE3MzQwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
```

```
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUE1y2NIKC
U+Rg4uu4u32koG9QEYIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAlxSmwcWnhT4uAeSinJuz+1BTcKhVSWb5jT8pYjQb8ZoZkXXRGb09mvYeU
NeqOBr27rvRAnaQ/9LUQf72+SahDFuS4CMI8nwowytqbmwquqFr4dxA/SDADyRiF
ea1UoMuNHTY49J/1vPomqsVn7mugTp+TbjqCfOJTpu0temHcFA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALFpzEAVWaQZMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU5MTJaGA8yMTk1MDExNzA4NTkxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjS2vqZu9mEOhOq+0bRpAbCUiapbZMFNQqRg7kTlr7Cf+gDqXKpHPjsng
SfNz+JHQd8WPI+pmNs+q0Z2aTe23klmf2U52KH9/j1k8RlIbap/yFibFTSedmegX
E5r447GbJRsHUmuIIfZTZ/oRlpuIIO5/Vz7SOj22tdkdY2ADp7caZkNxhSP915fk
2jJMTBUOzyXUS2rBU/ulNHbTTeePjcEkvzVYPahD30TeQ+/A+uWUu89bHSQOJR8h
Um4cFApzZgN3aD5j2LrSMu2pctkQwf9CaWyVznqrsGYjYOY66LuFzSCXwqSnFBfv
fFBAFsjCgY24G2DoMyYkF3MyZlu+rwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUrynSPp4uqSECwy+PiO4qyJ8TWSkwgY4GA1UdIwSBhjCBg4AUrynS
Pp4uqSECwy+PiO4qyJ8TWSmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALFpzEAVWaQZMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADW/s8lXijwdP6NkEoH1m9XLrvK4YTqkNfR6
er/uRRgTx2QjFcMNrx+g87gAml11z+D0crAZ5LbEhDMs+JtZYR3ty0HkDk6SJM85
haoJNAFF7EQ/zCp1EJRIkLLsC7bcDL/Eriv1swt78/BB4RnC9W9kSp/sxd5svJMg
N9a6FAplpNRsWAnbP8JBlAP93oJzblX2LQXgykTghMkQO7NaY5hg/H5o4dMPclTK
lYGqlFUCH6A2vdrxmpKDLmTn5//5pujdD2MN0df6sZWtxwZ0osljV4rDjm9Q3VpA
NWIsDEcp3GUB4proOR+C7PNkY+VGODitBOw09qBGosCBstwyEqY=
-----END CERTIFICATE-----
```

USA West (Nordkalifornien) – us-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
```

```
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUK2zmY9PUSTR7rc1k2OwPYu4+g7wwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MDI0M1oXDTI5MDQyODE3MDI0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUK2zmY9PU
STR7rc1k2OwPYu4+g7wwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQA1Ng4QmN4n7iPh5CnadSOc0ZfM7by0dBePwZJyGvOHdaw6P6E/vEk76KsC
Q8p+akuzVzVPkU4kBK/TRqLp19wEWoVwhhTaxHjQ1tTRHqXIVlrkw4JrtFbeNM21
GlkSLonuzmNZdivn9WuQYeGe7nUD4w3q9GgiF3CPorJe+UxtbA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJANNPkIpcyEtIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
```

```
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAzMDdaGA8yMTk1MDQwMzA5MDMwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApHQGvHvq3SVCzDrC7575BW7GWLzcj8CLqYcL3YY7Jffupz7OjcftO57Z
4fo5Pj0CaS8DtPzh8+8vdwUSMbiJ6cDd3ooio3MnCq6DwzmsY+pY7CiI3UVG7KcH
4TriDqr1Iii7nB5MiPJ8wTeAqX89T3SYaf6Vo+4GCb3LCDGvnkZ9TrGcz2CHkJsj
AIGwgopFpwhIjVYm7obmuIxSIUv+oNH0wXgDL029Zd98SnIYQd/njiqkzE+lvXgk
4h4Tu17xZIKBgFcTtWPky+POGu81DYFqiWVEyR2JKKm2/iR1dL1YsT39kbNg47xY
aR129sS4nB5Vw3TRQA2jL0ToTIxzhQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUgepyiONs8j+q67dmcWu+mKKDa+gwgY4GA1UdIwSBhjCBg4AUgepy
iONs8j+q67dmcWu+mKKDa+ihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJANNPkIpcyEtIMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGLFWyutf1u0xcAc+kmnMPqtc/Q6b79VIX0E
tNoKMI2KR8lcV8ZElXDb0NC6v8UeLpe1WBKjaWQtEjL1ifKg9hdY9RJj4RXIDSK7
33qCQ8juF4vep2U5TTBd6hfWxt1Izi88xudjixmbpUU4YKr8UPbmixldYR+BEx0u
B1KJi9l1lxvuc/Igy/xeHOAZEjAXzVvHp8Bne33VVwMiMxWECZCiJxE4I7+Y6fqJ
pLLSFFJKbNaFyXlDiJ3kXyePEZSc1xiWeyRB2ZbTi5eu7vMG4i3AYWuFVLthaBgu
lPfHafJpj/JDcqt2vKUKfur5edQ6j1CGdxqqjawhOTEqcN8m7us=
-----END CERTIFICATE-----
```

USA West (Oregon) – us-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
```

```
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFx8PxCkbHwpD31bOyCtyz3GclbgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE3MjM1OVoXDTI5MDQyODE3MjM1OVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFx8PxCkb
HwpD31bOyCtyz3GclbgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBzOl+9Xy1+UsbUBI95HO9mbbdnuX+aMJXgG9uFZNjgNEbMcvx+h8P9IMko
z7PzFdheQQ1NLjsHH9mSR1SyC4m9ja6BsejH5nLBWyCdjfdP3muZM4O5+r7vUa1O
dWU+hP/T7DUrPAIVMOE7mpYa+WPWJrN6BlRwQkKQ7twm9kDalA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALZL3lrQCSTMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAxMzJaGA8yMTk1MDExNzA5MDEzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA02Y59qtAA0a6uzo7nEQcnJ26OKF+LRPwZfixBH+EbEN/Fx0gYy1jpjCP
s5+VRNg6/WbfqAsV6X2VSjUKN59ZMnMY9ALA/Ipz0n00Huxj38EBZmX/NdNqKm7C
qWu1q5kmIvYjKGiadfboU8wLwLcHo8ywvfgI6FiGGsEO9VMC56E/hL6Cohko11LW
dizyvRcvg/IidazVkJQCN/4zC9PUOVyKdhW33jXy8BTg/QH927QuNk+ZzD7HH//y
tIYxDhR6TIZsSnRjz3bOcEHxt1nsidc65mY0ejQty4hy7ioSiapw316mdbtE+RTN
fcH9FPIFKQNBpiqfAW5Ebp3Lal3/+wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU7coQx8Qnd75qA9XotSWT3IhvJmowgY4GA1UdIwSBhjCBg4AU7coQ
x8Qnd75qA9XotSWT3IhvJmqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
```

```
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALZL3lrQCSTMMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFZ1e2MnzRaXCaLwEC1pW/f0oRG8nHrlPZ9W
OYZEWbh+QanRgaikBNDtVTwARQcZm3z+HWSkaIx3cyb6vM0DSkZuiwzm1LJ9rDPc
aBm03SEt5v8mcc7sXWvgFjCnUpzosmky6JheCD4O1Cf8k0olZ93FQnTrbg62OK0h
83mGCDeVKU3hLH97FYoUq+3N/IliWFDhvibAYYKFJydZLhIdlCiiB99AM6Sg53rm
oukS3csyUxZyTU2hQfdjyo1nqW9yhvFAKjnnggiwxNKTTPZzstKW8+cnYwiiTwJN
QpVoZdt0SfbuNnmwRUMi+QbuccXweav29QeQ3ADqjgB0CZdSRKk=
-----END CERTIFICATE-----
```

Afrika (Kapstadt) – af-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7DCCAqwCCQCncbCtQbjuyzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA2MDQxMjQ4MDVaFw00
NTA2MDQxMjQ4MDVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQC12Nr1gMrHcFSZ7S/A
pQBSCMHWmn2qeoQTMVWqe50fnTd0zGFxDdIjKxUK58/8zjWG5uR4TXRzmZpGpmXB
bSufAR6BGqud2LnT/HIWGJAsnX2uOtSyNfCoJigqwhea5w+CqZ6I7iBDdnB4TtTw
qO6TlnExHFVj8LMkylZgiaE1CQIVAIhdobse4K0QnbAhCL6R2euQzloXAoGAV/21
WUuMz/79Ga0JvQcz1FNy1sT0pU9rU4TenqLQIt5iccn/7EIfNtvVO5TZKulIKq7J
gXZr0x/KIT8zsNweetLOaGehPIYRMPX0vunMMR7hN7qA7W17WZv/76adywIsnDKq
ekfe15jinaX8MsKUdyDK7Y+ifCG4PVhoM4+W2XwDgYQAAoGAIxOKbVgwLxbn6Pi2
6hBOihFv16jKxAQI0hHzXJLV0Vyv9QwnqjJJRfOCy3dB0zicLXiIxeIdYfvqJr+u
hlN8rGxEZYYJjEUKMGvsc0DW85jonXz0bNfcP0aaKH0lKKVjL+OZi5n2kn9wgdo5
F3CVnMl8BUra8A1Tr2yrrE6TVZ4wCQYHKoZIzjgEAwMvADAsAhQfa7MCJZ+/TEY5
AUr0J4wm8VzjoAIUSYZVu2NdRJ/ERPmDfhW5EsjHlCA=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAKumfZiRrNvHMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTExMjcw
NzE0MDVaGA8yMTk5MDUwMjA3MTQwNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
```

```
gQDFd571nUzVtke3rPyRkYfvs3jh0C0EMzzG72boyUNjnfw1+m0TeFraTLKb9T6F
7TuB/ZEN+vmlYqr2+5Va8U8qLbPF0bRH+FdaKjhgWZdYXxGzQzU3ioy5W5ZM1VyB
7iUsxEAlxsybC3ziPYaHI42UiTkQNahmoroNeqVyHNnBpQIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAAJLylWyElEgOpW4B1XPyRVD4pAds8Guw2+krgqkY0HxLCdjosuH
RytGDGN+q75aAoXzW5a7SGpxLxk6Hfv0xp3RjDHsoeP0i1d8MD3hAC5ezxS4oukK
s5gbPOnokhKTMPXbTdRn5ZifCbWlx+bYN/mTYKvxho7b5SVg2o1La9aK
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAIFI+O5A6/ZIMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA2MDQx
MjQ4MDRaGA8yMTk4MTEwNzEyNDgwNFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy7/WHBBHOrk+20aumT07g8rxrSM0UXgki3eYgKauPCG4Xx//vwQbuZwI
oeVmR9nqnhfij2wOcQdbLandh0EGtbxerete3IoXzd1KXJb11PVmzrzyu5SPBPuP
iCeV4qdjjkXo2YWM6t9YQ911hcG96YSp89TBXFYUh3KLxfqAdTVhuC0NRGhXpyii
j/czo9njofHhqhTr7UEyPun8NVS2QWctLQ86N5zWR3Q0GRoVqqMrJs0cowHTrVw2
9Qr7QBjjBOVbyYmtYxm/DtiKprYV/e6bCAVok015X1sZDd3oCOQNoGlv5XbHJe2o
JFD8GRRy2rkWO/lNwVFDcwec6zC3QwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCE
goqzjpCpmMgCpszFHwvRaSMbspKtK7wNImUjrSBOfBJsfFulyg1Zgn2nDCK7kQhx
jMJmNIvXbps3yMqQ2cHUkKcKf5t+WldfeT4Vk1Rz6HSA8sd0kgVcIesIaoy2aaXU
VEB/oQziRGyKdN1d4TGYVZXG44CkrzSDvlbmfiTq5tL+kAieznVF3bzHgPZW6hKP
EXC3G/IXrXicFEe6YyE1Rakl62VncYSXiGe/i2XvsiNH3Qlmnx5XS7W0SCN0oAxW
EH9twibauv82DVg1WOkQu8EwFw8hFde9X0Rkiu0qVcuU8lJgFEvPWMDFU5sGB6ZM
gkEKTzMvlZpPbBhg99Jl
-----END CERTIFICATE-----
```

Asien-Pazifik (Hongkong) – ap-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq4CCQCO7MJe5Y3VLjAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDMwMjIxMjFaFw00
NTAyMDMwMjIxMjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDvQ9RzVvf4MAwGbqfX
```

```
blCvCoVb9957OkLGn/04CowHXJ+vTBR7eyIa6AoXltsQXBOmrJswToFKKxT4gbuw
jK7s9QQX4CmTRWcEgO2RXtZSVjOhsUQMh+yf7Ht4OVL97LWnNfGsX2cwjcRWHYgI
7lvnuBNBzLQHdSEwMNq0Bk76PwIVAMan6XIEEPnwr4e6u/RNnWBGKd9FAoGBAOCG
eSNmxpW4QFu4pIlAykm6EnTZKKHT87gdXkAkfoC5fAfOxxhnE2HezZHp9Ap2tMV5
8bWNvoPHvoKCQqwfm+OUBlAxC/3vqoVkKL2mG1KgUH9+hrtpMTkwO3RREnKe7I5O
x9qDimJpOihrL4I0dYvy9xUOoz+DzFAW8+ylWVYpA4GFAAKBgQDbnBAKSxWr9QHY
6Dt+EFdGz6lAZLedeBKpaP53Z1DTO34J0C55YbJTwBTFGqPtOLxnUVDlGiD6GbmC
80f3jvogPR1mSmGsydbNbZnbUEVWrRhe+y5zJ3g9qs/DWmDW0deEFvkhWVnLJkFJ
9pdOu/ibRPH1lE2nz6pK7GbOQtLyHTAJBgcqhkjOOAQDAzAAMC0CFQCoJlwGtJQC
cLoM4p/jtVFOj26xbgIUUS4pDKyHaG/eaygLTtFpFJqzWHc=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICSzCCAbQCCQDtQvkVxRvK9TANBgkqhkiG9w0BAQsFADBqMQswCQYDVQQGEwJV
UzETMBEGA1UECBMKV2FzaGluZ3RvbjEQMA4GA1UEBxMHU2VhdHRsZTEYMBYGA1UE
ChMPQW1hem9uLmNvbSBJbmMuMRowGAYDVQQDExFlYzIuYW1hem9uYXdzLmNvbTAe
Fw0xOTAyMDMwMzAwMDZaFw0yOTAyMDIwMzAwMDZaMGoxCzAJBgNVBAYTAlVTMRMw
EQYDVQQIEwpXYXNoaW5ndG9uMRAwDgYDVQQHEwdTZWF0dGxlMRgwFgYDVQQKEw9B
bWF6b24uY29tIEluYy4xGjAYBgNVBAMTEWVjMi5hbWF6b25hd3MuY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC1kkHXYTfc7gY5Q55JJhjTieHAgacaQkiR
Pity9QPDE3b+NXDh4UdP1xdIw73JcIIG3sG9RhWiXVCHh6KkuCTqJfPUknIKk8vs
M3RXflUpBe8Pf+P92pxqPMCz1Fr2NehS3JhhpkCZVGxxwLC5gaG0Lr4rFORubjYY
Rh84dK98VwIDAQABMA0GCSqGSIb3DQEBCwUAA4GBAA6xV9f0HMqXjPHuGILDyaNN
dKcvplNFwDTydVg32MNubAGnecoEBtUPtxBsLoVYXCOb+b5/ZMDubPF9tU/vSXuo
TpYM5Bq57gJzDRaBOntQbX9bgHiUxw6XZWaTS/6xjRJDT5p3S1E0mPI3lP/eJv4o
Ezk5zb3eIf10/sqt4756
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMoxixvs3YssMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA3MjAw
ODQ0NDRaGA8yMTk3MTIyMzA4NDQ0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA4T1PNsOg0FDrGlWePoHeOSmOJTA3HCRy5LSbYD33GFU2eBrOIxoU/+SM
rInKu3GghAMfH7WxPW3etIAZiyTDDU5RLcUq2Qwdr/ZpXAWpYocNc/CEmBFtfbxF
z4uwBIN3/drM0RSbe/wP9EcgmNUGQMMZWeAji8sMtwpOblNWAP9BniUG0Flcz6Dp
uPovwDTLdAYT3TyhzlohKL3f6O48TR5yTaV+3Ran2SGRhyJjfh3FRpP4VC+z5LnT
```

```
WPQHN74Kdq35UgrUxNhJraMGCzznolUuoR/tFMwR93401GsM9fVA7SW3jjCGF81z
PSzjy+ArKyQqIpLW1YGWDFk3sf08FQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDK
2/+C3nPMgtyOFX/I3Cyk+Pui44IgOwCsIdNGwuJysdqp5VIfnjegEu2zIMWJSKGO
lMZoQXjffkVZZ97J7RNDW06oB7kj3WVE8a7U4WEOfnO/CbMUf/x99CckNDwpjgW+
K8V8SzAsQDvYZs2KaE+18GFfLVF1TGUYK2rPSZMHyX+v/TIlc/qUceBycrIQ/kke
jDFsihUMLqgmOV2hXKUpIsmiWMGrFQV4AeV0iXP8L/ZhcepLf1t5SbsGdUA3AUY1
3If8s81uTheiQjwY5t9nM0SY/1Th/tL3+RaEI79VNEVfG1FQ8mgqCK0ar4m0oZJl
tmmEJM7xeURdpBBx36Di
-----END CERTIFICATE-----
```

Asien-Pazifik (Hyderabad) – ap-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXjrQ4+XMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAJCKGBBoxIUxqBk94JHhwZZbgvbP0DAOoHENQWxp/98lI7/
YOfYJOVMJS22aCnHDurofmo5rvNIkgXi7Rztbhu
+lko9rK6DgpmpUwBU0WZtf34aZ2IWNBwHaVhHvWAQf9/46u18dMa2YucK1Wi+Vc+M
+KldrvgXmhym6ErNlzhJyMAkGByqGSM44BAMDLwAwLAIUaaPKxaOHoYvwz709xXpsQueIq+UCFFa/
GpzoDOSokl1057NU/2hnsiW4
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLj9CMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+sFcobrjvcAYm0PNRD8f4R1jAzvoLt2+qGeOTAyO1Httj6cmsYN3AP1hN5iYuppFiYsl2eNPa/
CD0Vg0BAfDFlV5rzjpA0j7TJabVh4kj7JvtD+xYMi6wEQA4x6SPONY4OeZ2+8o/
HS8nucpWDVdPRO6ciWUlMhjmDmwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAAy6sgTdRkTqELHBeWj69q60xHyUmsWqHAQ
TGGbYP0yP2qfMl0cCImzRI5W0gn8gogdervfeT7nH5ih0TWEy/QDWfkQ601L4erm4yh4YQq8vcqAPSkf04N
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
```

```
MIIEEjCCAvqgAwIBAgIJAIVWfPw/X82fMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MDQx
NDMwMjhaGA8yMjAxMTIwODE0MzAyOFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAg29QEFriG+qFEjYW/v62nN70lMJY/Hevx5TtmU/VIYBPQa3HUGTBAbbI
2Tmy8UMpa8kZeaYeI3RAfiQWt0Ws7wUrBuO2Pdp518WDPaJUH7RWEuu1BDDkyZRW
NAMNPCn3ph7Od243IFcLGku7HVekel5poqRpSfojrMasjlf+CvixUeAJbmFoxUHK
kh5unzG2sZyO4wHXcJPQkRf5a8zSTPe9YZP1kXPPEv4p/jTSggaYPxXyS6QVaTlV
zLeLFZ0fesLPMeil3KYQtV7IKLQiEA2F6dxWnxNWQlyMHtdq6PucfEmVx17i/Xza
yNBRo0azY8WUNVkEXrRhp/pU8Nh3GQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU9AO1aZk9RLXk2ZvRVoUxYvQy9uwwgY4GA1UdIwSBhjCBg4AU9AO1
aZk9RLXk2ZvRVoUxYvQy9uyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAIVWfPw/X82fMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBADexluMRQRftqViahCnauEWGdMvLCBr8A+Yr
6hJq0guoxEk/lahxR137DnfMPuSbi1Rx5QKo7oBrWfG/zsgQUnF2IwHTzwD+i/2m
XCane6FiS5RpK3lGdILq8ZmlhQk+6iI8yoZLr0LCfTh+CLgIKHOknfR5lFzgzAiF
SI8/Q9mm+uvYtSTZECI6Zh57QZPoETAG/yl+9jiOy2lAelqa/k1i+Qo8gMfOc+Pm
dwY7o6fV+oucgRlsdey6VM45LeyILQqv0RXtVzjuowanzmCCFMjgqiO9oZAWu4Oh
+F3unijELo01vZJs8s2N3KGlo3/jtUFTX6RTKShZlAPLwBi5GMI=
-----END CERTIFICATE-----
```

Asien-Pazifik (Jakarta) – ap-southeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCArCgAwIBAgIGAXbVDEikMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24g
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYUAAoGBAPjuiEx05N3JQ6cVwntJie67D8OuNo4jGRn
+crEtL7YO0jSVB9zGE1ga
+UgRPIaYETL293S8rTJTVgXAqdpBwfaHC6NUzre8U8iJ8FMNnlP9Gw1oUIlgQBjORyynVJexoB31TDZM
+/52g9O/bpq1QqNyKbeIgyBBlc1dAtr1QLnsMAkGByqGSM44BAMDLwAwLAIUK8E6RDIRtwK+9qnaTOBhv0/
njuQCFFocyT1OxK+UDR888oNsdgtif2Sf
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXbVDG2yMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
Vbt0gQ1ebWcur2hSO7PnJifE4OPxQ7RgSAlc4/spJp1sDP+ZrS0LO1ZJfKhXf1R9S3AUwLnsc7b
+IuVXdY5LK9RKqu64nyXP5dx170zoL8loEyCSuRR2fs+04i2QsWBVP+KFNAn7P5L1EHRjkgTO8kjNKviwRV
+OkP9ab5wIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAI4WUy6+DKh0JDSzQEZNyBgNlSoSuC2owtMxCwGB6nBfzzfcekWvs
+87w/g9lNwUnUt0ZHYyh2tuBG6hVJuUEwDJ/z3wDd6wQviLOTF3MITawt9P8siR1hXqLJNxpjRQFZrgHqi
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMtdyRcH51j9MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MDgx
MjM5MTZaGA8yMjAxMDkxMjEyMzkxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvUsKCxoH6KXRYJLeYTWAQfaBQeCwhJaR56mfUeFHJE4g8aFjWkiN4uc1
TvOyYNnIZKTHWmzmulmdinWNbwP0GiROHb/i7ro0Hhvnptyyc Gt8ag8affiIbx5X
7ohdwSN2KJ6G0IKflIx7f2NEI0oAMM/9k+T1eVF+MVWzpZoiDp8frLNkqp8+RAgz
ScZsbRfwv3u/if5xJAvdg2nCkIWDMSHEVPoz0lJo7v0ZuDtWWsL1LHnL5ozvsKEk
+ZJyEi23r+U1hIT1NTBdp4yoigNQexedtwCSr7q36oOdDwvZpqYlkLi3uxZ4ta+a
01pzOSTwMLgQZSbKWQrpMvsIAPrxoQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU1GgnGdNpbnL3lLF30Jomg7Ji9hYwgY4GA1UdIwSBhjCBg4AU1Ggn
GdNpbnL3lLF30Jomg7Ji9hahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMtdyRcH51j9MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACVl00qQlatBKVeiWMrhpczsJroxDxlZTOba
6wTMZk7c3akb6XMOSZFbGaifkebPZqTHEhDlrClM2j9AIlYcCx6YCrTf4cuhn2mD
gcJN33143eOWSaeRY3ee4j+V9ne98y3kO2wLz95VrRgclPFR8po2iWGzGhwUi+FG
q8dXeCH3N0DZgQsSgQWwmdNQXZZej6RHLU/8In5trHKLY0ppnLBjn/UZQbeTyW5q
RJB3GaveXjfgFUWj2qOcDuRGaikdS+dYaLsi5z9cA3FolHzWxx9MOs8io8vKqQzV
XUrLTNWwuhZy88cOlqGPxnoRbw7TmifwPw/cunNrsjUUOgs6ZTk=
-----END CERTIFICATE-----
```

Asien-Pazifik (Melbourne) ap-southeast-4

DSA

```
-----BEGIN CERTIFICATE-----
```

```
MIIC7zCCAq
+gAwIBAgIGAXjWF7P2MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAPRXSsQP9E3dw8QXKlrgBgEVCprLHdK/bbrMas0XMu1EhOD
+q
+0PcTr8+iwbtoXlY5MCeatWIp1GrXQjVqsF8vQqxlEuRuYKbR3nq4mWwaeGlx9AG5EjQHRa3GQ44wWHOdof0M3NRI1MP
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSh40SMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+qWTGAbGsPeMX4hBMjAJUKys2NIRcRZaLM/BCew2FIPVjNtlaj6Gwn9ipU4Mlz3zIwAMWi1AvGMSreppt
+wV6MRtfOjh0Dvj/veJe88aEZJMozNgkJFRS
+WFWsckQeL56tf6kY6QTlNo8V/0CsQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAF7vpPghH0FRo5gu49EArRNPrIvW1egM
wcgkqIwwuXYj+1rhlL+/
iMpQWjdVGEqIZSeXn5fLmdx50eegFCwND837r9e8XYTiQS143Sxt9+Yi6BZ7U7YD8kK9NBWoJxFqUeHdpRCs0O7COjT3
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAN4GTQ64zVs8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTMx
MzMzMDBaGA8yMjAxMTIxNzEzMzMwMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA2BYgeCr+Rk/jIAEDOHS7wJql62vc83QEwjuzk0qOFEReIZzlN1fBRNXK
g0T178Kd3gLYcE59wEFbTe/X5yOA1Lo95x1anSAo7R+Cisf9C2HQuJp+gVb+zx71
lniPF7gHziGpm0M8DdAU/IW+wkZwGbP4z7Hq9+bJ0P2ltvPJ5yxSgkFuDsI9VBHa
CLoprHsCHh2VdP8KcMgQQMmHe1NmBpyTk0ul/aLmQkCQEX6ZIRGOeq228fwlh/t+
Ho+jv87duihVKic6MrL32SlD+maX0LSDUydWdaOLLTGkh7oV7+bFuH6msrXUu+Ur
ZEP1r/MidCWMhfgrFzeTBzOHA97qxQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUcHMd1cHqzmsQ5hpUK3EMLhHdsi4wgY4GA1UdIwSBhjCBg4AUcHMd
1cHqzmsQ5hpUK3EMLhHdsi6hYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAN4GTQ64zVs8MBIGA1UdEwEB/wQIMAYBAf8C
```

```
AQAwDQYJKoZIhvcNAQELBQADggEBAI4PFyVN+7EGSObioiPnv0LL0f70SSzUZJ8p
XO90d4rWea7jIbgZ2AKb+ErynkU9xVg7XQQ5k6KDWgp/4jYFL2dqnt/YAY4PS0un
RSrYElawxLT0BcLn4rcSDC79vQe1xGC5//wDdV6b399COAHRAK6axWYy5w32u9PL
uw0cIp3Ch8JoNwcgTHKRRGzePmBeR4PNqhHTArG4/dJk6/aUO4OpX0WzI6L67CGY
6Nex3dau+gkLCK93dTEkrXtyXHu4wB0J9zd1w+iQ0SEa9eKc78/NjEsF/FZdGrWC
t57lIMOOXJhQ1kRgSwNeZdQWV1dRakvO6sfcvVYkfj1wAvZvvAw=
-----END CERTIFICATE-----
```

Asien-Pazifik (Mumbai) – ap-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUDLA+x6tTAP3LRTr0z6nOxfsozdMwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MTMwMVoXDTI5MDQyODE0MTMwMVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
```

```
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUDLA+x6tT
AP3LRTr0z6nOxfsozdMwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAZ7rYKoAwwiiH1M5GJbrT/BEk3OO2VrEPw8ZxgpqQ/EKlzMlOs/0Cyrmp7
UYyUgYFQe5nq37Z94rOUSeMgv/WRxaMwrLlLqD78cuF9DSkXaZIX/kECtVaUnjk8
BZx0QhoIHOpQocJUSlm/dLeMuE0+0A3HNR6JVktGsUdv9ulmKw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPRYyD8TtmC0MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjAzMDcx
MDQ1MDFaGA8yMTk1MDgxMTEwNDUwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA0LSS5I/eCT2PM0+qusorBx67QL26BIWQHd/yF6ARtHBb/1DdFLRqE5Dj
07Xw7eENC+T79mOxOAbeWg91KaODOzw6i9I/2/HpK0+NDEdD6sPKDA1d45jRra+v
CqAjI+nV9Vw91wv7HjMk3RcjWGziM8/hw+3YNIutt7aQzZRwIWlBpcqx3/AFd8Eu
2UsRMSHgkGUW6UzUF+h/U8218XfrauKNGmNKDYUhtmyBrHT+k6J0hQ4pN7fe6h+Z
w9RVHm24BGhlLxLHLmsOIxvbrF277uX9Dxu1HfKfu5D2kimTY7xSZDNLR2dt+kNY
/+iWdIeEFpPT0PLSILt52wP6stF+3QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBI
E6w+WWC2gCfoJO6c9HMyGLMFEpqZmz1n5IcQt1h9iyO7Vkm1wkJiZsMhXpk73zXf
TPxuXEacTX3SOEa07OIMCFwkusO5f6leOyFTynHCzBgZ3U0UkRVZA3WcpbNB6Dwy
h7ysVlqyT9WZd7EOYm5j5oue2G2xdei+6etgn5UjyWm6liZGrcOF6WPTdmzqa6WG
ApEqanpkQd/HM+hUYex/ZS6zEhd4CCDLgYkIjlrFbFb3pJ1OVLztIfSN5J4Oolpu
JVCfIq5u1NkpzL7ys/Ub8eYipbzI6P+yxXiUSuF0v9b98ymczMYjrSQXIf1e8In3
OP2CclCHoZ8XDQcvvKAh
-----END CERTIFICATE-----
```

Asien-Pazifik (Osaka) – ap-northeast-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
```

```
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUHTRhxHhBZFOGvTFKxHoy9+f5Hl8wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NTQwN1oXDTI5MDQyODE2NTQwN1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUHTRhxHhB
ZFOGvTFKxHoy9+f5Hl8wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAUZx7DcYbhWNTD4BNGhr5beruT2OUoGHH9J73UKxwdqeb9bH1LIWhIZO0X
/1mjn3bWBgCwfoS8gjZwsVB6fZbNBRy8urdBZJ87xF/4JPBjt7S9oGx/zthDUYrC
yK0Y0v4G0PgiS81CvYLg09LpmYhLSJbXENlkC04v5yxdKxZxyg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAMn1yPk22ditMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA3MTkx
```

```
MTEyNThaGA8yMTk2MTIyMjExMTI1OFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArznEYef8IjhrJoazI0QGZkmlmHm/4rEbyQbMNifxjsDE8YWtHNwaM91z
zmyK6Sk/tKlWxcnl3g31iq305ziyFPEewe5Qbwf1iz2cMsvfNBcTh/E6u+mBPH3J
gvGanqUJt6c4IbipdEouIjjnynyVWd4D6erLl/ENijeR1OxVpaqSW5SBK7jms49E
pw3wtbchEl3qsE42Ip4IYmWxqjgaxB7vps91n4kfyzAjUmklcqTfMfPCkzmJCRgp
Vh1C79vRQhmriVKD6BXwfZ8tG3a7mijeDn7kTsQzgO07Z2SAE63PIO48JK8HcObH
tXORUQ/XF1jzi/SIaUJZT7kq3kWl8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBj
ThtO9dLvU2QmKuXAhxXjsIdlQgGG3ZGh/Vke4If1ymgLx95v2Vj9Moxk+gJuUSRL
BzFte3TT6b3jPolbECgmAorjj8NxjC17N8QAAI1d0S0gI8kqkG7V8iRyPIFekv+M
pcai1+cIv5IV5qAz8QOMGYfGdYkcoBjsgiyvMJu/2N2UbZJNGWvcEGkdjGJUYYOO
NaspCAFm+6HA/K7BD9zXB1IKsprLgqhiIUgEaW3UFEbThJT+z8UfHG9fQjzzfN/J
nT6vuY/0RRu1xAZPyh2gr5okN/s6rnmh2zmBHU1n8cbCc64MVfXe2g3EZ9Glq/9n
izPrI09hMypJDP04ugQc
-----END CERTIFICATE-----
```

Asien-Pazifik (Seoul) – ap-northeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUbBSn2UIO6vYk4iNWV0RPxJJtHlgwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEzMzg0NloXDTI5MDQyODEzMzg0NlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUbBSn2UIO
6vYk4iNWV0RPxJJtHlgwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQAmjTjalG8MGLqWTC2uYqEM8nzI3px1eo0ArvFRsyqQ3fgmWcQpxExqUqRy
l3+2134Kv8dFab04Gut5wlfRtc2OwPKKicmv/IXGN+9bKFnQFjTqif08NIzrDZch
aFT/uvxrIiM+oN2YsHq66GUhO2+xVRXDXVxM/VObFgPERbJpyA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANuCgCcHtOJhMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTQx
NTU3NDRaGA8yMTk1MDIxNzE1NTc0NFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA66iNv6pJPmGM20W8HbVYJSlKcAg2vUGx8xeAbzZIQdpGfkabVcUHGB6m
Gy59VXDMDlrJckDDk6dxUOhmcX9z785TtVZURq1fua9QosdbTzX4kAgHGdp4xQEs
mO6QZqg5qKjBP6xr3+PshfQ1rB8Bmwg0gXEm22CC7o77+7N7Mu2sWzWbiUR7vil4
9FjWS8XmMNwFTlShp4l1TDTevDWW/uYmC30RThM9S4QPvTZ0rAS18hHVam8BCTxa
LHaVCH/Yy52rsz0hM/FlghnSnK105ZKj+b+KIp3adBL8OMCjgc/Pxi0+j3HQLdYE
32+FaXWU84D2iP2gDT28evnstzuYTQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC1
mA4q+12pxy7By6g3nBk1s34PmWikNRJBwOqhF8ucGRv8aiNhRRye9lokcXomwo8r
KHbbqvtK85l0xUZp/Cx4sm4aTgcMvfJP29jGLclDzeqADIvkWEJ4+xncxSYVlS9x
+78TvF/+8h9U2LnSl64PXaKdxHy2IsHIVRN4GtoaP2Xhpa1S0M328Jykq/571nfN
1WRD1c/fQf1edgzRjhQ4whcAhv7WRRF+qTbfQJ/vDxy8lkiOsvU9XzUaZ0fZSfXX
wXxZamQbONvFcxVHY/0PSiM8nQoUmkkBQuKleDwRWvkoJKYKyr3jvXK7HIWtMrO4
jmXe0aMy3thyK6g5sJVg
```

```
-----END CERTIFICATE-----
```

Asien-Pazifik (Singapur) – ap-southeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUSqP6ih+++5KF07NXngrWf26mhSUwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE0MzAxNFoXDTI5MDQyODE0MzAxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUSqP6ih++
+5KF07NXngrWf26mhSUwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
```

```
AAOBgQAw13BxW11U/JL58j//Fmk7qqtrZTqXmaz1qm2WlIpJpW750MOcP4ux1uPy
eM0RdVZ4jHSMv5gtLAv/PjExBfw9n6vNCk+5GZG4Xec5DoapBZHXmfMo93sjxBFP
4x9rWn0GuwAVO9ukjYPevq2Rerilrq5VvppHtbATVNY2qecXDA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAJVMGw5SHkcvMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
ODU3MTlaGA8yMTk1MDQwMzA4NTcxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlaSSLfBl7OgmikjLReHuNhVuvM20dCsVzptUyRbut+KmIEEc24wd/xVy
2RMIrydGedkW4tUjkUyOyfET5OAyT43jTzDPHZTkRSVkYjBdcYbe9o/0Q4P7IVS3
XlvwrUu0qo9nSID0mxMnOoF1l8KAqnn10tQ0W+lNSTkasW7QVzcb+3okPEVhPAOq
MnlY3vkMQGI8zX4iOKbEcSVIzf6wuIffXMGHVC/JjwihJ2USQ8fq6oy686g54P4w
ROg415kLYcodjqThmGJPNUpAZ7MOc5Z4pymFuCHgNAZNvjhZDA842Ojecqm62zcm
Tzh/pNMNeGCRYq2EQX0aQtYOIj7bOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU6SSB+3qALorPMVNjToM1Bj3oJMswgY4GA1UdIwSBhjCBg4AU6SSB
+3qALorPMVNjToM1Bj3oJMuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIEExMQ4IJAJVMGw5SHkcvMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAF/0dWqkIEZKg5rca8o0P0VS+tolJJE/FRZO
atHOeaQbWzyac6NEwjYeeV2kY63skJ+QPuYbSuIBLM8p/uTRIvYM4LZYImLGUvoO
IdtJ8mAzq8CZ3ipdMs1hRqF5GRp8lg4w2QpX+PfhnW47iIOBiqSAUkIr3Y3BDaDn
EjeXF6qS4iPIvBaQQ0cvdddNh/pE33/ceghbkZNTYkrwMyBkQlRTTVKXFN7pCRUV
+L9FuQ9y8mP0BYZa5e1sdkwebydU+eqVzsil98ntkhpjvRkaJ5+Drs8TjGaJWlRw
5WuOr8unKj7YxdL1bv7//RtVYVVi296ldoRUYv4SCvJF11z0OdQ=
-----END CERTIFICATE-----
```

Asien-Pazifik (Sydney) – ap-southeast-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
```

```
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFxWyAdk4oiXIOC9PxcgjYYh71mwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MjE0M1oXDTI5MDQyODE1MjE0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFxWyAdk4
oiXIOC9PxcgjYYh71mwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQByjeQe6lr7fiIhoGdjBXYzDfkX0lGGvMIhRh57G1bbceQfaYdZd7Ptc0jl
bpycKGaTvhUdkpMOiV2Hi9dOOYawkdhyJDstmDNKu6P9+b6Kak8He5z3NU1tUR2Y
uTwcz7Ye8Nldx//ws3raErfTI7D6s9m63OX8cAJ/f8bNgikwpw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL2bOgb+dq9rMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
OTAwNTdaGA8yMTk1MDQwMzA5MDA1N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
```

```
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAmRcyLWraysQS8yDC1b5Abs3TUaJabjqWu7d5gHik5Icd6dKl8EYpQSeS
vz6pLhkgO4xBbCRGlgE8LS/OijcZ5HwdrxBiKbicR1YvIPaIyEQQvF5sX6UWkGYw
Ma5IRGj4YbRmJkBybw+AAV9Icb5LJNOMWPi34OWM+2tMh+8L234v/JA6ogpdPuDr
sM6YFHMZ0NWo58MQ0FnEj2D7H58Ti//vFPl0TaaPWaAIRF85zBiJtKcFJ6vPidqK
f2/SDuAvZmyHC8ZBHg1moX9bR5FsU3QazfbW+c+JzAQWHj2AaQrGSCITxCMlS9sJ
l51DeoZBjnx8cnRe+HCaC4YoRBiqIQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU/wHIo+r5U31VIsPoWoRVsNXGxowwgY4GA1UdIwSBhjCBg4AU/wHI
o+r5U31VIsPoWoRVsNXGxoyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL2bOgb+dq9rMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACobLvj8IxlQyORTz/9q7/VJL509/p4HAeve
92riHp6+Moi0/dSEYPeFTgdWB9W3YCNc34Ss9TJq2D7t/zLGGlbI4wYXU6VJjL0S
hCjWeIyBXUZOZKFCb0DSJeUElsTRSXSFuVrZ9EAwjLvHni3BaC9Ve34iP71ifr75
8Tpk6PEj0+JwiijFH8E4GhcV5chB0/iooU6ioQqJrMwFYnwo1cVZJD5v6D0mu9bS
TMIJLJKv4QQQqPsNdjiB7G9bfkB6trP8fUVYLHLsVlIy5lGx+tgwFEYkG1N8IOO/
2LCawwaWm8FYAFd3IZl04RImNs/IMG7VmH1bf4swHOBHgCN1uYo=
-----END CERTIFICATE-----
```

Asien-Pazifik (Tokio) – ap-northeast-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULgwDh7TiDrPPBJwscqDwiBHkEFQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTEyMjMxMFoXDTI5MDQyODEyMjMxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULgwDh7Ti
DrPPBJwscqDwiBHkEFQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBtjAglBde1t4F9EHCZOj4qnY6Gigy07Ou54i+lR77MhbpzE8V28Li9l+YT
QMIn6SzJqU3/fIycIro1OVY1lHmaKYgPGSEZxBenSBHfzwDLRmC9oRp4QMe0BjOC
gepj1lUoiN7OA6PtA+ycNlsP0oJvdBjhvayLiuM3tUfLTrgHbw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAL9KIB7Fgvg/MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTAwMjVaGA8yMTk1MDExNzA5MDAyNVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAz0djWUcmRW85C5CiCKPFiTIvj6y2OuopFxNE5d3Wtab10bm06vnXVKXu
tz3AndG+Dg0zIL0gMlU+QmrSR0PH2PfV9iejfLak9iwdm1WbwRrCEAj5VxPe0Q+I
KeznOtxzqQ5Wo5NLE9bA61sziUAFNVsTFUzphEwRohcekYyd3bBC4v/RuAjCXHVx
40z6AIksnAOGN2VABMlTeMNvPItKOCIeRLlllSqXX1gbtL1gxSW40JWdF3WPB68E
e+/1U3F7OEr7XqmNODOL6yh92QqZ8fHjG+afOL9Y2Hc4g+P1nk4w4iohQOPABqzb
MPjK7B2Rze0f9OEc51GBQu13kxkWWQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU5DS5IFdU/QwYbikgtWvkU3fDwRgwgY4GA1UdIwSBhjCBg4AU5DS5
IFdU/QwYbikgtWvkU3fDwRihYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAL9KIB7Fgvg/MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAG/N7ua8IE9IMyno0n5T57erBvLTOQ79fIJN
Mf+mKRM7qRRsdg/eumFft0rLOKo54pJ+Kim2cngCWNhkzctRHBV567AJNt4+ZDG5
```

```
hDgV0IxWO1+eaLE4qzqWP/9VrO+p3reuumgFZLVpvVpwXBBeBFUf2drUR14aWfI2
L/6VGINXYs7uP8v/2VBS7r6XZRnPBUy/R4hv5efYXnjwA9gq8+a3stC2ur8m5ySl
faKSwE4H320yAyaZWH4gpwUdbUlYgPHtm/ohRtiWPrN7KEG5Wq/REzMIjZCnxOfS
6KR6PNjlhxBsImQhmBvz6j5PLQxOxBZIpDoiK278e/1Wqm9LrBc=
-----END CERTIFICATE-----
```

Kanada (Zentral) – ca-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUIrLgixJJB5C4G8z6pZ5rB0JU2aQwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1MzU0M1oXDTI5MDQyODE1MzU0M1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
```

```
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUIrLgixJJ
B5C4G8z6pZ5rB0JU2aQwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBHiQJmzyFAaSYs8SpiRijIDZW2RIo7qBKb/pI3rqK6yOWDlPuMr6yNI81D
IrKGGftg4Z+2KETYU4x76HSf0s//vfH3QA57qFaAwddhKYy4BhteFQl/Wex3xTlX
LiwI07kwJvJy3mS6UfQ4HcvZy219tY+0iyOWrz/jVxwq7TOkCw==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAJNKhJhaJOuMMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA3Mjkx
MTM3MTdaGA8yMTk2MDEwMjExMzcxN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAhDUh6j1ACSt057nSxAcwMaGr8Ez87VA2RW2HyY8l9XoHndnxmP50Cqld
+26AJtltlqHpI1YdtnZ6OrVgVhXcVtbvte0lZ3ldEzC3PMvmISBhHs6A3SWHA9ln
InHbToLX/SWqBHLOX78HkPRaG2k0COHpRy+fG9gvz8HCiQaXCbWNFDHZev9OToNI
xhXBVzIa3AgUnGMalCYZuh5AfVRCEeALG60kxMMC8IoAN7+HG+pMdqAhJxGUcMO0
LBvmTGGeWhi04MUZWfOkwn9JjQZuyLg6B1OD4Y6s0LB2P1MovmSJKGY4JcF8Qu3z
xxUbl7Bh9pvzFR5gJN1pjM2n3gJEPwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ
UNKM+gIIHNk0G0tzv6vZBT+o/vt+tIp8lEoZwaPQh1121iw/I7ZvhMLAigx7eyvf
IxUt9/nf8pxWaeGzi98RbSmbap+uxYRynqe1p5rifTamOsguuPrhVpl12OgRWLcT
rjg/K60UMXRsmg2w/cxV45pUBcyVb5h6Op5uEVAVq+CVns13ExiQL6kk3guG4+Yq
LvP1p4DZfeC33a2Rfre2IHLsJH5D4SdWcYqBsfTpf3FQThH0l0KoacGrXtsedsxs
9aRd7OzuSEJ+mBxmzxSjSwM84Ooh78DjkdpQgv967p3d+8NiSLt3/n7MgnUy6WwB
KtDujDnB+ttEHwRRngX7
-----END CERTIFICATE-----
```

Kanada West (Calgary) – ca-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAYPouptUMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
```

```
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAMITzTJUa6cBsIfdHN69zW/
aHjUB4r1ZfKb1FMhIp9EZtEf5n+06oXjUG2+dKRSlFQeEK333ehNZsPd6uqey6TYKtHpFb5XRLS8BpqB
+7gnbAd0CBZM5o4NWesSQ1GLnTdQcGZkYG/
QESkbadoCXQTifCujJE682hTDLIVt1d4ewwCQYHKoZIzjgEAwMvADAsAhRJc4gRS/HWTkCR2MESaQEe/
jOMNQIUNoTwLvuPrmGPupPlGiHe0veZiO8=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAYPou9weMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
v4XBVH13ZCMgqlRHMqV8AWI5iO6gFn2A9sN3AZXTMqwtZeiDdebq3k6Wt7ieYvpXTg0qvgsjQIovRZWaBDBJy9x8C2hW
+w9lMQjFHkJ7Jy/
PHCJ69EzebQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGe9Snkz1A6rHBH6/5kDtYvtPYwhx2sXNxztbhkXErFk40Nw5l4
gvDVtWG7qyb6fAqgoisyAbk8K9LzxSim2S1nmT9vD84B/t/VvwQBylc
+ej8kRxMH7fquZLp7IXfmtBzyUqu6Dpbne+chG2
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALyTn5IHrIZjMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMzEyMDcx
NTM3MDFaGA8yMjAzMDUxMzE1MzcwMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA1GP5os424BJmGPCKOSgOclP7lzUiB85du03M4hfjzSOszsBpmBGFDLz1
owYHtIxlq3+Vi1Lt5Qlx3id/ov1QyaBPFWXVeklHVXy9vieCcI3TdjGjTl1W/8MM
m3X26QPcsnHM/Kk2wJ7s186MrqmdSsp3SCPpxv4vEG2Q9yR2bXY41hpc2rWlW8qU
D0JGXluvmmAdFnto20l1XWZ6xFen1h60DRugek/ufCbN+ljKy0xLqPoavH0Ybjsb
UpsAsBs7phaoN+X/5hIERfbp5LfVnqq54pNG5KNu4KynfW9+kA/WS4cJ6FTTN5t+
y0P1HvcL+BL2RuDy6T2bB21xw5WqtQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQURTvu/Dd4zDnmS5G5CfVLnmUBNOswgY4GA1UdIwSBhjCBg4AURTvu
/Dd4zDnmS5G5CfVLnmUBNOuhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALyTn5IHrIZjMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAFt523A3Aug6/F8xxyITgA8gkU0btFhlXNSP
U4U2OQ9n0tWI9WqnKNWH3KBxwY5EPitU6b3LM4xc9lDWpz7h2Pto+WhxP9LVKe6f
r8r7teTLCVZ7cfYZHzHg+flZjVpAgzE5BVfrRlj3QKpv0hYT3J1wMtI++Vorq5Nf
aPjzedehJLhmZVALwnfqfLrgv6/gmraP9Vmoa8U4D6AljNiQGYaLwyoPoRm3bUs2
```

```
v1Mh9GkEQ1b9+1pFXcqgzJJTGRuiPCyPbECI79FAnx5JM/CkGJV8HlOmjIW1qkK1
Y2qT7wzErrKLJyB53Pw15BdIM1onbDAQreZb0yZQLdoEl/tx7Uk=
-----END CERTIFICATE-----
```

Europa (Frankfurt) – eu-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUFD5GsmkxRuecttwsCG763m3u63UwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE1NTUyOVoXDTI5MDQyODE1NTUyOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
```

```
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUFD5Gsmkx
RuecttwsCG763m3u63UwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBBh0WaXlBsW56Hqk588MmJxsOrvcKfDjF57RgEDgnGnQaJcStCVWDO9UYO
JX2tdsPw+E7AjDqjsuxYaotLn3Mr3mK0sNOXq9BljBnWD4pARg89KZnZI8FN35HQ
O/LYOVHCknuPL123VmVRNs51qQA9hkPjvw21UzpDLxaUxt9Z/w==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAKD+v6LeR/WrMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
OTA4MTlaGA8yMTk1MDExNzA5MDgxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAka8FLhxs1cSJGK+Q+q/vTf8zVnDAPZ3U6oqppOW/cupCtpwMAQcky8DY
Yb62GF7+C6usniaq/9W6xPn/3o//wti0cNt6MLsiUeHqNl5H/4U/Q/fR+GA8pJ+L
npqZDG2tFi1WMvvGhGgIbScrjR4VO3TuKy+rZXMYvMRk1RXZ9gPhk6evFnviwHsE
jV5AEjxLz3duD+u/SjPp1vloxe2KuWnyC+EKInnka909sl4ZAUh+qIYfZK85DAjm
GJP4W036E9wTJQF2hZJrzsiB1MGyC1WI9veRISd30izZZL6VVXLXUtHwVHnVASrS
zZDVpzj+3yD5hRXsvFigGhY0FCVFnwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUxC2l6pvJaRflgu3MUdN6zTuP6YcwgY4GA1UdIwSBhjCBg4AUxC2l
6pvJaRflgu3MUdN6zTuP6YehYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAKD+v6LeR/WrMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAIK+DtbUPppJXFqQMv1f2Gky5/82ZwgbbfXa
HBeGSii55b3tsyC3ZW5ZlMJ7Dtnr3vUkiWbV1EUaZGOUlndUFtXUMABCb/coDndw
CAr53XTv7UwGVNe/AFO/6pQDdPxXn3xBhF0mTKPrOGdvYmjZUtQMSVb9lbMWCFfs
w+SwDLnm5NF4yZchIcTs2fdpoyZpOHDXy0xgxO1gWhKTnYbaZOxkJvEvcckxVAwJ
obF8NyJla0/pWdjhlHafEXEN8lyxyTTyOa0BGTuYOBD2cTYYynauVKY4fqHUkr3v
Z6fboaHEd4RFamShM8uvSu6eEFD+qRmvqlcodbpsSOhuGNLzhOQ=
-----END CERTIFICATE-----
```

Europa (Irland) – eu-west-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
```

```
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUakDaQ1Zqy87Hy9ESXA1pFC116HkwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MTgxMFoXDTI5MDQyODE2MTgxMFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUakDaQ1Zq
y87Hy9ESXA1pFC116HkwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQADIkn/MqaLGPuK5+prZZ5Ox4bBZLPtreO2C7r0pqU2kPM2lVPyYYydkvP0
lgSmmsErGu/oL9JNztDe2oCA+kNy17ehcsf8cw0uP861czNFKCeU8b7FgBbL+sIm
qi33rAq6owWGi/5uEcfCR+JP7W+oSYVir5r/yDmWzx+BVH5S/g==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOrmqHuaUt0vMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEwMjkw
```

```
OTA2MTlaGA8yMTk1MDQwMzA5MDYxOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAjE7nVu+aHLtzp9FYV25Qs1mvJ1JXD7J0iQ1Gs/RirW9a5ZECCtc4ssnf
zQHq2JRVr0GRchvDrbm1HaP/avtFQR/Thvfltwu9AROVT22dUOTvERdkNzveoFCy
hf52Rqf0DMrLXG8ZmQPPXPDFAv+sVMWCDftcChxRYZ6mP9O+TpgYNT1krD5PdvJU
7HcXrkNHDYqbsg8A+Mu2hzl0QkvUET83Csg1ibeK54HP9w+FsD6F5W+6ZSHGJ88l
FI+qYKs7xsjJQYgXWfEt6bbckWs1kZIaIOyMzYdPF6ClYzEec/UhIe/uJyUUNfpT
VIsI5OltBbcPF4c7Y20jOIwwI2SgOQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUF2DgPUZivKQR/Zl8mB/MxIkjZDUwgY4GA1UdIwSBhjCBg4AUF2Dg
PUZivKQR/Zl8mB/MxIkjZDWhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOrmqHuaUt0vMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGm6+57W5brzJ3+T8/XsIdLTuiBSe5ALgSqI
qnO5usUKAeQsa+kZIJPyEri5i8LEodh46DAF1RlXTMYgXXxl0YggX88XPmPtok17
l4hib/D9/lu4IaFIyLzYNSzsETYWKWoGVe7ZFz60MTRTwY2u8YgJ5dec7gQgPSGj
avB0vTIgoW41G58sfw5b+wjXCsh0nROon79RcQFFhGnvup0MZ+JbljyhZUYFzCli
31jPZiKzqWa87xh2DbAyvj2KZrZtTe2LQ48Z4G8wWytJzxEeZdREe4NoETf+Mu5G
4CqoaPR05KWkdNUdGNwXewydb3+agdCgfTs+uAjeXKNdSpbhMYg=
-----END CERTIFICATE-----
```

Europa (London) – eu-west-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
```

```
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUCgCV/DPxYNND/swDgEKGiC5I+EwwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MjkxNFoXDTI5MDQyODE2MjkxNFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUCgCV/DPx
YNND/swDgEKGiC5I+EwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQATPu/sOE2esNa4+XPEGKlEJSgqzyBSQLQc+VWo6FAJhGG9fp7D97jhHeLC
5vwfmtTAfnGBxadfAOT3ASkxnOZhXtnRna460LtnNHm7ArCVgXKJo7uBn6ViXtFh
uEEw4y6p9YaLQna+VC8Xtgw6WKq2JXuKzuhuNKSFaGGw9vRcHg==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANBx0E2bOCEPMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNjA4MTEx
NDU2NDJaGA8yMTk2MDExNTE0NTY0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEArYS3mJLGaMrh2DmiPLbqr4Z+xWXTzBWCjOwpsuHE9H6dWUUyl2Bgnu+Z
d8QvW306Yleec45M4F2RA3J4hWHtShzsMlOJVRt+YulGeTf9OCPr26QmIFfs5nD4
fgsJQEry2MBSGA9Fxq3Cw6qkWcrOPsCR+bHOU0XykdKl0MnIbpBf0kTfciAupQEA
dEHnM2J1L2iI0NTLBgKxy5PXLH9weX20BFauNmHH9/J07OpwL20SN5f8TxcM9+pj
Lbk8h1V4KdIwVQpdWkbDL9BCGlYjyadQJxSxz1J343NzrnDM0M4h4HtVaKOS7bQo
Bqt2ruopLRCYgcuFHck/1348iAmbRQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBG
wujwU1Otpi3iBgmhjMClgZyMMn0aQIxMigoFNqXMUNx1Mq/e/Tx+SNaOEAu0n2FF
aiYjvY0/hXOx75ewzZvM7/zJWIdLdsgewpUqOBH4DXFhbSk2TxggSPb0WRqTBxq5
Ed7F7+7GRIeBbRzdLqmISDnfqey8ufW0ks51XcQNomDIRG5s9XZ5KHviDCar8FgL
HngBCdFI04CMagM+pwTO9XN1Ivt+NzUj208ca3oP1IwEAd5KhIhPLcihBQA5/Lpi
```

```
h1s3170z1JQ1HZbDrH1pgp+8hSI0DwwDVb3IIH8kPR/J0Qn+hvOl2HOpaUg2Ly0E
pt1RCZe+W7/dF4zsbqwK
-----END CERTIFICATE-----
```

Europa (Mailand) – eu-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAqwCCQCMElHPdwG37jAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTA0MjkyMDM1MjJaFw00
NTA0MjkyMDM1MjJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbYwggErBgcqhkjOOAQBMIIBHgKBgQDAkoL4YfdMI/MrQ0oL
NPfeEk94eiCQA5xNOnU7+2eVQtEqjFbDADFENh1p3sh9Q9OoheLFH8qpSfNDWn/0
ktCS909ApTY6Esx1ExjGSeQq/U+SC2JSuuTT4WFMKJ63a/czMtFkEPPnVIjJJJmT
HJSKSsVUgpdDIRvJXuyB0zdB+wIVALQ3OLaVGdlPMNfS1nD/Yyn+32wnAoGAPBQ3
7XHg5NLOS4326eFRUT+4ornQFjJjP6dp3pOBEzpImNmZTtkCNNUKE4Go9hv5T4lh
R0pODvWv0CBupMAZVBP9ObplXPCyEIZtuDqVa7ukPOUpQNgQhLLAqkigTyXVOSmt
ECBj9tu5WNP/x3iTZTHJ+g0rhIqpgh012UwJpKADgYQAAoGAV1OEQPYQUg5/M3xf
6vE7jKTxxyFWEyjKfJK7PZCzOIGrE/swgACy4PYQW+AwcUweSlK/Hx2OaZVUKzWo
wDUbeu65DcRdw2rSwCbBTU342sitFo/iGCV/Gjf+BaiAJtxniZze7J1ob8vOBeLv
uaMQmgOYeZ5e0fl04GtqPl+lhcQwCQYHKoZIzjgEAwMwADAtAhQdoeWLrkm0K49+
AeBK+j6m2h9SKQIVAIBNhS2a8cQVABDCQXVXrc0tOmO8
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICNjCCAZ+gAwIBAgIJAOZ3GEIaDcugMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTEwMjQx
NTE5MDlaGA8yMTk5MDMyOTE1MTkwOVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQCjiPgW3vsXRj4JoA16WQDyoPc/eh3QBARaApJEc4nPIGoUolpAXcjFhWplo2O+
ivgfCsc4AU9OpYdAPha3spLey/bhHPRi1JZHRNqScKP0hzsCNmKhfnZTIEQCFvsp
DRp4zr91/WS06/flJFBYJ6JHhp0KwM81XQG59lV6kkoW7QIDAQABMA0GCSqGSIb3
DQEBCwUAA4GBAGLLrY3P+HH6C57dYgtJkuGZGT2+rMkk2n81/abzTJvsqRqGRrWv
XRKRXlKdM/dfiuYGokDGxiC0Mg6TYy6wvsR2qRhtXW1OtZkiHWcQCnOttz+8vpew
wx8JGMvowtuKB1iMsbwyRqZkFYLcvH+Opfb/Aayi20/ChQLdI6M2R5VU
```

```
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAO/+DgYF78KwMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTA0Mjky
MDM1MjJaGA8yMTk4MTAwMjIwMzUyMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAv1ZLV+Z/P6INq+R1qLkzETBg7sFGKPiwHekbpuB6lrRxKHhj8V9vaReM
lnv1Ur5LAPpMPYDsuJ4WoUbPYAqVqyMAo7ikJHCCM1cXgZJefgN6z9bpS+uA3YVh
V/0ipHh/X2hc2S9wvxKWiSHu6Aq9GVpqL035tJQD+NJuqFd+nXrtcw4yGtmvA6wl
5Bjn8WdsP3xOTKjrByYY1BhXpP/f1ohU9jE9dstsRXLa+XTgTPWcWdCS2oRTWPGR
c5Aeh47nnDsyQfP9gLxHeYeQItV/BD9kU/2Hn6mnRg/B9/TYH8qzlRTzLapXp4/5
iNwusrTNexGl8BgvAPrfhjDpdgYuTwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQB7
5ya11K/hKgvaRTvZwVV8GlVZt0CGPtNvOi4AR/UN6TMm51BzUB5nurB4z0R2MoYO
Uts9sLGvSFALJ4otoB77hyNpH3drttU1CVVwal/yK/RQLSon/IoUkaGEbqalu+mH
nYad5IG4tEbmepX456XXcO58MKmnczNbPyw3FRzUZQtI/sf94qBwJ1Xo6XbzPKMy
xjL57LHIZCssD+XPifXay69OFlsCIgLim11HgPkRIHEOXLSf3dsW9r+4CjoZqB/Z
jj/P4TLCxbYCLkvglwaMjgEWF40Img0fhx7yT2X92MiSrs3oncv/IqfdVTiN8OXq
jgnq1bf+EZEZKvb6UCQV
-----END CERTIFICATE-----
```

Europa (Paris) – eu-west-3

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
```

```
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUaC9fX57UDr6u1vBvsCsECKBZQyIwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MzczOFoXDTI5MDQyODE2MzczOFowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUaC9fX57U
Dr6u1vBvsCsECKBZQyIwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCARv1bQEDaMEzYI0nPlu8GHcMXgmgA94HyrXhMMcaIlQwocGBs6VILGVhM
TXP2r3JFaPEpmXSQNQHvGA13clKwAZbni8wtzv6qXb4L4muF34iQRHF0nYrEDoK7
mMPR8+oXKKuPO/mv/XKo6XAV5DDERdSYHX5kkA2R9wtvyZjPnQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALWSfgHuT/ARMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNzA1MzEx
MTE4MTZaGA8yMTk2MTEwMzExMTgxNlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy5V7KDqnEvF3DrSProFcgu/oL+QYD62b1U+Naq8aPuljJe127Sm9WnWA
EBdOSASkOaQ9fzjCPoG5SGgWKxYoZjsevHpmzjVv9+Ci+F57bSuMbjgUbvbRIFUB
bxQojVoXQPHgK5v433ODxkQ4sjRyUbf4YV1AFdfU7zabC698YgPVOExGhXPlTvco
8mlc631ubw2g52j0lzaozUkHPSbknTomhQIvO6kUfX0e0TDMH4jLDG2ZIrUB1L4r
OWKG4KetduFrRZyDHF6ILZu+s6ywiMicUd+2UllDFC6oas+a8D11hmO/rpWU/ieV
jj4rWAFrsebpn+Nhgy96iiVUGS2LuQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDE
```

```
iYv6FQ6knXCg+svlcaQG9q59xUC5z8HvJZ1+SxzPKKC4PKQdKvIIfE8GxVXqlZG1
cl5WKTFDMapnzb9RV/DTaVzWx3cMYT77vm1Hl1XGjhx611CGcENH1egI3lOTILsa
+KfopuJEQQ9TDMAIkGjhA+KieU/U5Ctv9fdej6d0GC6OEuwKkTNzPWue6UMq8d4H
2xqJboWsE1t4nybEosvZfQJcZ8jyIYcYBnsG13vCLM+ixjuU5MVVQNMY/gBJzqJB
V+U0QiGiuT5cYgY/QihxdHt99zwGaE0ZBC7213NKrlNuLSrqhDI2NLu8NsExqOFy
OmY0v/xVmQUQl26jJXaM
-----END CERTIFICATE-----
```

Europa (Spanien) – eu-south-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC8DCCAq
+gAwIBAgIGAXjwLk46MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAGG2m8EKmaf5qQqj3Z
+rzSaTaXE3B/R/4A2VuGqRYR7MljPtwdmU6/3CPjCACcZmTIcOAKbFiDHqadQgBZXfzGpzw8Zo
+eYmmk5fXycgnj57PYH1dIWU6I7mCbAah5MZMcmHaTmIsomGrhcnWB8d8qOU7oZ0UWK4lbiAQs1MihoUwCQYHKoZIzjg
WmbaU7YM5GwCFCvIJOesO5hZ8PHC52dAR8WWC6oe
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjwLkiaMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
VvR1+45Aey5zn3vPk6xBm5o9grSDL6D2iAuprQnfVXn8CIbSDbWFhA3fi5ippjKkh3sl8VyCvCOUXKdOaNrYBrPRkrdH
+3m/
rxIUZ2IK1fDlC6sWAjddf6sBrV2w2a78H0H8EwuwiSgttURBjwJ7KPPJCqaqrQIDAQABMA0GCSqGSIb3DQEBBQUAA4GB
+FzqQDzun/
iMMzcFucmLMl5BxEblrFXOz7IIuOeiGkndmrqUeDCykztLku45s7hxdNy4ltTuVAaE5aNBdw5J8U1mRvsKvHLy2ThH6h
+hBgiphYp84DUbWVYeP8YqLEJSqscKscWC
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALWSmO6DvSpQMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
```

```
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
MzU4NDNaGA8yMjAxMTIyMjEzNTg0M1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAuAAhuSpsHC00/fD2zNlBDpNLRndi9qbHsNeuz3WqN7Samj2aSrM2hS+i
hUxx0BspZj0tZCOsbpPZ+i74NOEQtFeqQoEGvKhB1nJiF4y5I81HDhs5qHvoIivm
7rbbik3zgm1PqS/DmDjVQaXPcD31Rd9ILwBmWEwJqHigyNVlxYtCzTQcrlBrvNZM
dnNgCDAdX/HBEFxx9O12xeu0bSt0s+PJWZ1RTbYrNe7LIH6ntUqHxP/ziQ5trXEZ
uqy7aWk1L8uK4jmyNph0lbaqBa3Y6pYmU1nC27UE4i3fnPB0LSiAr+SrwVvX1g4z
ilo8kr+tbIF+JmcgYLBvO8Jwp+EUqQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUwvGzKJL9A5LReJ4Fxo5K6I20xcowgY4GA1UdIwSBhjCBg4AUwvGz
KJL9A5LReJ4Fxo5K6I20xcqhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALWSmO6DvSpQMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAJAZd31jyoTGLawAD2+v/vQsaB9vZIx5EImi
G8YGkd61uFWeNhAmtrwyE/i6FDSIphDrMHBkvw/D3BsqK+Ev/JOK/VYuaYDx/8fp
H4cwp9jC57CXzdIDREWNf6M9PsHFg2WA9XNNtClOZL5WJiJwel8eDSg+sqJUxE0l
MW+QChq/20F6niyaRK4bXrZq14as7h+F9u3A9xHEOVP7Zk9C2ehrBXzCMLSDt3GV
fEuMea2RxMhozwz34Hkdb6j18qoCfygubulovRNQjKw/cEmgPR16KfZPP5caILVt
9qkYPvePmbiVswZDee73cDymJYxLqILpOZwyXvUH8StiH42FHZQ=
-----END CERTIFICATE-----
```

Europa (Stockholm) – eu-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
```

```
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUN1c9U6U/xiVDFgJcYKZB4NkH1QEwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2MDYwM1oXDTI5MDQyODE2MDYwM1owXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUN1c9U6U/
xiVDFgJcYKZB4NkH1QEwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBTIQdoFSDRHkpqNPUbZ9WXR2O5v/9bpmHojMYZb3Hw46wsaRso7STiGGX/
tRqjIkPUIXsdhZ3+7S/RmhFznmZc8e0bjU4n5vi9CJtQSt+1u4E17+V2bF+D3h/7
wcfE0l3414Q8JaTDtfEf/aF3F0uyBvr4MDMd7mFvAMmDmBPSlA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALc/uRxg++EnMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
NDAwMTFaGA8yMTk3MDkxMzE0MDAxMVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzwCGJEJIxqtr2PD2a1mA6LhRzKhTBa1AZsg3eYfpETXIVlrpojMfvVoN
qHvGshWLgrGTT6os/3gsaADheSaJKavxwX3X6tJA8fvEGqr3a1C1MffH9hBWbQqC
LbfUTAbkwis4GdTUwOwPjT1Cm3u9R/VzilCNwkj7iQ65AFAI8Enmsw3UGldEsop4
yChKB3KW3WI0FTh0+gD0YtjrqqYJxpGOYBpJp5vwdd3fZ4t1vidmDMs7liv4f9Bx
p0oSmUobU4GUlFhBchK1DukICVQdnOVzdMonYm7s+HtpFbVHR8yf6QoixBKGdSal
mBf7+y0ixjCn0pnC0VLVooGo4mi17QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQDG
4ONZiixgk2sjJctwbyD5WKLTH6+mxYcDw+3y/F0fWz561YORhP2FNnPOmEkf0Sl/
Jqk4svzJbCbQeMzRoyaya/46d7UioXMHRZam5IaGBhOdQbi97R4VsQjwQj0RmQsq
```

```
yDueDyuKTwWLK9KnvI+ZA6e6bRkdNGflK4N8GGKQ+fBhPwVELkbT9f16OJkezeeN
S+F/gDADGJgmPXfjogICb4Kvshq0H5Lm/xZlDULF2g/cYhyNY6EOI/eS5m1I7R8p
D/m6WoyZdpInxJfxW616OMkxQMRVsruLTNGtby3u1g6ScjmpFtvAMhYejBSdzKG4
FEyxIdEjoeO1jhTsck3R
-----END CERTIFICATE-----
```

Europa (Zürich) – eu-central-2

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXiKJnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAYNjaCNg/
cfgQOl1BUj5ClUulqwZ9Q+SfDzPZh9D2C0VbiRANiZoxrV8RdgmzzC5T7VcriVwjwvta2Ch//
b+sZ86E5h0XWWr+BeEjD9cu3eDj12XB5sWEbNHNx49p5Tmtu5r2LDtlL8X/
Rpfalu2Z2OJgjFJWGf7hRwxe456n
+lowCQYHKoZIzjgEAwMvADAsAhRChsLcj4U5CVb2cp5M0RE1XbXmhAIUeGSnH+aiUQIWmPEFja+itWDufIk=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjSGFGiMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
opKZAUusJx2hpgU3pUHhlp9ATh/VeVD582jTd9IY
+8t5MDa6Z3fGliByEiXz0LEHdi8MBacLREu1TwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAILlpoE3k9o7KdALAxsFJNit
+g3RMzdbiFM+7MA63Nv5fsf+0xgcjSNBElvPCDKFvTJl4QQhToy056llO5GvdS9RK
+H8xrP2mrqngApoKTApv93vHBixgFSn5KrczRO0YSm3OjkqbydU7DFlmkXXR7GYE+5jbHvQHYiT1J5sMu
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJALvT012pxTxNMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTgx
```

```
NTEyMDdaGA8yMjAxMTIyMjE1MTIwN1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAyn+Lsnq1ykrfYlZkk6aAAYNReNd9Iw8AUwCBkgOr2eBiBBepYxHwU85N
++moQ+j0EV2VaahBeTLShGZZS1HsyK8+cYT2QzpghIoamcYhrPXyIxlWiRQlaqSg
OFiE9bsqL3rCF5Vz+tOiTe5W/7ojfOFls6++g7ZpobwJlpMbuJepqyeHMPyjvO5A
age81lJewc4bxo2ntaW0HCqNksqfYB78j6X6kn3PFpX7FaYAwZA+Xx6C7UCY7rNi
UdQzfAo8htfJi4chz7frpUdQ9kl3IOQrsLshBB5fFUjl09NiFipCGBwi+8ZMeSn1
5qwBI01BWXPfG7WX6Owyjhmh6JtE1wIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU8HN4vvJrsZgPQeksMBgJb9xR1yYwgY4GA1UdIwSBhjCBg4AU8HN4
vvJrsZgPQeksMBgJb9xR1yahYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJALvT012pxTxNMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAGlHYDtcHpfBvdHx9HeQE8HgNugJUPdEqxun
t9U33p8VFrs+uLPtrOd9HDJEGvvs5h84EUie/oGJxRt7V1Vlid1PvHf6cRmpjgqY
YdggAVkZtY/PnFVmzf2bMVlSQPrqCl7U0zaw2Kvnj4zgX0rZyCetgrRZSUSxotyp
978Wy9ccXwVSeYG/YAr5rJpS6ZH7eRQvUY0IzwFNeaOPgOTEVpcjWlV6+MQEvsEx
W85q+s6AVr49eppEx8SLJsl0C23yB+L+t32tAveQImRWtJMpzZ5cxh/sYgDVeoC0
85H1NK/7H9fAzT1cPu1oHSnB0xYzzHGOAmXmusMfwUk8fL1RQkE=
-----END CERTIFICATE-----
```

Israel (Tel Aviv) – il-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq+gAwIBAgIGAX0QPi
+9MAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcMB1NlYX
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/
hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAbazCL5XXyPmcw3+oMYQUF5/9YogW6D0FZbYuyPgjOoUwWdl6fjlzWca
pq+l1ezuK2DFOzNTEyPEwwCQYHKoZIzjgEAwMvADAsAhRt1jkpXsvrS
+xTo2M9h2s2uLAhEQIUOZ2FcnTSrshF2EIdixZZwtNv66Q=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
```

```
MIICMzCCAZygAwIBAgIGAX0QQGVLMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
+S8vOy5hpLoRe4RkOrY0cM3bN07GdEMlin5mU0y1t8y3ct4YewvmkgT42kTyMM
+t1K4S0xsqjXxxS716uGYh7eWtkxrCihj8AbXN/6pa095h
+7TZyl2n83keiNUzM2KoqQVMwIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADwA6VVEIIZD2YL00F12po40xDLzIc9XvqFPS
FmU7H8s62/jD6cOR1A1cClIyZUe1yT1ZbPySCs43J+Thr8i8FSRxzDBSZZi5foW
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAOVp1h2I9wW7MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA3MTUx
MjQ0MTJaGA8yMjAxMTIxOTEyNDQxMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEA13PkyWvl61iV/SYfO1UFO76UpDfPm2SF/Rz/o33cm699X++EYPxTnoEc
vmWeS0I7eDXc4OCUiToG0sEx0klE0CX1Z1tK6qJ+zgWQLZ9SZEC9H0NsSA6LhrHu
Nq0dzeK3LjhdfcX46/4GqdiptpdTuM4m/hOQ5yx4JMQ/n1sdpv4M5VLRWwWW9Lem
ufb79Id7O9SispxgRsz1KXIjp7N9S4BY7itSXz97uSyzTqEjWZ6mDUhTu3t21GKC
6flALGTTrG2yghEhz53rkvLsvwzjPSSlT6LIf0mrRPzHaf+EdaKoasElE1SHh+ZH
9mI81HywpE+HZ+W+5hBCvjYp90Y1fwIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQU58tN2JO+yEGq5JbIXxGi4vRVPyIwgY4GA1UdIwSBhjCBg4AU58tN
2JO+yEGq5JbIXxGi4vRVPyKhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAOVp1h2I9wW7MBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBANBN0e1EqNy4+IU2yQzMJ+Wy5ZIOtTP6GSBR
7muVY1bDeAwtNTEOpwgrZVlC7/xq5Q0LC1y0Z70hHXEf8au7qStaAoUtxzvhTAZI
NC0lwoFU56UFw4N0vZII17iqEfoqRC4PpI3OxqEJHFy0VLlvAzJoKB4QLLqDAYVA
LXCiOLoVT+y9tRYsxw5MyO0Bi6fxQIIADl2bE9xkunTN1Jkkwqo3LxNy/ryz4QWR
8K7jHUItifv4h/hxBKpHEquN8CkdvM9oeGl7I8PFrSFEpGr1euDXY0euZzzYiDBV
m6GpTJgzpVsEuIX52dPcPemwQncoIfZyhWDW85MJUnby2WTEcFo=
-----END CERTIFICATE-----
```

Naher Osten (Bahrain) – me-south-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7jCCAq4CCQCVWIgSmP8RhTAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xOTAyMDUxMzA2MjFaFw00
```

```
NTAyMDUxMzA2MjFaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbgwggEsBgcqhkjOOAQBMIIBHwKBgQDcwojQfgWdV1QliO0B
8n6cLZ38VE7ZmrjZ9OQV//Gst6S1h7euhC23YppKXi1zovefSDwFU54zi3/oJ++q
PHlP1WGL8IZ34BUgRTtG4TVolvp0smjkMvyRu5hIdKtzjV93Ccx15gVgyk+o1IEG
fZ2Kbw/Dd8JfoPS7KaSCmJKxXQIVAIZbIaDFRGa2qcMkW2HWASyNDl7bAoGBANtz
IdhfMq+l2I5iofY2oj3HI21Kj3LtZrWEg3W+/4rVhL3lTm0Nne1rl9yGujrjQwy5
Zp9V4A/w9w2O10Lx4K6hj34Eefy/aQnZwNdNhv/FQP7Az0fju+Yl6L13OOHQrL0z
Q+9cF7zEosekEnBQx3v6psNknKgD3Shgx+GO/LpCA4GFAAKBgQCVS7m77nuNAlZ8
wvUqcooxXMPkxJFl54NxAsAul9KP9KN4svm0O3Zrb7t2FOtXRM8zU3TqMpryq1o5
mpMPsZDg6RXo9BF7Hn0DoZ6PJTamkFA6md+NyTJWJKvXC7iJ8fGDBJqTciUHuCKr
12AztQ8bFWsrTgTzPE3p6U5ckcgV1TAJBgcqhkjOOAQDAy8AMCwCFB2NZGWm5EDl
86ayV3c1PEDukgQIAhQow38rQkN/VwHVeSW9DqEshXHjuQ==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDPDCCAqWgAwIBAgIJAMl6uIV/zqJFMA0GCSqGSIb3DQEBCwUAMHIxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0dGxlMSAw
HgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwRZWMyLmFt
YXpvbmF3cy5jb20wIBcNMTkwNDI2MTQzMjQ3WhgPMjE5ODA5MjkxNDMyNDdaMHIx
CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApXYXNoaW5ndG9uMRAwDgYDVQQHDAdTZWF0
dGxlMSAwHgYDVQQKDBdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzEaMBgGA1UEAwwR
ZWMyLmFtYXpvbmF3cy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALVN
CDTZEnIeoX1SEYqq6k1BV0ZlpY5y3KnoOreCAE589TwS4MX5+8Fzd6AmACmugeBP
Qk7Hm6b2+g/d4tWycyxLaQlcq81DB1GmXehRkZRgGeRge1ePWd1TUA0I8P/QBT7S
gUePm/kANSFU+P7s7u1NNl+vynyi0wUUrw7/wIZTAgMBAAGjgdcwgdQwHQYDVR0O
BBYEFILtMd+T4YgH1cgc+hVsVOV+480FMIGkBgNVHSMEgZwwgZmAFILtMd+T4YgH
1cgc+hVsVOV+480FoXakdDByMQswCQYDVQQGEwJVUzETMBEGA1UECAwKV2FzaGlu
Z3RvbjEQMA4GA1UEBwwHU2VhdHRsZTEgMB4GA1UECgwXQW1hem9uIFdlYiBTZXJ2
aWNlcyBMTEMxGjAYBgNVBAMMEWVjMi5hbWF6b25hd3MuY29tggkAyXq4hX/OokUw
DAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQsFAAOBgQBhkNTBIFgWFd+ZhC/LhRUY
4OjEiykmbEp6hlzQ79T0Tfbn5A4NYDI2icBP0+hmf6qSnIhwJF6typyd1yPK5Fqt
NTpxxcXmUKquX+pHmIkK1LKDO8rNE84jqxrxRsfDi6by82fjVYf2pgjJW8R1FAw+
mL5WQRFexbfB5aXhcMo0AA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANZkFlQR2rKqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
```

```
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xOTAyMDUx
MzA2MjBaGA8yMTk4MDcxMTEzMDYyMFowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAy4Vnit2eBpEjKgOKBmyupJzJAiT4fr74tuGJNwwa+Is2vH12jMZn9Il1
UpvvEUYTIboIgISpf6SJ5LmV5rCv4jT4a1Wm0kjfNbiIlkUi8SxZrPypcw24m6ke
BVuxQZrZDs+xDUYIZifTmdgD50u5YE+TLg+YmXKnVgxBU6WZjbuK2INohi71aPBw
2zWUR7Gr/ggIpf635JLU3KIBLNEmrkXCVSnDFlsK4eeCrB7+UNak+4BwgpuykSGG
Op9+2vsuNqFeU1l9daQeG9roHR+4rIWSPa0opmMxv5nctgypOrE6zKXx2dNXQldd
VULv+WH7s6Vm4+yBeG8ctPYH5GOo+QIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBs
ZcViiZdFdpcXESZP/KmZNDxB/kktlIEIhsQ+MNn29jayE5oLmtGjHj5dtA3XNKlr
f6PVygVTKbtQLQqunRT83e8+7iCZMKI5ev7pITUQVvTUwI+Fc01JkYZxRFlVBuFA
WGZO+98kxCS4n6tTwVt+nSuJr9BJRVC17apfHBgSS8c5OWna0VU/Cc9ka4eAfQR4
7pYSDU3wSRE01cs30q34lXZ629IyFirSJ5TTOIc0osNL7vwMQYj8HOn4OBYqxKy8
ZJyvfXsIPh0Na76PaBIs6ZlqAOflLrjGzxBPiwRM/XrGmF8ze4KzoUqJEnK13O6A
KHKgfiigQZ1+gv5FlyXH
-----END CERTIFICATE-----
```

Naher Osten (VAE) – me-central-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7zCCAq
+gAwIBAgIGAXjXhqnnMAkGByqGSM44BAMwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgMEFdhc2hpbmd0b24gU3RhdGUxED
U4EddRIpUt9KnC7s5Of2EbdSPO9EAMMeP4C2USZpRV1AIlH7WT2NWPq/
xfW6MPbLm1Vs14E7gB00b/JmYLdrmVClpJ+f6AR7ECLCT7up1/63xhv4O1fnxqimFQ8E
+4P208UewwI1VBNaFpEy9nXzrith1yrv8iIDGZ3RSAHHAhUAl2BQjxUjC8yykrmCouuEC/
BYHPUCgYEA9+GghdabPd7LvKtcNrhXuXmUr7v6OuqC+VdMCz0HgmdRWVeOutRZT
+ZxBxCBgLRJFnEj6EwoFhO3zwkyjMim4TwWeotUfI0o4KOuHiuzpnWRbqN/C/ohNWLx
+2J6ASQ7zKTxvqhRkImog9/hWuWfBpKLZl6Ae1UlZAFMO/7PSSoDgYQAAoGAW+csuHsWp/7/
pv8CTKFwxsYudxuR6rbWaHCykIeAydXL9AWnphK6yp1ODEMBFl68Xq8Hp23sOWyf8moOhqCom9+0+ovuUFdpvCie86bp
TOZU568Ty1ff3dDWbdRzeNQRHodRG+XEQSizMkAreeWt4kBa+PUwCQYHKoZIzjgEAwMvADAsAhQD3Z
+XGmzKmgaLgGcVX/Qf1+Tn4QIUH1cgksBSVKbWj81tovBMJeKgdYo=
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIICMzCCAZygAwIBAgIGAXjRrnDjMA0GCSqGSIb3DQEBBQUAMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIDBBXYXNoaW5n
KyA6zyruJQrYy00a6wqLA7eeUzk3bMiTkLsTeDQfrkaZMfBAjGaaOymRo1C3qzE4rIenmahvUplu9ZmLwL1idWXMRX2R
+d2SeoKOKQWoc2UOFZMHYxDue7zkyk1CIRaBukTeY13/
```

```
RIrlc6X61zJ5BBtZXlHwayjQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBABTqTy3R6RXKPW45FA+cgo7YZEj/
Cnz5YaoUivRRdX2A83BHuBTvJE2+WX00FTEj4hRVjameE1nENoO8Z7fUVloAFDlDo69fhkJeSvn51D1WRrPnoWGgEfr1
B+Wqm3kVEz/QNcz6npmA6
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAM4h7b1CVhqqMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0yMjA0MTEx
MDE1MDNaGA8yMjAxMDkxNTEwMTUwM1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEApybTWfMOhSoMpqPo72eqAmnn1dXGZM+G8EoZXzwHwT/+IHEXNB4q5N6k
tudYLre1bJxuzEw+iProSHjmb9bB9YscRTofjVhBlt35Fc+i8BaMeH94SR/eE8QO
mll8gnLNW3d62lyuhzuyv1e5wVlRqzYw+X2zRH4/wRDOCOpzjKoHIgyPKsMgwsw5
aTZhNMsGxZN9dbkf0iCGeQLDytwU/JTh/HqvSr3VfUOapTJJiyAxoCtZWgp1/7wC
RvOCSMRJobpUqxZgl/VsttwNkikSFz1wGkcYeSQvk+odbnYQckA8tdddoVI56eD4
qtREQvfpMAX5v7fcqLexl5d5vH8uZQIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUOadrbTs+OhzwoAgUJ7RqQNdwufkwgY4GA1UdIwSBhjCBg4AUOadr
bTs+OhzwoAgUJ7RqQNdwufmhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAM4h7b1CVhqqMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBAICTdAOGEOnII8HaGCpCB8us/hGFaLptJaAf
D5SJAyVy66/mdfjGzE1BKkKxnbxemEVUIzbRidOnyilB+pKwN3edAjTZtWdpVA0V
R/G/qQPmcVljtycBz4VC6SuOUYflGzLH1GZ6GJWbuDtFzw8r7HGdRN1wrEPe3UF2
sMpuVezqnRUdvVRoVQP4jFgNsE7kNvtn2NiPhb/CtrxpcwIQ7r6YeoHcBSheuV1Z
xZDHynC3KUprQGx1+Z9QqPrDf180MaoqAlTl4+W6Pr2NJYrVUFGS/ivYshMg574l
CPU6r4wWZSKwEUXq4BInYX6z6iclp/p/J5QnJp2mAwyi6M+I13Y=
-----END CERTIFICATE-----
```

Südamerika (São Paulo) – sa-east-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
```

```
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUX4Bh4MQ86Roh37VDRRX1MNOB3TcwDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDQyOTE2NDYwOVoXDTI5MDQyODE2NDYwOVowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCHvRjf/0kStpJ248khtIaN8qkDN3tkw4VjvA9nvPl2anJO+eIB
UqPfQG09kZlwpWpmyO8bGB2RWqWxCwuB/dcnIob6w420k9WY5C0IIGtDRNauN3ku
vGXkw3HEnF0EjYr0pcyWUvByWY4KswZV42X7Y7XSS13hOIcL6NLA+H94/QIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQUJdbMCBXKtvCcWdwUUizvtUF2
UTgwgZkGA1UdIwSBkTCBjoAUJdbMCBXKtvCcWdwUUizvtUF2UTihYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUX4Bh4MQ8
6Roh37VDRRX1MNOB3TcwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBnhocfH6ZIX6F5K9+Y9V4HFk8vSaaKL5ytw/P5td1h9ej94KF3xkZ5fyjN
URvGQv3kNmNJBoNarcP9I7JIMjsNPmVzqWawyCEGCZImoARxSS3Fc5EAs2PyBfcD
9nCtzMTaKO09Xyq0wqXVYn1xJsE5d5yBDsGrzaTHKjxo61+ezQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIEEjCCAvqgAwIBAgIJAMcyoxx4U0xxMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQw
ODU4MDJaGA8yMTk1MDExNzA4NTgwMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
```

```
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAw45IhGZVbQcy1fHBqzROhO8CsrDzxj/WP4cRbJo/2DAnimVrCCDs5O86
FA39Zo1xsDuJHDlwMKqeXYXkJXHYbcPWc6EYYAnR+PlLG+aNSOGUzsy202S03hT0
B20hWPCqpPp39itIRhG4id6nbNRJOzLm6evHuepMAHR4/OV7hyGOiGaV/v9zqiNA
pMCLhbh2xk0PO35HCVBuWt3HUjsgeks2eEsu9Ws6H3JXTCfiqp0TjyRWapM29OhA
cRJfJ/d/+wBTz1fkWOZ7TF+EWRIN5ITEadlDTPnF1r8kBRuDcS/lIGFwrOOHLo4C
cKoNgXkhTqDDBDu6oNBb2rS0K+sz3QIDAQABo4HUMIHRMAsGA1UdDwQEAwIHgDAd
BgNVHQ4EFgQUqBy7D847Ya/w321Dfr+rBJGsGTwwgY4GA1UdIwSBhjCBg4AUqBy7
D847Ya/w321Dfr+rBJGsGTyhYKReMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQ4IJAMcyoxx4U0xxMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDQYJKoZIhvcNAQELBQADggEBACOoWSBf7b9AlcNrl4lr3QWWSc7k90/tUZal
PlT0G3Obl2x9T/ZiBsQpbUvs0lfotG0XqGVVHcIxF38EbVwbw9KJGXbGSCJSEJkW
vGCtc/jYMHXfhx67Szmftm/MTYNvnzsyQQ3v8y3Rdah+xe1NPdpFrwmfL6xe3pFF
cY33KdHA/3PNLdn9CaEsHmcmj3ctaaXLFIzZhQyyjtsrgGfTLvXeXRokktvsLDS/
YgKedQ+jFjzVJqgr4NjfY/Wt7/8kbbdhzaqlB5pCPjLLzv0zp/XmO6k+JvOePOGh
JzGk5t1QrSju+MqNPFk3+1O7o910Vrhqw1QRB0gr1ExrviLbyfU=
-----END CERTIFICATE-----
```

China (Peking) – cn-north-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
```

```
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAOtrM5XLDSjCMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA4MTQx
MDAxNDJaGA8yMTk1MDExNzEwMDE0MlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAvVBz+WQNdPiM9S+aUULOQEriTmNDUrjLWLr7SfaOJScBzis5D5ju0jh1
+qJdkbuGKtFX5OTWTm8pWhInX+hIOoS3exC4BaANoa1A3o6quoG+Rsv72qQf8LLH
sgEi6+LMlCN9TwnRKOToEabmDKorss4zFl7VSsbQJwcBSfOcIwbdRRaW9Ab6uJHu
79L+mBR3Ea+G7vSDrVIA8goAPkae6jY9WGw9KxsOrcvNdQoEkqRVtHo4bs9fMRHU
Etphj2gh4ObXlFN92VtvzD6QBs3CcoFWgyWGvzg+dNG5VCbsiiuRdmii3kcijZ3H
Nv1wCcZoEAqH72etVhsuvNRC/xAP8wIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA8
ezx5LRjzUU9EYWYhyYIEShFlP1qDHs7F4L46/5lc4pL8FPoQm5CZuAF31DJhYi/b
fcV7i3n++/ymQbCLC6kAg8DUB7NrcROll5ag8d/JXGzcTCnlDXLXx1905fPNa+jI
0q5quTmdmiSi0taeaKZmyUdhrB+a7ohWdSdlokEIOtbH1P+g5yll3bI2leYE6Tm8
LKbyfK/532xJPqO9abx4Ddn89ZEC6vvWVNDgTsxERg992Wi+/xoSw3XxkgAryIv1
```

```
zQ4dQ6irFmXwCWJqc6kHg/M5W+z60S/94+wGTXmp+19U6Rkq5jVMLh16XJXrXwHe
4KcgIS/aQGVgjM6wivVA
-----END CERTIFICATE-----
```

China (Ningxia) – cn-northwest-1

DSA

```
-----BEGIN CERTIFICATE-----
MIIDNjCCAh4CCQD3yZ1w1AVkTzANBgkqhkiG9w0BAQsFADBcMQswCQYDVQQGEwJV
UzEZMBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEg
MB4GA1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEMwIBcNMTUwNTEzMDk1OTE1
WhgPMjE5NDEwMTYwOTU5MTVaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNo
aW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24g
V2ViIFNlcnZpY2VzIExMQzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AMWk9vyppSmDU3AxZ2Cy2bvKeK3F1UqNpMuyeriizi+NTsZ8tQqtNloaQcqhto/l
gsw9+QSnEJeYWnmivJWOBdn9CyDpN7cpHVmeGgNJL2fvImWyWe2f2Kq/BL9l7N7C
P2ZT52/sH9orlck1n2zO8xPi7MItgPHQwu3OxsGQsAdWucdxjHGtdchulpo1uJ31
jsTAPKZ3p1/sxPXBBAgBMatPHhRBqhwHO/Twm4J3GmTLWN7oVDds4W3bPKQfnw3r
vtBj/SM4/IgQ3xJslFcl90TZbQbgxIi88R/gWTbs7GsyT2PzstU30yLdJhKfdZKz
/aIzraHvoDTWFaOdy0+OOaECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAdSzN2+0E
V1BfR3DPWJHWRf1b7zl+1X/ZseW2hYE5r6YxrLv+1VPf/L5I6kB7GEtqhZUqteY7
zAceoLrVu/7OynRyfQetJVGichaaxLNM3lcr6kcxOowb+WQQ84cwrB3keykH4gRX
KHB2rlWSxta+2panSEO1JX2q5jhcFP90rDOtZjlpYv57N/Z9iQ+dvQPJnChdq3BK
5pZlnIDnVVxqRike7BFy8tKyPj7HzoPEF5mh9Kfnn1YoSVu+61lMVv/qRjnyKfS9
c96nE98sYFj0ZVBzXw8Sq4Gh8FiVmFHbQp1peGC19idOUqxPxWsasWxQXO0azYsP
9RyWLHKxH1dMuA==
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDCzCCAnSgAwIBAgIJALSOMbOoU2svMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0yMzA3MDQw
ODM1MzlaFw0yODA3MDIwODM1MzlaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBX
YXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6
b24gV2ViIFNlcnZpY2VzIExMQzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
uhhUNlqAZdcWWB/OSDVDGk3OA99EFzOn/mJlmciQ/Xwu2dFJWmSCqEAE6gjufCjQ
q3voxAhC2CF+elKtJW/C0Sz/LYo60PUqd6iXF4h+upB9HkOOGuWHXsHBTsvgkgGA
1CGgel4U0Cdq+23eANr8N8m28UzljjSnTlrYCHtzN4sCAwEAAaOB1DCB0TALBgNV
HQ8EBAMCB4AwHQYDVR0OBBYEFBkZu3wT27NnYgrfH+xJz4HJaNJoMIGOBgNVHSME
```

```
gYYwgYOAFBkZu3wT27NnYgrfH+xJz4HJaNJooWCkXjBcMQswCQYDVQQGEwJVUzEZ
MBcGA1UECBMQV2FzaGluZ3RvbiBTdGF0ZTEQMA4GA1UEBxMHU2VhdHRsZTEgMB4G
A1UEChMXQW1hem9uIFdlYiBTZXJ2aWNlcyBMTEOCCQC0jjGzqFNrLzASBgNVHRMB
Af8ECDAGAQH/AgEAMA0GCSqGSIb3DQEBCwUAA4GBAECji43p+oPkYqmzll7e8Hgb
oADS0ph+YUz5P/bUCm61wFjlxaTfwKcuTR3ytj7bFLoW5Bm7Sa+TCl3lOGb2taon
2h+9NirRK6JYk87LMNvbS40HGPFumJL2NzEsGUeK+MRiWu+Oh5/lJGii3qw4YByx
SUDlRyNy1jJFstEZjOhs
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJAPu4ssY3BlzcMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTEyMDMy
MTI5MzJaGA8yMTk1MDUwODIxMjkzMlowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAsOiGi4A6+YTLzCdIyP8b8SCT2M/6PGKwzKJ5XbSBoL3gsnSWiFYqPg9c
uJPNbiy9wSA9vlyfWMd90qvTfiNrT6vewP813QdJ3EENZOx4ERcf/Wd22tV72kxD
yw1Q3I1OMH4bOItGQAxU5OtXCjBZEEUZooOkU8RoUQOU2Pql4NTiUpzWacNutAn5
HHS7MDc4lUlsJqbN+5QW6fFrcNG/0Mrib3JbwdFUNhrQ5j+Yq5h78HarnUivnX/3
Ap+oPbentv1qd7wvPJu556LZuhfqI0TohiIT1Ah+yUdN5osoaMxTHKKtf/CsSJ1F
w3qXqFJQA0VWsqjFyHXFI32I/GOupwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQCn
Um00QHvUsJSN6KATbghowLynHn3wZSQsuS8E0COpcFJFxP2SV0NYkERbXu0n/Vhi
yq5F8v4/bRA2/xpedLWmvFs7QWlomuXhSnYFkd33Z5gnXPb9vRkLwiMSw4uXls35
qQraczUJ9EXDhrv7VmngIk9H3YsxYrlDGEqh/oz4Ze4ULOgnfkauanHikk+BUEsg
/jsTD+7e+niEzJPihHdsvKFDlud5pakEzyxovHwNJ1GS2I//yxrJFIL91mehjqEk
RLPdNse7N6UvSnuXcOokwu6l6kfzigGkJBxkcq4gre3szZFdCQcUioj7Z4xtuTL8
YMqfiDtN5cbD8R8ojw9Y
-----END CERTIFICATE-----
```

AWS GovCloud (US-Ost) — -1 us-gov-east

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
```

```
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIULVyrqjjwZ461qelPCiShB1KCCj4wDQYJKoZIhvcNAQEL
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE1MjIzNloXDTI5MDUwNjE1MjIzNlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IULVyrqjjw
Z461qelPCiShB1KCCj4wEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQBfAL/YZv0y3zmVbXjyxQCsDloeDCJjFKIu3ameEckeIWJbST9LMto0zViZ
puIAf05x6GQiEqfBMk+YMxJfcTmJB4Ebaj4egFlslJPSHyC2xuydHlr3B04INOH5
Z2oCM68u6GGbj0jZjg7GJonkReG9N72kDva/ukwZKgq8zErQVQ==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJALPB6hxFhay8MA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xODA0MTAx
MjMyNDlaGA8yMTk3MDkxMzEyMzI0OVowXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
```

```
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAva9xsI9237KYb/SPWmeCVzi7giKNron8hoRDwlwwMC9+uHPd53UxzKLb
pTgtJWAPkZVxEdl2Gdhwr3SULoKcKmkqE6ltVFrVuPT33La1UufguT9k8ZDDuO9C
hQNHUdSVEuVrK3bLjaSsMOS7Uxmnn7lYT990IReowvnBNBsBlcabfQTBV04xfUG0
/m0XUiUFjOxDBqbNzkEIblW7vK7ydSJtFMSljga54UAVXibQt9EAIF7B8k9l2iLa
mu9yEjyQy+ZQICTuAvPUEWe6va2CHVY9gYQLA31/zU0VBKZPTNExjaqK4j8bKs1/
7dOV1so39sIGBz21cUBec1o+yCS5SwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQBt
hO2W/Lm+Nk0qsXW6mqQFsAou0cASc/vtGNCyBfoFNX6aKXsVCHxq2aq2TUKWENs+
mKmYu1lZVhBOmLshyllh3RRoL3Ohp3jCwXytkWQ7ElcGjDzNGc0FArzB8xFyQNdK
MNvXDi/ErzgrHGSpcvmGHiOhMf3UzChMWbIr6udoDlMbSIO7+8F+jUJkh4Xl1lKb
YeN5fsLZp7T/6YvbFSPpmbn1YoE2vKtuGKxObRrhU3h4JHdp1Zel1pZ6lh5iM0ec
SD11SximGIYCjfZpRqI3q50mbxCd7ckULz+UUPwLrfOds4VrVVSj+x0ZdY19Plv2
9shw5ez6Cn7E3IfzqNHO
-----END CERTIFICATE-----
```

AWS GovCloud (US-West) — -1 us-gov-west

DSA

```
-----BEGIN CERTIFICATE-----
MIIC7TCCAq0CCQCWukjZ5V4aZzAJBgcqhkjOOAQDMFwxCzAJBgNVBAYTAlVTMRkw
FwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYD
VQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAeFw0xMjAxMDUxMjU2MTJaFw0z
ODAxMDUxMjU2MTJaMFwxCzAJBgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9u
IFN0YXRlMRAwDgYDVQQHEwdTZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNl
cnZpY2VzIExMQzCCAbcwggEsBgcqhkjOOAQBMIIBHwKBgQCjkvcS2bb1VQ4yt/5e
ih5OO6kK/n1Lzllr7D8ZwtQP8fOEpp5E2ng+D6Ud1Z1gYipr58Kj3nssSNpI6bX3
VyIQzK7wLclnd/YozqNNmgIyZecN7EglK9ITHJLP+x8FtUpt3QbyYXJdmVMegN6P
hviYt5JH/nYl4hh3Pa1HJdskgQIVALVJ3ER11+Ko4tP6nwvHwh6+ERYRAoGBAI1j
k+tkqMVHuAFcvAGKocTgsjJem6/5qomzJuKDmbJNu9Qxw3rAotXau8Qe+MBcJl/U
hhy1KHVpCGl9fueQ2s6IL0CaO/buycU1CiYQk40KNHCcHfNiZbdlx1E9rpUp7bnF
lRa2v1ntMX3caRVDdbtPEWmdxSCYsYFDk4mZrOLBA4GEAAKBgEbmeve5f8LIE/Gf
MNmP9CM5eovQOGx5ho8WqD+aTebs+k2tn92BBPqeZqpWRa5P/+jrdKml1qx4llHW
MXrs3IgIb6+hUIB+S8dz8/mmO0bpr76RoZVCXYab2CZedFut7qc3WUH9+EUAH5mw
vSeDCOUMYQR7R9LINYwouHIziqQYMAkGByqGSM44BAMDLwAwLAIUWXBlk40xTwSw
7HX32MxXYruse9ACFBNGmdX2ZBrVNGrN9N2f6ROk0k9K
-----END CERTIFICATE-----
```

RSA

```
-----BEGIN CERTIFICATE-----
MIIDITCCAoqgAwIBAgIUe5wGF3jfb7lUHzvDxmM/ktGCLwwwDQYJKoZIhvcNAQEL
```

```
BQAwXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAO
BgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExD
MB4XDTI0MDUwNzE3MzAzMloXDTI5MDUwNjE3MzAzMlowXDELMAkGA1UEBhMCVVMx
GTAXBgNVBAgTEFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAe
BgNVBAoTF0FtYXpvbiBXZWIgU2VydmljZXMgTExDMIGfMA0GCSqGSIb3DQEBAQUA
A4GNADCBiQKBgQCpohwYUVPH9I7Vbkb3WMe/JB0Y/bmfVj3VpcK445YBRO9K80al
esjgBc2tAX4KYg4Lht4EBKccLHTzaNi51YEGX1aLNrSmxhz1+WtzNLNUsyY3zD9z
vwX/3k1+JB2dRA+m+Cpwx4mjzZyAeQtHtegVaAytkmqtxQrSCexBxvqRqQIDAQAB
o4HfMIHcMAsGA1UdDwQEAwIHgDAdBgNVHQ4EFgQU1ZXneBYnPvYXkHVlVjg7918V
gE8wgZkGA1UdIwSBkTCBjoAU1ZXneBYnPvYXkHVlVjg7918VgE+hYKReMFwxCzAJ
BgNVBAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdT
ZWF0dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQ4IUe5wGF3jf
b7lUHzvDxmM/ktGCLwwwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsF
AAOBgQCbTdpx1Iob9SwUReY4exMnlwQlmkTLyA8tYGWzchCJOJJEPfsW0ryy1A0H
YIuvyUty3rJdp9ib8h3GZR71BkZnNddHhy06kPs4p8ewF8+d8OWtOJQcI+ZnFfG4
KyM4rUsBrljpG2aOCm12iACEyrvgJJrS8VZwUDZS6mZEnn/lhA==
-----END CERTIFICATE-----
```

RSA-2048

```
-----BEGIN CERTIFICATE-----
MIIDOzCCAiOgAwIBAgIJANCOF0Q6ohnuMA0GCSqGSIb3DQEBCwUAMFwxCzAJBgNV
BAYTAlVTMRkwFwYDVQQIExBXYXNoaW5ndG9uIFN0YXRlMRAwDgYDVQQHEwdTZWF0
dGxlMSAwHgYDVQQKExdBbWF6b24gV2ViIFNlcnZpY2VzIExMQzAgFw0xNTA5MTAx
OTQyNDdaGA8yMTk1MDIxMzE5NDI0N1owXDELMAkGA1UEBhMCVVMxGTAXBgNVBAgT
EFdhc2hpbmd0b24gU3RhdGUxEDAOBgNVBAcTB1NlYXR0bGUxIDAeBgNVBAoTF0Ft
YXpvbiBXZWIgU2VydmljZXMgTExDMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAzIcGTzNqie3f1olrrqcfzGfbymSM2QfbTzDIOG6xXXeFrCDAmOq0wUhi
3fRCuoeHlKOWAPu76B9os71+zgF22dIDEVkpqHCjBrGzDQZXXUwOzhm+PmBUI8Z1
qvbVD4ZYhjCujWWzrsX6Z4yEK7PEFjtf4M4W8euw0RmiNwjy+knIFa+VxK6aQv94
lW98URFP2fD84xedHp6ozZlr3+RZSIFZsOiyxYsgiwTbesRMI0Y7LnkKGCIHQ/XJ
OwSISWaCddbu59BZeADnyhl4f+pWaSQpQQ1DpXvZAVBYvCH97J1oAxLfH8xcwgSQ
/se3wtn095VBt5b7qTVjOvy6vKZazwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQA/
S8+a9csfASkdtQUOLsBynAbsBCH9Gykq2m8JS7YE4TGvqlpnWehz78rFTzQwmz4D
fwq8byPkl6DjdF9utqZ0JUo/Fxelxom0h6oievtBlSkmZJNbgc2WYm1zi6ptViup
Y+4S2+vWZyg/X1PXD7wyRWuETmykk73uEyeWFBYKCHWsO9sI+62O4Vf8Jkuj/cie
1NSJX8fkervfLrZSHBYhxLbL+actVEo00tiyZz8GnhgWx5faCY38D/k4Y/j5Vz99
7lUX/+fWHT3+lTL8ZZK7fOQWh6NQpI0wTP9KtWqfOUwMIbgFQPoxkP00TWRmdmPz
WOwTObEf9ouTnjG9OZ20
-----END CERTIFICATE-----
```

Instance-Identitätsrollen

Jede Instance, die Sie starten, hat eine Instance-Identitätsrolle, die ihre Identität repräsentiert. Eine Instance-Identitätsrolle ist eine Art von IAM-Rolle. AWS Dienste und Funktionen, die zur Verwendung der Instanzidentitätsrolle integriert sind, können sie verwenden, um die Instanz für den Dienst zu identifizieren.

Auf die Anmeldeinformationen für die Instance-Identitätsrolle können Sie über den Instance Metadata Service (IMDS) unter `/identity-credentials/ec2/security-credentials/ec2-instance` zugreifen. Die Anmeldeinformationen bestehen aus einem AWS temporären Zugriffsschlüsselpaar und einem Sitzungstoken. Sie werden verwendet, um AWS Sigv4-Anfragen an die AWS Dienste zu signieren, die die Instanzidentitätsrolle verwenden. Die Anmeldeinformationen sind in den Instance-Metadaten vorhanden, unabhängig davon, ob ein Service oder ein Feature, welches Instance-Identitätsrollen verwendet, in der Instance aktiviert ist.

Instance-Identitätsrollen werden automatisch erstellt, wenn eine Instance gestartet wird. Sie haben kein Rollenvertrauensrichtliniendokument und unterliegen keiner Identitäts- oder Ressourcenrichtlinie.

Unterstützte Services

Die folgenden AWS Dienste verwenden die Instanzidentitätsrolle:

- Amazon EC2 — EC2 Instance Connect verwendet die Instance-Identitätsrolle, um die Hostschlüssel für eine Linux-Instance zu aktualisieren.
- Amazon GuardDuty — Runtime Monitoring verwendet die Instance-Identitätsrolle, damit der Runtime-Agent Sicherheitstelemetrie an den GuardDuty VPC-Endpunkt senden kann.
- AWS Security Token Service (AWS STS) — Die Anmeldeinformationen für die Instance-Identitätsrolle können für die AWS STS `GetCallerIdentity`Aktion verwendet werden.
- AWS Systems Manager— Bei Verwendung der Standard-Host-Management-Konfiguration wird die Identität AWS Systems Manager verwendet, die von der Instance-Identitätsrolle bereitgestellt wird, um EC2-Instances zu registrieren. Nach der Identifizierung Ihrer Instance kann Systems Manager Ihre `AWSSystemsManagerDefaultEC2InstanceManagementRole`-IAM-Rolle an Ihre Instance weitergeben.

Instance-Identitätsrollen können nicht mit anderen AWS Diensten oder Funktionen verwendet werden, da sie nicht mit Instance-Identitätsrollen integriert sind.

Instance-Identitäts-Rollen-ARN

Die Instance-Identitätsrollen-ARN hat das folgende Format:

```
arn:aws-partition:iam::account-number:assumed-role/aws:ec2-instance/instance-id
```

Beispielsweise:

```
arn:aws:iam::0123456789012:assumed-role/aws:ec2-instance/i-0123456789example
```

Weitere Informationen zu ARNs finden Sie unter Amazon-Ressourcennamen (ARNs) im IAM-Benutzerhandbuch.

Führen Sie beim Start Befehle auf Ihrer Amazon EC2 EC2-Instance aus

Wenn Sie eine Amazon EC2 EC2-Instance starten, können Sie Benutzerdaten an die Instance übergeben, die zur Ausführung automatisierter Konfigurationsaufgaben oder zur Ausführung von Skripts nach dem Start der Instance verwendet wird.

Wenn Sie an komplexeren Automatisierungsszenarien interessiert sind, könnten Sie AWS CloudFormation oder AWS OpsWorks in Betracht ziehen. Weitere Informationen finden Sie hier:

- Bereitstellen von Anwendungen auf Amazon EC2 mit dem AWS CloudFormation im AWS CloudFormation -Benutzerhandbuch..
- AWS OpsWorks Benutzerleitfaden.

Auf Linux-Instances können Sie zwei Arten von Benutzerdaten an Amazon EC2 übergeben: Shell-Skripts und Cloud-Init-Direktiven. Sie können diese Daten auch als Klartext, als Datei (dies ist nützlich, um Instances mit den Befehlszeilentools zu starten) oder als Base64-codierten Text (für API-Aufrufe) an den Launch-Instance-Assistenten übergeben.

Auf Windows-Instances verarbeiten die Launch-Agents Ihre Benutzerdatenskripts. In den folgenden Abschnitten werden die Unterschiede im Umgang mit Benutzerdaten auf den einzelnen Betriebssystemen beschrieben.

So verarbeitet Amazon EC2 Benutzerdaten für Linux-Instances

In den folgenden Beispielen werden die Befehle von Install a LAMP server on Amazon Linux 2 in ein Shell-Skript und eine Reihe von Cloud-Init-Direktiven umgewandelt, die beim Start der Instance ausgeführt werden. In den Beispielen werden die folgenden Aufgaben von den Benutzerdaten ausgeführt:

- Die Softwarepakete der Bereitstellung werden aktualisiert.
- Der notwendige Webserver sowie die ebensolchen php- und `mariadb`-Pakete werden installiert.
- Der `httpd`-Service wird mithilfe des Befehls systemctl gestartet und aktiviert.
- Der `ec2-user` wird der Apache-Gruppe hinzugefügt.
- Eigentümer und Dateiberechtigungen für das Webverzeichnis und die darin enthaltenen Daten werden festgelegt.
- Zum Testen des Webservers und der PHP-Engine wird eine einfache Webseite erstellt.

Inhalt

Voraussetzungen

Die Beispiele in diesem Thema setzen Folgendes voraus:

- Ihre Instance verfügt bereits über einen öffentlichen DNS-Namen, der über das Internet erreichbar ist.
- Die Ihrer Instance zugeordnete Sicherheitsgruppe ist so konfiguriert, dass sie SSH-Datenverkehr (Port 22) zulässt, sodass Sie eine Verbindung zur Instance herstellen können, um die Ausgabeprotokolldateien anzuzeigen.
- Ihre Instance wird mit einem Amazon-Linux-2-AMI gestartet. Diese Anleitung ist zur Verwendung mit Amazon Linux 2 gedacht. Die Befehle und Anweisungen funktionieren möglicherweise nicht

bei anderen Linux-Distributionen. Weitere Informationen zu anderen Bereitstellungen, z. B. zu ihrer Unterstützung von Cloud-Init, finden Sie in der jeweiligen Dokumentation.

Benutzerdaten und Shell-Skripts

Shell-Skripts sind, sofern Sie sich damit auskennen, die einfachste und vollständigste Methode, mit der Sie einer Instance beim Start Anweisungen übermitteln. Wenn diese Skripts beim Start ausgeführt werden, verlängert sich dadurch die Dauer des Instance-Starts. Erlauben Sie einige Minuten für die vollständige Ausführung der Aufgaben, bevor Sie überprüfen, ob die Benutzerskripte vollständig ausgeführt wurden.

> **Important**
>
> Standardmäßig werden Benutzerdatenskripte und Cloud-init-Direktiven nur während des Startzyklus ausgeführt, wenn Sie eine Instance zum ersten Mal starten. Sie können Ihre Konfiguration aktualisieren, um sicherzustellen, dass Ihre Benutzerdatenskripte und Cloud-Init-Direktiven bei jedem Neustart der Instance ausgeführt werden. Weitere Informationen finden Sie unter Wie kann ich Benutzerdaten verwenden, um bei jedem Neustart meiner Amazon EC2 EC2-Linux-Instance automatisch ein Skript auszuführen? im AWS Knowledge Center.

Benutzerdaten-Shell-Skripts müssen mit den Zeichen #! und dem Pfad zu dem Interpreter beginnen, der das Skript lesen soll (üblicherweise /bin/bash)). Eine Einführung in Shell-Scripting finden Sie im Bash Reference Manual auf der Website des GNU-Betriebssystems.

Als Benutzerdaten eingegebene Skripte werden als Stammbenutzer ausgeführt. Verwenden Sie daher nicht den sudo-Befehl im Skript. Denken Sie daran, dass alle von Ihnen erstellten Dateien dem Stammbenutzer gehören. Wenn Sie Zugriff auf die Dateien durch einen anderen Benutzer als den Stammbenutzer benötigen, sollten Sie die Berechtigungen im Skript entsprechend ändern. Außerdem können Sie keine Befehle verwenden, die Benutzerfeedback erfordern (z. B. yum update ohne das -y-Flag), da das Skript nicht interaktiv ausgeführt wird.

Wenn Sie eine AWS API, einschließlich der AWS CLI, in einem Benutzerdatenskript verwenden, müssen Sie beim Starten der Instance ein Instanzprofil verwenden. Ein Instanzprofil stellt die entsprechenden AWS Anmeldeinformationen bereit, die das Benutzerdatenskript benötigt, um den API-Aufruf auszuführen. Weitere Informationen finden Sie unter Verwenden von Instance-Profilen im IAM-Benutzerhandbuch. Die Berechtigungen, die Sie der IAM-Rolle zuweisen, hängen davon

ab, welche Dienste Sie mit der API aufrufen. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.

Die Ausgabeprotokolldatei von Cloud-Init zeichnet die Ausgabe der Konsole auf, was die Behebung von Fehlern an den Skripts vereinfacht, falls sich die Instance nach dem Start nicht verhält wie erwartet. Um die Protokolldatei anzuzeigen, stellen Sie eine Verbindung mit der Instance her und öffnen Sie `/var/log/cloud-init-output.log`.

Wird ein Benutzerdatenskript verarbeitet, dann wird es nach kopiert und von dort aus ausgeführ `/var/lib/cloud/instances/instance-id/`. Das Skript wird nach der Ausführung nicht gelöscht. Stellen Sie sicher, dass Sie die Benutzerdatenskripts aus `/var/lib/cloud/instances/instance-id/` löschen, bevor Sie ein AMI aus der Instance erstellen. Andernfalls ist das Skript in diesem Verzeichnis auf jeder Instance vorhanden, die vom AMI gestartet wird.

Benutzerdaten und die Konsole

Sie können Instance-Benutzerdaten angeben, wenn Sie die Instance starten. Wenn das Root-Volume der Instance ein EBS-Volume ist, können Sie die Instance auch anhalten und ihre Benutzerdaten aktualisieren.

Angeben von Instance-Benutzerdaten beim Start

Folgen Sie dem Verfahren unter Starten einer Instance. Das Feld User data (Benutzerdaten) befindet sich im Abschnitt Erweiterte Details des Launch Instance Wizard. Geben Sie Ihr Shell-Skript im Feld User Data (Benutzerdaten) ein und führen Sie dann das Verfahren zum Starten der Instance aus.

Im nachstehenden Beispielskript erstellt und konfiguriert das Skript einen Webserver.

```
#!/bin/bash
 yum update -y
 amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
 yum install -y httpd mariadb-server
 systemctl start httpd
 systemctl enable httpd
 usermod -a -G apache ec2-user
 chown -R ec2-user:apache /var/www
 chmod 2775 /var/www
 find /var/www -type d -exec chmod 2775 {} \;
 find /var/www -type f -exec chmod 0664 {} \;
 echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

Geben Sie der Instance ausreichend Zeit zum Starten und zum Ausführen der Befehle Ihres Skripts, dann überprüfen Sie, ob das Skript die gewünschten Aufgaben ausgeführt hat.

Geben Sie unserem Beispiel folgend in einem Webbrowser die URL der PHP-Testdatei ein, die das Skript erstellt hat. Diese URL ist die öffentliche DNS-Adresse Ihrer Instance, gefolgt von einem Schrägstrich und dem Dateinamen.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Die PHP-Informationsseite wird angezeigt. Wenn Sie die PHP-Informationsseite nicht anzeigen können, prüfen Sie, ob die verwendete Sicherheitsgruppe eine Regel enthält, um den HTTP-Datenverkehr (Port 80) zuzulassen. Weitere Informationen finden Sie unter Hinzufügen von Regeln zu einer Sicherheitsgruppe.

(Optional) Wenn Ihr Skript nicht die Aufgaben erfüllt hat, die Sie erwartet haben oder wenn Sie nur überprüfen möchten, ob Ihr Skript ohne Fehler abgeschlossen wurde, stellen Sie eine Verbindung mit der Instance her, untersuchen Sie die Cloud-init-Ausgabeprotokolldatei (`/var/log/cloud-init-output.log`) und suchen Sie nach Fehlermeldungen in der Ausgabe.

Weitere Informationen zur Fehlerbehebung erhalten Sie, indem Sie ein mehrteiliges Mime-Archiv erstellen, dass einen Abschnitt mit Cloud-Init-Daten enthält, darunter die folgende Anweisung:

```
output : { all : '| tee -a /var/log/cloud-init-output.log' }
```

Diese Anweisung übermittelt die Befehlsausgaben vom Skript an `/var/log/cloud-init-output.log`. Weitere Informationen zu Cloud-Init-Datenformaten und zur Erstellung von mehrteiligen Mime-Archiven finden Sie unter cloud-init Formats.

Anzeigen und Aktualisieren der Instance-Benutzerdaten

Um die Instance-Benutzerdaten aktualisieren zu können, müssen Sie zuerst die Instance anhalten. Wenn die Instance ausgeführt wird, können Sie die Benutzerdaten anzeigen, sie können jedoch nicht ändern.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Ändern von Instance-Benutzerdaten

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und dann Instance state (Instance-Status), Stop instance (Instance anhalten) aus. Wenn diese Option deaktiviert ist, wurde die Instance entweder bereits angehalten oder das Root-Gerät ist ein Instance-Speicher-Volume.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus. Das Anhalten der Instance kann einige Minuten dauern.
5. Wählen Sie mit der ausgewählten Instance Aktionen, Instance-Einstellungen, Benutzerdaten bearbeiten aus.
6. Ändern Sie die Benutzerdaten nach Bedarf und wählen Sie dann Speichern.
7. Starten Sie die Instance. Die neuen Benutzerdaten werden nach dem Start in Ihrer Instance angezeigt, Benutzerdatenskripts werden jedoch nicht ausgeführt.

Benutzerdaten und Cloud-Init-Anweisungen

Das Cloud-Init-Paket konfiguriert bestimmte Aspekte einer neuen Amazon Linux-Instance bei deren Start. Insbesondere wird die Datei `.ssh/authorized_keys` für den ec2-user konfiguriert, sodass Sie sich mit dem eigenen privaten Schlüssel anmelden können. Weitere Informationen zu den Konfigurationsaufgaben, die das Cloud-Init-Paket für Amazon Linux-Instances ausführt, finden Sie unter Using cloud-init on Amazon Linux 2 im Amazon Linux 2-Benutzerhandbuch.

Die Cloud-Init-Anweisungen können wie ein Skript auch beim Start einer Instance an diese weitergeleitet werden, wenngleich sich die Syntax unterscheidet. Weitere Informationen zu cloud-init finden Sie unter http://cloudinit.readthedocs.org/en/latest/index.html.

> **Important**
>
> Standardmäßig werden Benutzerdatenskripte und Cloud-init-Direktiven nur während des Startzyklus ausgeführt, wenn Sie eine Instance zum ersten Mal starten. Sie können Ihre Konfiguration aktualisieren, um sicherzustellen, dass Ihre Benutzerdatenskripte und Cloud-Init-Direktiven bei jedem Neustart der Instance ausgeführt werden. Weitere Informationen finden Sie unter Wie kann ich Benutzerdaten verwenden, um bei jedem Neustart meiner Amazon EC2 EC2-Linux-Instance automatisch ein Skript auszuführen? im AWS Knowledge Center.

Wenn diese Skripts beim Start ausgeführt werden sollen, verlängert sich dadurch die Dauer des Instance-Starts. Erlauben Sie einige Minuten für die vollständige Ausführung der Aufgaben, bevor Sie überprüfen, ob die Benutzerdatenanweisungen vollständig durchgeführt wurden.

Leiten Sie Cloud-Init-Anweisungen wie folgt an eine Instance mit Benutzerdaten weiter:

1. Folgen Sie dem Verfahren unter Starten einer Instance. Das Feld User data (Benutzerdaten) befindet sich im Abschnitt Erweiterte Details des Launch Instance Wizard. Geben Sie den Text Ihrer cloud-init-Anweisung im Feld User Data (Benutzerdaten) ein und führen Sie dann das Verfahren zum Starten der Instance aus.

   Das folgende Beispiel zeigt, wie Anweisungen einen Webserver in Amazon Linux 2 erstellen und konfigurieren. Die Zeile `#cloud-config` ganz oben ist erforderlich, um die Befehle als cloud-init-Anweisungen zu identifizieren.

   ```
   #cloud-config
    repo_update: true
    repo_upgrade: all

    packages:
    - httpd
    - mariadb-server

    runcmd:
    - [ sh, -c, "amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2" ]
    - systemctl start httpd
    - sudo systemctl enable httpd
    - [ sh, -c, "usermod -a -G apache ec2-user" ]
    - [ sh, -c, "chown -R ec2-user:apache /var/www" ]
    - chmod 2775 /var/www
    - [ find, /var/www, -type, d, -exec, chmod, 2775, {}, \; ]
    - [ find, /var/www, -type, f, -exec, chmod, 0664, {}, \; ]
    - [ sh, -c, 'echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php' ]
   ```

2. Geben Sie der Instance ausreichend Zeit zum Starten und zum Ausführen der Anweisungen in Ihren Benutzerdaten, dann überprüfen Sie, ob die Anweisungen die gewünschten Aufgaben ausgeführt haben.

   Geben Sie für dieses Beispiel in einem Webbrowser die URL der PHP-Testdatei ein, die die Anweisungen erstellt haben. Diese URL ist die öffentliche DNS-Adresse Ihrer Instance, gefolgt von einem Schrägstrich und dem Dateinamen.

```
http://my.public.dns.amazonaws.com/phpinfo.php
```

Die PHP-Informationsseite wird angezeigt. Wenn Sie die PHP-Informationsseite nicht anzeigen können, prüfen Sie, ob die verwendete Sicherheitsgruppe eine Regel enthält, um den HTTP-Datenverkehr (Port 80) zuzulassen. Weitere Informationen finden Sie unter Hinzufügen von Regeln zu einer Sicherheitsgruppe.

3. (Optional) Wenn Ihre Anweisungen nicht die Aufgaben erfüllt haben, die Sie erwartet haben oder wenn Sie nur überprüfen möchten, ob Ihre Direktiven ohne Fehler abgeschlossen wurden, stellen Sie eine Verbindung mit der Instance her, untersuchen Sie die Ausgabeprotokolldatei (`/var/log/cloud-init-output.log`) und suchen Sie nach Fehlermeldungen in der Ausgabe. Weitere Informationen zur Fehlerbehebung erhalten Sie, indem Sie den Anweisungen die folgende Zeile hinzufügen:

   ```
   output : { all : '| tee -a /var/log/cloud-init-output.log' }
   ```

   Diese Anweisung übermittelt die Ausgabe von runcmd an `/var/log/cloud-init-output.log`.

Benutzerdaten und die AWS CLI

Sie können den verwenden, AWS CLI um die Benutzerdaten für Ihre Instanz anzugeben, zu ändern und anzuzeigen. Informationen zum Anzeigen von Benutzerdaten Ihrer Instance mithilfe von Instance-Metadaten erhalten Sie unter Abrufen von Instance-Benutzerdaten aus Ihrer Instance.

Unter Windows können Sie den AWS Tools for Windows PowerShell anstelle von verwenden AWS CLI. Weitere Informationen finden Sie unter Benutzerdaten und die Tools für Windows PowerShell.

Beispiel: Angeben von Benutzerdaten beim Start

Verwenden Sie den Befehl run-instances mit dem Parameter `--user-data`, um Benutzerdaten beim Start Ihrer Instance anzugeben. Mit run-instances AWS CLI führt der die Base64-Kodierung der Benutzerdaten für Sie durch.

Im folgenden Beispiel wird gezeigt, wie Sie ein Skript als String auf der Befehlszeile angeben:

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
 --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
```

```
 --user-data echo user data
```

Im folgenden Beispiel wird gezeigt, wie Sie ein Skript mithilfe einer Textdatei angeben: Verwenden Sie beim Angeben der Datei das Präfix `file://`.

```
aws ec2 run-instances --image-id ami-abcd1234 --count 1 --instance-type m3.medium \
 --key-name my-key-pair --subnet-id subnet-abcd1234 --security-group-ids sg-abcd1234 \
 --user-data file://my_script.txt
```

Das folgende Element ist eine Beispieltextdatei mit einem Shell-Skript.

```
#!/bin/bash
 yum update -y
 service httpd start
 chkconfig httpd on
```

Beispiel: Modifizieren der Benutzerdaten einer angehaltenen Instance

Sie können die Benutzerdaten einer angehaltenen Instance mit dem Befehl modify-instance-attribute ändern. Mit modify-instance-attribute AWS CLI führt der keine Base64-Kodierung der Benutzerdaten für Sie durch.

- Verwenden Sie auf einem Linux-Computer den Befehl „base64“, um die Benutzerdaten zu codieren.

  ```
  base64 my_script.txt >my_script_base64.txt
  ```

- Verwenden Sie auf einem, Windows-Computer den Befehl „certutil“, um die Benutzerdaten zu codieren. Bevor Sie diese Datei mit dem verwenden können AWS CLI, müssen Sie die erste (BEGIN CERTIFICATE) und die letzte Zeile (END CERTIFICATE) entfernen.

  ```
  certutil -encode my_script.txt my_script_base64.txt
   notepad my_script_base64.txt
  ```

Verwenden Sie die Parameter `--attribute` und `--value`, um die codierte Textdatei zur Angabe der Benutzerdaten zu verwenden. Verwenden Sie beim Angeben der Datei das Präfix `file://`.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData --value file://my_script_base64.txt
```

Beispiel: Löschen der Benutzerdaten einer angehaltenen Instance

Um die vorhandenen Benutzerdaten zu löschen, verwenden Sie den Befehl modify-instance-attribute wie folgt:

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --user-data Value=
```

Beispiel: Anzeigen von Benutzerdaten

Verwenden Sie den Befehl describe-instance-attribute, um die Benutzerdaten für eine Instance aufzurufen. Mit describe-instance-attribute AWS CLI führt der keine Base64-Decodierung der Benutzerdaten für Sie durch.

```
aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
 userData
```

Im folgenden Beispiel wird die Ausgabe mit base64-Benutzerdaten verschlüsselt.

```
{
 "UserData": {
     "Value":
 "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAteQpzZXJ2aWNlIGh0dHBkIHN0YXJ0CmNoa2NvbmZpZyBodHRwZCBvbg=="
 },
 "InstanceId": "i-1234567890abcdef0"
 }
```

- Verwenden Sie auf einem Linux-Computer die Option `--query`, um die codierten Benutzerdaten abzurufen, und den Befehl „base64“, um sie zu decodieren.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" | base64 --decode
  ```

- Verwenden Sie auf einem Windows-Computer die Option `--query`, um die codierten Benutzerdaten abzurufen, und den Befehl „certutil“, um sie zu decodieren. Die codierte Ausgabe wird in einer, die decodierte Ausgabe in einer anderen Datei gespeichert.

  ```
  aws ec2 describe-instance-attribute --instance-id i-1234567890abcdef0 --attribute
   userData --output text --query "UserData.Value" >my_output.txt
   certutil -decode my_output.txt my_output_decoded.txt
   type my_output_decoded.txt
  ```

Es folgt eine Beispielausgabe.

```
#!/bin/bash
 yum update -y
 service httpd start
 chkconfig httpd on
```

Kombinieren von Shell-Skripts und cloud-init-Anweisungen

Standardmäßig können Sie jeweils nur einen Inhaltstyp in Benutzerdaten einbeziehen. Allerdings können Sie die Inhaltstypen `text/cloud-config` und `text/x-shellscript` in einer mehrteiligen MIME-Datei verwenden, um sowohl ein Shell-Skript als auch cloud-init-Anweisungen in Ihren Benutzerdaten einzubeziehen.

Nachfolgend wird das mehrteilige MIME-Format veranschaulicht.

```
Content-Type: multipart/mixed; boundary="//"
 MIME-Version: 1.0

 --//
 Content-Type: text/cloud-config; charset="us-ascii"
 MIME-Version: 1.0
 Content-Transfer-Encoding: 7bit
 Content-Disposition: attachment; filename="cloud-config.txt"

 #cloud-config
 cloud-init directives

 --//
 Content-Type: text/x-shellscript; charset="us-ascii"
 MIME-Version: 1.0
 Content-Transfer-Encoding: 7bit
 Content-Disposition: attachment; filename="userdata.txt"

 #!/bin/bash
 shell script commands
 --//--
```

Die folgenden Benutzerdaten enthalten beispielsweise cloud-init-Anweisungen und ein Bash-Shell-Skript. Die cloud-init-Anweisungen erstellen eine Datei (`/test-cloudinit/cloud-init.txt`) und schreiben `Created by cloud-init` in diese Datei. Das Bash-Shell-Skript erstellt eine Datei (`/`

`test-userscript/userscript.txt`) und schreibt `Created by bash shell script` in diese Datei.

```
Content-Type: multipart/mixed; boundary="//"
 MIME-Version: 1.0

 --//
 Content-Type: text/cloud-config; charset="us-ascii"
 MIME-Version: 1.0
 Content-Transfer-Encoding: 7bit
 Content-Disposition: attachment; filename="cloud-config.txt"

 #cloud-config
 runcmd:
 - [ mkdir, /test-cloudinit ]
 write_files:
 - path: /test-cloudinit/cloud-init.txt
 content: Created by cloud-init

 --//
 Content-Type: text/x-shellscript; charset="us-ascii"
 MIME-Version: 1.0
 Content-Transfer-Encoding: 7bit
 Content-Disposition: attachment; filename="userdata.txt"

 #!/bin/bash
 mkdir test-userscript
 touch /test-userscript/userscript.txt
 echo "Created by bash shell script" >> /test-userscript/userscript.txt
 --//--
```

So verarbeitet Amazon EC2 Benutzerdaten für Windows-Instances

Auf Windows-Instances verarbeiten die Standard-Launch-Agents für Ihre Betriebssystemversion Benutzerdaten wie folgt.

- EC2Launch v2führt Benutzerdatenskripts auf Windows Server 2022 aus
- ???führt Benutzerdatenskripts auf Windows Server 2016 und 2019 aus
- ???führt Benutzerdatenskripts auf Windows Server-Versionen vor Windows Server 2016 aus

Beispiele für die Zusammenstellung einer `UserData` Eigenschaft in einer AWS CloudFormation Vorlage finden Sie unter Base64 Encoded Property und Base64 Encoded UserData UserData Property with and. AccessKey SecretKey

Ein Beispiel für die Ausführung von Befehlen auf einer Instance innerhalb einer Auto Scaling Scaling-Gruppe, die mit Lifecycle-Hooks arbeitet, finden Sie unter Tutorial: Benutzerdaten konfigurieren, um den Ziellebenszyklusstatus über Instance-Metadaten abzurufen im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Inhalt

Benutzerdatenskripts

`EC2Launch`Um Skripts auszuführen `EC2Config` oder auszuführen, müssen Sie das Skript in ein spezielles Tag einschließen, wenn Sie es zu den Benutzerdaten hinzufügen. Welches Tag Sie verwenden, hängt davon ab, ob die Befehle in einem Befehlszeilenfenster (Batch-Befehle) oder unter Windows PowerShell ausgeführt werden.

Wenn Sie sowohl ein Batch-Skript als auch ein PowerShell Windows-Skript angeben, wird das Batch-Skript zuerst und das PowerShell Windows-Skript als Nächstes ausgeführt, unabhängig von der Reihenfolge, in der sie in den Instanzbenutzerdaten erscheinen.

Wenn Sie eine AWS API, einschließlich der AWS CLI, in einem Benutzerdatenskript verwenden, müssen Sie beim Starten der Instanz ein Instanzprofil verwenden. Ein Instanzprofil stellt die entsprechenden AWS Anmeldeinformationen bereit, die das Benutzerdatenskript für den API-Aufruf benötigt. Weitere Informationen finden Sie unter Instance-Profile. Die Berechtigungen, die Sie der IAM-Rolle zuweisen, hängen davon ab, welche Dienste Sie mit der API aufrufen. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.

Skripttyp

- Base64-Codierung

Syntax für Batch-Skripts

Geben Sie ein Batch-Skript unter Verwendung des `script`-Tags (Markierung) an. Trennen Sie die Befehle durch Zeilenumbrüche, wie im folgenden Beispiel gezeigt.

```
<script>
 echo Current date and time >> %SystemRoot%\Temp\test.log
 echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
 </script>
```

In der Standardeinstellung werden Benutzerdatenskripte einmal ausgeführt, wenn Sie die Instance starten. Um die Benutzerdaten-Skripts bei jedem Neustart oder Starten der Instance auszuführen, fügen Sie den Benutzerdaten `<persist>true</persist>` hinzu.

```
<script>
 echo Current date and time >> %SystemRoot%\Temp\test.log
 echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
 </script>
 <persist>true</persist>
```

EC2Launch-v2-Agent

Um ein XML-Benutzerdatenskript als getrennten Prozess mit der EC2Launch-v2-executeScript-Aufgabe in der `UserData`-Stufe auszuführen, fügen Sie Ihren Benutzerdaten das folgende Tag hinzu.

`<detach>true</detach>`

> **Note**
>
> Das Abtrennungs-Tag wird auf früheren Startagenten nicht unterstützt.

```
<script>
 echo Current date and time >> %SystemRoot%\Temp\test.log
 echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
 </script>
```

```
<detach>true</detach>
```

Syntax für PowerShell Windows-Skripts

Die AWS Windows-AMIs enthalten die AWS Tools for Windows PowerShell, sodass Sie diese Cmdlets in Benutzerdaten angeben können. Wenn Sie Ihrer Instance eine IAM-Rolle zuordnen, müssen Sie keine Anmeldeinformationen für die Cmdlets angeben, da Anwendungen, die auf der Instance ausgeführt werden, die Anmeldeinformationen der Rolle verwenden, um auf AWS Ressourcen (z. B. Amazon S3 S3-Buckets) zuzugreifen.

Geben Sie mithilfe des Tags ein PowerShell Windows-Skript an. `<powershell>` Trennen Sie die Befehle mithilfe von Zeilenumbrüchen voneinander. Beim `<powershell>`-Tag wird die Groß- und Kleinschreibung beachtet.

Beispielsweise:

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
```

Standardmäßig werden die Benutzerdatenskripts einmal ausgeführt, wenn Sie die Instance starten. Um die Benutzerdaten-Skripts bei jedem Neustart oder Starten der Instance auszuführen, fügen Sie den Benutzerdaten `<persist>true</persist>` hinzu.

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
 <persist>true</persist>
```

Sie können ein oder mehrere PowerShell Argumente mit dem `<powershellArguments>` Tag angeben. Wenn keine Argumente übergeben werden, fügen EC2Launch und EC2Launch v2 standardmäßig das folgende Argument hinzu:. `-ExecutionPolicy Unrestricted`

Beispiel:

```
<powershell>
   $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
```

```
   New-Item $file -ItemType file
 </powershell>
 <powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

EC2Launch-v2-Agent

Um ein XML-Benutzerdatenskript als getrennten Prozess mit der EC2Launch-v2-executeScript-Aufgabe in der `UserData`-Stufe auszuführen, fügen Sie Ihren Benutzerdaten das folgende Tag hinzu.

```
<detach>true</detach>
```

> **Note**
>
> Das Abtrennungs-Tag wird auf früheren Startagenten nicht unterstützt.

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
 <detach>true</detach>
```

Syntax für YAML-Konfigurationsskripts

Wenn Sie mit EC2Launch v2 Skripte ausführen, können Sie das YAML-Format verwenden. Informationen zum Anzeigen von Konfigurationsaufgaben, Details und Beispielen für EC2Launch v2 finden Sie unter Aufgabenkonfiguration in EC2Launch v2.

Geben Sie ein YAML-Skript mit der Aufgabe `executeScript` an.

Beispiel für eine YAML-Syntax zum Ausführen eines Skripts PowerShell

```
version: 1.0
 tasks:
 - task: executeScript
   inputs:
   - frequency: always
     type: powershell
```

```
    runAs: localSystem
    content: |-
      $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
      New-Item $file -ItemType file
```

YAML-Beispielsyntax zum Ausführen eines Batch-Skripts

```
version: 1.1
 tasks:
 - task: executeScript
   inputs:
   - frequency: always
     type: batch
     runAs: localSystem
     content: |-
       echo Current date and time >> %SystemRoot%\Temp\test.log
       echo %DATE% %TIME% >> %SystemRoot%\Temp\test.log
```

Base64-Codierung

Wenn Sie die Amazon EC2-API oder ein Tool verwenden, mit dem keine Base64-Codierung der Benutzerdaten durchgeführt wird, müssen Sie die Benutzerdaten selbst codieren. Andernfalls wird ein Fehler ausgegeben, der darauf hinweist, dass keine auszuführenden `script`- oder `powershell`-Tags gefunden wurden. Im Folgenden finden Sie ein Beispiel, das mit Windows codiert. PowerShell

```
$UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Das Folgende ist ein Beispiel für die Dekodierung mit. PowerShell

```
$Script =
 [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData))
```

Weitere Informationen zur Base64-Kodierung finden Sie unter https://www.ietf.org/rfc/rfc4648.txt.

Ausführung von Benutzerdaten

Standardmäßig ist bei allen AWS Windows-AMIs die Ausführung von Benutzerdaten für den ersten Start aktiviert. Sie können vorgeben, dass die Benutzerdaten-Skripts beim nächsten Neustart oder erneuten Starten der Instance ausgeführt werden sollen. Alternativ können Sie vorgeben, dass die

Benutzerdaten-Skripts bei jedem Neustart oder erneuten Starten der Instance ausgeführt werden sollen.

> **Note**
>
> Benutzerdaten können nach dem ersten Start nicht standardmäßig ausgeführt werden. Informationen darüber, wie Sie Benutzerdaten beim Neustart oder beim Starten der Instance ausführen können, finden Sie unter Nachfolgende Neustart- oder Startvorgänge.

Benutzerdaten-Skripts werden vom lokalen Administratorkonto ausgeführt, wenn ein zufälliges Passwort generiert wird. Andernfalls werden Benutzerdaten-Skripts vom Systemkonto ausgeführt.

Instance-Start

Skripts in den Instance-Benutzerdaten werden beim ersten Start der Instance ausgeführt. Ist der `persist`-Tag (Markierung) vorhanden, wir die Ausführung der Benutzerdaten für nachfolgende Neustarts oder Starts aktiviert. Die Protokolldateien für EC2Launch v2, EC2Launch und EC2Config enthalten die Ausgabe aus den Standard-Ausgabestreams und den Standard-Fehlerstreams.

EC2Launch v2

Die Protokolldatei für EC2Launch v2 lautet `C:\ProgramData\Amazon\EC2Launch\log\agent.log`.

> **Note**
>
> Der Ordner `C:\ProgramData` ist möglicherweise ausgeblendet. Zum Anzeigen des Ordners müssen Sie die ausgeblendeten Dateien und Ordner einblenden.

Bei der Ausführung von Benutzerdaten werden die folgenden Informationen protokolliert:

- `Info: Converting user-data to yaml format`: Wenn die Benutzerdaten im XML-Format bereitgestellt wurden
- `Info: Initialize user-data state`: Der Beginn der Benutzerdatenausführung
- `Info: Frequency is: always`: Wenn die Benutzerdatenaufgabe bei jedem Start ausgeführt wird
- `Info: Frequency is: once`: Wenn die Benutzerdatenaufgabe nur einmal ausgeführt wird

- `Stage: postReadyUserData execution completed`: Das Ende der Ausführung von Benutzerdaten

EC2Launch

Die Protokolldatei für EC2Launch lautet `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\UserdataExecution.log`.

Der Ordner `C:\ProgramData` ist möglicherweise ausgeblendet. Zum Anzeigen des Ordners müssen Sie die ausgeblendeten Dateien und Ordner einblenden.

Bei der Ausführung von Benutzerdaten werden die folgenden Informationen protokolliert:

- `Userdata execution begins`: Der Beginn der Benutzerdatenausführung
- `<persist> tag was provided: true`: Wenn das persist-Tag (Markierung) gefunden wird
- `Running userdata on every boot`: Wenn der persist-Tag (Markierung) gefunden wird
- `<powershell> tag was provided.. running powershell content`: Wenn der powershell-Tag (Markierung) gefunden wird
- `<script> tag was provided.. running script content`: Wenn der Skript-Tag (Markierung) gefunden wird
- `Message: The output from user scripts`: Wenn Benutzerdatenskripte ausgeführt werden, wird deren Ausgabe protokolliert

EC2Config

Die Protokolldatei für EC2config lautet `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2Config.log`. Bei der Ausführung von Benutzerdaten werden die folgenden Informationen protokolliert:

- `Ec2HandleUserData: Message: Start running user scripts`: Der Beginn der Benutzerdatenausführung
- `Ec2HandleUserData: Message: Re-enabled userdata execution`: Wenn der persist-Tag (Markierung) gefunden wird
- `Ec2HandleUserData: Message: Could not find <persist> and </persist>`: Wenn der persist-Tag (Markierung) nicht gefunden wird
- `Ec2HandleUserData: Message: The output from user scripts`: Wenn Benutzerdatenskripte ausgeführt werden, wird deren Ausgabe protokolliert

Nachfolgende Neustart- oder Startvorgänge

Wenn Sie Instance-Benutzerdaten aktualisieren, werden Benutzerdaten-Skripts nicht automatisch ausgeführt, wenn Sie die Instance neu starten oder starten. Sie können die Ausführung von Benutzerdaten jedoch so aktivieren, dass Benutzerdaten-Skripts einmalig beim Neustart oder Starten der Instance oder bei jedem Neustart oder Starten der Instance ausgeführt werden.

Wenn Sie die OptionShutdown with Sysprep (Herunterfahren mit Sysprep) wählen, werden Benutzerdaten-Skripts beim Neustart oder Starten der Instance ausgeführt, auch wenn Sie die Ausführung der Benutzerdaten für nachfolgende Neustarts oder Starts nicht aktiviert haben. Die Benutzerdaten-Skripts werden bei nachfolgenden Neustarts oder Starts nicht ausgeführt.

So aktivieren Sie die Ausführung von Benutzerdaten mit EC2Launch v2 (Vorschau-AMIs)

- Wenn eine Aufgabe beim ersten Start für Benutzerdaten ausgeführt werden soll, setzen Sie `frequency` auf `once`.
- Wenn eine Aufgabe bei jedem Start für Benutzerdaten ausgeführt werden soll, setzen Sie `frequency` auf `always`.

So aktivieren Sie die Ausführung von Benutzerdaten mit EC2Launch (Windows Server 2016 oder höher)

1. Herstellen einer Verbindung mit Ihrer Windows-Instance.
2. Öffnen Sie ein PowerShell Befehlsfenster und führen Sie den folgenden Befehl aus:

   ```
   C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
   ```

3. Trennen Sie die Verbindung zu Ihrer Windows-Instance. Um beim nächsten Starten der Instance aktualisierte Skripts auszuführen, halten Sie die Instance an und aktualisieren die Benutzerdaten.

So aktivieren Sie die Ausführung von Benutzerdaten mit EC2config (Windows Server 2012 R2 und früher)

1. Herstellen einer Verbindung mit Ihrer Windows-Instance.
2. Öffnen `C:\Program Files\Amazon\Ec2ConfigService\Ec2ConfigServiceSetting.exe`.
3. Wählen Sie unter Benutzerdaten die Option UserDataAusführung für den nächsten Dienststart aktivieren aus.

4. Trennen Sie die Verbindung zu Ihrer Windows-Instance. Um beim nächsten Starten der Instance aktualisierte Skripts auszuführen, halten Sie die Instance an und aktualisieren die Benutzerdaten.

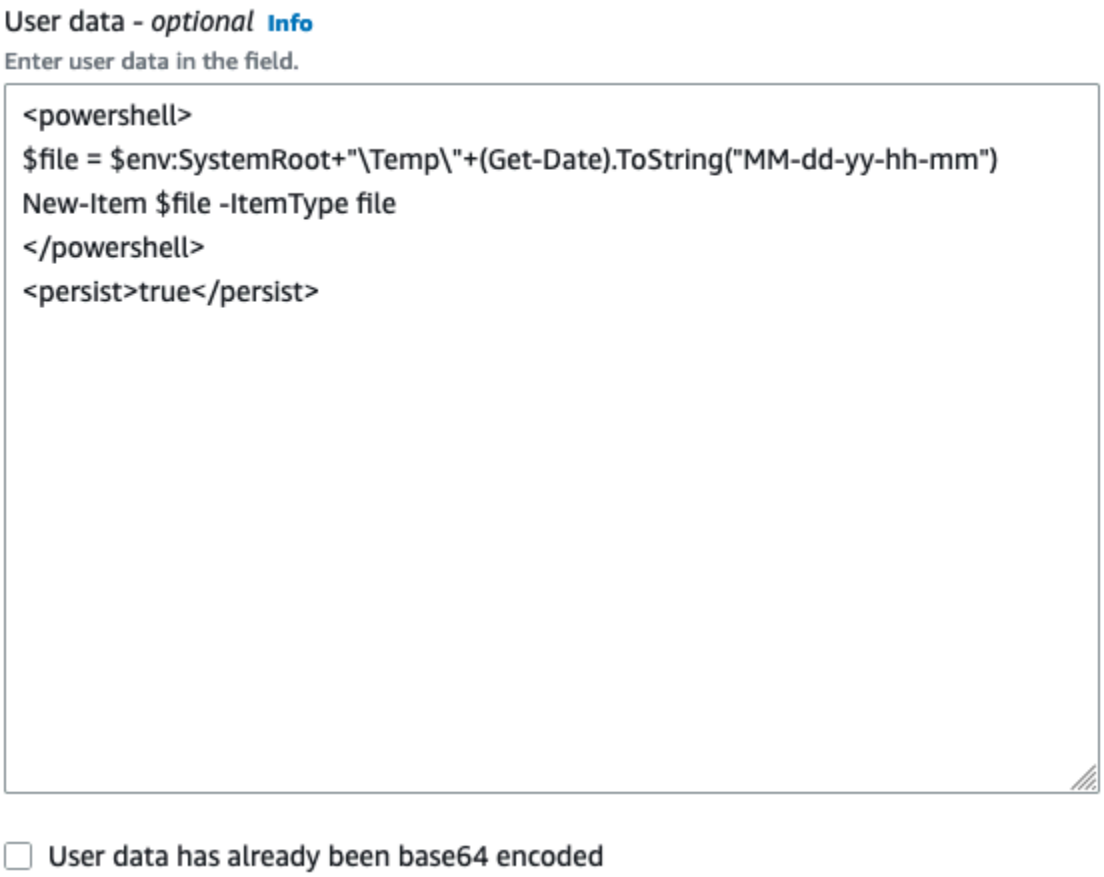
Benutzerdaten und die Konsole

Sie können Instance-Benutzerdaten angeben, wenn Sie die Instance starten. Wenn das Root-Volume der Instance ein EBS-Volume ist, können Sie die Instance auch anhalten und ihre Benutzerdaten aktualisieren.

Angeben von Instance-Benutzerdaten beim Start

Folgen Sie dem Verfahren unter Starten einer Instance. Das Feld User data (Benutzerdaten) befindet sich im Abschnitt Erweiterte Details des Launch Instance Wizard. Geben Sie Ihr PowerShell Skript in das Feld Benutzerdaten ein und schließen Sie dann den Vorgang zum Starten der Instanz ab.

Im folgenden Screenshot des Feldes Benutzerdaten erstellt das Beispielskript eine Datei im temporären Windows-Ordner und verwendet das aktuelle Datum und die Uhrzeit im Dateinamen. Wenn Sie `<persist>true</persist>` einfügen, wird das Skript bei jedem Neustart oder Start der Instance ausgeführt. Wenn Sie das Kontrollkästchen Benutzerdaten wurden bereits mit Base64 codiert leer lassen, führt die Amazon-EC2-Konsole die Base64-Codierung für Sie durch.



Anzeigen und Aktualisieren der Instance-Benutzerdaten

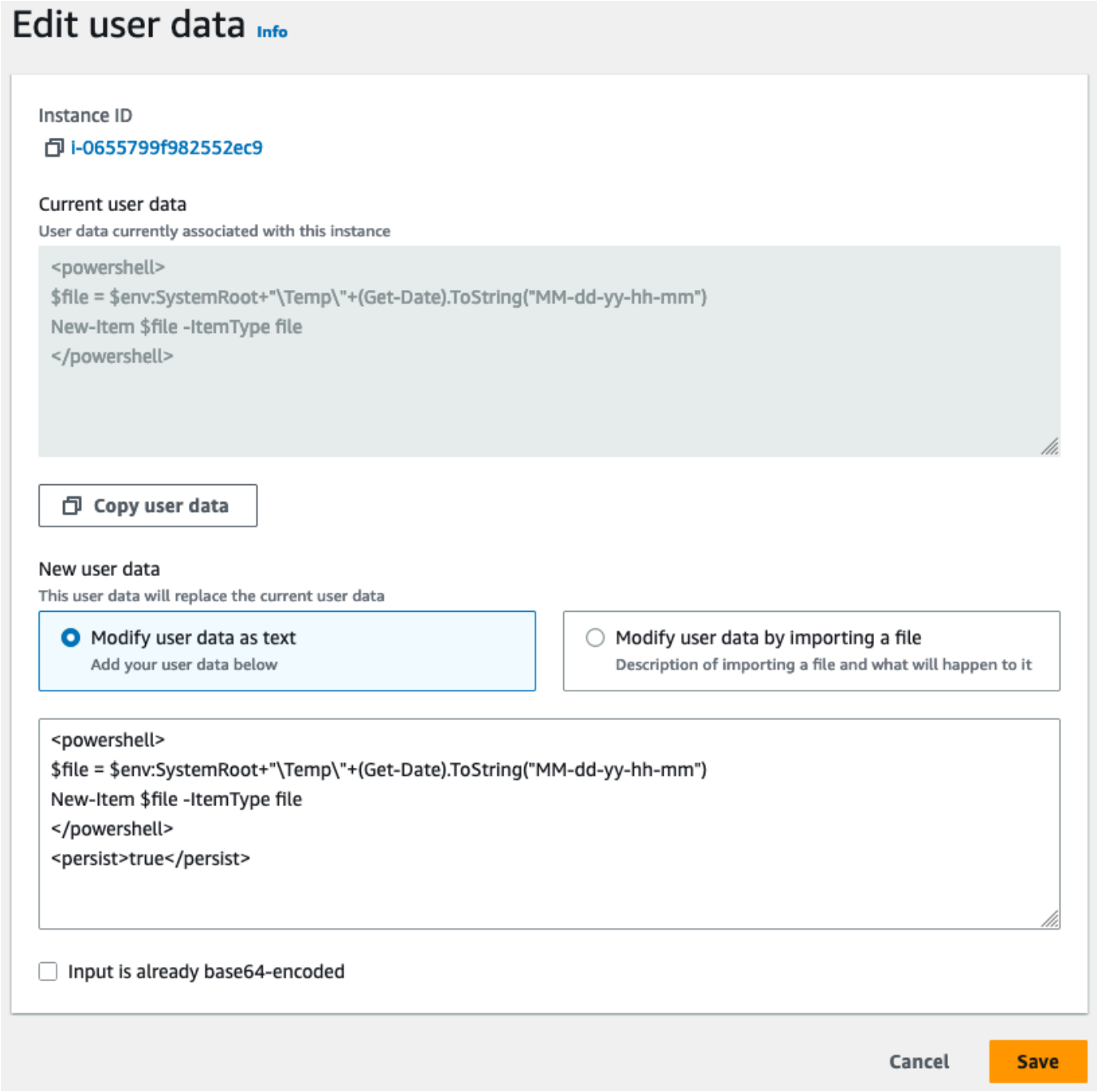
Sie können die Instance-Benutzerdaten für jede beliebige Instance anzeigen und die Instance-Benutzerdaten für eine angehaltene Instance aktualisieren.

So aktualisieren Sie die Benutzerdaten für eine Instance mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und dann Aktionen, Instance-Status, Instance anhalten aus.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Stop aus. Das Anhalten der Instance kann einige Minuten dauern.
5. Wählen Sie mit der ausgewählten Instance Aktionen, Instance-Einstellungen, Benutzerdaten bearbeiten aus. Die Benutzerdaten können nicht geändert werden, solange die Instance ausgeführt wird; Sie können die Benutzerdaten nur anzeigen.
6. Aktualisieren Sie die Benutzerdaten im Dialogfeld View/Change User Data (Benutzerdaten anzeigen/ändern) und wählen Sie dann die Option Save (Speichern). Um die Benutzerdaten-Skripts bei jedem Neustart oder Starten der Instance auszuführen, fügen Sie `<persist>true</persist>` hinzu, wie im folgenden Beispiel gezeigt:



7. Starten Sie die Instance. Wenn Sie die Ausführung von Benutzerdaten für nachfolgende Neustarts oder Starts aktiviert haben, werden die aktualisierten Benutzerdaten-Skripts als Teil des Instance-Startprozesses ausgeführt.

Benutzerdaten und die Tools für Windows PowerShell

Sie können die Tools für Windows verwenden, PowerShell um die Benutzerdaten für Ihre Instanz anzugeben, zu ändern und anzuzeigen. Informationen zum Anzeigen von Benutzerdaten Ihrer Instance mithilfe von Instance-Metadaten erhalten Sie unter Abrufen von Instance-Benutzerdaten aus Ihrer Instance. Hinweise zu Benutzerdaten und dem AWS CLI finden Sie unterBenutzerdaten und die AWS CLI.

Beispiel: Angeben von Instance-Benutzerdaten beim Start

Erstellen Sie eine Textdatei mit Instance-Benutzerdaten. Um die Benutzerdaten-Skripts bei jedem Neustart oder Starten der Instance auszuführen, fügen Sie `<persist>true</persist>` hinzu, wie im folgenden Beispiel gezeigt.

```
<powershell>
 $file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
 New-Item $file -ItemType file
 </powershell>
 <persist>true</persist>
```

Verwenden Sie den New-EC2InstanceBefehl, um die Benutzerdaten für die Instanz anzugeben, wenn Sie Ihre Instance starten. Dieser Befehl führt keine Base64-Codierung der Benutzerdaten für Sie durch Verwenden Sie die folgenden Befehle, um die Benutzerdaten in einer Textdatei namens `script.txt` zu codieren.

```
PS C:\> $Script = Get-Content -Raw script.txt
 PS C:\> $UserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($Script))
```

Verwenden Sie den Parameter `-UserData`, um die Benutzerdaten an den Befehl New-EC2Instance zu übergeben.

```
PS C:\> New-EC2Instance -ImageId ami-abcd1234 -MinCount 1 -MaxCount 1 -
InstanceType m3.medium \
 -KeyName my-key-pair -SubnetId subnet-12345678 -SecurityGroupIds sg-1a2b3c4d \
 -UserData $UserData
```

Beispiel: Aktualisieren von Instance-Benutzerdaten einer angehaltenen Instance

Sie können die Benutzerdaten einer gestoppten Instance mithilfe des Edit-EC2InstanceAttributeBefehls ändern.

Erstellen Sie eine Textdatei mit dem neuen Skript. Verwenden Sie die folgenden Befehle, um die Benutzerdaten in der Textdatei namens `new-script.txt` zu codieren.

```
PS C:\> $NewScript = Get-Content -Raw new-script.txt
 PS C:\> $NewUserData =
 [System.Convert]::ToBase64String([System.Text.Encoding]::ASCII.GetBytes($NewScript))
```

Verwenden Sie die Parameter `-UserData` und `-Value`, um die Benutzerdaten anzugeben.

```
PS C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute userData -
Value $NewUserData
```

Beispiel: Anzeige von Instance-Benutzerdaten

Verwenden Sie den Get-EC2InstanceAttributeBefehl, um die Benutzerdaten für eine Instanz abzurufen.

```
PS C:\> (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -Attribute
 userData).UserData
```

Es folgt eine Beispielausgabe. Beachten Sie, dass die Benutzerdaten codiert sind.

```
PHBvd2Vyc2hlbGw
+DQpSZW5hbWUtQ29tcHV0ZXIgLU5ld05hbWUgdXNlci1kYXRhLXRlc3QNCjwvcG93ZXJzaGVsbD4=
```

Verwenden Sie die folgenden Befehle, um die codierten Benutzerdaten in einer Variablen zu speichern und anschließend zu decodieren.

```
PS C:\> $UserData_encoded = (Get-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -
Attribute userData).UserData
 PS C:
\> [System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($UserData_encoded)
```

Es folgt eine Beispielausgabe.

```
<powershell>
```

```
$file = $env:SystemRoot + "\Temp\" + (Get-Date).ToString("MM-dd-yy-hh-mm")
New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Beispiel: Umbenennen der Instance entsprechend des Tag (Markierung)-Werts

Sie können den Get-EC2TagBefehl verwenden, um den Tag-Wert zu lesen, die Instance beim ersten Start so umzubenennen, dass sie dem Tag-Wert entspricht, und den Computer neu zu starten. Um diesen Befehl erfolgreich auszuführen, müssen Sie über eine Rolle mit `ec2:DescribeTags`-Berechtigungen verfügen, die der Instance zugeordnet sind, da Tag-Informationen per API-Aufruf abgerufen werden müssen. Weitere Informationen zu Einstellungsberechtigungen mithilfe von IAM-Rollen finden Sie unterAnfügen einer IAM-Rolle an eine Instance.

> **Note**
>
> Dieses Skript schlägt bei Windows Server-Versionen vor 2008 fehl.

```
<powershell>
 $instanceId = (invoke-webrequest http://169.254.169.254/latest/meta-data/instance-id -
UseBasicParsing).content
 $nameValue = (get-ec2tag -filter @{Name="resource-id";Value=
$instanceid},@{Name="key";Value="Name"}).Value
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
 and 15 characters in length and contains only alphanumeric or hyphen characters"}
 </powershell>
```

Sie können die Instance auch mit Tags aus Instance-Metadaten umbenennen, wenn Ihre Instance so konfiguriert ist, dass über die Instance-Metadaten auf Tags zugegriffen wird. Weitere Informationen finden Sie unter Arbeiten mit Instance-Tags in Instance-Metadaten.

> **Note**
>
> Dieses Skript schlägt bei Windows Server-Versionen vor 2008 fehl.

```
<powershell>
 $nameValue = Get-EC2InstanceMetadata -Path /tags/instance/Name
 $pattern = "^(?![0-9]{1,15}$)[a-zA-Z0-9-]{1,15}$"
 #Verify Name Value satisfies best practices for Windows hostnames
 If ($nameValue -match $pattern)
     {Try
         {Rename-Computer -NewName $nameValue -Restart -ErrorAction Stop}
     Catch
         {$ErrorMessage = $_.Exception.Message
         Write-Output "Rename failed: $ErrorMessage"}}
 Else
     {Throw "Provided name not a valid hostname. Please ensure Name value is between 1
 and 15 characters in length and contains only alphanumeric or hyphen characters"}
 </powershell>
```

Connect zu Ihrer EC2-Instance her

Dieser Abschnitt des Amazon EC2 EC2-Benutzerhandbuchs enthält Informationen, die Ihnen helfen, nach dem Start eine Verbindung zu Ihrer Amazon EC2 EC2-Instance herzustellen. Er enthält auch Informationen, die Ihnen helfen, Ihre Instance mit einer anderen AWS Ressource zu verbinden.

Themen

- Herstellen einer Verbindung zur Linux-Instance
- Herstellen einer Verbindung mit Ihrer -Windows-Instance
- Herstellen einer Verbindung über Session Manager
- Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu Ihren Instances her
- Verbinden Ihrer EC2-Instance mit einer AWS -Ressource

Herstellen einer Verbindung zur Linux-Instance

Es gibt viele Möglichkeiten, eine Verbindung zu Ihrer Linux-Instance herzustellen. Einige variieren je nach Betriebssystem des lokalen Rechners, von dem aus Sie die Verbindung herstellen. Andere, wie

EC2 Instance Connect, AWS Systems Manager Session Manager oder , variiere nicht. In diesem Abschnitt erfahren Sie, wie Sie eine Verbindung zu Ihrer Linux-Instance herstellen und Dateien zwischen Ihrem lokalen Computer und Ihrer Instance übertragen.

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie eine Verbindung mit Ihrer Linux-Instance herstellen.

- Anfordern von Informationen zu Ihrer Instance
- Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen
- (Optional) Anfordern des Instance-Fingerabdrucks

Wählen Sie dann eine der folgenden Optionen, um eine Verbindung zu Ihrer Linux-Instance herzustellen.

Verbindungsoptionen basierend auf Ihrem lokalen Betriebssystem

- Verbindung von einem lokalen Linux- oder macOS-Rechner mithilfe von SSH herstellen
- Verbindung von einem lokalen Windows-Rechner herstellen

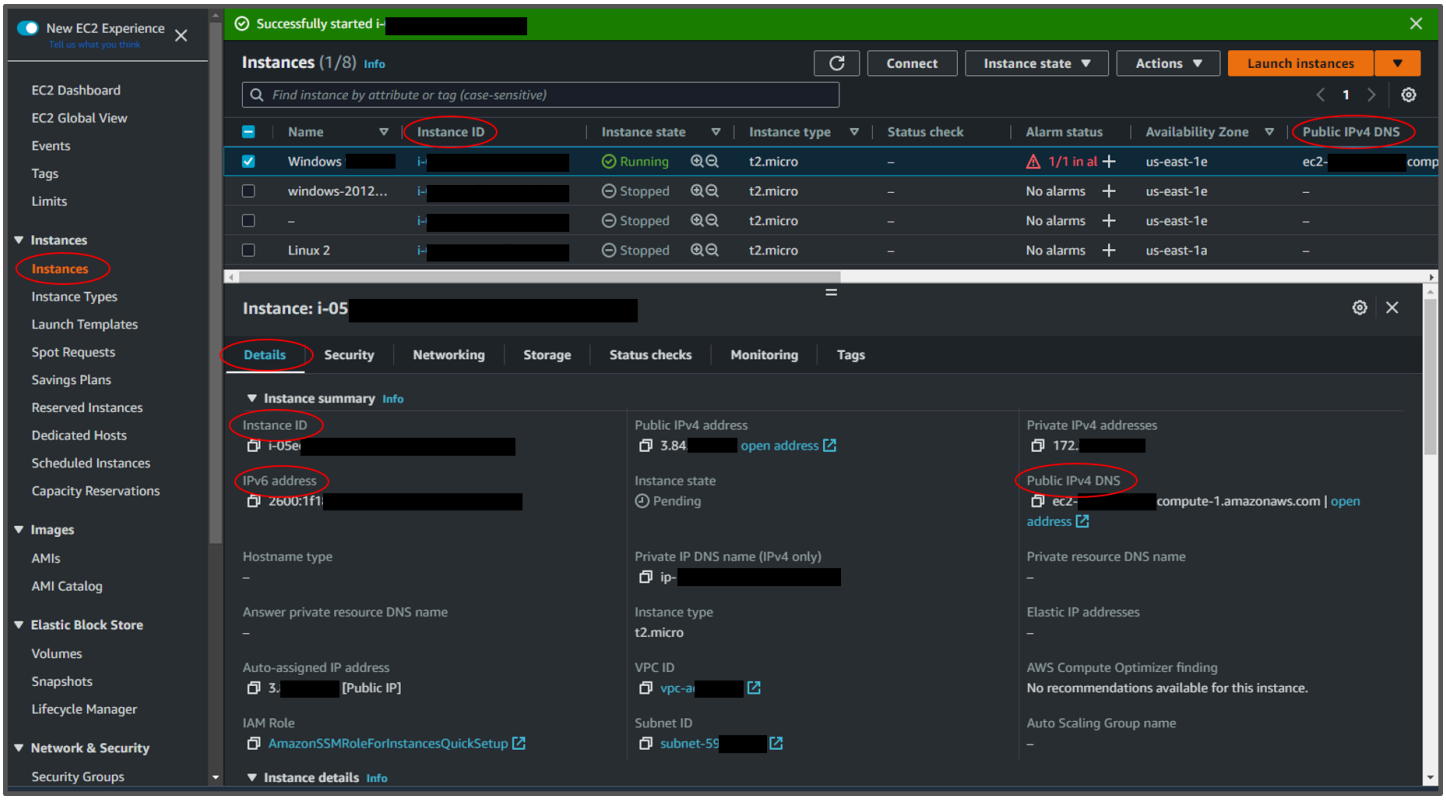
Optionen zum Herstellen einer Verbindung von jedem lokalen Betriebssystem aus

- Herstellen einer Verbindung über Session Manager
- Herstellen einer Verbindung zu Ihrer Linux-Instance mit EC2 Instance Connect.

> **Note**
>
> Tipps zur Fehlerbehebung bei der Instance-Verbindung finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.
> Um Start-, Netzwerkkonfigurations- und andere Probleme für Instances zu beheben, die auf dem AWS -Nitro-System entwickelt sind, können Sie die Serielle EC2-Konsole für Amazon EC2 EC2-Instances verwenden.

Anfordern von Informationen zu Ihrer Instance

Rufen Sie zur Vorbereitung der Verbindung mit einer Instance die folgenden Informationen über die Amazon-EC2-Konsole ab oder verwenden Sie die AWS CLI.



- Rufen Sie den öffentlichen DNS-Namen der Instance ab.

  Sie können das öffentliche DNS für Ihre Instance über die Amazon-EC2-Konsole abrufen. Überprüfen Sie die Spalte Öffentliches IPv4-DNS im Instances-Bereich. Wenn diese Spalte ausgeblendet ist, wählen Sie das Einstellungssymbol (

) in der oberen rechten Ecke des Bildschirms und wählen Sie Öffentliches IPv4-DNS aus. Sie finden das öffentliche DNS auch im Bereich „Instance-Informationen“ des Instances-Bereichs. Wenn Sie die Instance im Instances-Bereich der Amazon-EC2-Konsole auswählen, werden Informationen zu dieser Instance in der unteren Hälfte der Seite angezeigt. Suchen Sie auf der Registerkarte Details nach Öffentliches IPv4-DNS.

  Wenn Sie möchten, können Sie die Befehle describe-instances (AWS CLI) oder Get-EC2Instance(AWS Tools for Windows PowerShell) verwenden.

  Wenn kein Öffentliches IPv4-DNS angezeigt wird, stellen Sie sicher, dass der Instance-Status Wird ausgeführt lautet und dass Sie die Instance nicht in einem privaten Subnetz gestartet haben. Wenn Sie Ihre Instance mit dem Launch Instance Wizard gestartet haben, haben Sie möglicherweise das Feld Öffentliche IP automatisch zuweisen unter Netzwerkeinstellungen bearbeitet und den Wert in

Deaktivieren geändert. Wenn Sie die Option Öffentliche IP automatisch zuweisen deaktivieren, wird der Instance beim Start keine öffentliche IP-Adresse zugewiesen.

- (Nur IPv6) Rufen Sie die IPv6-Adresse der Instance ab.

  Wenn Sie Ihrer Instance eine IPv6-Adresse zugewiesen haben, können Sie optional eine Verbindung zur Instance mithilfe ihrer IPv6-Adresse anstelle einer öffentlichen IPv4-Adresse oder eines öffentlichen IPv4-DNS-Hostnamens herstellen. Ihr lokaler Computer muss über eine IPv6-Adresse verfügen und für die Verwendung von IPv6 konfiguriert sein. Sie können die IPv6-Adresse Ihrer Instance über die Amazon-EC2-Konsole abrufen. Überprüfen Sie die Spalte IPv6-IPs im Instances-Bereich. Alternativ können Sie die IPv6-Adresse im Abschnitt mit den Instance-Informationen finden. Wenn Sie die Instance im Instances-Bereich der Amazon-EC2-Konsole auswählen, werden Informationen zu dieser Instance in der unteren Hälfte der Seite angezeigt. Suchen Sie auf der Registerkarte Details nach IPv4-Adresse.

  Wenn Sie möchten, können Sie die Befehle describe-instances (AWS CLI) oder Get-EC2Instance() verwenden.AWS Tools for Windows PowerShell Weitere Informationen zu IPv6 finden Sie unter IPv6-Adressen.
- Abrufen des Benutzernamens für Ihre Instance

  Sie können mit dem Benutzernamen für Ihr Benutzerkonto oder dem Standardbenutzernamen für das AMI, das Sie zum Starten Ihrer Instance verwendet haben, eine Verbindung zu Ihrer Instance herstellen.

  - Abrufen des Benutzernamens für Ihr Benutzerkonto ab.

    Weitere Informationen zum Erstellen eines Benutzerkontos finden Sie unter Verwalten Sie Systembenutzer auf Ihrer Linux-Instance.
  - Abrufen des Standardbenutzernamens für das AMI, das Sie zum Starten der Instance verwendet haben:

Zum Starten der Instance verwendetes AMI	Standardbenutzername
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` oder `ec2-user`

Zum Starten der Instance verwendetes AMI	Standardbenutzername
Debian	`admin`
Fedora	`fedora` oder `ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen

Sie müssen den Speicherort Ihrer privaten Schlüsseldatei kennen, um eine Verbindung zu Ihrer Instance herzustellen. Für SSH-Verbindungen müssen Sie die Berechtigungen so festlegen, dass nur Sie die Datei lesen können.

Informationen zur Funktionsweise von Schlüsselpaaren bei der Verwendung von Amazon EC2 finden Sie unter Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances.

- Auffinden des privaten Schlüssels

  Rufen Sie den vollständig qualifizierten Pfad des Speicherorts auf Ihrem Computer für die Datei `.pem` für das beim Start der Instance angegebene Schlüsselpaar ab. Weitere Informationen finden Sie unter the section called “Identifizieren des öffentlichen Schlüssels, der beim Start angegeben wurde”.

  Wenn Sie Ihre private Schlüsseldatei nicht finden können, finden Sie weitere Informationen unter

  Falls Sie den privaten Schlüssel für eine per EBS abgesicherte Instance verlieren, können Sie den Zugriff auf Ihre Instance zurückerlangen. Sie müssen die Instance anhalten, das

Stamm-Volume trennen, es einer anderen Instance als Daten-Volume anfügen, die Datei `authorized_keys` mit einem neuen öffentlichen Schlüssel modifizieren, das Volume zurück zur ursprünglichen Instance verschieben und die Instance neu starten. Weitere Informationen zum Starten, Herstellen von Verbindungen und Anhalten von Instances finden Sie im Abschnitt Instance-Lebenszyklus.

Dieses Verfahren wird nur für Instance mit EBS-Stamm-Volumes unterstützt. Wenn es sich beim Stammgerät um ein Instance-Speicher-Volume handelt, können Sie dieses Verfahren nicht verwenden, um den Zugriff auf Ihre Instance wiederherzustellen. Sie benötigen den privaten Schlüssel, um eine Verbindung mit der Instance herzustellen. Zur Feststellung des Root-Gerätetyps Ihrer Instance öffnen Sie die Amazon-EC2-Konsole, wählen Sie Instances, wählen Sie die Instance aus, wählen Sie die Registerkarte Speicher und überprüfen Sie im Abschnitt Root-Gerätedetails den Wert des Root-Gerätetyps.

Der Wert ist entweder `EBS` oder `INSTANCE-STORE`.

Wenn Sie Ihren privaten Schlüssel verlieren, gibt es weitere Möglichkeiten, eine Verbindung mit Ihrer Linux-Instance herzustellen. Weitere Informationen finden Sie unter Wie kann ich eine Verbindung zu meiner Amazon EC2 Instance herstellen, wenn ich mein SSH-Schlüsselpaar nach dem ersten Start verloren habe?

Schritte für die Herstellung einer Verbindung zu einer EBS-gestützten Instance mittels eines anderen Schlüsselpaars

- Schritt 1: Erstellen eines neuen Schlüsselpaars
- Schritt 2: Abrufen von Informationen über die ursprüngliche Instance und ihr Stamm-Volume
- Schritt 3: Anhalten der ursprünglichen Instance
- Schritt 4: Starten einer temporären Instance
- Schritt 5: Trennen des Stamm-Volumes von der ursprünglichen Instance und Anfügen an die temporäre Instance
- Schritt 6: Hinzufügen des neuen öffentlichen Schlüssels zu authorized_keys auf dem ursprünglichen Volume, das auf der temporären Instance gemountet wird
- Schritt 7: Aufheben der Bereitstellung und Trennen des ursprünglichen Volumes von der temporären Instance und erneutes Anfügen an die ursprüngliche Instance
- Schritt 8: Verbinden Sie sich mit der ursprünglichen Instance mit dem neuen Schlüsselpaar
- Schritt 9: Bereinigen

Schritt 1: Erstellen eines neuen Schlüsselpaars

Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole oder einem Tool eines Drittanbieters. Falls der Name des neuen Schlüsselpaares dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen. Weitere Informationen zum Erstellen eines neuen Schlüsselpaars finden Sie unter Erstellen eines Schlüsselpaars mit Amazon EC2 oder Erstellen Sie ein Schlüsselpaar mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel in Amazon EC2.

Schritt 2: Abrufen von Informationen über die ursprüngliche Instance und ihr Stamm-Volume

Notieren Sie sich die folgenden Informationen, da Sie sie benötigen werden, um dieses Verfahren abzuschließen.

So erhalten Sie Informationen zu Ihrer ursprünglichen Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann die Instance aus, zu der Sie eine Verbindung herstellen möchten. (Wir bezeichnen diese als ursprüngliche Instance.)
3. Notieren Sie sich auf der Registerkarte Details die Instance-ID und die AMI-ID.
4. Notieren Sie sich auf der Registerkarte Network (Netzwerk) die Availability Zone.
5. Notieren Sie sich auf der Registerkarte Storage (Speicher) den Gerätenamen für das Root-Volume unter Root device name (Root-Gerätename) (z. B. `/dev/xvda`). Suchen Sie diesen Gerätenamen unter Block devices (Geräte blockieren) und notieren Sie sich die Volume-ID (z. B. vol-0a1234b5678c910de).

Schritt 3: Anhalten der ursprünglichen Instance

Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten). Wenn diese Option deaktiviert ist, wurde die Instance entweder bereits angehalten oder das Root-Gerät ist ein Instance-Speicher-Volume.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Schritt 4: Starten einer temporären Instance

New console

So starten Sie eine temporäre Instance

1. Wählen Sie im Navigationsbereich Instances und Launch instances (Instances starten) aus.
2. Im Abschnitt Name and tags (Name und Tags) geben Sie beiName Temporary (Temporär) ein.
3. Im Abschnitt Application and OS Images (Anwendungs- und Betriebssystem-Images) wählen Sie dasselbe AMI aus, das Sie beim Start der ursprünglichen Instance verwendet haben. Falls diese AMI nicht verfügbar ist, können Sie eine AMI erstellen, die Sie von der angehaltenen Instance verwenden können. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.
4. Behalten Sie im Abschnitt Instance type (Instance-Typ) den standardmäßigen Instance-Typ bei.
5. Im Abschnitt Key pair (Schlüsselpaar) unter Key pair name (Schlüsselpaarname) wählen Sie das vorhandene Schlüsselpaar aus, das Sie verwenden oder erstellen Sie ein neues.
6. Im Abschnitt Network settings (Netzwerkeinstellungen) wählen Sie Edit (Bearbeiten), aus. Wählen Sie dann unter Subnet (Subnetz) ein Subnetz in derselben Availability Zone wie die ursprüngliche Instance aus.
7. Wählen Sie im Bereich Summary (Übersicht) Launch (Starten) aus.

Old console

Wählen Sie Launch Instances (Instances starten), und verwenden Sie dann den Start-Assistenten, um eine temporäre Instance mit den folgenden Optionen zu starten:

- Wählen Sie auf der Seite Choose an AMI (AMI wählen) dieselbe AMI aus, die Sie beim Start der ursprünglichen Instance verwendet haben. Falls diese AMI nicht verfügbar ist, können Sie eine AMI erstellen, die Sie von der angehaltenen Instance verwenden können. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.
- Lassen Sie auf der Seite Choose an Instance Type (Instance-Typ wählen) den Standard-Instance-Typ, den der Assistent für Sie auswählt, unverändert.
- Geben Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) dieselbe Availability Zone wie für die ursprüngliche Instance an. Falls Sie eine Instance in einem VPC starten, wählen Sie ein Subnetz in dieser Availability Zone.
- Fügen Sie auf der Seite Add Tags (Tags (Markierungen) hinzufügen) das Tags (Markierungen) `Name=Temporary` zur Instance hinzu, um anzugeben, dass es sich um eine temporäre Instance handelt.
- Klicken Sie auf der Seite Review auf Launch. Wählen Sie das Schlüsselpaar aus, das Sie in Schritt 1 erstellt haben, und wählen Sie dann Launch Instances (Instances starten) aus.

Schritt 5: Trennen des Stamm-Volumes von der ursprünglichen Instance und Anfügen an die temporäre Instance

1. Wählen Sie im Navigationsbereich Volumes und wählen Sie das Root-Geräte-Volume für die ursprüngliche Instance aus (Sie haben die Volume-ID in einem früheren Schritt notiert). Wählen Sie Actions (Aktionen) und danach Detach volume (Volume trennen) aus, gefolgt von Detach (Trennen). Warten Sie, bis der Status des Volumes `available` wird. (Sie müssen möglicherweise das Symbol Refresh (Aktualisieren) wählen.)
2. Wählen Sie bei ausgewähltem Volume Actions (Aktionen) und wählen Sie dann Attach Volume (Volume anfügen) aus. Wählen Sie die Instance-ID der vorübergehenden Instance aus, notieren Sie den Gerätenamen unter Device name (Gerätenamen) (zum Beispiel `/dev/sdf`) und wählen Sie dann Attach volume (Volume anhängen) aus.

> **Note**
>
> Wenn Sie Ihre ursprüngliche Instance von einem AWS Marketplace AMI aus gestartet haben und Ihr Volume AWS Marketplace Codes enthält, müssen Sie zuerst die temporäre Instance beenden, bevor Sie das Volume anhängen können.

Schritt 6: Hinzufügen des neuen öffentlichen Schlüssels zu **authorized_keys** auf dem ursprünglichen Volume, das auf der temporären Instance gemountet wird

1. Stellen Sie eine Verbindung mit der temporären Instance her.
2. Mounten Sie in der temporären Instance das Volume, das Sie an die Instance angefügt haben, damit Sie auf ihr Dateisystem zugreifen können. Beispiel: Falls der Gerätename `/dev/sdf` lautet, verwenden Sie die folgenden Befehle zum Mounten des Volume als `/mnt/tempvol`.

   > **Note**
   >
   > Der Gerätename wird auf Ihrer Instance möglicherweise anders angezeigt. Beispiel: Geräte, die als `/dev/sdf` gemountet wurden, werden auf der Instance möglicherweise als `/dev/xvdf` angezeigt. Einige Versionen von Red Hat (oder Varianten wie CentOS) können den letzten Buchstaben möglicherweise noch um 4 Zeichen erhöhen, wobei `/dev/sdf` zu `/dev/xvdk` wird.

   a. Verwenden Sie den Befehl lsblk, um zu ermitteln, ob das Volume partitioniert ist.

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   ##xvda1 202:1    0    8G  0 part /
   xvdf    202:80   0  101G  0 disk
   ##xvdf1 202:81   0  101G  0 part
   xvdg    202:96   0   30G  0 disk
   ```

   Im Beispiel oben sind `/dev/xvda` und `/dev/xvdf` partitionierte Volumes und `/dev/xvdg` nicht. Falls Ihr Volume partitioniert ist, mounten Sie die Partition (`/dev/xvdf1`) anstelle des Rohdatenträgers (`/dev/xvdf`) in den nächsten Schritten.

   b. Erstellen Sie ein temporäres Verzeichnis zum Mounten des Volumes.

   ```
   [ec2-user ~]$ sudo mkdir /mnt/tempvol
   ```

   c. Mounten Sie das Volume (oder die Partitionierung) am temporären Mount-Punkt mithilfe des Volume-Namens oder des Gerätenamens, den Sie vorher in Erfahrung

gebracht haben. Der erforderliche Befehl hängt vom Dateisystem Ihres Betriebssystems ab. Beachten Sie, dass der Gerätename auf Ihrer Instance möglicherweise anders angezeigt wird. Weitere Informationen finden Sie in note in Schritt 6.

- Amazon Linux, Ubuntu und Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 und RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Wenn Sie einen Fehler erhalten, der besagt, dass das Dateisystem beschädigt ist, führen Sie den folgenden Befehl aus, um mit dem Dienstprogramm fsck das Dateisystem zu prüfen und mögliche Probleme zu beheben:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Verwenden Sie in der temporären Instance den folgenden Befehl, um `authorized_keys` mit dem neuen öffentlichen Schlüssel über `authorized_keys` für die temporäre Instance am gemounteten Volume zu aktualisieren.

> **Important**
>
> Die folgenden Beispiele verwenden den Amazon Linux-Benutzernamen `ec2-user`. Sie können ihn durch einen anderen Benutzernamen ersetzen, wie etwa `ubuntu` für Ubuntu-Instances.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Falls diese Kopie erfolgreich verlief, können Sie mit dem nächsten Schritt fortfahren.

(Optional) Falls Sie keine Berechtigung zum Bearbeiten von Dateien in `/mnt/tempvol` besitzen, müssen Sie die Datei mithilfe von sudo aktualisieren und dann die Berechtigungen für die Datei überprüfen, um zu gewährleisten, dass Sie sich an der ursprünglichen Instance anmelden können. Führen Sie den folgenden Befehl aus, um die Berechtigungen für die Datei zu prüfen.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

In dieser Beispielausgabe lautet die Benutzer-ID *222* und die Gruppen-ID *500*. Verwenden Sie als Nächstes sudo, um den fehlgeschlagenen Kopierbefehl erneut auszuführen.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Führen Sie den folgenden Befehl noch einmal aus, um zu ermitteln, ob sich die Berechtigungen geändert haben.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Falls sich die Benutzer-ID und die Gruppen-ID geändert haben, verwenden Sie den folgenden Befehl, um sie wiederherzustellen.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Schritt 7: Aufheben der Bereitstellung und Trennen des ursprünglichen Volumes von der temporären Instance und erneutes Anfügen an die ursprüngliche Instance

1. Entfernen Sie in der temporären Instance das Volume, das Sie angefügt haben, damit Sie es wieder an der ursprünglichen Instance anhängen können. Verwenden Sie beispielsweise den folgenden Befehl, um die Bereitstellung des Volumes unter aufzuhebe `/mnt/tempvol`.

```
[ec2-user ~]$ sudo umount /mnt/tempvol
```

2. Trennen Sie das Volume von der temporären Instance (Sie haben das Mounting der Bereitstellung im vorherigen Schritt aufgehoben): Wählen Sie in der Amazon EC2-Konsole im NavigationsbereichVolumes wählen sie das Stamm-Gerät-Volume für die ursprüngliche Instance (Sie haben die Volume-ID in einem vorherigen Schritt notiert) wählen Sie Actions (Aktionen), Detach volume (Volumen trennen) und dann Detach (Trennen) aus. Warten Sie, bis der Status des Volumes `available` wird. (Sie müssen möglicherweise das Symbol Refresh (Aktualisieren) wählen.)
3. Erneutes Anfügen des Volume an die ursprüngliche Instance: Wählen Sie bei weiter ausgewähltem Volume Actions (Aktionen) die Option Attach Volume (Volume anfügen) aus. Wählen Sie die Instance-ID der ursprünglichen Instance aus, geben Sie den Gerätenamen an, den Sie zuvor in Schritt 2 für die ursprüngliche Stammgeräte-Anlage (`/dev/sda1` oder `/dev/xvda`) notiert haben, und wählen Sie dann Attach volume (Volume anhängen) aus.

   Important

   Falls Sie nicht denselben Gerätenamen als ursprünglichen Anhang angeben, können Sie die ursprüngliche Instance nicht starten. Amazon EC2 erwartet den Root-Gerät-Datenträger unter `sda1` oder `/dev/xvda`.

Schritt 8: Verbinden Sie sich mit der ursprünglichen Instance mit dem neuen Schlüsselpaar

Wählen Sie die ursprüngliche Instance und dann Instance state (Instance-Status), Start instance (Instance starten). Wenn die Instance den Status `running` erhält, können Sie mit der Datei mit dem privaten Schlüssel für Ihr neues Schlüsselpaar eine Verbindung zu ihr herstellen.

Note

Falls sich der Name Ihres neuen Schlüsselpaars und der entsprechenden Datei mit dem privaten Schlüssel vom Namen des ursprünglichen Schlüsselpaars unterscheidet, müssen Sie den Namen der Datei mit dem neuen privaten Schlüssel angeben, wenn Sie eine Verbindung mit Ihrer Instance herstellen.

Schritt 9: Bereinigen

(Optional) Sie können die temporäre Instance beenden, falls Sie keine weitere Verwendung mehr dafür haben. Wählen Sie die temporäre Instance und dann Instance state (Instance-Status), Terminate instance (Instance beenden) aus.

Wenn Sie mit Putty eine Verbindung zu Ihrer Instance herstellen und die `.pem`-Datei in `.ppk` konvertieren müssen, finden Sie weitere Informationen unter Konvertieren Ihres privaten Schlüssels mit PuTTYgen im Herstellen einer Verbindung zu Ihrer Linux-Instance über Windows mit PuTTY-Thema in diesem Abschnitt.

- Festlegen der Berechtigungen für Ihren privaten Schlüssel, so dass nur Sie diesen lesen können
  - Herstellen einer Verbindung über macOS oder Linux

    (Linux-Instanzen) Wenn Sie einen SSH-Client auf einem macOS- oder Linux-Computer verwenden möchten, um eine Verbindung zu Ihrer Linux-Instance herzustellen, verwenden Sie den folgenden Befehl, um die Berechtigungen Ihrer privaten Schlüsseldatei so festzulegen, dass nur Sie sie lesen können.

    ```
    chmod 400 key-pair-name.pem
    ```

    Wenn Sie diese Berechtigungen nicht festlegen, können Sie unter Verwendung dieses Schlüsselpaars keine Verbindung zu Ihrer Instance herstellen. Weitere Informationen finden Sie unter Fehler: Ungeschützte private Schlüsseldatei.
  - Herstellen einer Verbindung über Windows

    Öffnen Sie den Datei-Explorer und klicken Sie mit der rechten Maustaste auf die `.pem`-Datei. Wählen Sie Eigenschaften > Registerkarte Sicherheit und dann Erweitert aus. Wählen Sie Vererbung deaktivieren. Entfernen Sie den Zugriff für alle Benutzer mit Ausnahme des aktuellen Benutzers.

(Optional) Anfordern des Instance-Fingerabdrucks

Um sich vor man-in-the-middle Angriffen zu schützen, können Sie die Echtheit der Instanz, zu der Sie eine Verbindung herstellen möchten, überprüfen, indem Sie den angezeigten Fingerabdruck überprüfen. Die Überprüfung des Fingerabdrucks ist nützlich, wenn Sie Ihre Instance über ein öffentliches AMI gestartet haben, das von einem Drittanbieter bereitgestellt wird.

Übersicht über die Aufgaben

Rufen Sie zunächst den Instance-Fingerabdruck von der Instance ab. Wenn Sie dann eine Verbindung mit der Instanz herstellen und aufgefordert werden, den Fingerabdruck zu verifizieren, vergleichen Sie den Fingerabdruck, den Sie in diesem Verfahren erhalten haben, mit dem angezeigten Fingerabdruck. Wenn die Fingerabdrücke nicht übereinstimmen, versucht möglicherweise jemand einen man-in-the-middle Angriff. Wenn sie übereinstimmen, können Sie bedenkenlos eine Verbindung mit der Instance herstellen.

Voraussetzungen für das Abrufen des Instance-Fingerabdrucks

- Die Instance darf sich nicht im Status `pending` befinden. Der Fingerabdruck ist erst verfügbar, nachdem der erste Start der Instance abgeschlossen ist.
- Sie müssen der Instance-Eigentümer sein, um die Konsolenausgabe zu erhalten.
- Es gibt verschiedene Möglichkeiten, den Instanz-Fingerabdruck zu erhalten. Wenn Sie den verwenden möchten AWS CLI, muss er auf Ihrem lokalen Computer installiert sein. Informationen zur Installation von finden Sie unter Installation von AWS Command Line Interface im AWS Command Line Interface Benutzerhandbuch. AWS CLI

So fordern Sie den Instance-Fingerabdruck an

In Schritt 1 erhalten Sie die Konsolenausgabe, die den Instanz-Fingerabdruck enthält. In Schritt 2 finden Sie den Instanz-Fingerabdruck in der Konsolenausgabe.

1. Rufen Sie die Konsolenausgabe mit einer der folgenden Methoden ab.

   Console

   1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
   2. Wählen Sie im linken Navigator Instances aus.
   3. Wählen Sie Ihre Instanz aus und wählen Sie dann Aktionen, Überwachung und Fehlerbehebung, Systemprotokoll abrufen aus.

   AWS CLI

   Verwenden Sie auf Ihrem lokalen Computer (nicht auf der Instanz, zu der Sie eine Verbindung herstellen) den Befehl get-console-output (AWS CLI). Wenn die Ausgabe umfangreich ist, können Sie sie an eine Textdatei weiterleiten, wo sie möglicherweise

einfacher zu lesen ist. Beachten Sie, dass Sie eine angeben müssen, AWS-Region wenn Sie den verwenden AWS CLI, entweder explizit oder indem Sie eine Standardregion festlegen. Informationen zum Festlegen oder Angeben einer Region finden Sie unter Konfigurationsgrundlagen im AWS Command Line Interface -Benutzerhandbuch.

```
aws ec2 get-console-output --instance-id instance_id --query Output --output
 text > temp.txt
```

2. Suchen Sie in der Konsolenausgabe nach dem Instanz-Fingerabdruck (Host-Fingerprint), der sich unter befindet`BEGIN SSH HOST KEY FINGERPRINTS`. Möglicherweise gibt es mehrere Instanz-Fingerabdrücke. Wenn Sie eine Verbindung zu Ihrer Instance herstellen, wird nur einer der Fingerabdrücke angezeigt.

   Die genaue Ausgabe kann je nach Betriebssystem, AMI-Version und davon, ob AWS die Schlüsselpaare erstellt hat, variieren. Es folgt eine Beispielausgabe.

```
ec2:#############################################################
ec2: -----BEGIN SSH HOST KEY FINGERPRINTS-----
ec2: 256 SHA256:l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY no comment (ECDSA)
ec2: 256 SHA256:kpEa+rw/Uq3zxaYZN8KT501iBtJOIdHG52dFi66EEfQ no comment (ED25519)
ec2: 2048 SHA256:L8l6pepcA7iqW/jBecQjVZClUrKY+o2cHLI0iHerbVc no comment (RSA)
ec2: -----END SSH HOST KEY FINGERPRINTS-----
ec2: #############################################################
```

> **Note**
>
> Sie verweisen auf diesen Fingerabdruck, wenn Sie eine Verbindung mit der Instance herstellen.

Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH

Sie können Secure Shell (SSH) verwenden, um von einem lokalen Computer aus, auf dem ein Linux- oder macOS-Betriebssystem ausgeführt wird, eine Verbindung zu Ihrer Linux-Instance herzustellen, oder Sie können ein plattformunabhängiges Verbindungstool wie EC2 Instance Connect oder AWS Systems Manager Session Manager verwenden. Weitere Informationen zu plattformunabhängigen Tools finden Sie unter Herstellen einer Verbindung zur Linux-Instance.

Auf dieser Seite erfahren Sie, wie Sie die Verbindung zu Ihrer Instance mit einem SSH-Client herstellen. Informationen zum Herstellen einer Verbindung zu Ihrer Linux-Instance von Windows aus finden Sie unter Herstellen einer Verbindung über Windows.

> **Note**
>
> Wenn Sie beim Versuch, eine Verbindung zu Ihrer Instance herzustellen, eine Fehlermeldung erhalten, stellen Sie sicher, dass Ihre Instance alle Voraussetzungen für eine SSH-Verbindung erfüllt. Wenn alle Voraussetzungen erfüllt sind und Sie immer noch keine Verbindung zu Ihrer Linux-Instance herstellen können, lesen Sie Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

Inhalt

Voraussetzungen für eine SSH-Verbindung

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie eine Verbindung mit Ihrer Linux-Instance herstellen.

Überprüfen Ihres Instance-Status

Wenn Sie die Instance starten, kann es einige Minuten dauern, bis die Instance zur Verbindung bereitsteht. Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Sie können diese Informationen auf der Seite Instances in der Spalte Status check (Statusprüfung) anzeigen.

Holen Sie sich den öffentlichen DNS-Namen und den Benutzernamen zum Herstellen einer Verbindung mit Ihrer Instance

Informationen zum öffentlichen DNS-Namen oder der IP-Adresse Ihrer Instance und zum Benutzernamen, den Sie für die Verbindung mit Ihrer Instance verwenden sollten, finden Sie unter Anfordern von Informationen zu Ihrer Instance.

Auffinden des privaten Schlüssels und Festlegen der Berechtigungen

Informationen zum Suchen des privaten Schlüssels, der für die Verbindung mit der Instance erforderlich ist, und zum Festlegen der Schlüsselberechtigungen finden Sie unter Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen.

Installieren eines SSH-Client auf dem lokalen Computer je nach Bedarf

Auf Ihrem lokalen Computer ist möglicherweise standardmäßig ein SSH-Client installiert. Sie können dies überprüfen, indem Sie in der Befehlszeile ssh eingeben. Wenn Ihr Computer den Befehl nicht erkennt, können Sie einen SSH-Client installieren.

- Aktuelle Versionen von Windows Server 2019 und Windows 10 – OpenSSH ist als installierbare Komponente enthalten. Weitere Informationen finden Sie unter OpenSSH in Windows.
- Frühere Versionen von Windows – Laden Sie OpenSSH herunter und installieren Sie es. Weitere Informationen finden Sie unter Win32-OpenSSH.
- Linux und macOS X – Laden Sie OpenSSH herunter und installieren Sie es. Weitere Informationen finden Sie unter https://www.openssh.com.

Verbinden mit der Linux-Instance über einen SSH-Client

Verwenden Sie die folgende Vorgehensweise, um per SSH-Client eine Verbindung mit Ihrer Linux-Instance herzustellen. Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

Herstellung einer Verbindung zu Ihrer Instance mit SSH

1. Verwenden Sie in einem Terminalfenster den Befehl ssh, um eine Verbindung mit der Instance herzustellen. Sie geben den Pfad und Dateinamen des privaten Schlüssels (`.pem`), den Benutzernamen für Ihre Instance und den öffentlichen DNS-Namen oder die IPv6-Adresse für Ihre Instance an. Weitere Informationen zum Suchen des privaten Schlüssels, des Benutzernamens für Ihre Instance und des DNS-Namens oder der IPv6-Adresse für eine Instance finden Sie unter Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen und Anfordern von Informationen zu Ihrer Instance. Um eine Verbindung mit Ihrer Instance herzustellen, verwenden Sie einen der folgenden Befehle.
   - (Öffentliches DNS) Geben Sie den folgenden Befehl ein, um eine Verbindung mit dem öffentlichen DNS-Namen Ihrer Instance herzustellen.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, geben Sie alternativ den folgenden Befehl ein, um eine Verbindung mit der IPv6-Adresse Ihrer Instance herzustellen.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Sie erhalten in etwa folgende Antwort:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

2. (Optional) Vergewissern Sie sich, dass der Fingerabdruck in der Sicherheitswarnung mit dem Fingerabdruck übereinstimmt, den Sie zuvor unter (Optional) Anfordern des Instance-Fingerabdrucks abgerufen haben. Wenn diese Fingerabdrücke nicht übereinstimmen, versucht möglicherweise jemand einen Angriff. man-in-the-middle Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren.
3. Geben Sie ei **`yes`**.

   Sie erhalten in etwa folgende Antwort:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Übertragen von Dateien auf Linux-Instances mit einem SCP-Client

Eine Möglichkeit, Dateien zwischen Ihrem lokalen Computer und einer Linux-Instance zu übertragen, ist die Verwendung von Secure Copy Protocol (SCP). In diesem Abschnitt wird beschrieben, wie Sie Dateien mit SCP übertragen. Die Vorgehensweise ähnelt den Schritten zum Herstellen einer Verbindung mit einer Instance per SSH.

Voraussetzungen

- Überprüfen Sie die allgemeinen Voraussetzungen für das Übertragen von Dateien zu Ihrer Instance.

Bevor Sie Dateien zwischen Ihrem lokalen Rechner und Ihrer Instance übertragen, stellen Sie mit den folgenden Aktionen sicher, dass Sie über alle benötigten Informationen verfügen.

- Anfordern von Informationen zu Ihrer Instance
- Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen
- (Optional) Anfordern des Instance-Fingerabdrucks

- Installieren eines SCP-Clients

  Die meisten Linux-, Unix- und Apple-Computer enthalten standardmäßig einen SCP-Client. Falls dies bei Ihnen nicht der Fall ist, können Sie über das OpenSSH-Projekt die kostenlose Implementierung der gesamten SSH-Tools nutzen, einschließlich des SCP-Clients. Weitere Informationen finden Sie unter https://www.openssh.com.

Das folgende Verfahren führt Sie durch die Verwendung von SCP zum Übertragen einer Datei unter Verwendung des öffentlichen DNS-Namens der Instance oder der IPv6-Adresse, falls Ihre Instance eine hat.

So verwenden Sie SCP zum Übertragen von Dateien zwischen Ihrem Computer und Ihrer Instance

1. Bestimmen Sie den Speicherort der Quelldatei auf Ihrem Computer und den Zielpfad auf der Instance. In den folgenden Beispielen lautet der Name der privaten Schlüsseldatei `key-pair-name.pem`, die zu übertragende Datei ist `my-file.txt`, der Benutzername für die Instance ist ec2-user, der öffentliche DNS-Name der Instance ist `instance-public-dns-name` und die IPv6-Adresse der Instance ist `instance-IPv6-address`.
   - (Öffentlicher DNS) Um eine Datei an das Ziel der Instance zu übertragen, geben Sie den folgenden Befehl von Ihrem Computer aus ein.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@instance-public-dns-name:path/
     ```

   - (IPv6) Um eine Datei an das Ziel der Instance zu übertragen, wenn die Instance eine IPv6-Adresse hat, geben Sie den folgenden Befehl von Ihrem Computer aus ein. Die IPv6-Adresse muss in eckige Klammern (`[ ]`) gesetzt werden, die mit einem Escape-Zeichen (\) versehen sein müssen.

     ```
     scp -i /path/key-pair-name.pem /path/my-file.txt ec2-user@\[instance-IPv6-address\]:path/
     ```

2. Wenn Sie noch keine Verbindung mit der Instance über SSH hergestellt haben, wird eine Antwort wie etwa die folgende angezeigt:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

(Optional) Sie können optional überprüfen, ob der Fingerabdruck in der Sicherheitswarnung mit dem Fingerabdruck der Instance übereinstimmt. Weitere Informationen finden Sie unter (Optional) Anfordern des Instance-Fingerabdrucks.

Geben Sie **`yes`** ein.

3. Wenn die Übertragung erfolgreich ist, ähnelt die Antwort der folgenden:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
my-file.txt                                   100%   480     24.4KB/s   00:00
```

4. Kehren Sie die Reihenfolge der Host-Parameter um, um eine Datei in der anderen Richtung zu übertragen (von der Amazon EC2 Instance auf Ihren Computer). Sie können beispielsweise, wie in den folgenden Beispielen gezeigt, `my-file.txt` von Ihrer EC2-Instance zu einem Ziel als `my-file2.txt` auf Ihrem lokalen Computer übertragen.

   - (Öffentlicher DNS) Um eine Datei an ein Ziel auf Ihrem Computer zu übertragen, geben Sie den folgenden Befehl von Ihrem Computer aus ein.

     ```
     scp -i /path/key-pair-name.pem ec2-user@instance-public-dns-name:path/my-
     file.txt path/my-file2.txt
     ```

   - (IPv6) Um eine Datei an ein Ziel auf Ihrem Computer zu übertragen, wenn die Instance eine IPv6-Adresse hat, geben Sie den folgenden Befehl von Ihrem Computer aus ein. Die IPv6-Adresse muss in eckige Klammern (`[ ]`) gesetzt werden, die mit einem Escape-Zeichen (\) versehen sein müssen.

     ```
     scp -i /path/key-pair-name.pem ec2-user@\[instance-IPv6-address\]:path/my-
     file.txt path/my-file2.txt
     ```

Herstellen einer Verbindung zu Ihrer Linux-Instance über Windows

Mit den folgenden Methoden können Sie von einem lokalen Rechner mit einem Windows-Betriebssystem eine Verbindung zu Ihrer Linux-Instance herstellen.

Herstellen einer Verbindung zu Ihrer Linux Instance über Windows mit OpenSSH

Im Folgenden erfahren Sie, wie Sie von Windows aus mit OpenSSH, einem Open-Source-Tool für die Fernanmeldung über das SSH-Protokoll, eine Verbindung mit Ihrer Linux-Instance herstellen können. OpenSSH wird unter Windows-Server-2019-Betriebssystemen und höher unterstützt.

Inhalt

Voraussetzungen

Bevor Sie mit OpenSSH von Windows aus eine Verbindung mit Ihrer Linux-Instance herstellen, müssen Sie die folgenden Voraussetzungen erfüllen.

Überprüfen Sie, ob die Instance bereit ist.

> Wenn Sie die Instance starten, kann es einige Minuten dauern, bis die Instance zur Verbindung bereitsteht. Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Sie können diese Informationen auf der Seite Instances in der Spalte Status check (Statusprüfung) anzeigen.

Überprüfen der allgemeinen Voraussetzungen für das Herstellen einer Verbindung mit einer Instance

> Informationen zum Auffinden des öffentlichen DNS-Namens oder der IP-Adresse Ihrer Instance und des Benutzernamens, den Sie zum Herstellen einer Verbindung mit Ihrer Instance verwenden sollten, finden Sie unter Anfordern von Informationen zu Ihrer Instance.

Verifizieren Ihrer Windows-Version

> Um über OpenSSH eine Verbindung zu Ihrer Linux-Instance von Windows herzustellen, muss die Windows-Version Windows Server 2019 und höher sein.

Überprüfen Sie die Voraussetzungen PowerShell

Um OpenSSH auf Ihrem Windows-Betriebssystem zu installieren PowerShell, müssen Sie PowerShell Version 5.1 oder höher ausführen und Ihr Konto muss Mitglied der integrierten Administratorgruppe sein. Führen Sie den `$PSVersionTable.PSVersion` Befehl von aus PowerShell , um Ihre PowerShell Version zu überprüfen.

Führen Sie den folgenden PowerShell Befehl aus, um zu überprüfen, ob Sie Mitglied der integrierten Administratorgruppe sind:

```
(New-Object
 Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).Is
```

Wenn Sie Mitglied der integrierten Administratorgruppe sind, lautet die Ausgabe `True`.

Installieren Sie OpenSSH für Windows mit PowerShell

Führen Sie den folgenden Befehl aus PowerShell, um OpenSSH für Windows mit zu installieren: PowerShell

```
Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Erwartete Ausgabe:

```
Path          :
Online        : True
RestartNeeded : False
```

Herstellen einer Verbindung mit einer Linux-Instance von Windows mithilfe von OpenSSH

Nachdem Sie OpenSSH installiert haben, verwenden Sie das folgende Verfahren, um von Windows aus eine Verbindung zu Ihrer Linux-Instance mit OpenSSH herzustellen. Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

So stellen Sie mit OpenSSH eine Verbindung mit Ihrer Instance her

1. Verwenden Sie in PowerShell oder in der Befehlszeile den ssh Befehl, um eine Verbindung mit der Instanz herzustellen. Sie geben den Pfad und den Dateinamen des privaten Schlüssels (`.pem`), den Benutzernamen für Ihre Instance und den öffentlichen DNS-Namen oder die IPv6-

Adresse für Ihre Instance an. Weitere Informationen zum Auffinden des privaten Schlüssels, des Benutzernamens für Ihre Instance und des DNS-Namens oder der IPv6-Adresse für eine Instance finden Sie unter Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen und Anfordern von Informationen zu Ihrer Instance. Um eine Verbindung mit Ihrer Instance herzustellen, verwenden Sie einen der folgenden Befehle.

- (Öffentliches DNS) Geben Sie den folgenden Befehl ein, um eine Verbindung mit dem öffentlichen DNS-Namen Ihrer Instance herzustellen.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-public-dns-name
```

- (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, geben Sie alternativ den folgenden Befehl ein, um eine Verbindung mit der IPv6-Adresse Ihrer Instance herzustellen.

```
ssh -i /path/key-pair-name.pem instance-user-name@instance-IPv6-address
```

Sie erhalten in etwa folgende Antwort:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (198-51-100-1)'
 can't be established.
ECDSA key fingerprint is l4UB/neBad9tvkgJf1QZWxheQmR59WgrgzEimCG6kZY.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

2. (Optional) Vergewissern Sie sich, dass der Fingerabdruck in der Sicherheitswarnung mit dem Fingerabdruck übereinstimmt, den Sie zuvor unter (Optional) Anfordern des Instance-Fingerabdrucks abgerufen haben. Wenn diese Fingerabdrücke nicht übereinstimmen, versucht möglicherweise jemand einen man-in-the-middle Angriff. Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren.
3. Geben Sie ei **yes**.

   Sie erhalten in etwa folgende Antwort:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (ECDSA) to
 the list of known hosts.
```

Deinstallieren Sie OpenSSH von Windows mit PowerShell

Führen Sie den folgenden PowerShell Befehl aus, um OpenSSH PowerShell unter Windows zu deinstallieren:

```
Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
```

Erwartete Ausgabe:

```
Path          :
Online        : True
RestartNeeded : True
```

Herstellen einer Verbindung zu Ihrer Linux-Instance über Windows mit PuTTY

Wenn Sie Windows Server 2019 oder höher ausführen, empfehlen wir die Verwendung von OpenSSH, einem Open-Source-Konnektivitätstool für die Fernanmeldung mit dem SSH-Protokoll. Schritte zum Herstellen einer Verbindung mit einer Linux-Instance von Windows mit OpenSSH finden Sie unter Herstellen einer Verbindung zu Ihrer Linux Instance über Windows mit OpenSSH.

Im Folgenden wird beschrieben, wie Sie per PuTTY (kostenloser SSH-Client für Windows) eine Verbindung mit Ihrer Instance herstellen. Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

Inhalt

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie per PuTTY eine Verbindung mit Ihrer Linux-Instance herstellen:

Überprüfen Sie, ob die Instance bereit ist.

> Wenn Sie die Instance starten, kann es einige Minuten dauern, bis die Instance zur Verbindung bereitsteht. Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Sie können diese Informationen auf der Seite Instances in der Spalte Status check (Statusprüfung) anzeigen.

Überprüfen der allgemeinen Voraussetzungen für das Herstellen einer Verbindung mit einer Instance

Informationen zum Auffinden des öffentlichen DNS-Namens oder der IP-Adresse Ihrer Instance und des Benutzernamens, den Sie zum Herstellen einer Verbindung mit Ihrer Instance verwenden sollten, finden Sie unter Anfordern von Informationen zu Ihrer Instance.

Installieren Sie PuTTY auf dem lokalen Computer.

Laden Sie PuTTY über die Downloadseite für PuTTY herunter und führen Sie die Installation durch. Wenn Sie bereits eine frühere Version von PuTTY installiert haben, wird empfohlen, die neueste Version herunterzuladen. Vergewissern Sie sich, dass Sie die gesamte Suite installieren.

Konvertieren Ihres privaten PEM-Schlüssels in PPK-Format mit PuTTYgen

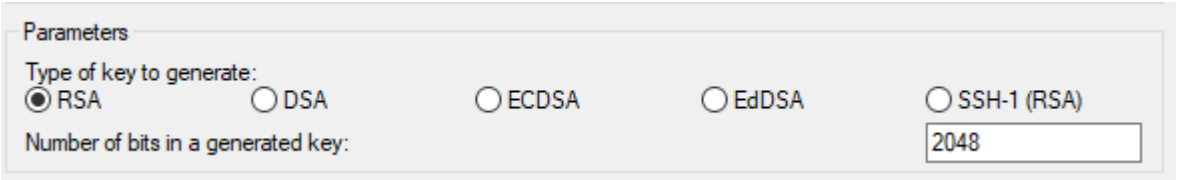
Wenn Sie für das Schlüsselpaar, das Sie beim Start der Instance angegeben haben, einen privaten Schlüssel im PEM-Format erstellt haben, müssen Sie ihn ins PPK-Format umwandeln, damit er mit PuTTY genutzt werden kann. Suchen Sie die private PEM-Datei und befolgen Sie dann die Schritte im nächsten Abschnitt.

Konvertieren Ihres privaten Schlüssels mit PuTTYgen

PuTTY unterstützt das PEM-Format für SSH-Schlüssel nicht nativ. PuTTY stellt ein Tool namens PuTTYgen bereit, das PEM-Schlüssel in das gewünschte Format „PPK“ für PuTTY konvertiert. Sie müssen Ihren privaten Schlüssel (PEM-Datei) wie folgt in dieses Format (PPK-Datei) konvertieren, bevor Sie mithilfe von PuTTY eine Verbindung mit Ihrer Instance herstellen können.

Einen privaten PEM-Schlüssel ins PPK-Format konvertieren

1. Wählen Sie im Menü Start All Programs (Alle Programme), PuTTY, PuTTYgen aus.
2. Wählen Sie unter Type of key to generate die Option RSA. Wenn Ihre Version von PuTTYgen diese Option nicht enthält, wählen Sie SSH-2 RSA.



3. Wählen Sie Load (Laden) aus. PuTTYgen zeigt standardmäßig nur Dateien mit der Erweiterung `.ppk` an. Damit Sie die `.pem`-Datei finden, wählen Sie die Option zur Anzeige aller Dateitypen aus.

4. Wählen Sie Ihre `.pem`-Datei für das Schlüsselpaar aus, das Sie beim Starten Ihrer Instance angegeben haben, und wählen Sie anschließend Open (Öffnen). PuTTYgen zeigt einen Hinweis an, dass die `.pem`-Datei erfolgreich importiert wurde. Klicken Sie auf OK.
5. Klicken Sie auf Save private key, um den Schlüssel in einem mit PuTTY kompatiblen Format zu speichern. PuTTYgen zeigt einen Warnhinweis zur Speicherung des Schlüssels ohne Passphrase an. Wählen Sie Yes (Ja).

> **Note**
>
> Eine Passphrase stellt bei einem privaten Schlüssel eine zusätzliche Schutzebene dar. Auch wenn Ihr privater Schlüssel erkannt wird, kann er ohne die Passphrase nicht verwendet werden. Der Nachteil einer Passphrase ist, dass sie die Automatisierung erschwert, da für Anmeldungen bei einer Instance oder dem Kopieren von Dateien zu einer Instance menschliche Eingriffe erforderlich sind.

6. Geben Sie den gleichen Namen für den Schlüssel an, den Sie für das Schlüsselpaar verwendet haben (z. B. `key-pair-name`), und wählen Sie Save (Speichern) aus. PuTTY fügt automatisch die Dateierweiterung `.ppk` hinzu.

Ihr persönlicher Schlüssel ist nun im korrekten Format zur Verwendung mit PuTTY. Sie können sich nun über den SSH-Client von PuTTY mit Ihrer Instance verbinden.

Herstellen einer Verbindung zur Linux-Instance

Verwenden Sie die folgende Vorgehensweise, um per PuTTY eine Verbindung mit Ihrer Linux-Instance herzustellen. Sie benötigen die `.ppk`-Datei, die Sie für Ihren privaten Schlüssel erstellt haben. Für weitere Informationen vgl. Konvertieren Ihres privaten Schlüssels mit PuTTYgen im vorherigen Abschnitt. Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

Letzte getestete Version von PuTTY: .78

So stellen Sie mithilfe von PuTTY eine Verbindung mit Ihrer Instance her

1. Starten Sie PuTTY (suchen Sie im Startmenü nach PuTTY und wählen Sie anschließend Öffnen aus).
2. Wählen Sie im Bereich Category die Option Session und füllen Sie die folgenden Felder aus:

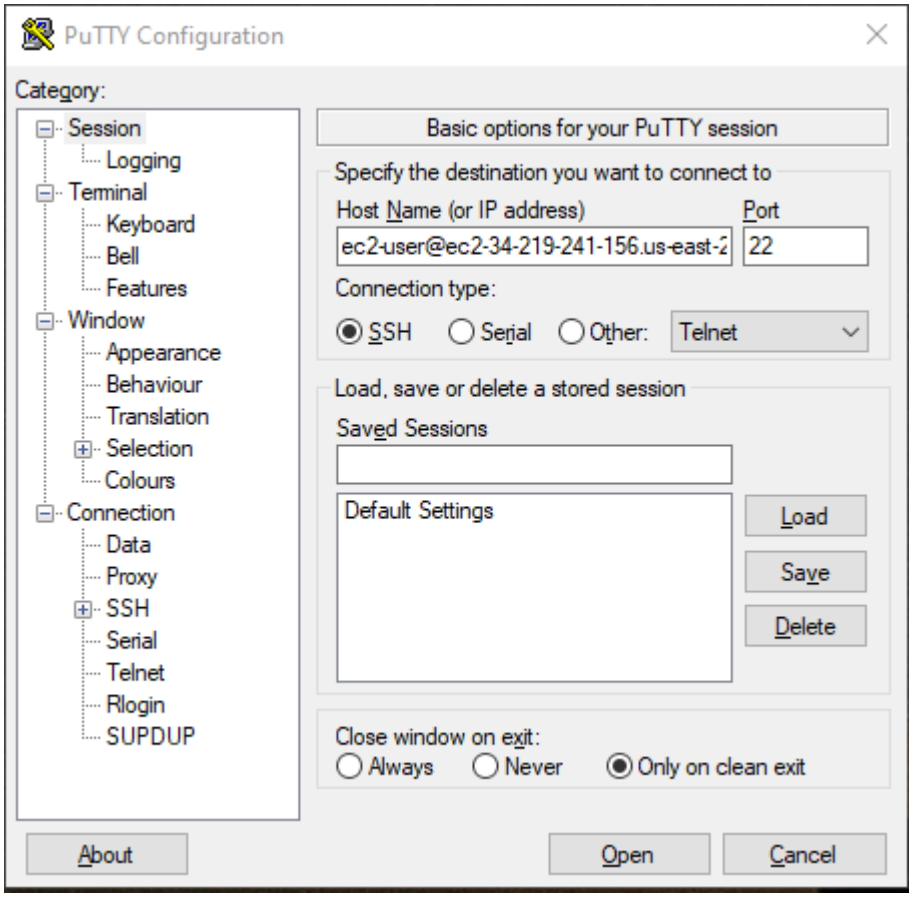
   a. Führen Sie im Feld Host Name (Hostname) einen der folgenden Schritte aus:

      - (Public DNS) Um eine Verbindung über den öffentlichen DNS-Namen Ihrer Instance herzustellen, geben Sie *instance-user-name*@*instance-public-dns-name* ein.
      - (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, können Sie sich auch mit der IPv6-Adresse Ihrer Instance verbinden, indem Sie *instance-user-name*@*instance-IPv6-address* eingeben.

      Informationen zum Abrufen des Benutzernamens für Ihre Instance sowie des öffentlichen DNS-Namens oder der IPv6-Adresse Ihrer Instance finden Sie unter Anfordern von Informationen zu Ihrer Instance.

   b. Vergewissern Sie sich, dass der Port-Wert 22 ist.

   c. Wählen Sie unter Connection type die Option SSH.



3. (Optional) Sie können konfigurieren, dass PuTTY in regelmäßigen Zeitabständen automatisch 'keepalive'-Daten sendet, um die Sitzung aktiv zu halten. Auf diese Weise können Sie vermeiden, dass die Verbindung mit Ihrer Instance aufgrund von Sitzungsinaktivität getrennt wird. Wählen Sie im Bereich Kategorie die Option Verbindung aus und geben Sie dann das erforderliche Intervall in Sekunden zwischen Keepalives ein. Wenn Ihre Sitzung z. B. nach 10 Minuten Inaktivität getrennt wird, geben Sie „180“ ein, damit PuTTY so konfiguriert wird, dass alle 3 Minuten keepalive-Daten gesendet werden.
4. Erweitern Sie im Bereich Kategorie die Optionen Verbindung, SSH und Authentifizierung. Wählen Sie Anmeldeinformationen aus.
5. Wählen Sie neben Private Schlüsseldatei für Authentifizierung: die Option Durchsuchen aus. Wählen Sie im Dialogfeld Private Schlüsseldatei auswählen die `.ppk`-Datei aus, die Sie für Ihr Schlüsselpaar generiert haben. Sie können entweder auf die Datei doppelklicken oder Öffnen im Dialogfeld Private Schlüsseldatei auswählen wählen.
6. (Optional) Wenn Sie planen, nach dieser Sitzung erneut eine Verbindung zu dieser Instance herzustellen, können Sie die Sitzungsinformationen für die zukünftige Verwendung speichern.

Wählen Sie im Bereich Kategorie die Option Sitzung aus. Geben Sie unter Gespeicherte Sitzungen einen Namen für die Sitzung ein und wählen Sie dann Speichern.

7. Um eine Verbindung mit der Instance herzustellen, wählen Sie Öffnen.
8. Wenn Sie zum ersten Mal eine Verbindung mit dieser Instance hergestellt haben, zeigt PuTTY ein Dialogfeld mit einer Sicherheitswarnung an. Darin werden Sie gefragt, ob Sie dem Host vertrauen, mit dem die Verbindung hergestellt werden soll.

   a. (Optional) Vergewissern Sie sich, dass der Fingerabdruck im Dialogfeld der Sicherheitswarnung mit dem Fingerabdruck übereinstimmt, den Sie zuvor unter (Optional) Anfordern des Instance-Fingerabdrucks abgerufen haben. Wenn diese Fingerabdrücke nicht übereinstimmen, wird ggf. versucht, einen Man-In-the-Middle-Angriff durchzuführen. Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren.

   b. Wählen Sie Accept (Akzeptieren) aus. Ein neues Fenster wird geöffnet, und Sie sind mit Ihrer Instance verbunden.

> **Note**
>
> Falls Sie eine Passphrase angegeben haben, als Sie den persönlichen Schlüssel in das PuTTY-Format konvertiert hatten, müssen Sie diese Passphrase eingeben, wenn Sie sich bei der Instance anmelden.

Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

Übertragen von Dateien auf Ihre Linux-Instance mit dem Secure Copy-Client von PuTTY

Der Secure Copy-Client von PuTTY (PSCP) ist ein Befehlszeilen-Tool, das Sie zum Übertragen von Dateien zwischen Ihrem Windows-Computer und Ihrer Linux-Instance verwenden können. Wenn Sie eine grafische Benutzeroberfläche (GUI) bevorzugen, können Sie das Open-Source-GUI-Tool WinSCP verwenden. Weitere Informationen finden Sie unter Übertragen von Dateien auf Ihre Linux-Instance per WinSCP.

Für die Verwendung von PSCP benötigen Sie den privaten Schlüssel, den Sie unter Konvertieren Ihres privaten Schlüssels mit PuTTYgen generiert haben. Sie benötigen auch den öffentlichen DNS-Namen Ihrer Linux-Instance oder die IPv6-Adresse, wenn Ihre Instance über eine verfügt.

Im folgenden Beispiel wird die Datei `Sample_file.txt` vom Laufwerk „C:\“ auf einem Windows-Computer in das Stammverzeichnis `instance-user-name` auf einer Amazon Linux-Instance übertragen. Um eine Datei zu übertragen, verwenden Sie einen der folgenden Befehle.

- (Öffentliches DNS) Geben Sie den folgenden Befehl ein, um eine Datei mithilfe des öffentlichen DNS-Namens Ihrer Instance zu übertragen.

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@instance-public-dns-name:/home/instance-user-name/Sample_file.txt
```

- (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, geben Sie alternativ den folgenden Befehl ein, um eine Datei mit der IPv6-Adresse Ihrer Instance zu übertragen. Die IPv6-Adresse muss in eckige Klammern (`[ ]`) gesetzt werden.

```
pscp -i C:\path\my-key-pair.ppk C:\path\Sample_file.txt instance-user-name@[instance-IPv6-address]:/home/instance-user-name/Sample_file.txt
```

Übertragen von Dateien auf Ihre Linux-Instance per WinSCP

WinSCP ist ein GUI-basierter Dateimanager für Windows, mit dem Sie Dateien mithilfe der Protokolle SFTP, SCP, FTP und FTPS hochladen und auf einen Remotecomputer übertragen können. Mit WinSCP können Sie Dateien per Drag-and-Drop von Ihrem Windows-Computer auf Ihre Linux-Instance ziehen oder ganze Verzeichnisstrukturen zwischen den beiden Systemen synchronisieren.

Voraussetzungen

- Sie müssen über den privaten Schlüssel verfügen, den Sie in Konvertieren Ihres privaten Schlüssels mit PuTTYgen generiert haben.
- Außerdem benötigen Sie den öffentlichen DNS-Namen Ihrer Linux-Instance.
- Ihre Linux-Instance muss `scp` installiert haben. Bei einigen Betriebssystemen installieren Sie das `openssh-clients`-Paket. Für andere, z. B. die Amazon ECS-optimierte AMI, installieren Sie das `scp`-Paket. Überprüfen Sie die Dokumentation für Ihre Linux-Distribution.

So stellen Sie per WinSCP eine Verbindung mit Ihrer Instance her:

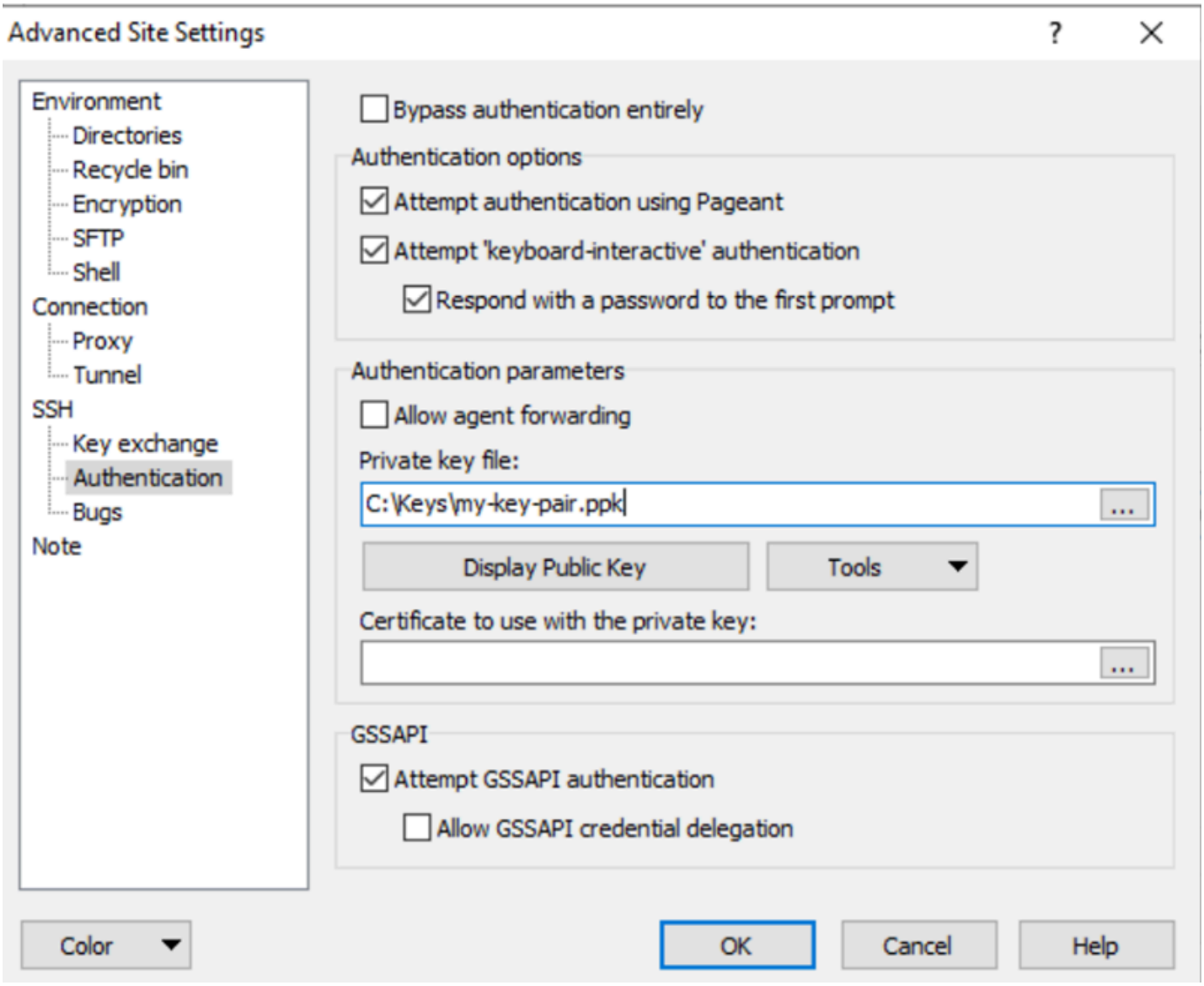
1. Laden Sie WinSCP von http://winscp.net/eng/download.php herunter und installieren Sie die Anwendung. Für die meisten Benutzer sind die Standardinstallationsoptionen geeignet.
2. Starten Sie WinSCP.

3. Machen Sie auf dem Bildschirm WinSCP-Anmeldung für Hostname eine der folgenden Angaben:
   - (Öffentliche DNS- oder IPv4-Adresse) Um sich mit dem öffentlichen DNS-Namen oder der öffentlichen IPv4-Adresse Ihrer Instance anzumelden, geben Sie den öffentlichen DNS-Namen oder die öffentliche IPv4-Adresse für Ihre Instance ein.
   - (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, geben Sie alternativ die IPv6-Adresse für Ihre Instance ein, um sich mit der IPv6-Adresse Ihrer Instance anzumelden.
4. Geben Sie als Benutzername den Standardbenutzernamen für Ihr AMI ein.
   - Bei AL2023, Amazon Linux 2 oder dem Amazon-Linux-AMI lautet der Benutzername `ec2-user`.
   - Bei einem CentOS-AMI lautet der Benutzername `centos` oder `ec2-user`.
   - Für ein Debian-AMI lautet der Benutzername `admin`.
   - Bei einem Fedora-AMI lautet der Benutzername `fedora` oder `ec2-user`.
   - Bei einem RHEL-AMI lautet der Benutzername `ec2-user` oder `root`.
   - Bei einem SUSE-AMI lautet der Benutzername `ec2-user` oder `root`.
   - Für ein Ubuntu-AMI lautet der Benutzername `ubuntu`.
   - Bei einem Oracle-AMI lautet der Benutzername `ec2-user`.
   - Für ein Bitnami-AMI lautet der Benutzername `bitnami`.

   > **Note**
   >
   > Um den Standardbenutzernamen für andere Linux-Distributionen zu finden, wenden Sie sich an den AMI-Anbieter.

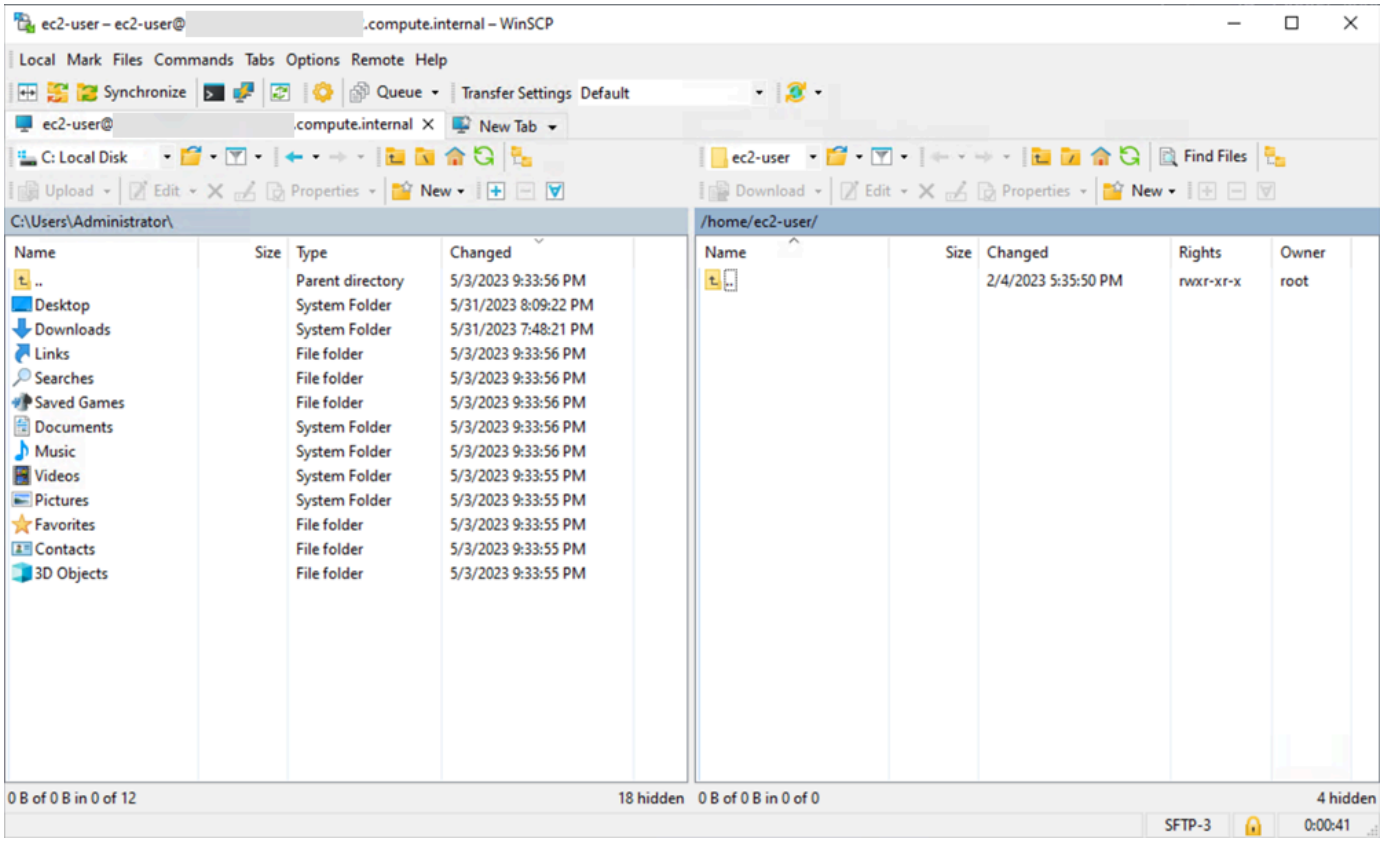
5. Geben Sie den privaten Schlüssel für Ihre Instance an.
   a. Wählen Sie die Schaltfläche Erweitert....
   b. Wählen Sie unter SSH die Option Authentifizierung aus.
   c. Geben Sie den Pfad für Ihre private Schlüsseldatei an oder wählen Sie die...-Schaltfläche, um zur Schlüsselpaardatei zu navigieren.
   d. Wählen Sie OK aus.

   Hier ist ein Screenshot aus Version 6.1 von WinSCP:



Für WinSCP ist eine PuTTY-Datei mit einem privaten Schlüssel (`.ppk`) erforderlich. Sie können eine `.pem`-Datei mit einem Sicherheitsschlüssel mit PuTTYgen in das Format `.ppk` konvertieren. Weitere Informationen finden Sie unter Konvertieren Ihres privaten Schlüssels mit PuTTYgen.

6. (Optional) Wählen Sie im linken Bereich Directories (Verzeichnisse) aus. Geben Sie für Remote directory (Remote-Verzeichnis) den Pfad zu dem Verzeichnis ein, zu dem die Dateien hinzugefügt werden. Wählen Sie zum Öffnen der erweiterten Standorteinstellungen bei neueren Version von WinSCP Advanced (Erweitert) aus. Zum Finden der Einstellung Remote directory (Remote-Verzeichnis) wählen Sie unter Environment (Umgebung) die Option Directories (Verzeichnisse) aus.
7. Wählen Sie Login (Anmelden) aus. Wählen Sie Yes (Ja) aus, um den Host-Fingerabdruck zum Host-Cache hinzuzufügen.



8. Nachdem Sie die Verbindung hergestellt haben, ist Ihre Linux-Instance im Verbindungsfenster rechts und Ihr lokaler Computer links angeordnet. Sie können Dateien zwischen dem Remote-Dateisystem und Ihrem lokalen Computer ziehen und ablegen. Weitere Informationen zu WinSCP erhalten Sie in der Projektdokumentation unter http://winscp.net/eng/docs/start.

   Wenn Sie eine Fehlermeldung erhalten, dass Sie SCP nicht ausführen können, um die Übertragung zu starten, überprüfen Sie, ob Sie scp auf der Linux-Instance installiert haben.

Herstellen einer Verbindung zu Ihrer Linux-Instance über Windows mit Windows-Subsystem für Linux (WSL)

Nachdem Sie Ihre Instance gestartet haben, können Sie sich mit ihr verbinden und sie so verwenden wie einen Computer, vor dem Sie sitzen.

In den folgenden Anweisungen wird erläutert, wie Sie mit einer Linux-Distribution auf dem Windows-Subsystem für Linux (WSL) eine Verbindung zu Ihrer Instance herstellen. WSL kann kostenlos heruntergeladen werden und ermöglicht Ihnen, native Linux-Befehlszeilen-Tools direkt unter Windows neben Ihrem herkömmlichen Windows-Desktop auszuführen, und zwar ohne den Aufwand einer virtuellen Maschine.

Durch Installieren von WSL können Sie eine native Linux-Umgebung anstatt PuTTY oder PuTTYgen verwenden, um eine Verbindung mit Ihren EC2-Instances herzustellen. Die Linux-Umgebung vereinfacht die Verbindungsherstellung mit Ihren Linux-Instances, da sie einen nativen SSH-Client umfasst, den Sie verwenden können, um eine Verbindung mit Ihren Linux-Instances herzustellen und die Berechtigungen der PEM-Schlüsseldatei zu ändern. Die Amazon EC2-Konsole stellt den SSH-Befehl für die Verbindung mit der Linux-Instance bereit und Sie können eine ausführliche Ausgabe vom SSH-Befehl zwecks Fehlerbehebung abrufen. Weitere Informationen finden Sie in der Dokumentation zum Windows-Subsystem für Linux.

> **Note**
>
> Nach der Installation von WSL gelten alle Voraussetzungen und Schritte wie in Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH beschrieben und die Benutzererfahrung entspricht der mit nativem Linux.

Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

Inhalt

Voraussetzungen

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie eine Verbindung mit Ihrer Linux-Instance herstellen.

Überprüfen Sie, ob die Instance bereit ist.

Wenn Sie die Instance starten, kann es einige Minuten dauern, bis die Instance zur Verbindung bereitsteht. Stellen Sie sicher, dass Ihre Instance ihre Statusprüfungen bestanden hat. Sie können diese Informationen auf der Seite Instances in der Spalte Status check (Statusprüfung) anzeigen.

Überprüfen der allgemeinen Voraussetzungen für das Herstellen einer Verbindung mit einer Instance

Informationen zum öffentlichen DNS-Namen oder der IP-Adresse Ihrer Instance und zum Benutzernamen, den Sie für die Verbindung mit Ihrer Instance verwenden sollten, finden Sie unter Anfordern von Informationen zu Ihrer Instance.

Installieren des Windows-Subsystems für Linux (WSL) sowie einer Linux-Distribution auf Ihrem lokalen Computer

Installieren Sie WSL und eine Linux-Distribution mithilfe der Anleitung im Installationshandbuch für Windows 10. Mit dem in der Anleitung genannten Beispiel wird die Ubuntu-Distribution von Linux installiert, Sie können jedoch jede beliebige Distribution installieren. Sie werden zum Neustart Ihres Computers aufgefordert, damit die Änderungen wirksam werden.

Den privaten Schlüssel aus Windows in WSL kopieren

Kopieren Sie in einem WSL-Terminal-Fenster die Datei `.pem` (für das Schlüsselpaar, das Sie beim Start der Instance angegeben haben) aus Windows in WSL. Beachten Sie den vollqualifizierten Pfad zur Datei `.pem` in WSL, der zum Herstellen der Verbindung mit Ihrer Instance verwendet wird. Informationen dazu, wie Sie den Pfad zu Ihrem Windows-Laufwerk angeben, finden Sie unter How do I access my C drive?. Weitere Informationen zu Schlüsselpaaren und Windows-Instances finden Sie unter Amazon EC2-Schlüsselpaare und Windows-Instances.

```
cp /mnt/<Windows drive letter>/path/my-key-pair.pem ~/WSL-path/my-key-pair.pem
```

Herstellen einer Verbindung zu Ihrer Linux-Instance mit WSL

Führen Sie die folgenden Schritte aus, um mit dem Windows-Subsystem für Linux (WSL) eine Verbindung mit Ihrer Linux-Instance herzustellen. Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance.

So stellen Sie per SSH eine Verbindung mit Ihrer Instance her

1. Verwenden Sie in einem Terminalfenster den Befehl ssh, um eine Verbindung mit der Instance herzustellen. Sie geben den Pfad und Dateinamen des privaten Schlüssels (`.pem`), den Benutzernamen für Ihre Instance und den öffentlichen DNS-Namen oder die IPv6-Adresse für Ihre Instance an. Weitere Informationen zum Suchen des privaten Schlüssels, des Benutzernamens für Ihre Instance und des DNS-Namens oder der IPv6-Adresse für

eine Instance finden Sie unter Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen und Anfordern von Informationen zu Ihrer Instance. Um eine Verbindung mit Ihrer Instance herzustellen, verwenden Sie einen der folgenden Befehle.

- (Öffentliches DNS) Geben Sie den folgenden Befehl ein, um eine Verbindung mit dem öffentlichen DNS-Namen Ihrer Instance herzustellen.

```
ssh -i /path/key-pair-name.pem instance-user-name@my-instance-public-dns-name
```

- (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, können Sie alternativ über ihre IPv6-Adresse eine Verbindung mit der Instance herstellen. Geben Sie den Befehl ssh mit dem Pfad zur Datei mit dem privaten Schlüssel (.pem), den entsprechenden Benutzernamen und die IPv6-Adresse an.

```
ssh -i /path/key-pair-name.pem instance-user-name@my-instance-IPv6-address
```

Sie erhalten in etwa folgende Antwort:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

2. (Optional) Vergewissern Sie sich, dass der Fingerabdruck in der Sicherheitswarnung mit dem Fingerabdruck übereinstimmt, den Sie zuvor unter (Optional) Anfordern des Instance-Fingerabdrucks abgerufen haben. Wenn diese Fingerabdrücke nicht übereinstimmen, wird ggf. versucht, einen Man-In-the-Middle-Angriff durchzuführen. Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren.
3. Geben Sie ei `yes`.

   Sie erhalten in etwa folgende Antwort:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
```

Übertragen von Dateien aus Linux auf Linux-Instances per SCP

Eine Möglichkeit, Dateien zwischen Ihrem lokalen Computer und einer Linux-Instance zu übertragen, ist die Verwendung von Secure Copy Protocol (SCP). In diesem Abschnitt wird beschrieben, wie

Sie Dateien mit SCP übertragen. Die Vorgehensweise ähnelt den Schritten zum Herstellen einer Verbindung mit einer Instance per SSH.

Voraussetzungen

- Überprüfen Sie die allgemeinen Voraussetzungen für das Übertragen von Dateien zu Ihrer Instance.

  Bevor Sie Dateien zwischen Ihrem lokalen Rechner und Ihrer Instance übertragen, stellen Sie mit den folgenden Aktionen sicher, dass Sie über alle benötigten Informationen verfügen.

  - Anfordern von Informationen zu Ihrer Instance
  - Lokalisieren des privaten Schlüssels und Festlegen von Berechtigungen
  - (Optional) Anfordern des Instance-Fingerabdrucks
- Installieren eines SCP-Clients

  Die meisten Linux-, Unix- und Apple-Computer enthalten standardmäßig einen SCP-Client. Falls dies bei Ihnen nicht der Fall ist, können Sie über das OpenSSH-Projekt die kostenlose Implementierung der gesamten SSH-Tools nutzen, einschließlich des SCP-Clients. Weitere Informationen finden Sie unter https://www.openssh.com.

Im Folgenden wird die Verwendung von SCP zum Übertragen einer Datei Schritt für Schritt beschrieben. Wenn Sie bereits per SSH eine Verbindung mit der Instance hergestellt und die dazugehörigen Fingerabdrücke überprüft haben, können Sie mit dem Schritt beginnen, der den SCP-Befehl enthält (Schritt 4).

So verwenden Sie SCP zum Übertragen einer Datei

1. Übertragen Sie eine Datei auf Ihre Instance, indem Sie den öffentlichen DNS-Namen der Instance verwenden. Verwenden Sie beispielsweise einen der folgenden Befehle, um die Datei in das Stammverzeichnis `instance-user-name` zu kopieren, wenn der Name der Datei mit dem privaten Schlüssel `key-pair-name`, die zu übertragende Datei `SampleFile.txt`, der Benutzername `instance-user-name` und der öffentliche DNS-Name für die Instance `my-instance-public-dns-name` oder die IPv6-Adresse `my-instance-IPv6-address` lautet.
   - (Öffentliches DNS) Geben Sie den folgenden Befehl ein, um eine Datei mithilfe des öffentlichen DNS-Namens Ihrer Instance zu übertragen.

```
scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@my-instance-public-dns-name:~
```

- (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, können Sie eine Datei mit der IPv6-Adresse der Instance übertragen. Die IPv6-Adresse muss in eckige Klammern (`[ ]`) gesetzt werden, die mit einem Escape-Zeichen (\) versehen sein müssen.

```
scp -i /path/key-pair-name.pem /path/SampleFile.txt instance-user-name@\[my-instance-IPv6-address\]:~
```

Sie erhalten in etwa folgende Antwort:

```
The authenticity of host 'ec2-198-51-100-1.compute-1.amazonaws.com (10.254.142.33)'
can't be established.
RSA key fingerprint is 1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f.
Are you sure you want to continue connecting (yes/no)?
```

2. (Optional) Vergewissern Sie sich, dass der Fingerabdruck in der Sicherheitswarnung mit dem Fingerabdruck übereinstimmt, den Sie zuvor unter (Optional) Anfordern des Instance-Fingerabdrucks abgerufen haben. Wenn diese Fingerabdrücke nicht übereinstimmen, wird ggf. versucht, einen Man-In-the-Middle-Angriff durchzuführen. Falls die Fingerabdrücke übereinstimmen, können Sie mit dem nächsten Schritt fortfahren.
3. Geben Sie ei **`yes`**.

   Sie erhalten in etwa folgende Antwort:

```
Warning: Permanently added 'ec2-198-51-100-1.compute-1.amazonaws.com' (RSA)
to the list of known hosts.
Sending file modes: C0644 20 SampleFile.txt
Sink: C0644 20 SampleFile.txt
SampleFile.txt                                100%   20     0.0KB/s   00:00
```

   Wenn Sie den Fehler „bash: scp: command not found“ erhalten, müssen Sie auf Ihrer Linux-Instance zuerst scp installieren. Bei einigen Betriebssystemen ist SCP im `openssh-clients`-Paket enthalten. Verwenden Sie für Amazon Linux-Varianten, z. B. das Amazon ECS-optimierte AMI, den folgenden Befehl zum Installieren von scp:

```
[ec2-user ~]$ sudo yum install -y openssh-clients
```

4. Kehren Sie die Reihenfolge der Hostparameter um, um Dateien in der anderen Richtung zu übertragen (von der Amazon EC2 Instance auf Ihren lokalen Computer). Verwenden Sie beispielsweise einen der folgenden Befehle auf Ihrem lokalen Computer, um die Datei `SampleFile.txt` von Ihrer EC2-Instance unter dem Namen `SampleFile2.txt` zurück in das Stammverzeichnis Ihres lokalen Computers zu übertragen.
   - (Öffentliches DNS) Geben Sie den folgenden Befehl ein, um eine Datei mithilfe des öffentlichen DNS-Namens Ihrer Instance zu übertragen.

     ```
     scp -i /path/key-pair-name.pem instance-user-
     name@ec2-198-51-100-1.compute-1.amazonaws.com:~/SampleFile.txt ~/
     SampleFile2.txt
     ```

   - (IPv6) Wenn Ihre Instance über eine IPv6-Adresse verfügt, geben Sie alternativ den folgenden Befehl ein, um Dateien mit der IPv6-Adresse der Instance in die andere Richtung zu übertragen.

     ```
     scp -i /path/key-pair-name.pem instance-user-name@
     \[2001:db8:1234:1a00:9691:9503:25ad:1761\]:~/SampleFile.txt ~/SampleFile2.txt
     ```

Deinstallieren des WSL

Informationen zum Deinstallieren des Windows-Subsystems für Linux finden Sie unter How do I uninstall a WSL Distribution?.

Herstellen einer Verbindung zu Ihrer Linux-Instance mit EC2 Instance Connect

Amazon EC2 Instance Connect bietet eine einfache und sichere Möglichkeit, über Secure Shell (SSH) eine Verbindung zu Ihren Linux-Instances herzustellen. Mit EC2 Instance Connect verwenden Sie AWS Identity and Access Management (IAM) -Richtlinien und -Prinzipale, um den SSH-Zugriff auf Ihre Instances zu kontrollieren, sodass SSH-Schlüssel nicht mehr gemeinsam genutzt und verwaltet werden müssen. Alle Verbindungsanfragen, die EC2 Instance Connect verwenden, werden protokolliert, AWS CloudTrail sodass Sie Verbindungsanfragen überprüfen können.

Sie können EC2 Instance Connect verwenden, um sich über die Amazon-EC2-Konsole oder einen SSH-Client Ihrer Wahl mit Ihren Instances zu verbinden.

Wenn Sie über EC2 Instance Connect eine Verbindung mit einer Instance herstellen, überträgt die Instance-Connect-API per Push einen öffentlichen SSH-Schlüssel an die Instance-Metadaten, wo er 60 Sekunden verbleibt. Eine an Ihren Benutzer angefügte IAM-Richtlinie autorisiert Ihren Benutzer,

den öffentlichen Schlüssel an die Instance-Metadaten zu übertragen. Der SSH-Daemon verwendet `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser`, die bei der Installation von Instance Connect konfiguriert werden, um zur Authentifizierung den öffentlichen Schlüssel in der Instance-Metadaten zu suchen, und stellt eine Verbindung mit der Instance her.

Sie können EC2 Instance Connect verwenden, um eine Verbindung zu Instances herzustellen, die öffentliche oder private IP-Adressen haben. Weitere Informationen finden Sie unter Verbindung über EC2 Instance Connect.

Einen Blogbeitrag, der erörtert, wie Sie die Sicherheit Ihrer Bastion-Hosts mithilfe von EC2 Instance Connect verbessern können, finden Sie unter Sichern Ihrer Bastion-Hosts mit Amazon EC2 Instance Connect.

> **Tip**
>
> EC2 Instance Connect ist eine der Optionen, mit denen Sie eine Verbindung zu Ihrer Linux-Instance herstellen können. Weitere Optionen finden Sie unter Herstellen einer Verbindung zur Linux-Instance. Informationen zum Herstellen einer Verbindung mit einer Windows-Instance finden Sie unterHerstellen einer Verbindung mit Ihrer -Windows-Instance.

Inhalt

Tutorial: Schließen Sie die Konfiguration ab, die für die Verbindung mit Ihrer Instance mithilfe von EC2 Instance Connect erforderlich ist

Um über EC2 Instance Connect in der Amazon EC2 EC2-Konsole eine Verbindung zu Ihrer Instance herzustellen, müssen Sie zunächst die erforderliche Konfiguration abschließen, damit Sie erfolgreich eine Verbindung zu Ihrer Instance herstellen können. Der Zweck dieses Tutorials besteht darin, Sie durch die Aufgaben zum Abschließen der erforderlichen Konfiguration zu führen.

Überblick über das Tutorial

In diesem Tutorial werden Sie die folgenden vier Aufgaben erledigen:

- Aufgabe 1: Eine IAM-Richtlinie erstellen und anhängen, damit Sie EC2 Instance Connect verwenden können

  Zunächst erstellen Sie eine IAM-Richtlinie, die die IAM-Berechtigungen enthält, mit denen Sie einen öffentlichen Schlüssel für die Instance-Metadaten bereitstellen können. Sie fügen diese Richtlinie Ihrer IAM-Identität (Benutzer, Benutzergruppe oder Rolle) hinzu, sodass Ihre IAM-Identität diese Berechtigungen erhält.
- Aufgabe 2: Erstellen Sie eine Sicherheitsgruppe, um eingehenden Datenverkehr vom EC2 Instance Connect-Dienst zu Ihrer Instance zuzulassen

  Anschließend erstellen Sie eine Sicherheitsgruppe, die den Datenverkehr vom EC2 Instance Connect-Dienst zu Ihrer Instance zulässt. Dies ist erforderlich, wenn Sie EC2 Instance Connect in der Amazon EC2 EC2-Konsole verwenden, um eine Verbindung zu Ihrer Instance herzustellen.
- Aufgabe 3: Starten Sie Ihre Instance

  Anschließend starten Sie eine EC2-Instance mit einem AMI, auf dem EC2 Instance Connect vorinstalliert ist, und fügen die Sicherheitsgruppe hinzu, die Sie im vorherigen Schritt erstellt haben.
- Aufgabe 4: Connect zu Ihrer Instance her

  Schließlich verwenden Sie EC2 Instance Connect in der Amazon EC2 EC2-Konsole, um eine Verbindung zu Ihrer Instance herzustellen. Wenn Sie eine Verbindung herstellen können, können Sie sicher sein, dass die erforderliche Konfiguration, die Sie in den Aufgaben 1, 2 und 3 abgeschlossen haben, erfolgreich war.

Aufgabe 1: Eine IAM-Richtlinie erstellen und anhängen, damit Sie EC2 Instance Connect verwenden können

Wenn Sie über EC2 Instance Connect eine Verbindung mit einer Instance herstellen, überträgt die Instance-Connect-API per Push einen öffentlichen SSH-Schlüssel an die Instance-Metadaten, wo er 60 Sekunden verbleibt. Sie benötigen eine IAM-Richtlinie, die an Ihre IAM-Identität (Benutzer, Benutzergruppe oder Rolle) angehängt ist, um Ihnen die erforderliche Berechtigung zu erteilen, den öffentlichen Schlüssel in die Instance-Metadaten zu übertragen.

Ziel der Aufgabe

In dieser Aufgabe erstellen Sie die IAM-Richtlinie, die die Erlaubnis erteilt, den öffentlichen Schlüssel an die Instance weiterzuleiten. Die spezifische Aktion, die zugelassen werden soll, ist`ec2-instance-connect:SendSSHPublicKey`. Sie müssen die `ec2:DescribeInstances` Aktion auch zulassen, damit Sie Ihre Instance in der Amazon EC2 EC2-Konsole anzeigen und auswählen können.

Sobald Sie die Richtlinie erstellt haben, fügen Sie die Richtlinie Ihrer IAM-Identität (Benutzer, Benutzergruppe oder Rolle) hinzu, sodass Ihre IAM-Identität die entsprechenden Berechtigungen erhält.

Sie erstellen eine Richtlinie, die wie folgt konfiguriert ist:

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeInstances",
            "Resource": "*"
        }
    ]
}
```

Important

Die in diesem Tutorial erstellte IAM-Richtlinie ist sehr freizügig. Sie ermöglicht es Ihnen, mit einem beliebigen AMI-Benutzernamen eine Verbindung zu jeder Instance herzustellen. Wir verwenden diese sehr freizügige Richtlinie, um das Tutorial einfach zu halten und uns auf die spezifischen Konfigurationen zu konzentrieren, die in diesem Tutorial vermittelt werden. In einer Produktionsumgebung empfehlen wir jedoch, dass Ihre IAM-Richtlinie so konfiguriert ist, dass Berechtigungen mit den geringsten Rechten bereitgestellt werden. Beispiele für IAM-Richtlinien finden Sie unter Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect.

Schritte zum Erstellen und Anhängen der IAM-Richtlinie

Gehen Sie wie folgt vor, um die IAM-Richtlinie zu erstellen und anzuhängen. Eine Animation der Schritte finden Sie unter Eine Animation anzeigen: Erstellen Sie eine IAM-Richtlinie undSehen Sie sich eine Animation an: Hängen Sie eine IAM-Richtlinie an.

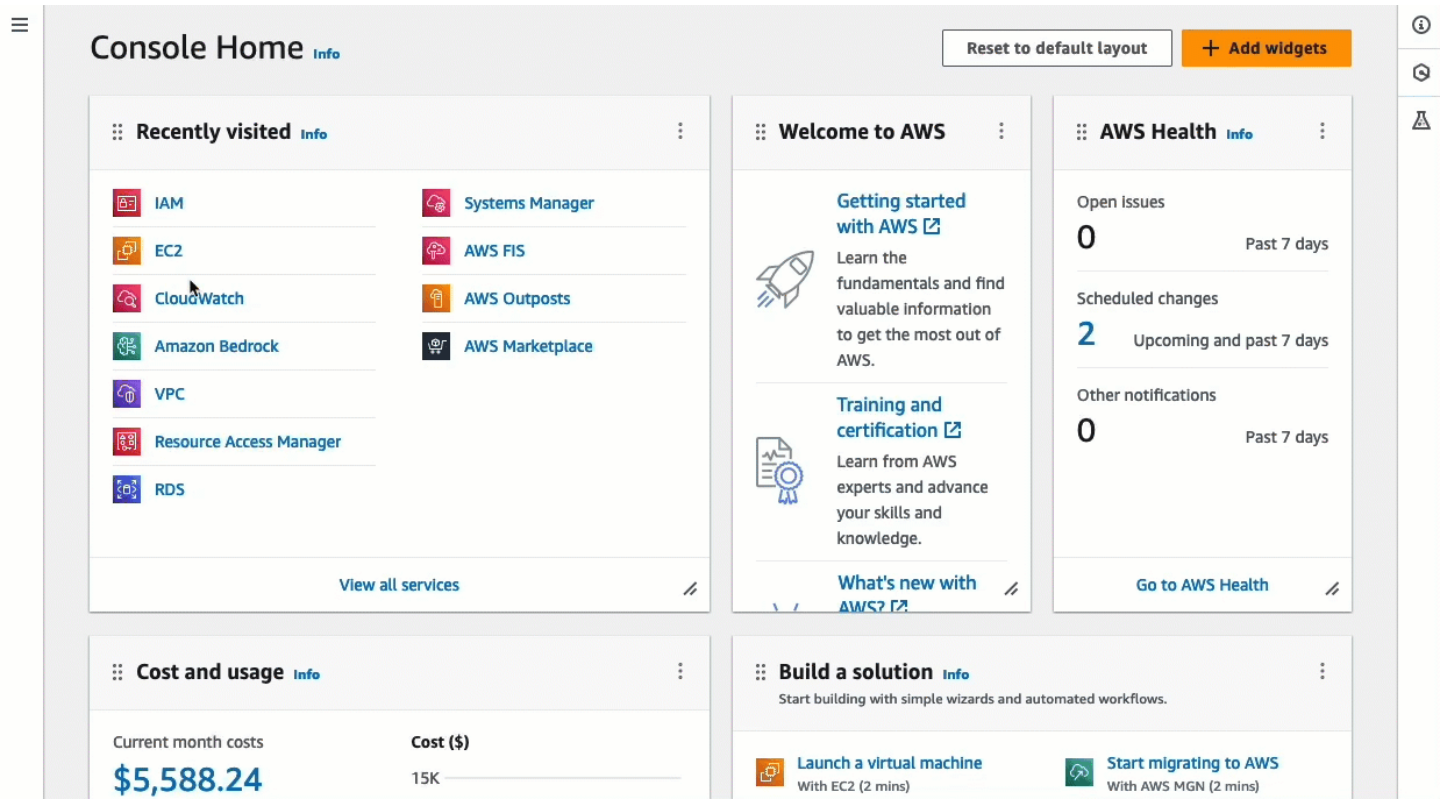
Um eine IAM-Richtlinie zu erstellen und anzuhängen, die es Ihnen ermöglicht, EC2 Instance Connect zu verwenden, um eine Verbindung zu Ihren Instances herzustellen

1. Erstellen Sie zunächst die IAM-Richtlinie
   a. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
   b. Wählen Sie im Navigationsbereich Policies aus.
   c. Wählen Sie Richtlinie erstellen aus.
   d. Gehen Sie auf der Seite „Berechtigung angeben“ wie folgt vor:
      i. Wählen Sie für Service EC2 Instance Connect.
      ii. Beginnen Sie unter Zulässige Aktionen im Suchfeld mit der Eingabe, **`send`** um die entsprechenden Aktionen anzuzeigen, und wählen Sie dann PublicKeySendSSH aus.
      iii. Wählen Sie unter Ressourcen die Option Alle aus. Für eine Produktionsumgebung empfehlen wir, die Instanz anhand ihres ARN anzugeben, aber für dieses Tutorial lassen Sie alle Instanzen zu.
      iv. Wählen Sie Add more permissions aus.
      v. Wählen Sie bei -Service EC2 aus.
      vi. Beginnen Sie unter Zulässige Aktionen im Suchfeld mit der Eingabe**`describein`**, um die entsprechenden Aktionen anzuzeigen, und wählen Sie dann aus DescribeInstances.
      vii. Wählen Sie Weiter aus.
   e. Gehen Sie auf der Seite Überprüfen und erstellen wie folgt vor:
      i. Geben Sie unter Policy Name (Richtlinienname) einen Namen für diese Richtlinie ein.
      ii. Wählen Sie Richtlinie erstellen aus.
2. Fügen Sie dann die Richtlinie Ihrer Identität hinzu
   a. Wählen Sie im Navigationsbereich der IAM-Konsole die Option Policies.
   b. Wählen Sie in der Liste der Richtlinien das Optionsfeld neben dem Namen der Richtlinie aus, die Sie erstellt haben. Sie können über das Suchfeld die Liste der Gruppen filtern.
   c. Wählen Sie Actions (Aktionen) und Attach (Anfügen).

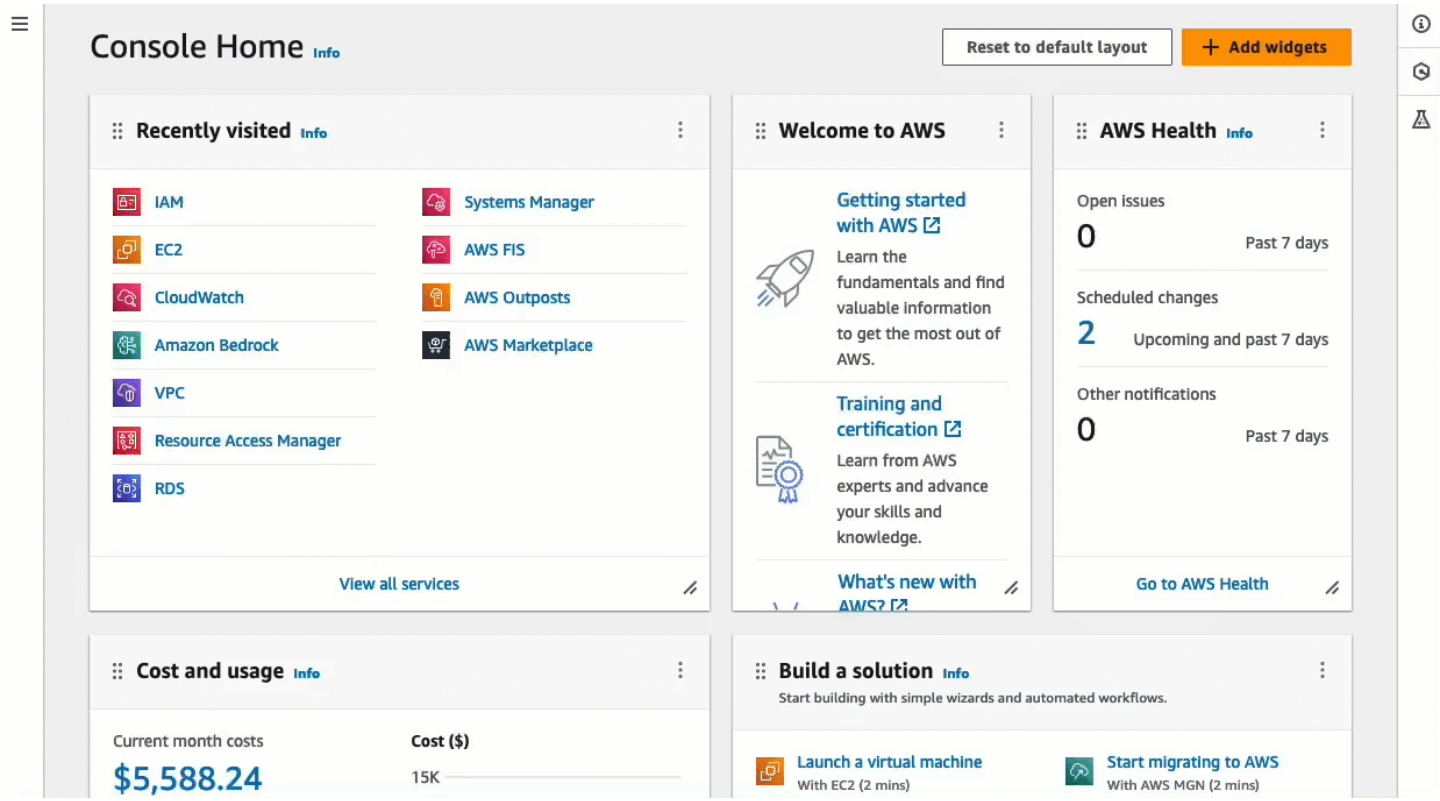
d. Aktivieren Sie unter IAM-Entitäten das Kontrollkästchen neben Ihrer Identität (Benutzer, Benutzergruppe oder Rolle). Sie können das Suchfeld verwenden, um die Liste der Entitäten zu filtern.

e. Wählen Sie Richtlinie anfügen aus.

Eine Animation anzeigen: Erstellen Sie eine IAM-Richtlinie



Sehen Sie sich eine Animation an: Hängen Sie eine IAM-Richtlinie an



Aufgabe 2: Erstellen Sie eine Sicherheitsgruppe, um eingehenden Datenverkehr vom EC2 Instance Connect-Dienst zu Ihrer Instance zuzulassen

Wenn Sie EC2 Instance Connect in der Amazon EC2 EC2-Konsole verwenden, um eine Connect zu einer Instance herzustellen, ist der Datenverkehr, der die Instance erreichen darf, Datenverkehr vom EC2 Instance Connect-Service. Dies unterscheidet sich von der Verbindung von Ihrem lokalen Computer zu einer Instance. In diesem Fall müssen Sie den Datenverkehr von Ihrem lokalen Computer zu Ihrer Instance zulassen. Um Datenverkehr vom EC2 Instance Connect-Dienst zuzulassen, müssen Sie eine Sicherheitsgruppe erstellen, die eingehenden SSH-Verkehr aus dem IP-Adressbereich für den EC2 Instance Connect-Dienst zulässt.

Die IP-Adressbereiche für die AWS Dienste sind unter https://ip-ranges.amazonaws.com/ip-ranges.json verfügbar. Die IP-Adressbereiche von EC2 Instance Connect werden durch `"service": "EC2_INSTANCE_CONNECT"` identifiziert.

Ziel der Aufgabe

In dieser Aufgabe finden Sie zunächst den IP-Adressbereich für den, `EC2_INSTANCE_CONNECT` AWS-Region in dem sich Ihre Instance befindet. Anschließend erstellen Sie eine Sicherheitsgruppe, die eingehenden SSH-Verkehr auf Port 22 aus diesem IP-Adressbereich zulässt.

Schritte zum Erstellen der Sicherheitsgruppe

Gehen Sie wie folgt vor, um die Sicherheitsgruppe zu erstellen. Eine Animation der Schritte finden Sie unter Animation anzeigen: Rufen Sie den IP-Adressbereich für EC2 Instance Connect für eine bestimmte Region ab undSehen Sie sich eine Animation an: Konfigurieren Sie eine Sicherheitsgruppe.

Um eine Sicherheitsgruppe zu erstellen, die eingehenden Datenverkehr vom EC2 Instance Connect-Dienst zu Ihrer Instance zulässt

1. Rufen Sie zunächst den IP-Adressbereich für den EC2 Instance Connect-Dienst ab.

   a. Öffnen Sie die JSON-Datei mit den AWS IP-Adressbereichen unter https://ip-ranges.amazonaws.com/ip-ranges.json.

   b. Wählen Sie Rohdaten.

   c. Suchen Sie den IP-Adressbereich `EC2_INSTANCE_CONNECT` für den, AWS-Region in dem sich Ihre Instance befindet. Sie können das Suchfeld des Browsers verwenden, um nach dem Dienst zu suchen`EC2_INSTANCE_CONNECT`, und die Suche fortsetzen, bis Sie die Region gefunden haben, in der sich Ihre Instance befindet.

      Wenn sich Ihre Instance beispielsweise in der Region USA Ost (Nord-Virginia) (`us-east-1`) befindet, lautet der IP-Adressbereich für `EC2_INSTANCE_CONNECT` diese Region`18.206.107.24/29`.

      > **Note**
      >
      > Die IP-Adressbereiche sind jeweils unterschiedlich AWS-Region.

   d. Kopieren Sie den IP-Adressbereich, der neben angezeigt wird`ip_prefix`. Sie werden diesen IP-Adressbereich später in diesem Verfahren verwenden.

   Weitere Informationen zum Herunterladen der JSON-Datei für AWS IP-Adressbereiche und zum Filtern nach Service finden Sie unter AWS IP-Adressbereiche im Amazon VPC-Benutzerhandbuch.

2. Erstellen Sie dann die Sicherheitsgruppe mit einer Regel für eingehenden Datenverkehr, um Datenverkehr aus dem kopierten IP-Adressbereich zuzulassen

   a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

b. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.

c. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.

d. Gehen Sie unter Basic details (Grundlegende Angaben) wie folgt vor:

   i. Geben Sie unter Name der Sicherheitsgruppe einen aussagekräftigen Namen für Ihre Sicherheitsgruppe ein.

   ii. Geben Sie unter Beschreibung eine aussagekräftige Beschreibung für Ihre Sicherheitsgruppe ein.

e. Gehen Sie unter Regeln für eingehenden Datenverkehr wie folgt vor:

   i. Wählen Sie Regel hinzufügen aus.

   ii. Wählen Sie unter Typ die Option SSH aus.

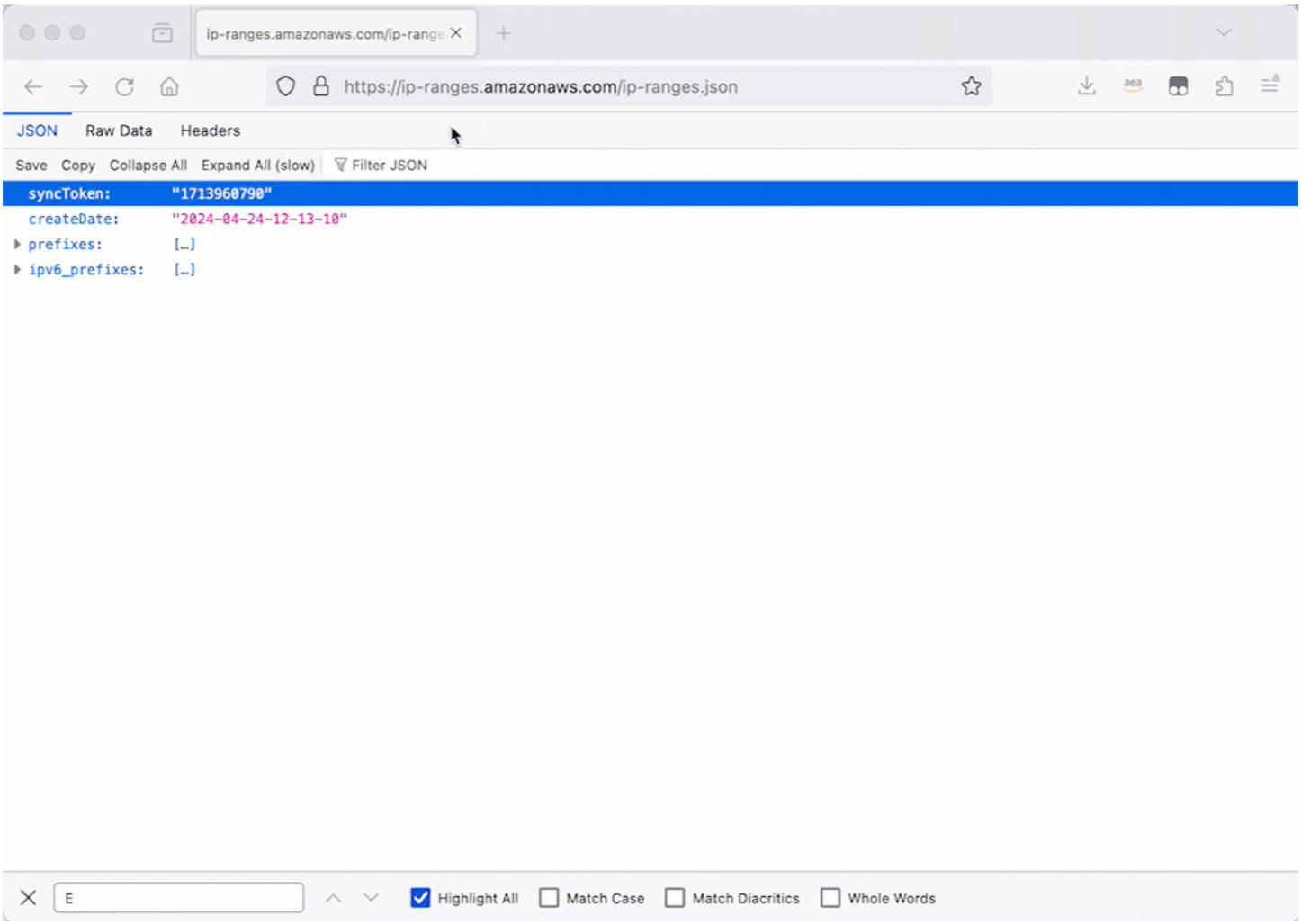
   iii. Lassen Sie für Quelle den Wert Benutzerdefiniert übrig.

   iv. Fügen Sie in das Feld neben Quelle den IP-Adressbereich für den EC2 Instance Connect-Dienst ein, den Sie zuvor in diesem Verfahren kopiert haben.

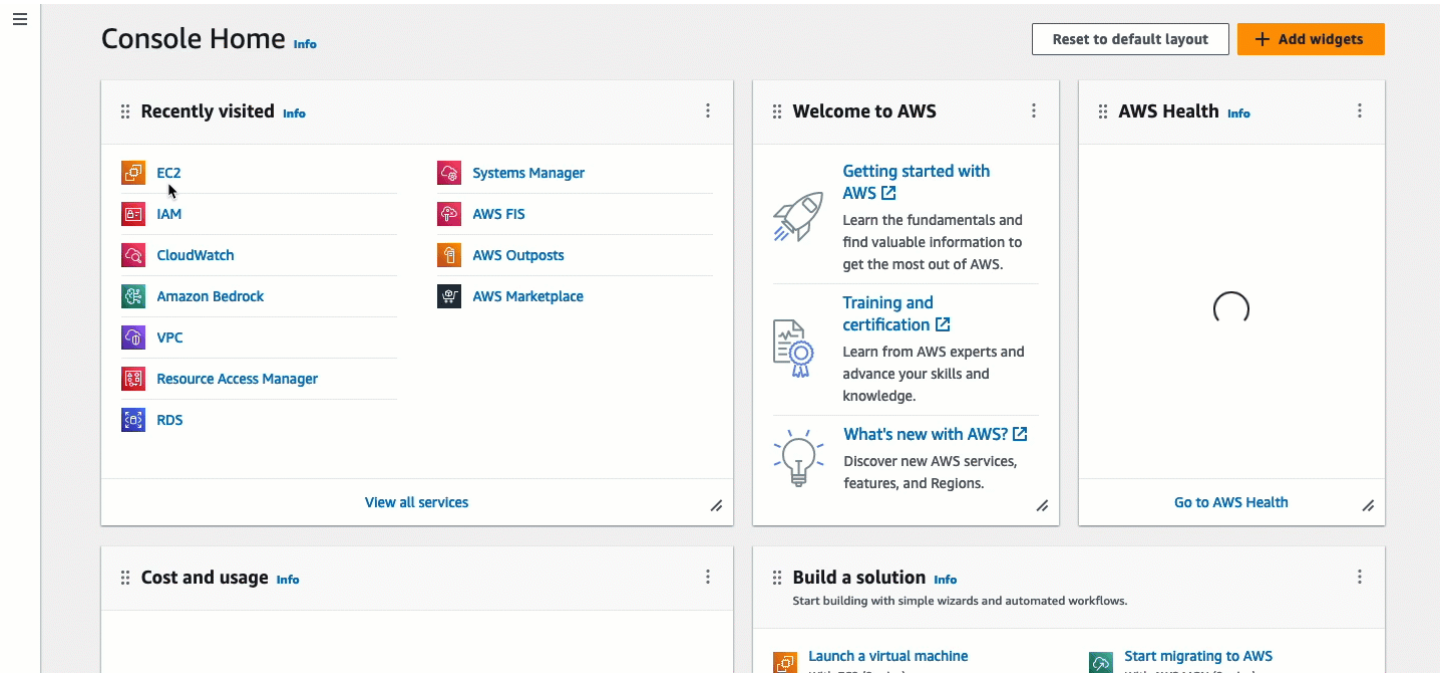
   Wenn sich Ihre Instance beispielsweise in der Region USA Ost (Nord-Virginia) (`us-east-1`) befindet, fügen Sie den folgenden IP-Adressbereich in das Feld ein: `18.206.107.24/29`

f. Wählen Sie Sicherheitsgruppe erstellen aus.

Animation anzeigen: Rufen Sie den IP-Adressbereich für EC2 Instance Connect für eine bestimmte Region ab



Sehen Sie sich eine Animation an: Konfigurieren Sie eine Sicherheitsgruppe



Aufgabe 3: Starten Sie Ihre Instance

Wenn Sie eine Instance starten, müssen Sie ein AMI angeben, das die Informationen enthält, die zum Starten der Instance erforderlich sind. Sie können wählen, ob Sie eine Instance mit oder ohne vorinstalliertes EC2 Instance Connect starten möchten. In dieser Aufgabe geben wir ein AMI an, auf dem EC2 Instance Connect vorinstalliert ist.

Wenn Sie Ihre Instance starten, ohne dass EC2 Instance Connect vorinstalliert ist, und Sie EC2 Instance Connect verwenden möchten, um eine Verbindung zu Ihrer Instance herzustellen, müssen Sie zusätzliche Konfigurationsschritte ausführen. Diese Schritte würden den Rahmen dieses Tutorials sprengen.

Ziel der Aufgabe

In dieser Aufgabe starten Sie eine Instance mit dem Amazon Linux 2023 AMI, auf dem EC2 Instance Connect vorinstalliert ist. Sie geben auch die Sicherheitsgruppe an, die Sie zuvor erstellt haben, sodass Sie EC2 Instance Connect in der Amazon EC2 EC2-Konsole verwenden können, um eine Verbindung zu Ihrer Instance herzustellen. Da Sie EC2 Instance Connect verwenden, um eine Verbindung zu Ihrer Instance herzustellen, wodurch ein öffentlicher Schlüssel an die Metadaten Ihrer Instance weitergegeben wird, müssen Sie beim Starten Ihrer Instance keinen SSH-Schlüssel angeben. Sie müssen jedoch sicherstellen, dass Ihre Instance über eine öffentliche IPv4-Adresse

verfügt, da die Verwendung von EC2 Instance Connect in der Amazon EC2 EC2-Konsole nur Verbindungen zu Instances mit öffentlichen IPv4-Adressen unterstützt.

Schritte zum Starten Ihrer Instance

Gehen Sie wie folgt vor, um Ihre Instance zu starten. Eine Animation der Schritte finden Sie unterAnimation anzeigen: Starten Sie Ihre Instance.

Um eine Instance zu starten, die EC2 Instance Connect in der Amazon EC2 EC2-Konsole für die Verbindung verwenden kann

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. In der Navigationsleiste oben auf dem Bildschirm wird die aktuelle AWS Region angezeigt (z. B. Irland). Wählen Sie eine Region aus, in der Sie Ihre Instance starten möchten. Diese Auswahl ist wichtig, da Sie eine Sicherheitsgruppe erstellt haben, die Traffic für eine bestimmte Region zulässt. Sie müssen also dieselbe Region auswählen, in der Sie Ihre Instance starten möchten.
3. Wählen Sie im Dashboard der Amazon EC2-Konsole die Option Instance starten aus.
4. (Optional) Geben Sie unter Name und Tags für Name einen beschreibenden Namen für Ihre Instance ein.
5. Wählen Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Quick Start aus. Amazon Linux ist standardmäßig ausgewählt. Unter Amazon Machine Image (AMI) ist Amazon Linux 2023 AMI standardmäßig ausgewählt. Behalten Sie die Standardauswahl für diese Aufgabe bei.
6. Behalten Sie unter Instanztyp für Instanztyp die Standardauswahl bei, oder wählen Sie einen anderen Instanztyp.
7. Wählen Sie unter key pair (Anmeldung) für Name des Schlüsselpaars die Option Ohne Schlüsselpaar fortfahren (nicht empfohlen) aus. Wenn Sie EC2 Instance Connect verwenden, um eine Verbindung zu einer Instance herzustellen, überträgt EC2 Instance Connect ein key pair an die Metadaten der Instance, und dieses key pair wird für die Verbindung verwendet.
8. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:

    a. Lassen Sie für Automatische Zuweisung von öffentlichen IP-Adressen die Option Enable stehen.

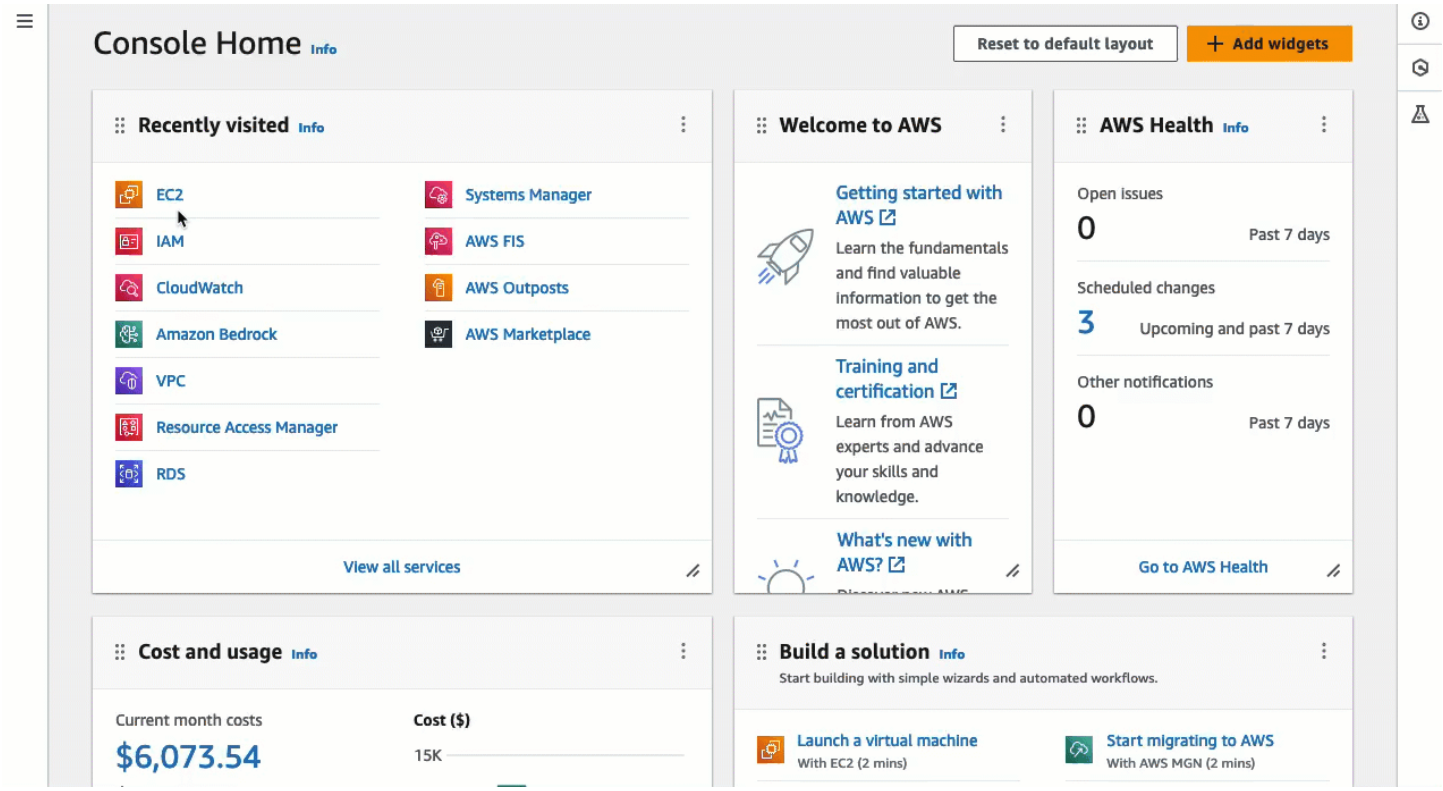
> **Note**
>
> Um EC2 Instance Connect in der Amazon EC2 EC2-Konsole zu verwenden, um eine Verbindung zu einer Instance herzustellen, muss die Instance über eine öffentliche IPv4-Adresse verfügen.

b. Wählen Sie für Firewall (Sicherheitsgruppen) die Option Bestehende Sicherheitsgruppe auswählen aus.

c. Wählen Sie unter Allgemeine Sicherheitsgruppen die Sicherheitsgruppe aus, die Sie zuvor erstellt haben.

9. Wählen Sie in der Übersicht Launch instance (Instance starten) aus.

Animation anzeigen: Starten Sie Ihre Instance



Aufgabe 4: Connect zu Ihrer Instance her

Wenn Sie über EC2 Instance Connect eine Verbindung mit einer Instance herstellen, überträgt die Instance-Connect-API per Push einen öffentlichen SSH-Schlüssel an die Instance-Metadaten, wo er 60 Sekunden verbleibt. Der SSH-Daemon verwendet `AuthorizedKeysCommand`

und`AuthorizedKeysCommandUser`, um den öffentlichen Schlüssel aus den Instanz-Metadaten für die Authentifizierung nachzuschlagen, und verbindet Sie mit der Instance.

Ziel der Aufgabe

In dieser Aufgabe stellen Sie mithilfe von EC2 Instance Connect in der Amazon EC2 EC2-Konsole eine Verbindung zu Ihrer Instance her. Wenn Sie die erforderlichen Aufgaben 1, 2 und 3 abgeschlossen haben, sollte die Verbindung erfolgreich sein.

Schritte zum Herstellen einer Verbindung mit Ihrer Instance

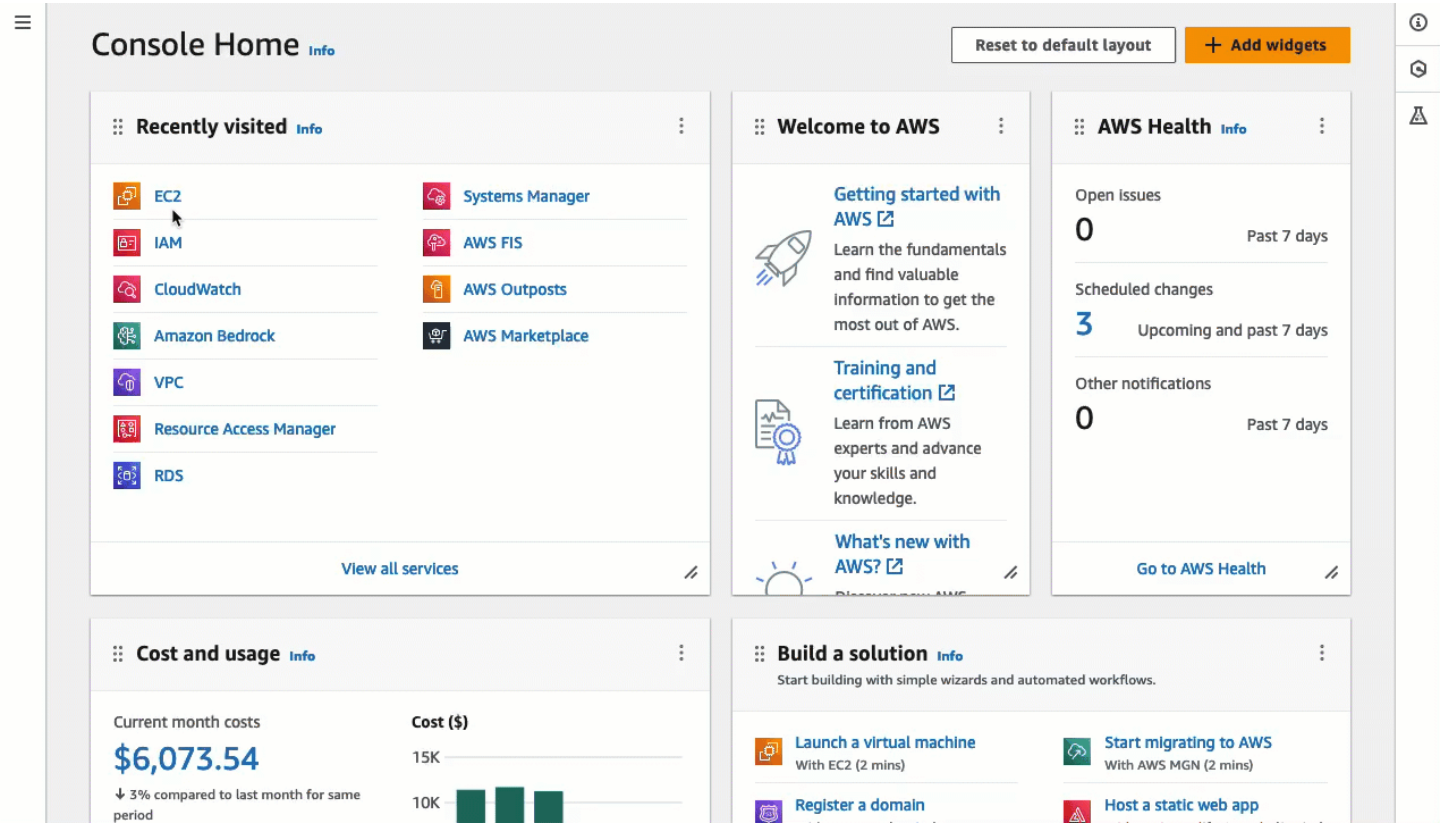
Gehen Sie wie folgt vor, um eine Verbindung zu Ihrer Instance herzustellen. Eine Animation der Schritte finden Sie unterEine Animation ansehen: Connect zu Ihrer Instance her.

So verbinden Sie eine Instance mithilfe von EC2 Instance Connect in der Amazon EC2 EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. In der Navigationsleiste oben auf dem Bildschirm wird die aktuelle AWS Region angezeigt (z. B. Irland). Wählen Sie die Region aus, in der sich Ihre Instance befindet.
3. Wählen Sie im Navigationsbereich Instances aus.
4. Wählen Sie Ihre Instance aus und wählen Sie Connect.
5. Wählen Sie die Registerkarte EC2 Instance Connect aus.
6. Wählen Sie als Verbindungstyp Connect using EC2 Instance Connect aus.
7. Wählen Sie Connect aus.

   Im Browser wird ein Terminalfenster geöffnet, und Sie sind mit Ihrer Instance verbunden.

Eine Animation ansehen: Connect zu Ihrer Instance her



Voraussetzungen

Im Folgenden sind die Voraussetzungen für die Installation von EC2 Instance Connect und für die Verwendung von EC2 Instance Connect zur Verbindung mit einer Instance aufgeführt:

- AWS-Regionen
- Local Zones
- AMIs
- EC2 Instance Connect installieren
- IPv4 address (IPv4-Adresse)
- Netzwerkzugriff
- Sicherheitsgruppenregel
- Erteilen Sie Berechtigungen
- Einrichtung des lokalen Computers
- Username

AWS-Regionen

Wird in allen Ländern AWS-Regionen außer Canada West (Calgary) unterstützt.

Local Zones

Nicht unterstützt

AMIs

EC2 Instance Connect ist auf den folgenden AMIs vorinstalliert:

- AL2023
- Amazon Linux 2 2.0.20190618 oder höher
- macOS Sonoma 14.2.1 oder höher
- macOS Ventura 13.6.3 oder höher
- macOS Monterey 12.7.2 oder höher
- Ubuntu 20.04 oder höher

EC2 Instance Connect ist auf den folgenden AMIs nicht vorinstalliert, aber Sie können es auf Instances installieren, die mit den folgenden AMIs gestartet werden:

- Amazon Linux 2 vor Version 2.0.20190618
- CentOS Stream 8 und 9
- macOS Sonoma vor 14.2.1, Ventura vor 13.6.3 und Monterey vor 12.7.2
- Red Hat Enterprise Linux (RHEL) 8 und 9
- Ubuntu 16.04 oder 18.04

EC2 Instance Connect installieren

Um EC2 Instance Connect zum Herstellen einer Verbindung mit einer Instance zu verwenden, muss EC2 Instance Connect installiert sein. Sie können die Instance entweder mit einem AMI starten, das mit EC2 Instance Connect vorinstalliert ist, oder Sie können EC2 Instance Connect auf Instances installieren, die mit unterstützten AMIs gestartet wurden. Informationen zu den unterstützten AMIs finden Sie im vorangegangenen Abschnitt. Installationsanweisungen finden Sie unter Installieren Sie EC2 Instance Connect auf Ihren Instances.

IPv4 address (IPv4-Adresse)

Ihre Instance muss eine IPv4-Adresse haben (entweder privat oder öffentlich). EC2 Instance Connect unterstützt keine Verbindung über eine IPv6-Adresse.

Netzwerkzugriff

Instances können so konfiguriert werden, dass Benutzer über das Internet oder über die private IP-Adresse der Instance eine Verbindung zu Ihrer Instance herstellen können. Je nachdem, wie sich Ihre Benutzer über EC2 Instance Connect mit Ihrer Instance verbinden werden, müssen Sie den folgenden Netzwerkzugang konfigurieren:

- Wenn sich Ihre Benutzer über das Internet mit Ihrer Instance verbinden, muss Ihre Instance eine öffentliche IP-Adresse haben und sich in einem öffentlichen Subnetz befinden. Weitere Informationen finden Sie unter Internetzugang aktivieren im Amazon VPC Benutzerhandbuch.
- Wenn Ihre Benutzer über die private IP-Adresse der Instance eine Verbindung zu Ihrer Instance herstellen, müssen Sie eine private Netzwerkkonnektivität zu Ihrer VPC einrichten, z. B. mithilfe von AWS Direct Connect AWS Site-to-Site VPN, oder VPC-Peering, damit Ihre Benutzer die private IP-Adresse der Instance erreichen können.

Wenn Ihre Instance über keine öffentliche IPv4-Adresse verfügt und Sie den Netzwerkzugriff nicht wie oben beschrieben konfigurieren möchten, können Sie den EC2-Instance-Connect-Endpunkt als Alternative zu EC2 Instance Connect in Betracht ziehen. Mit dem EC2-Instance-Connect-Endpunkt können Sie eine Verbindung zu einer Instance über SSH oder RDP herstellen, ohne dass die Instance eine öffentliche IPv4-Adresse haben muss. Weitere Informationen finden Sie unter Verbinden Sie sich mit Ihrer Linux-Instance über die Amazon-EC2-Konsole.

Sicherheitsgruppenregel

Stellen Sie sicher, dass die Ihrer Instance zugeordnete Sicherheitsgruppe eingehenden SSH-Verkehr auf Port 22 von Ihrer IP-Adresse oder Ihres Netzwerks aus zulässt. Die standardmäßige Sicherheitsgruppe für die VPC lässt keinen eingehenden SSH-Datenverkehr zu. Die über den Launch Instance Wizard erstellte Sicherheitsgruppe lässt eingehenden SSH-Datenverkehr standardmäßig zu. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.

EC2 Instance Connect verwendet bestimmte IP-Adressbereiche für browserbasierte SSH-Verbindungen zu Ihrer Instance (wenn Benutzer die Amazon-EC2-Konsole verwenden, um eine Verbindung zur Instance herzustellen). Wenn Ihre Benutzer die Amazon EC2-Konsole

verwenden, um sich mit einer Instance zu verbinden, stellen Sie sicher, dass die mit Ihrer Instance verbundene Sicherheitsgruppe eingehenden SSH-Verkehr aus dem IP-Adressbereich für `EC2_INSTANCE_CONNECT` erlaubt. Um den Adressbereich zu identifizieren, laden Sie die von bereitgestellte JSON-Datei herunter AWS und filtern Sie nach der Teilmenge für EC2 Instance Connect, die Sie `EC2_INSTANCE_CONNECT` als Dienstwert verwenden. Diese IP-Adressbereiche unterscheiden sich zwischen. AWS-Regionen Weitere Informationen zum Herunterladen der JSON-Datei und zum Filtern nach Services finden Sie unter AWS -IP-Adressbereiche im Benutzerhandbuch für Amazon VPC.

Erteilen Sie Berechtigungen

Sie müssen jedem IAM-Benutzer, der EC2 Instance Connect verwendet, um eine Verbindung zu einer Instance herzustellen, die erforderlichen Berechtigungen gewähren. Weitere Informationen finden Sie unter Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect.

Einrichtung des lokalen Computers

Wenn Ihre Benutzer eine Verbindung über SSH herstellen, müssen sie sicherstellen, dass ihr lokaler Computer über einen SSH-Client verfügt.

Auf Ihrem lokalen Computer ist höchstwahrscheinlich standardmäßig ein SSH-Client installiert. Sie können nach einem SSH-Client suchen, indem Sie in der Befehlszeile ssh eingeben. Wenn ihr lokaler Computer den Befehl nicht erkennt, können sie einen SSH-Client installieren. Weitere Informationen zum Installieren eines SSH-Client unter Linux oder macOS X finden Sie unter http://www.openssh.com. Weitere Informationen zur Installation eines SSH-Clients unter Windows 10 finden Sie unter OpenSSH unter Windows.

Ein SSH-Client muss nicht installiert werden, wenn Benutzer nur die Amazon-EC2-Konsole verwenden, um eine Verbindung zu einer Instance herzustellen.

Username

Wenn Sie EC2 Instance Connect verwenden, um eine Verbindung zu einer Instance herzustellen, muss der Benutzername die folgenden Voraussetzungen erfüllen:

- Erstes Zeichen: Muss ein Buchstabe (`A-Z`,`a-z`), eine Ziffer (`0-9`) oder ein Unterstrich (`_`) sein
- Nachfolgende Zeichen: Dabei kann es sich um Buchstaben (`A-Z`, `a-z`), Ziffern (`0-9`) oder die folgenden Zeichen handeln: `@ . _ -`
- Mindestlänge: 1 Zeichen.
- Maximale Länge: 31 Zeichen.

Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect

Um über EC2 Instance Connect eine Verbindung mit einer Instance herzustellen, müssen Sie eine IAM-Richtlinie erstellen, die Ihren Benutzern Berechtigungen für die folgenden Aktionen und Bedingungen erteilt:

- `ec2-instance-connect:SendSSHPublicKey`-Aktion – Erteilt einem -Benutzer die Berechtigung, den öffentlichen Schlüssel per Push zu einer Instance zu übertragen.
- `ec2:osuser`-Bedingung – Gibt den Namen des Betriebssystembenutzers an, der den öffentlichen Schlüssel per Push an die Instance übertragen kann. Verwenden Sie den Standardbenutzernamen für das AMI, mit dem Sie die Instance gestartet haben. Der Standardbenutzername für AL2023 und Amazon Linux 2 ist`ec2-user`, und für Ubuntu ist es`ubuntu`.
- `ec2:DescribeInstances`-Aktion – Erforderlich, wenn die EC2-Konsole verwendet wird, da der Wrapper diese Aktion aufruft. Benutzer besitzen möglicherweise bereits die Berechtigung zum Aufruf dieser Aktion in einer anderen Richtlinie.

Ziehen Sie die Einschränkung des Zugriffs auf bestimmte EC2-Instances in Betracht. Andernfalls können alle IAM-Prinzipale mit der Berechtigung für die `ec2-instance-connect:SendSSHPublicKey`-Aktion Verbindungen zu allen EC2-Instances herstellen. Sie können den Zugriff auch einschränken, indem Sie Ressourcen-ARNs angeben oder Ressourcen-Tags als Bedingungsschlüssel verwenden.

Weitere Informationen finden Sie im Abschnitt Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 Instance Connect.

Informationen zum Erstellen und Bearbeiten von IAM-Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Erlauben Sie Benutzern die Verbindung zu bestimmten Instances

Die folgende IAM-Richtlinie gewährt die Berechtigung, eine Verbindung zu bestimmten Instances herzustellen, die anhand ihrer Ressourcen-ARNs identifiziert werden.

In der folgenden Beispiel-IAM-Richtlinie werden die folgenden Aktionen und Bedingungen angegeben:

- Die `ec2-instance-connect:SendSSHPublicKey`-Aktion gewährt Benutzern die Berechtigung, eine Verbindung zu zwei Instances herzustellen, die durch die Ressourcen-ARNs angegeben

werden. Um Benutzern die Berechtigung zu gewähren, eine Verbindung zu allen EC2-Instances herzustellen, ersetzen Sie die Ressourcen-ARNs durch den *-Platzhalter.

- Die `ec2:osuser`-Bedingung gewährt nur dann die Berechtigung, eine Verbindung zu den Instances herzustellen, wenn der *`ami-username`* beim Herstellen der Verbindung angegeben wird.
- Die Aktion `ec2:DescribeInstances` wird angegeben, um Benutzern, die sich über die Konsole mit Ihren Instances verbinden wollen, eine Berechtigung zu erteilen. Sie können `ec2:DescribeInstances` auslassen, wenn Ihre Benutzer ausschließlich einen SSH-Client zum Herstellen von Verbindungen mit Ihren Instances verwenden. Beachten Sie, dass die `ec2:Describe*`-API-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "ec2-instance-connect:SendSSHPublicKey",
   "Resource": [
    "arn:aws:ec2:region:account-id:instance/i-1234567890abcdef0",
    "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
   ],
   "Condition": {
    "StringEquals": {
     "ec2:osuser": "ami-username"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeInstances",
   "Resource": "*"
  }
 ]
}
```

Erlauben Sie Benutzern die Verbindung zu Instances mit bestimmten Tags

Die attributebasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, die Berechtigungen auf der Grundlage von Tags definiert, die Benutzern und Ressourcen zugewiesen werden können.

AWS Sie können Ressourcen-Tags verwenden, um den Zugriff auf eine Instance zu steuern. Weitere Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf Ihre AWS Ressourcen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen im IAM-Benutzerhandbuch.

In der folgenden Beispiel-IAM-Richtlinie gewährt die `ec2-instance-connect:SendSSHPublicKey`-Aktion Benutzern die Berechtigung, eine Verbindung zu einer beliebigen Instance herzustellen (gekennzeichnet durch den *-Platzhalter im Ressourcen-ARN), sofern die Instance über ein Ressourcen-Tag mit key=`tag-key` und value=`tag-value` verfügt.

Die Aktion `ec2:DescribeInstances` wird angegeben, um Benutzern, die sich über die Konsole mit Ihren Instances verbinden wollen, eine Berechtigung zu erteilen. Sie können `ec2:DescribeInstances` auslassen, wenn Ihre Benutzer ausschließlich einen SSH-Client zum Herstellen von Verbindungen mit Ihren Instances verwenden. Beachten Sie, dass die `ec2:Describe*`-API-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich.

```
{
 "Version": "2012-10-17",
 "Statement": [{
   "Effect": "Allow",
   "Action": "ec2-instance-connect:SendSSHPublicKey",
   "Resource": "arn:aws:ec2:region:account-id:instance/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceTag/tag-key": "tag-value"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": "ec2:DescribeInstances",
   "Resource": "*"
  }
 ]
}
```

Installieren Sie EC2 Instance Connect auf Ihren Instances

Um EC2 Instance Connect zum Herstellen einer Verbindung mit einer Instance zu verwenden, muss in der Instance EC2 Instance Connect installiert sein.

Die folgenden AMIs sind mit EC2 Instance Connect vorinstalliert:

- AL2023 Standard-AMI
- Amazon Linux 2 2.0.20190618 oder höher
- macOS Sonoma 14.2.1 oder höher
- macOS Ventura 13.6.3 oder höher
- macOS Monterey 12.7.2 oder höher
- Ubuntu 20.04 oder höher

Wenn Sie Ihre Instance mit einem der AMIs in der Liste gestartet haben, können Sie dieses Verfahren überspringen.

> **Note**
>
> Wenn Sie die Einstellungen `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` für die SSH-Authentifizierung konfiguriert haben, aktualisiert die EC2 Instance Connect-Installation diese nicht. Daher können Sie EC2 Instance Connect nicht verwenden.

Voraussetzungen für die Installation von EC2 Instance Connect

- Starten Sie die Instance mit einem der folgenden unterstützten AMIs:

  Amazon Linux 2 vor Version 2.0.20190618

  AL2023 minimales AMI oder Amazon ECS-optimiertes AMI

  CentOS Stream 8 und 9

  macOS Sonoma vor 14.2.1, Ventura vor 13.6.3 und Monterey vor 12.7.2

  Red Hat Enterprise Linux (RHEL) 8 und 9

  Ubuntu 16.04 und 18.04

  Wenn Ihre Instance mit einer späteren Version von Amazon Linux 2, macOS Sonoma, Ventura oder Monterey oder Ubuntu gestartet wurde, ist EC2 Instance Connect vorinstalliert und Sie können dieses Verfahren überspringen.
- Überprüfen Sie die allgemeinen Voraussetzungen für das EC2 Instance Connect.

Weitere Informationen finden Sie unter Voraussetzungen.

- Überprüfen Sie die Voraussetzungen für die Verbindung zu Ihrer Instance mithilfe eines SSH-Clients auf Ihrem lokalen Rechner.

  Wenn es sich bei Ihrem lokalen Rechner um Linux oder macOS handelt, lesen Sie Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH. Wenn es sich bei Ihrem lokalen Rechner um Windows handelt, lesen Sie Voraussetzungen.

  Weitere Informationen finden Sie unter Voraussetzungen für eine SSH-Verbindung.

- Rufen Sie die ID der Instance ab.

  Sie können die ID Ihrer Instance über die Amazon EC2 Konsole (imInstance-ID-Spalte). Wenn Sie möchten, können Sie den Befehl describe-instances () oder ()AWS CLI verwenden. Get-EC2InstanceAWS Tools for Windows PowerShell

- Installieren Sie einen SSH-Client auf Ihrem lokalen Computer.

  Auf Ihrem lokalen Computer ist wahrscheinlich standardmäßig ein SSH-Client installiert. Sie können nach einem SSH-Client suchen, indem Sie in der Befehlszeile ssh eingeben. Wenn Ihr lokaler Computer den Befehl nicht erkennt, können Sie einen SSH-Client installieren. Weitere Informationen zum Installieren eines SSH-Client unter Linux oder macOS X finden Sie unter http://www.openssh.com. Weitere Informationen zur Installation eines SSH-Clients unter Windows 10 finden Sie unter OpenSSH unter Windows.

- (Ubuntu) Installieren Sie den AWS CLI auf Ihrer Instanz.

  Um EC2 Instance Connect auf einer Ubuntu-Instance zu installieren, müssen Sie den AWS CLI auf der Instance verwenden. Weitere Informationen zur Installation von finden Sie unter Installation von AWS CLI im AWS Command Line Interface Benutzerhandbuch. AWS CLI

EC2 Instance Connect installieren

Durch die Installation von EC2 Instance Connect wird der SSH-Daemon auf der Instance konfiguriert.

Verwenden Sie je nach Betriebssystem Ihrer Instance eines der folgenden Verfahren zur Installation von EC2 Instance Connect.

Amazon Linux 2

So installieren Sie EC2 Instance Connect auf einer Instance, die mit Amazon Linux 2 gestartet wurde

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Verwenden Sie das SSH-Schlüsselpaar, das Ihrer Instance beim Start zugewiesen wurde, und den Standardbenutzernamen des AMI, das Sie zum Starten Ihrer Instance verwendet haben. Für Amazon Linux 2 lautet der Standardbenutzername`ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH.

2. Installieren Sie das EC2 Instance Connect-Paket auf Ihrer Instance.

   ```
   [ec2-user ~]$ sudo yum install ec2-instance-connect
   ```

   Im Ordner `/opt/aws/bin/` sollten drei neue Skripts angezeigt werden:

   ```
   eic_curl_authorized_keys
   eic_parse_authorized_keys
   eic_run_authorized_keys
   ```

3. (Optional) Überprüfen Sie, ob EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

   ```
   [ec2-user ~]$ sudo less /etc/ssh/sshd_config
   ```

   EC2 Instance Connect wurde erfolgreich installiert, wenn die Zeilen `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` die folgenden Werte enthalten:

   ```
   AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
   ```

```
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.
- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie zuvor `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` konfiguriert haben, werden durch die Installation von EC2 Instance Connect die Werte nicht geändert und Sie können EC2 Instance Connect nicht verwenden.

CentOS

So installieren Sie EC2 Instance Connect auf einer Instance, die mit CentOS gestartet wurde

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Verwenden Sie das SSH-Schlüsselpaar, das Ihrer Instance beim Start zugewiesen wurde, und den Standardbenutzernamen des AMI, das Sie zum Starten Ihrer Instance verwendet haben. Für CentOS ist der Standardbenutzername `centos` oder`ec2-user`.

   ```
   $ ssh -i my_ec2_private_key.pem centos@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH.

2. Wenn Sie einen HTTP- oder HTTPS-Proxy verwenden, müssen Sie die `http_proxy` oder `https_proxy`-Umgebungsvariablen in der aktuellen Shell-Sitzung einstellen.

   Wenn Sie keinen Proxy verwenden, können Sie diesen Schritt überspringen.

   - Führen Sie für einen HTTP-Proxy-Server die folgenden Befehle aus:

```
$ export http_proxy=http://hostname:port
$ export https_proxy=http://hostname:port
```

- Führen Sie für einen HTTPS-Proxy-Server die folgenden Befehle aus:

```
$ export http_proxy=https://hostname:port
$ export https_proxy=https://hostname:port
```

3. Installieren Sie das EC2-Instance-Connect-Paket auf Ihrer Instance, indem Sie die folgenden Befehle ausführen.

   Die EC2-Instance-Connect-Konfigurationsdateien für CentOS werden in einem Red Hat Package Manager (RPM)-Paket mit unterschiedlichen RPM-Paketen für CentOS 8 und CentOS 9 sowie Instance-Typen bereitgestellt, die in Intel/AMD (x86_64) oder ARM (AArch64) ausgeführt werden.

   Verwenden Sie den Befehlsblock für Ihr Betriebssystem und Ihre CPU-Architektur.

   - CentOS 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /
     tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
     selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

     ARM (AArch64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /
     tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     ```

```
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- CentOS 9

  Intel/AMD (x86_64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
  instance-connect/ec2-instance-connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

  ARM (AArch64)

  ```
  [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-
  instance-connect/ec2-instance-connect.rpm
  [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
  west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
  selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
  selinux.rpm
  [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
  connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
  ```

Sie sollten das folgende neue Skript im Ordner `/opt/aws/bin/` sehen:

```
eic_run_authorized_keys
```

4. (Optional) Überprüfen Sie, ob EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

   - Für CentOS 8:

```
[ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

- Für CentOS 9:

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect wurde erfolgreich installiert, wenn die Zeilen `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` die folgenden Werte enthalten:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.
- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie zuvor `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` konfiguriert haben, werden durch die Installation von EC2 Instance Connect die Werte nicht geändert und Sie können EC2 Instance Connect nicht verwenden.

macOS

So installieren Sie EC2 Instance Connect auf einer Instance, die mit macOS gestartet wurde

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Verwenden Sie das SSH-Schlüsselpaar, das Ihrer Instance beim Start zugewiesen wurde, und den Standardbenutzernamen des AMI, das Sie zum Starten Ihrer Instance verwendet haben. Für macOS-Instanzen lautet der Standardbenutzernameec2-user.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH.

2. Aktualisieren Sie Homebrew mit dem folgenden Befehl. Das Update wird die Software auflisten, die Homebrew kennt. Das EC2 Instance Connect-Paket wird über Homebrew auf macOS-Instances bereitgestellt. Weitere Informationen finden Sie unter Aktualisieren Sie das Betriebssystem und die Software auf Mac-Instanzen.

```
[ec2-user ~]$ brew update
```

3. Installieren Sie das EC2 Instance Connect-Paket auf Ihrer Instance. Dadurch wird die Software installiert und sshd für die Verwendung konfiguriert.

```
[ec2-user ~]$ brew install ec2-instance-connect
```

Sie sollten das folgende neue Skript im Ordner `/opt/aws/bin/` sehen:

```
eic_run_authorized_keys
```

4. (Optional) Überprüfen Sie, ob EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect wurde erfolgreich installiert, wenn die Zeilen `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` die folgenden Werte enthalten:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.

- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie zuvor `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` konfiguriert haben, werden durch die Installation von EC2 Instance Connect die Werte nicht geändert und Sie können EC2 Instance Connect nicht verwenden.

RHEL

So installieren Sie EC2 Instance Connect auf einer Instance, die mit Red Hat Enterprise Linux (RHEL) gestartet wurde

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Verwenden Sie das SSH-Schlüsselpaar, das Ihrer Instance beim Start zugewiesen wurde, und den Standardbenutzernamen des AMI, das Sie zum Starten Ihrer Instance verwendet haben. Für RHEL lautet der Standardbenutzername oder. `ec2-user` `root`

   ```
   $ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
   west-2.compute.amazonaws.com
   ```

   Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH.

2. Wenn Sie einen HTTP- oder HTTPS-Proxy verwenden, müssen Sie die `http_proxy` oder `https_proxy`-Umgebungsvariablen in der aktuellen Shell-Sitzung einstellen.

   Wenn Sie keinen Proxy verwenden, können Sie diesen Schritt überspringen.

   - Führen Sie für einen HTTP-Proxy-Server die folgenden Befehle aus:

     ```
     $ export http_proxy=http://hostname:port
     $ export https_proxy=http://hostname:port
     ```

- Führen Sie für einen HTTPS-Proxy-Server die folgenden Befehle aus:

```
$ export http_proxy=https://hostname:port
$ export https_proxy=https://hostname:port
```

3. Installieren Sie das EC2-Instance-Connect-Paket auf Ihrer Instance, indem Sie die folgenden Befehle ausführen.

   Die EC2-Instance-Connect-Konfigurationsdateien für RHEL werden in einem Red Hat Package Manager (RPM)-Paket mit unterschiedlichen RPM-Paketen für RHEL 8 und RHEL 9 sowie Instance-Typen bereitgestellt, die in Intel/AMD (x86_64) oder ARM (AArch64) ausgeführt werden.

   Verwenden Sie den Befehlsblock für Ihr Betriebssystem und Ihre CPU-Architektur.

   - RHEL 8

     Intel/AMD (x86_64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rhel8.rpm -o /
     tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
     selinux.rpm
     [ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
     connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
     ```

     ARM (AArch64)

     ```
     [ec2-user ~]$ mkdir /tmp/ec2-instance-connect
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rhel8.rpm -o /
     tmp/ec2-instance-connect/ec2-instance-connect.rpm
     [ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
     west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
     selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
     selinux.rpm
     ```

```
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

- RHEL 9

  Intel/AMD (x86_64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

  ARM (AArch64)

```
[ec2-user ~]$ mkdir /tmp/ec2-instance-connect
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_arm64/ec2-instance-connect.rpm -o /tmp/ec2-
instance-connect/ec2-instance-connect.rpm
[ec2-user ~]$ curl https://amazon-ec2-instance-connect-us-west-2.s3.us-
west-2.amazonaws.com/latest/linux_amd64/ec2-instance-connect-
selinux.noarch.rpm -o /tmp/ec2-instance-connect/ec2-instance-connect-
selinux.rpm
[ec2-user ~]$ sudo yum install -y /tmp/ec2-instance-connect/ec2-instance-
connect.rpm /tmp/ec2-instance-connect/ec2-instance-connect-selinux.rpm
```

Sie sollten das folgende neue Skript im Ordner `/opt/aws/bin/` sehen:

```
eic_run_authorized_keys
```

4. (Optional) Überprüfen Sie, ob EC2 Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

   - Für RHEL 8:

```
[ec2-user ~]$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
```

- Für RHEL 9:

```
[ec2-user ~]$ sudo less /etc/ssh/sshd_config.d/60-ec2-instance-connect.conf
```

EC2 Instance Connect wurde erfolgreich installiert, wenn die Zeilen `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` die folgenden Werte enthalten:

```
AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys %u %f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.
- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie zuvor `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` konfiguriert haben, werden durch die Installation von EC2 Instance Connect die Werte nicht geändert und Sie können EC2 Instance Connect nicht verwenden.

Ubuntu

So installieren Sie EC2 Instance Connect auf einer Instance, die mit Ubuntu 16.04 oder höher gestartet wurde

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her.

   Ersetzen Sie die Beispielwerte im folgenden Befehl durch Ihre Werte. Verwenden Sie das SSH-Schlüsselpaar, das Ihrer Instance beim Start zugewiesen wurde, und verwenden Sie

den Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Für ein Ubuntu-AMI lautet der Benutzernameubuntu.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH.

2. (Optional) Stellen Sie sicher, dass Ihre Instance über das neueste Ubuntu-AMI verfügt.

   Führen Sie die folgenden Befehle aus, um alle Pakete auf Ihrer Instance zu aktualisieren.

   ```
   ubuntu:~$ sudo apt-get update
   ```

   ```
   ubuntu:~$ sudo apt-get upgrade
   ```

3. Installieren Sie das EC2 Instance Connect-Paket auf Ihrer Instance.

   ```
   ubuntu:~$ sudo apt-get install ec2-instance-connect
   ```

   Im Ordner `/usr/share/ec2-instance-connect/` sollten drei neue Skripts angezeigt werden:

   ```
   eic_curl_authorized_keys
   eic_parse_authorized_keys
   eic_run_authorized_keys
   ```

4. (Optional) Überprüfen Sie, ob Instance Connect erfolgreich auf Ihrer Instance installiert wurde.

   ```
   ubuntu:~$ sudo less /lib/systemd/system/ssh.service.d/ec2-instance-connect.conf
   ```

   EC2 Instance Connect wurde erfolgreich installiert, wenn die Zeilen `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` die folgenden Werte enthalten:

```
AuthorizedKeysCommand /usr/share/ec2-instance-connect/eic_run_authorized_keys %
%u %%f
AuthorizedKeysCommandUser ec2-instance-connect
```

- `AuthorizedKeysCommand` sorgt dafür, dass das Skript `eic_run_authorized_keys` die Schlüssel aus den Instance-Metadaten liest.
- `AuthorizedKeysCommandUser` legt den Systembenutzer als `ec2-instance-connect` fest.

> **Note**
>
> Wenn Sie zuvor `AuthorizedKeysCommand` und `AuthorizedKeysCommandUser` konfiguriert haben, werden durch die Installation von EC2 Instance Connect die Werte nicht geändert und Sie können EC2 Instance Connect nicht verwenden.

Weitere Informationen zum EC2 Instance Connect-Paket finden Sie unter aws/aws-ec2 - auf der Website. instance-connect-config GitHub

Verbindung über EC2 Instance Connect

Im Folgenden wird beschrieben, wie Sie über EC2 Instance Connect Verbindungen mit Ihrer Linux-Instance herstellen.

Entscheiden Sie, welche Verbindungsoption Sie verwenden möchten.Welche Verbindungsoption verwendet werden soll, hängt davon ab, ob Ihre Instance über eine öffentliche IPv4-Adresse verfügt:

- Amazon-EC2-Konsole – Um eine Verbindung über die Amazon-EC2-Konsole herzustellen, muss die Instance über eine öffentliche IPv4-Adresse verfügen.
- SSH-Client – Wenn die Instance keine öffentliche IP-Adresse hat, können Sie eine Verbindung über ein privates Netzwerk mithilfe eines SSH-Clients herstellen. Beispielsweise können Sie eine Verbindung innerhalb derselben VPC oder über eine VPN-Verbindung, ein Transit-Gateway oder AWS Direct Connect herstellen.

EC2 Instance Connect unterstützt keine Verbindung über eine IPv6-Adresse.

> **Tip**
>
> EC2 Instance Connect ist eine der Optionen, mit denen Sie eine Verbindung zu Ihrer Linux-Instance herstellen können. Weitere Optionen finden Sie unter Herstellen einer Verbindung zur Linux-Instance. Informationen zum Herstellen einer Verbindung mit einer Windows-Instance finden Sie unter. Herstellen einer Verbindung mit Ihrer -Windows-Instance

Verbindungsoptionen für EC2 Instance Connect

- Herstellen von Verbindungen über die Amazon-EC2-Konsole
- Herstellen von Verbindungen über Ihren eigenen Schlüssel und einen SSH-Client
- Connect mit dem her AWS CLI
- Fehlerbehebung

Herstellen von Verbindungen über die Amazon-EC2-Konsole

Sie können über die Amazon-EC2-Konsole Verbindungen mit einer Instance herstellen, indem Sie die Instance in der Konsole auswählen und die Verbindung über EC2 Instance Connect wählen. Instance Connect verarbeitet die Berechtigungen und stellt eine erfolgreiche Verbindung bereit.

Um eine Verbindung über die Amazon-EC2-Konsole herzustellen, muss die Instance über eine öffentliche IPv4-Adresse verfügen. Bevor Sie eine Verbindung herstellen, sollten Sie alle Voraussetzungen überprüfen.

So stellen Sie über den browserbasierten Client und die Amazon EC2-Konsole Verbindungen mit Ihrer Instance her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und Connect (Verbinden) aus.
4. Wählen Sie die Registerkarte EC2 Instance Connect aus.
5. Wählen Sie als Verbindungstyp Connect using EC2 Instance Connect aus.
6. Überprüfen Sie den Benutzernamen für den Benutzernamen.
7. Wählen Sie Verbinden aus, um ein Terminalfenster zu öffnen.

Herstellen von Verbindungen über Ihren eigenen Schlüssel und einen SSH-Client

Sie können mittels Ihres eigenen SSH-Schlüssels über einen SSH-Client Ihrer Wahl Verbindungen mit Ihrer Instance herstellen, während Sie die EC2 Instance Connect-API verwenden. Auf diese Weise können Sie die Instance Connect-Funktion für die Push-Übergabe öffentlicher Schlüssel an Instances nutzen. Diese Verbindungsmethode funktioniert für Instances mit öffentlichen und privaten IP-Adressen.

Voraussetzungen

- Anforderungen für Schlüsselpaare
  - Unterstützte Typen: RSA (OpenSSH und SSH2) und ED25519
  - Die unterstützten Längen sind 2048 und 4096.
  - Weitere Informationen finden Sie unter Erstellen Sie ein Schlüsselpaar mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel in Amazon EC2.
- Wenn Sie eine Verbindung zu einer Instance herstellen, die nur über private IP-Adressen verfügt, muss der lokale Computer, von dem aus Sie die SSH-Sitzung initiieren, Konnektivität zum EC2 Instance Connect-Service-Endpunkt (um Ihren öffentlichen SSH-Schlüssel auf die Instance zu übertragen) sowie über Netzwerkkonnektivität zur privaten IP-Adresse der Instance verfügen, um eine SSH-Sitzung zu etablieren. Der EC2-Instance-Connect-Service-Endpunkt ist über das Internet oder über eine öffentliche virtuelle AWS Direct Connect -Schnittstelle erreichbar. Um eine Verbindung mit der privaten IP-Adresse der Instance herzustellen, können Sie Dienste wie AWS Direct Connect, AWS Site-to-Site VPN oder VPC-Peering nutzen.

Bevor Sie eine Verbindung herstellen, sollten Sie alle Voraussetzungen überprüfen.

So stellen Sie eine Verbindung zu Ihrer Instance mit einem eigenen Schlüssel und einem beliebigen SSH-Client her

1. (Optional) Generieren neuer privater und öffentlicher SSH-Schlüssel.

   Sie können mit dem folgenden Befehl neue private und öffentliche SSH-Schlüssel, `my_key` und `my_key.pub`, erstellen:

   ```
   ssh-keygen -t rsa -f my_key
   ```

2. Übertragen Ihres öffentlichen SSH-Schlüssels per Push an die Instance.

   Verwenden Sie den send-ssh-public-key-Befehl, um Ihren öffentlichen SSH-Schlüssel an die Instance zu übertragen. Wenn Sie Ihre Instance mit AL2023 oder Amazon Linux 2 gestartet haben, lautet der Standardbenutzername für das AMI. `ec2-user` Wenn Sie Ihre Instance mit Ubuntu gestartet haben, lautet der Standardbenutzername für das AMI`ubuntu`.

   Im folgenden Beispiel wird der öffentliche Schlüssel per Push an die angegebene Instance in der angegebenen Availability Zone übertragen, um `ec2-user` zu authentifizieren.

   ```
   aws ec2-instance-connect send-ssh-public-key \
       --region us-west-2 \
       --availability-zone us-west-2b \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --instance-os-user ec2-user \
       --ssh-public-key file://my_key.pub
   ```

3. Stellen Sie mit Ihrem privaten Schlüssel eine Verbindung zu der Instance her.

   Stellen Sie mit dem Befehl ssh eine Verbindung zu Ihrer Instance mit dem privaten Schlüssel her, ehe der öffentliche Schlüssel aus den Instance-Metadaten entfernt wird. Sie haben dafür 60 Sekunden Zeit. Geben Sie den privaten Schlüssel an, der dem öffentlichen Schlüssel entspricht, den Standardbenutzernamen für das AMI, mit dem Sie Ihre Instance gestartet haben, und den öffentlichen DNS-Namen der Instance (wenn Sie eine Verbindung über ein privates Netzwerk herstellen, geben Sie den privaten DNS-Namen oder die IP-Adresse an). Fügen Sie die `IdentitiesOnly=yes`-Option hinzu, um sicherzustellen, dass nur die Dateien in der SSH-Konfiguration und der angegebene Schlüssel für die Verbindung verwendet werden.

   ```
   ssh -o "IdentitiesOnly=yes" -i my_key ec2-
   user@ec2-198-51-100-1.compute-1.amazonaws.com
   ```

Connect mit dem her AWS CLI

Wenn Sie Ihre Instance-ID kennen, können Sie den AWS CLI Befehl ec2-instance-connect verwenden, um über einen SSH-Client eine Verbindung zu Ihrer Instance herzustellen. Wenn Sie keinen Verbindungstyp angeben, versucht EC2 Instance Connect automatisch eine Verbindung zur öffentlichen IPv4-Adresse Ihrer Instance herzustellen. Wenn Ihre Instance keine öffentliche IPv4-Adresse hat, versucht EC2 Instance Connect, über einen EC2-Instance-Connect-Endpunkt eine Verbindung zur privaten IPv4-Adresse Ihrer Instance herzustellen. Wenn Ihre Instance keine private

IPv4-Adresse hat oder Ihre VPC keinen EC2-Instance-Connect-Endpunkt hat, versucht EC2 Instance Connect, sich mit der IPv6-Adresse Ihrer Instance zu verbinden.

> **Important**
>
> Bevor Sie mit dieser Methode eine Verbindung herstellen, stellen Sie sicher, dass Sie den konfiguriert haben AWS CLI, einschließlich der verwendeten Anmeldeinformationen, und dass Sie die neueste Version von verwenden. AWS CLI Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von AWS CLI und Konfiguration der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.

Verbindungstypen

`auto` (Standard)

Die CLI versucht, mithilfe der IP-Adressen der Instance in der folgenden Reihenfolge und mit dem entsprechenden Verbindungstyp eine Verbindung herzustellen:

- Öffentliche IPv4: `direct`
- Private IPv4: `eice`
- IPv6: `direct`

`direct`

Die CLI versucht, mithilfe der IP-Adressen der Instance in der folgenden Reihenfolge eine Verbindung herzustellen (sie stellt keine Verbindung über einen EC2-Instance-Connect-Endpunkt her):

- Öffentliche IPv4
- IPv6
- Private IPv4

`eice`

Die CLI verwendet immer die private IPv4-Adresse der Instance.

> **Note**
>
> In der Zukunft könnten wir das Verhalten des `auto`-Verbindungstyps ändern. Um sicherzustellen, dass Ihr gewünschter Verbindungstyp verwendet wird, empfehlen wir, dass Sie den `--connection-type` explizit entweder auf `direct` oder `eice` zu setzen.

Wenn Sie über EC2 Instance Connect eine Verbindung mit einer Instance herstellen, überträgt die Instance-Connect-API per Push einen öffentlichen SSH-Schlüssel an die Instance-Metadaten, wo er 60 Sekunden verbleibt. Eine an Ihren Benutzer angefügte IAM-Richtlinie autorisiert Ihren Benutzer, den öffentlichen Schlüssel an die Instance-Metadaten zu übertragen.

So stellen Sie unter Verwendung der Instance-ID eine Verbindung mit einer Instance her

Wenn Sie nur die Instance-ID kennen und EC2 Instance Connect den Verbindungstyp bestimmen lassen möchten, der für die Verbindung mit Ihrer Instance verwendet werden soll, verwenden Sie den CLI-Befehl ec2-instance-connect und geben Sie den `ssh` Parameter und die Instance-ID an.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example
```

> **Tip**
>
> Wenn Sie bei der Verwendung dieses Befehls eine Fehlermeldung erhalten, stellen Sie sicher, dass Sie Version 2 verwenden. AWS CLI Der `ssh` Parameter ist nur in AWS CLI Version 2 verfügbar. Weitere Informationen finden Sie unter Über AWS CLI Version 2 im AWS Command Line Interface Benutzerhandbuch.

So stellen Sie eine Verbindung zu einer Instance über die Instance-ID und einen EC2-Instance-Connect-Endpunkt her

Wenn Sie über einen EC2-Instance-Connect-Endpunkt eine Verbindung zu Ihrer Instance herstellen möchten, verwenden Sie den vorherigen Befehl und geben Sie auch den `--connection-type`-Parameter mit dem `eice`-Wert an.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

So stellen Sie mithilfe der Instance-ID und Ihrer eigenen privaten Schlüsseldatei eine Verbindung zu einer Instance her

Wenn Sie über einen EC2-Instance-Connect-Endpunkt mit Ihrem eigenen privaten Schlüssel eine Verbindung zu Ihrer Instance herstellen möchten, geben Sie die Instance-ID und den Pfad zur privaten Schlüsseldatei an. Fügen Sie *file://* nicht in den Pfad ein. Das folgende Beispiel wird fehlschlagen: *file: ///path/to/key*.

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --private-key-file /
path/to/key.pem
```

Fehlerbehebung

Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter:

- Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance
- Wie behebe ich Probleme bei der Verbindung mit meiner EC2-Instance mithilfe von EC2 Instance Connect?

Deinstallieren von EC2 Instance Connect

Um EC2 Instance Connect zu deaktivieren, stellen Sie eine Verbindung mit der Instance her und deinstallieren das `ec2-instance-connect`-Paket, das im Betriebssystem installiert ist. Wenn die `sshd`-Konfiguration mit den Werten übereinstimmt, auf die sie bei der Installation von EC2 Instance Connect festgelegt wurde, wird durch die Deinstallation von `ec2-instance-connect` auch die `sshd`-Konfiguration entfernt. Wenn Sie die `sshd`-Konfiguration nach der Installation von EC2 Instance Connect geändert haben, müssen Sie ein manuelles Update ausführen.

Amazon Linux

Sie können EC2 Instance Connect auf AL2023 und Amazon Linux 2 2.0.20190618 oder höher, wo EC2 Instance Connect vorkonfiguriert ist, deinstallieren.

So installieren Sie EC2 Instance Connect auf einer Instance, die mit Amazon Linux 2 gestartet wurde

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her. Geben Sie das SSH-Schlüsselpaar an, das Sie für Ihre Instance verwendet haben, als Sie sie gestartet haben, und den Standardbenutzernamen für das AL2023- oder Amazon Linux 2-AMI, nämlich. `ec2-user`

Der folgende ssh-Befehl stellt beispielsweise eine Verbindung mit einer Instance mit dem öffentlichen DNS-Namen `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` her. Hierfür wird das Schlüsselpaar `my_ec2_private_key.pem` verwendet.

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

2. Deinstallieren Sie das `ec2-instance-connect`-Paket mit dem yum-Befehl.

```
[ec2-user ~]$ sudo yum remove ec2-instance-connect
```

Ubuntu

So deinstallieren Sie EC2 Instance Connect in einer Instance, die mit einem Ubuntu-AMI gestartet wurde:

1. Stellen Sie per SSH eine Verbindung zu Ihrer -Instance her. Geben Sie das SSH-Schlüsselpaar an, das Sie für Ihre Instance verwendet haben, als Sie sie gestartet haben, und den Standardbenutzernamen für das Ubuntu-AMI, nämlich`ubuntu`.

   Der folgende ssh-Befehl stellt beispielsweise eine Verbindung mit einer Instance mit dem öffentlichen DNS-Namen `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` her. Hierfür wird das Schlüsselpaar `my_ec2_private_key.pem` verwendet.

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

2. Deinstallieren Sie das `ec2-instance-connect`-Paket mit dem apt-get-Befehl.

```
ubuntu:~$ sudo apt-get remove ec2-instance-connect
```

Herstellen einer Verbindung mit Ihrer -Windows-Instance

Sie können sich mit Amazon-EC2-Instances, die von den meisten Windows Amazon Machine Images (AMIs) erstellt werden, mithilfe des Remote Desktop verbinden. Das Remote Desktop verwendet das Remote Desktop Protocol (RDP) und bietet Ihnen die Möglichkeit, sich mit Ihrer Instance zu

verbinden und sie wie einen normalen (lokalen) Computer zu verwenden. Sie steht für die meisten Windows-Versionen und auch für Mac OS zur Verfügung.

Die Lizenz für das Windows Server-Betriebssystem ermöglicht zwei gleichzeitige Remote-Verbindungen zu Verwaltungszwecken. Die Lizenzkosten für Windows Server sind in den Kosten für Ihre Windows-Instance enthalten. Falls Sie mehr als zwei gleichzeitige Remote-Verbindungen benötigen, ist der Erwerb einer Remote Desktop Services-Lizenz (RDS) erforderlich. Wenn Sie versuchen, eine dritte Verbindung aufzubauen, erhalten Sie eine Fehlermeldung.

> **Tip**
>
> Wenn Sie eine Verbindung zu Ihrer Instance herstellen müssen, um Boot-, Netzwerkkonfigurations- und andere Probleme für Instances, die auf dem AWS Nitro System aufgebaut sind, zu beheben, können Sie die Serielle EC2-Konsole für Amazon EC2 EC2-Instances verwenden.

Inhalt

Stellen Sie mithilfe eines RDP-Clients eine Connect zu Ihrer Windows-Instanz her

Im folgenden Abschnitt werden die Voraussetzungen und der Prozess für die Verbindung mit Ihrer Instance unter Verwendung ihrer IPv4- oder IPv6-Adresse mit einem RDP-Client beschrieben.

Voraussetzungen

Sie müssen die folgenden Voraussetzungen erfüllen, um mithilfe eines RDP-Clients eine Verbindung zu Ihrer Windows-Instanz herzustellen.

- Installieren eines RDP-Clients
  - (Windows) Windows enthält standardmäßig einen RDP-Client. Zum Überprüfen geben Sie mstsc in ein Befehlseingabefenster ein. Wenn Ihr Computer diesen Befehl nicht erkennt, gehen Sie auf die Windows-Startseite und suchen Sie nach dem Download für die Microsoft Remote Desktop-App.

  - (macOS X) Laden Sie die Microsoft Remote Desktop-App aus dem Mac App Store herunter.
  - (Linux) Verwenden Sie Remmina.
- Auffinden des privaten Schlüssels

  Rufen Sie den vollständig qualifizierten Pfad des Speicherorts auf Ihrem Computer für die Datei `.pem` für das beim Start der Instance angegebene Schlüsselpaar ab. Weitere Informationen finden Sie unter the section called “Identifizieren des öffentlichen Schlüssels, der beim Start angegeben wurde”.

  Wenn Sie Ihre private Schlüsseldatei nicht finden können, finden Sie unter

  Wenn Sie eine Verbindung zu einer neu gestarteten Windows-Instance herstellen, entschlüsseln Sie das Passwort für das Administrator-Konto mithilfe des privaten Schlüssels des Schlüsselpaars, das Sie beim Starten der Instance festgelegt haben.

  Wenn Sie das Administratorpasswort und den privaten Schlüssel nicht mehr haben, müssen Sie das Passwort zurücksetzen oder eine neue Instance erstellen. Weitere Informationen finden Sie unter Zurücksetzen eines Windows-Administratorpassworts, das verloren oder abgelaufen ist. Schritte zum Zurücksetzen des Kennworts mithilfe eines Systems-Manager-Dokuments finden Sie unter Zurücksetzen von Kennwörtern und SSH-Schlüsseln auf EC2-Instances im AWS Systems Manager -Benutzerhandbuch.
- Aktivieren des eingehenden RDP-Datenverkehrs von der IP-Adresse zur Instance

  Stellen Sie sicher, dass die mit Ihrer Instance verknüpfte Sicherheitsgruppe eingehenden RDP-Datenverkehr (`port 3389`) von Ihrer IP-Adresse zulässt. Standardmäßig lässt die Sicherheitsgruppe keinen eingehenden RDP-Datenverkehr zu. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.

> **Tip**
>
> Sie können einen EC2 Instance Connect-Endpoint erstellen, um mithilfe von RDP ohne öffentliche IPv4-Adresse eine Verbindung zu Ihrer Windows-Instance herzustellen.

Stellen Sie mithilfe von RDP und seiner IPv4-Adresse eine Connect zu einer Windows-Instanz her

Um eine Verbindung zu einer Windows-Instanz herzustellen, müssen Sie das anfängliche Administratorkennwort abrufen und dieses Kennwort verwenden, wenn Sie über Remote Desktop

eine Verbindung zu Ihrer Instanz herstellen. (Nach dem Start der Instance dauert es einige Minuten, bis das Passwort verfügbar ist.)

Der Standardbenutzername für das Administratorkonto hängt von der Sprache des Betriebssystems (OS) ab, das im AMI enthalten ist. Um den richtigen Benutzernamen zu ermitteln, identifizieren Sie die Sprache des Betriebssystems Ihres AMI und wählen Sie dann den entsprechenden Benutzernamen. Für ein englisches Betriebssystem lautet der Benutzername beispielsweise`Administrator`, für ein französisches Betriebssystem ist es `Administrateur` und für ein portugiesisches Betriebssystem ist `Administrador` es. Wenn eine Sprachversion des Betriebssystems keinen Benutzernamen in derselben Sprache hat, wählen Sie den Benutzernamen`Administrator (Other)`. Weitere Informationen finden Sie unter Lokalisierte Namen für Administratorkonten in Windows im TechNet Microsoft-Wiki.

Wenn Sie Ihre Instance einer Domain zugewiesen haben, können Sie eine Verbindung mit Ihrer Instance mithilfe von Domain-Anmeldeinformationen herstellen, die Sie in AWS Directory Service definiert haben. Verwenden Sie auf dem Anmeldebildschirm für Remotedesktop anstelle des lokalen Computernamens und des generierten Kennworts den vollqualifizierten Benutzernamen für den Administrator (z. B. **`corp.example.com\Admin`**) und das Passwort für dieses Konto.

Weitere Informationen zu Problemen, die beim Aufbau einer Verbindung zu Instances auftreten können, finden Sie unter the section called “Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen”.

Verwenden Sie einen RDP Client, um sich mit Ihrer Windows-Instance zu verbinden.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Wählen Sie auf der Seite Mit Instanz Connect die Registerkarte RDP-Client aus.
5. Wählen Sie unter Benutzername den Standardbenutzernamen für das Administratorkonto aus. Der von Ihnen gewählte Benutzername muss der Sprache des Betriebssystems (OS) entsprechen, das im AMI enthalten ist, mit dem Sie Ihre Instance gestartet haben. Wenn es keinen Benutzernamen in derselben Sprache wie Ihr Betriebssystem gibt, wählen Sie Administrator (Andere).
6. Wählen Sie Passwort abrufen.
7. Gehen Sie auf der Seite Windows-Passwort abrufen wie folgt vor:

a. Wählen Sie Datei mit privatem Schlüssel hochladen und navigieren Sie zu der Datei mit dem privaten Schlüssel (`.pem`), die Sie beim Start der Instance angegeben haben. Wählen Sie die Datei aus und klicken Sie auf Open (Öffnen), um den gesamten Inhalt der Datei auf dieses Fenster zu kopieren.

b. Wählen Sie Passwort entschlüsseln. Die Seite „Windows-Passwort abrufen“ wird geschlossen, und das Standard-Administratorkennwort für die Instanz wird unter Passwort angezeigt. Es ersetzt den zuvor angezeigten Link „Passwort abrufen“.

c. Kopieren Sie das Passwort und speichern Sie es an einem sicheren Ort. Dieses Passwort wird benötigt, um eine Verbindung mit der Instance herzustellen.

8. Klicken Sie auf Download Remote Desktop File (Remotedesktop-Datei herunterladen). Klicken Sie nach dem Herunterladen der Datei auf Cancel (Abbrechen), um zur Seite Instances zurückzukehren. Navigieren Sie zu Ihrem Download-Verzeichnis und öffnen Sie die RDP-Datei.

9. Möglicherweise wird eine Warnmeldung angezeigt, dass der Herausgeber der Remote-Verbindung unbekannt ist. Wählen Sie Connect (Verbinden) aus, um eine Verbindung mit der Ihrer Instance herzustellen.

10. Standardmäßig wird das Administratorkonto ausgewählt. Fügen Sie das zuvor kopierte Passwort ein und wählen Sie dann OK.

11. Aufgrund der Art selbst signierter Zertifikate erhalten Sie möglicherweise eine Warnmeldung, dass das Sicherheitszertifikat nicht authentifiziert werden konnte. Führen Sie eine der folgenden Aktionen aus:

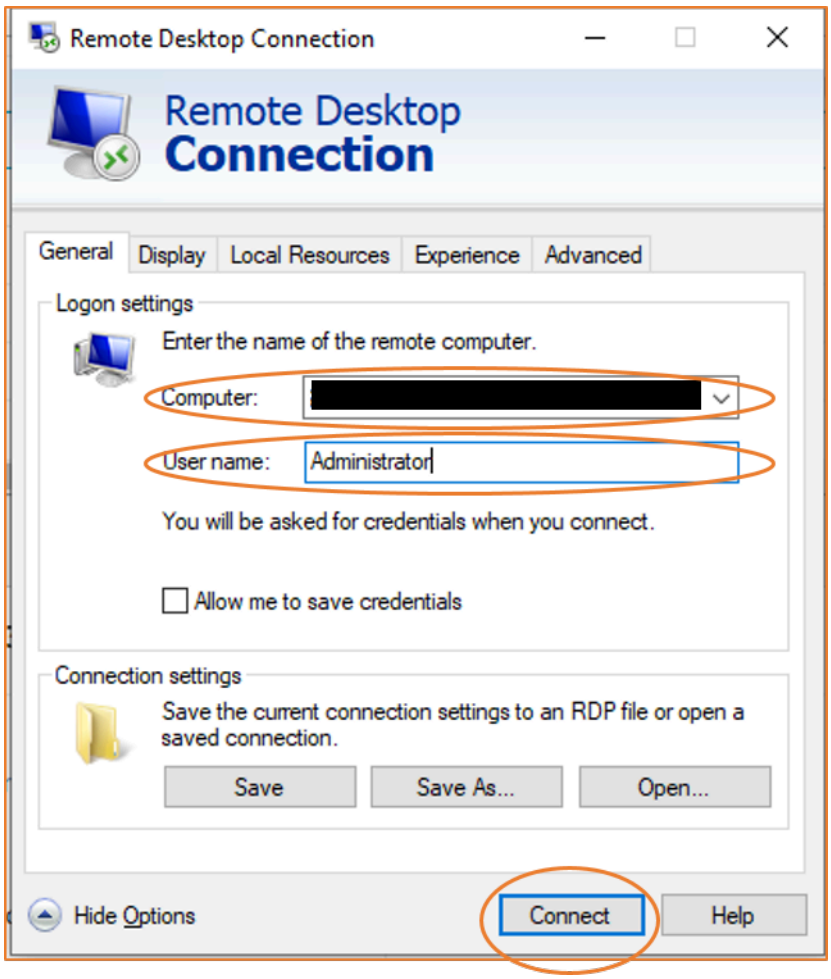
    - Wenn Sie dem Zertifikat vertrauen, wählen Sie Ja, um eine Verbindung zu Ihrer Instance herzustellen.
    - [Windows] Bevor Sie fortfahren, vergleichen Sie den Fingerabdruck des Zertifikats mit dem Wert im Systemprotokoll, um die Identität des Remotecomputers zu bestätigen. Wählen Sie Zertifikat anzeigen und dann auf der Registerkarte Details die Option Fingerabdruck aus. Vergleichen Sie diesen Wert mit dem Wert `RDPCERTIFICATE-THUMBPRINT` in Aktionen, Überwachung und Fehlerbehebung, Systemprotokoll abrufen.
    - [Mac OS X] Bevor Sie fortfahren, vergleichen Sie den Fingerabdruck des Zertifikats mit dem Wert im Systemprotokoll, um die Identität des Remote-Computers zu bestätigen. Wählen Sie „Zertifikat anzeigen“, erweitern Sie „Details“ und wählen Sie „SHA1-Fingerabdrücke“. Vergleichen Sie diesen Wert mit dem Wert `RDPCERTIFICATE-THUMBPRINT` in Aktionen, Überwachung und Fehlerbehebung, Systemprotokoll abrufen.

Stellen Sie mithilfe von RDP und seiner IPv6-Adresse eine Connect zu einer Windows-Instanz her

Wenn Sie Ihre VPC für IPv6 aktiviert und Ihrer Windows-Instance eine IPv6-Adresse zugewiesen haben, können Sie sich mithilfe eines RDP-Client mit ihrer IPv6-Adresse (zum Beispiel `2001:db8:1234:1a00:9691:9503:25ad:1761`) verbinden, anstelle ihre öffentliche IPv4-Adresse oder den öffentlichen DNS-Hostnamen zu verwenden.

Zum Verbinden mit Ihrer Windows-Instance mit deren IPv6-Adresse

1. Holen Sie sich das anfängliche Administratorkennwort für Ihre Instance, wie unter Stellen Sie mithilfe eines RDP-Clients eine Connect zu Ihrer Windows-Instanz her beschrieben. Dieses Passwort wird benötigt, um eine Verbindung mit Ihrer Instance herzustellen.
2. (Windows) Öffnen Sie den RDP-Client auf Ihrem Windows-Computer, wählen Sie „Optionen anzeigen“ und gehen Sie wie folgt vor:



- Für Computer geben Sie die IPv6-Adresse Ihrer Windows-Instance ein.
- Für User name (Benutzername) geben Sie Administrator ein.

- Wählen Sie Connect (Verbinden) aus.
- Geben Sie bei entsprechender Aufforderung das Passwort ein, das Sie zuvor gespeichert haben.

(MacOS X) Öffnen Sie den RDP-Client auf Ihrem Computer und gehen Sie wie folgt vor:

- Wählen Sie New (Neu).
- Für PC Name (Computer-Name) geben Sie die IPv6-Adresse Ihrer Windows-Instance ein.
- Für User name (Benutzername) geben Sie Administrator ein.
- Schließen Sie das Dialogfeld. Wählen Sie unter My Desktops (Eigene Desktops) die Verbindung aus und wählen Sie Start (Starten).
- Geben Sie bei entsprechender Aufforderung das Passwort ein, das Sie zuvor gespeichert haben.

3. Aufgrund der Art selbst signierter Zertifikate erhalten Sie möglicherweise eine Warnmeldung, dass das Sicherheitszertifikat nicht authentifiziert werden konnte. Wenn Sie dem Zertifikat vertrauen, können Sie Yes (Ja) oder Continue (Weiter) wählen. Andernfalls können Sie die Identität des Remote-Computers überprüfen, wie unter Stellen Sie mithilfe eines RDP-Clients eine Connect zu Ihrer Windows-Instanz her beschrieben.

Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von Fleet Manager

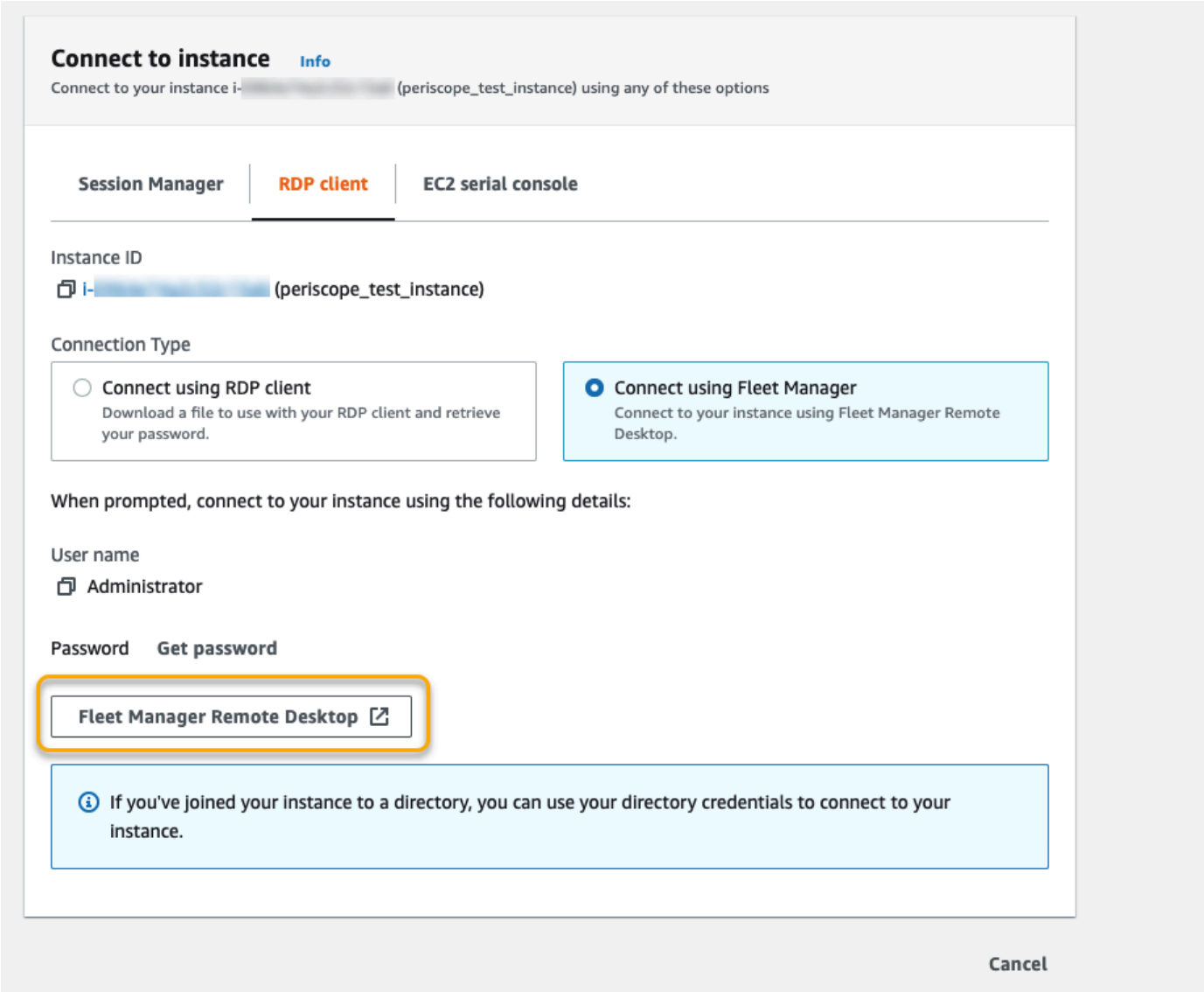
Sie können Fleet Manager, eine Funktion von AWS Systems Manager, verwenden, um mithilfe des Remote Desktop Protocol (RDP) eine Verbindung zu Windows-Instanzen herzustellen und bis zu vier Windows-Instanzen auf derselben Seite im anzuzeigen. AWS Management Console Sie können eine Verbindung mit der ersten Instance im Fleet Manager Remote Desktop direkt über die Seite Instances in der Amazon-EC2-Konsole herstellen. Weitere Informationen zu Fleet Manager finden Sie im AWS Systems Manager -Benutzerhandbuch unter Connect to a managed node using Remote Desktop.

Stellen Sie sicher, dass die erforderlichen Einrichtungsschritte abgeschlossen sind, bevor Sie versuchen, mithilfe von Fleet Manager eine Verbindung mit einer Instance herzustellen. Weitere Informationen finden Sie unter Einrichten Ihrer Umgebung.

> **Note**
>
> Sie müssen eingehenden RDP-Datenverkehr von Ihrer IP-Adresse nicht ausdrücklich zulassen, wenn Sie Fleet Manager für die Verbindung verwenden. Fleet Manager erledigt das für Sie.

So verbinden Sie Instances über RDP mit Instances mithilfe von Fleet Manager (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Connect (Verbinden).
4. Wählen Sie auf der Seite Connect to Instance (Mit Instance verbinden) die Option Connect using Fleet Manager (Verbindung über Fleet Manager) und dann Fleet Manager Remote Desktop aus. Daraufhin wird die Seite Fleet Manager Remote Desktop in der AWS Systems Manager -Konsole geöffnet.



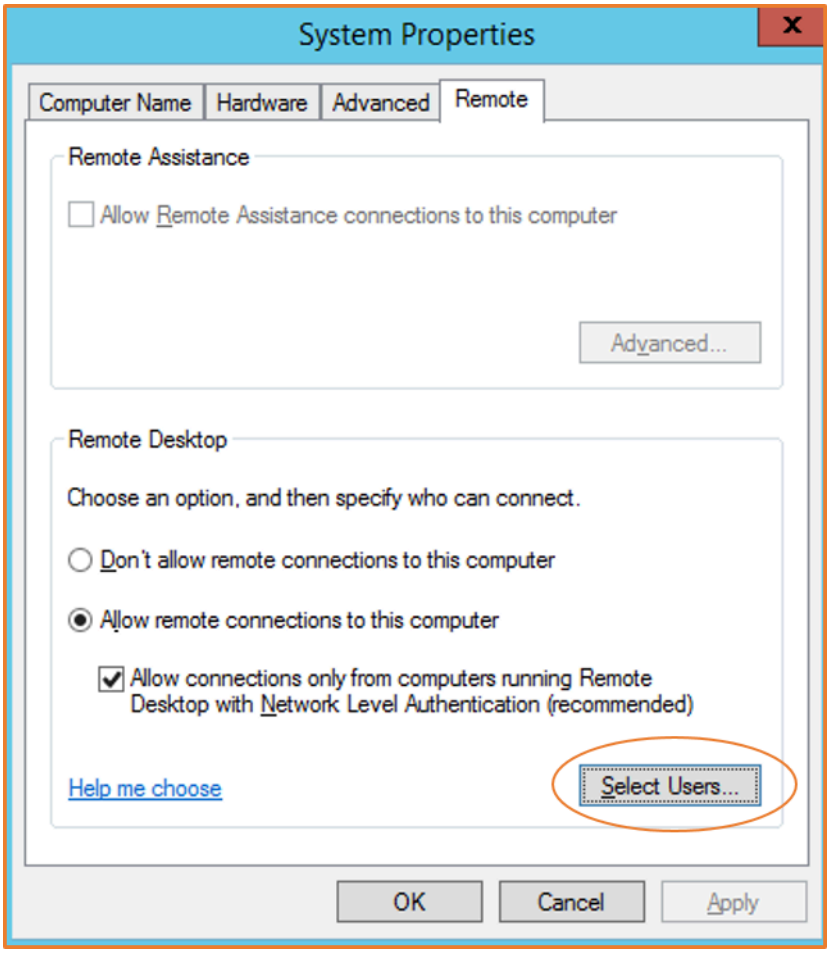
Weitere Informationen zum Herstellen einer Verbindung mit Windows-Instances von der Seite Fleet Manager Remote Desktop finden Sie unter Über Remote Desktop verbinden im AWS Systems Manager -Benutzerhandbuch.

Konfigurieren Ihrer Konten

Nachdem Sie die Verbindung über RDP hergestellt haben, empfehlen wir Ihnen, wie folgt vorzugehen:

- Ändern Sie das Standard-Passwort für den Administrator. Sie können das Passwort ändern, während Sie in der Instance angemeldet sind, genau wie bei jedem Computer, auf dem Windows-Server ausgeführt wird.

- Erstellen Sie einen anderen Benutzer mit Administratorrechten für die Instance. Dies dient als Sicherheitsmaßnahme, falls Sie das Administratorpasswort vergessen haben oder ein Problem mit dem Administratorkonto besteht. Der neue Benutzer muss über die Berechtigung zum Zugriff auf die Instance aus der Ferne verfügen. Öffnen Sie Systemeigenschaften durch einen Rechtsklick auf das Symbol Dieser Computer auf dem Windows-Desktop oder wählen Sie im Explorer Eigenschaften. Wählen Sie Remoteeinstellungen und danach Benutzer auswählen, um den Benutzer der Gruppe Remotedesktopbenutzer hinzuzufügen.



Übertragen von Dateien zu Windows-Instances

Sie können mit Ihrer Windows-Instance so wie mit jedem anderen Windows-Server arbeiten. Sie können beispielsweise Dateien zwischen einer Windows-Instanz und Ihrem lokalen Computer mithilfe der lokalen Dateifreigabefunktion der Microsoft Remote Desktop Connection (RDP) -Software übertragen. Sie können auf lokale Dateien auf Festplattenlaufwerken, DVD-Laufwerken, tragbaren Medienlaufwerken und zugeordneten Netzlaufwerken zugreifen.

Um von Ihren Windows-Instances aus auf Ihre lokalen Dateien zugreifen zu können, müssen Sie das Feature zur lokalen Dateifreigabe aktivieren, indem Sie das Laufwerk der Remotesitzung Ihrem lokalen Laufwerk zuordnen. Die Schritte unterscheiden sich geringfügig, je nachdem, ob Ihr lokales Computerbetriebssystem Windows oder macOS X ist.

Windows

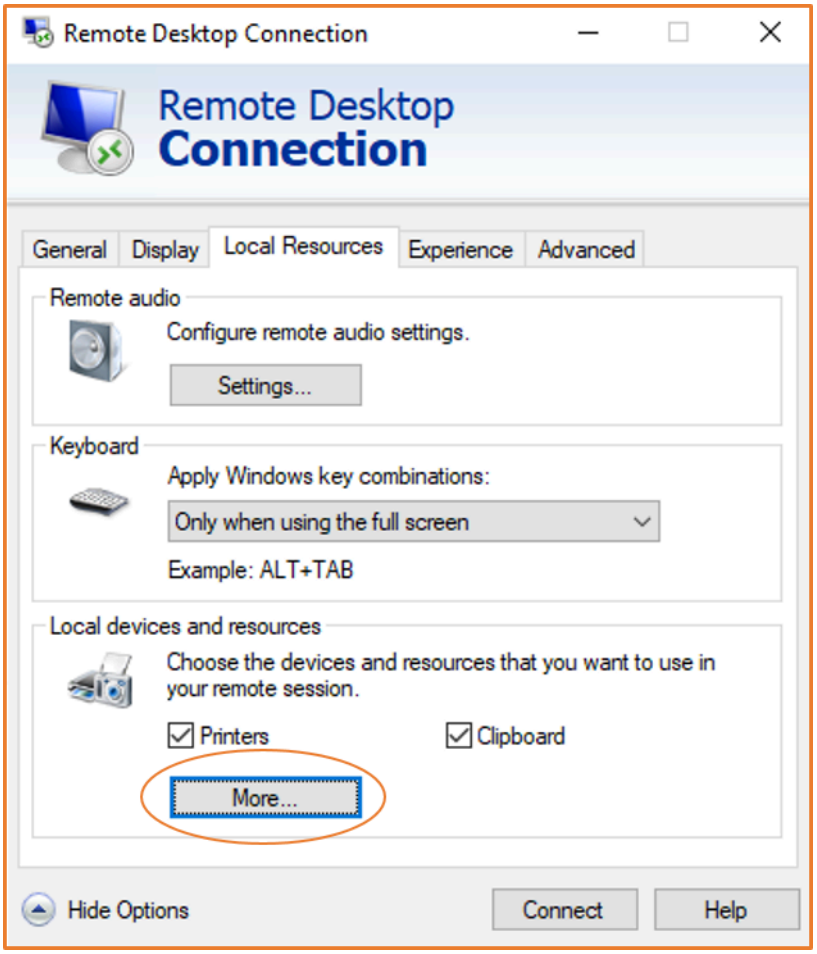
Laufwerk der Remotesitzung dem lokalen Laufwerk auf Ihrem lokalen Windows-Computer zuordnen

1. Öffnen Sie den Remote Desktop Connection-Client.
2. Wählen Sie Show Options aus.
3. Fügen Sie den Instance-Host-Namen dem Feld Computer und den Benutzernamen dem Feld User name (Benutzername) hinzu, wie nachfolgend gezeigt:

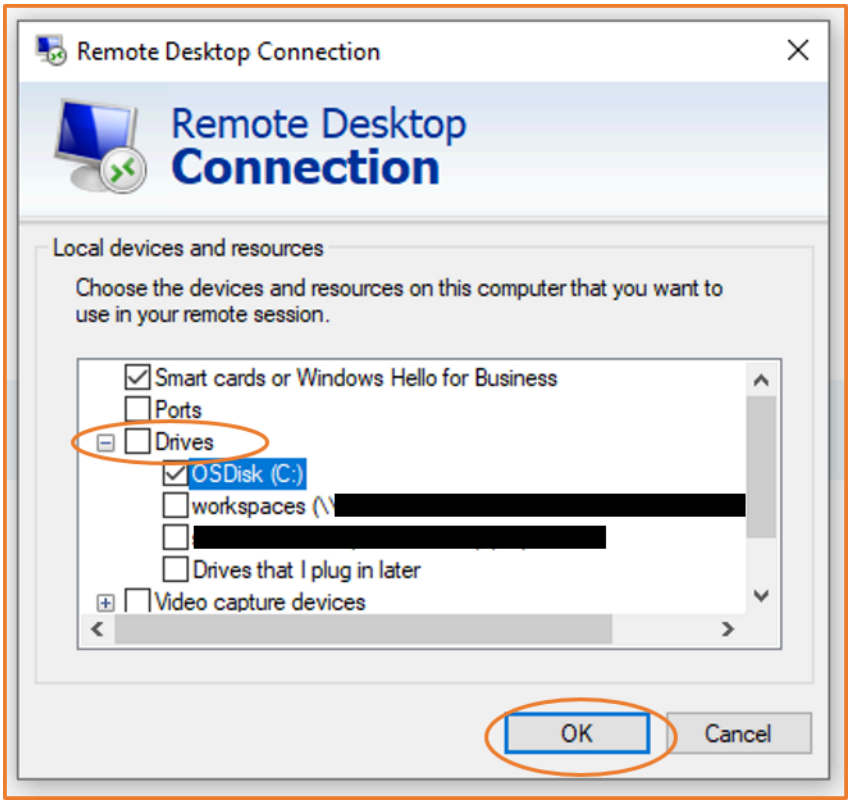
   a. Wählen Sie unter Connection settings (Verbindungseinstellungen) Open... (Öffnen…) aus und navigieren Sie zur RDP-Verknüpfungsdatei, die Sie in der Amazon-EC2-Konsole heruntergeladen haben. Die Datei enthält den öffentlichen IPv4-DNS-Hostnamen, der die Instance identifiziert, und den Benutzernamen des Administrators.

   b. Wählen Sie die Datei und dann Open (Öffnen) aus. Die Felder Computer und User name (Benutzername) werden mit den Werten aus der RDP-Verknüpfungsdatei gefüllt.

   c. Wählen Sie Speichern.
4. Wählen Sie die Registerkarte Local Resources (Lokale Ressourcen).
5. Wählen Sie unter Local devices and resources (Lokale Geräte und Ressourcen) die Option More... (Mehr...) aus.



6. Öffnen Sie Drives (Laufwerke) und wählen Sie das lokale Laufwerk aus, das Sie der Windows-Instance zuordnen möchten.
7. Klicken Sie auf OK.

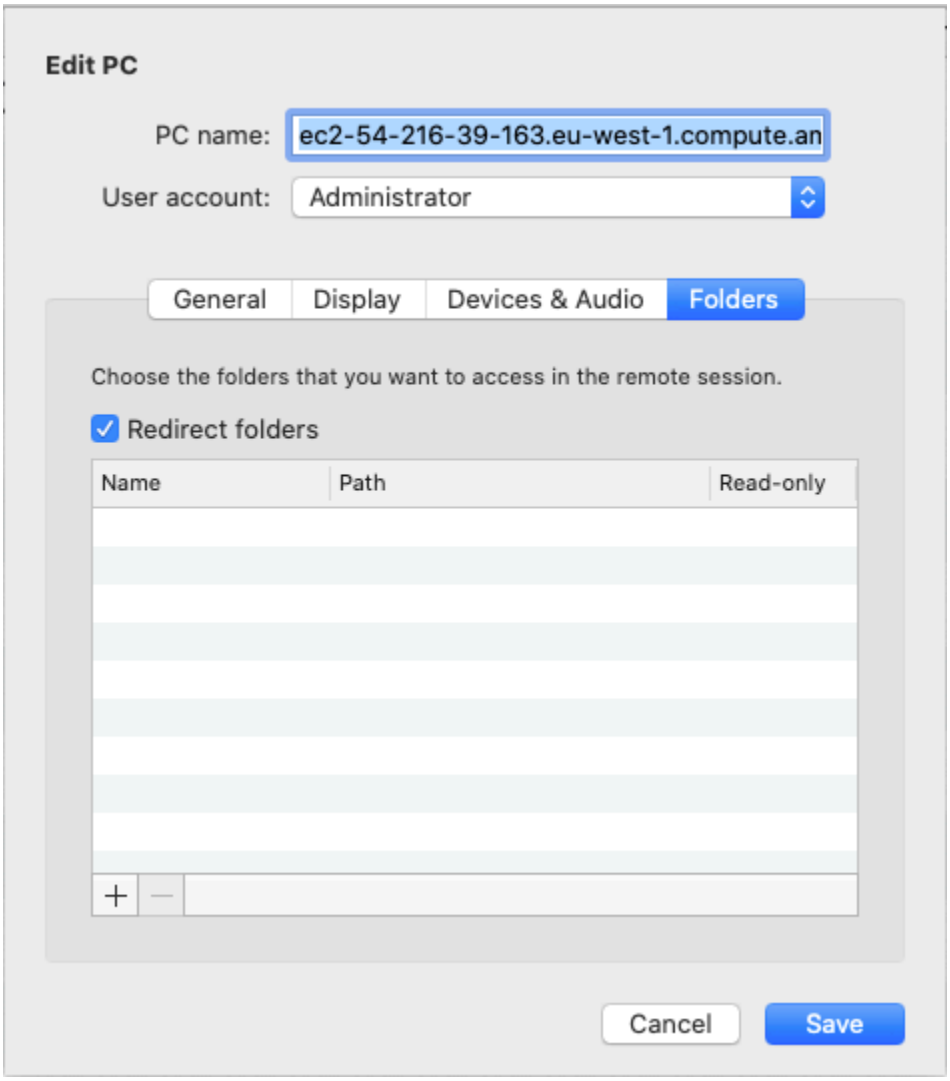


8. Wählen Sie Connect (Verbinden) aus, um eine Verbindung mit der Windows-Instance herzustellen.

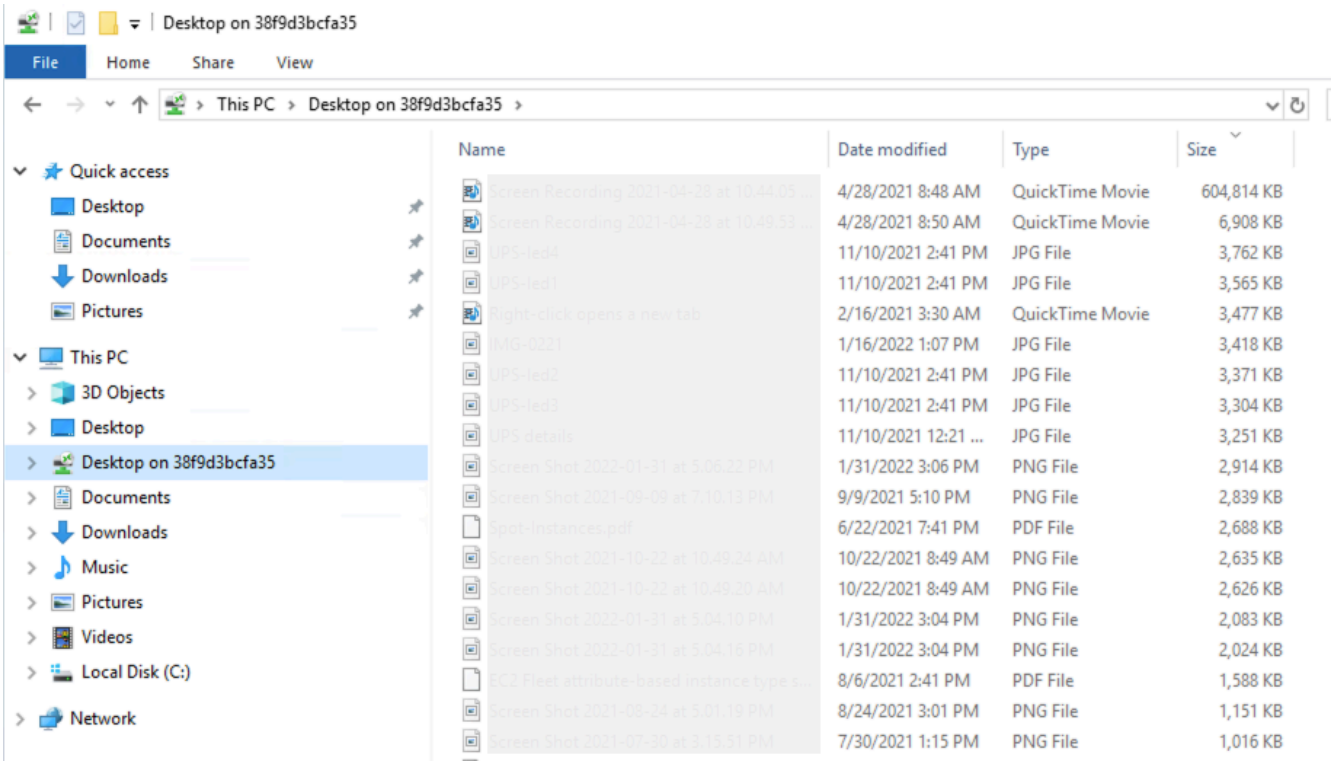
macOS X

Laufwerk der Remotesitzung dem lokalen Verzeichnis auf Ihrem lokalen macOS X-Computer zuordnen

1. Öffnen Sie den Remote Desktop Connection-Client.
2. Navigieren Sie zu der RDP-Datei, die Sie in der Amazon-EC2-Konsole heruntergeladen haben (als Sie erstmals die Verbindung zur Instance hergestellt haben), und ziehen Sie sie auf den Remotedesktopverbindungs-Client.
3. Klicken Sie mit der rechten Maustaste auf die RDP-Datei und wählen Sie Edit (Bearbeiten) aus.
4. Wählen Sie die Registerkarte Folders (Ordner) und dann das Kontrollkästchen Redirect folders (Ordner umleiten) aus.



5. Wählen Sie das +-Symbol unten links aus, navigieren Sie zu dem Ordner, den Sie zuordnen möchten, und wählen Sie Open (Öffnen) aus. Wiederholen Sie diesen Schritt für jeden Ordner, der zugeordnet werden soll.
6. Wählen Sie Speichern.
7. Wählen Sie Connect (Verbinden) aus, um eine Verbindung mit der Windows-Instance herzustellen. Sie werden zur Passworteingabe aufgefordert.
8. Erweitern Sie auf der Instance im Datei-Explorer Dieser PC und navigieren Sie zu dem freigegebenen Ordner, über den Sie auf Ihre lokalen Dateien zugreifen können. Im folgenden Screenshot wurde der Ordner Desktop auf dem lokalen Computer dem Laufwerk der Remotesitzung auf der Instance zugeordnet.



Weitere Informationen dazu, wie Sie lokale Geräte für eine Remotesitzung auf einem Mac-Computer verfügbar machen, finden Sie unter Erste Schritte mit dem macOS-Client.

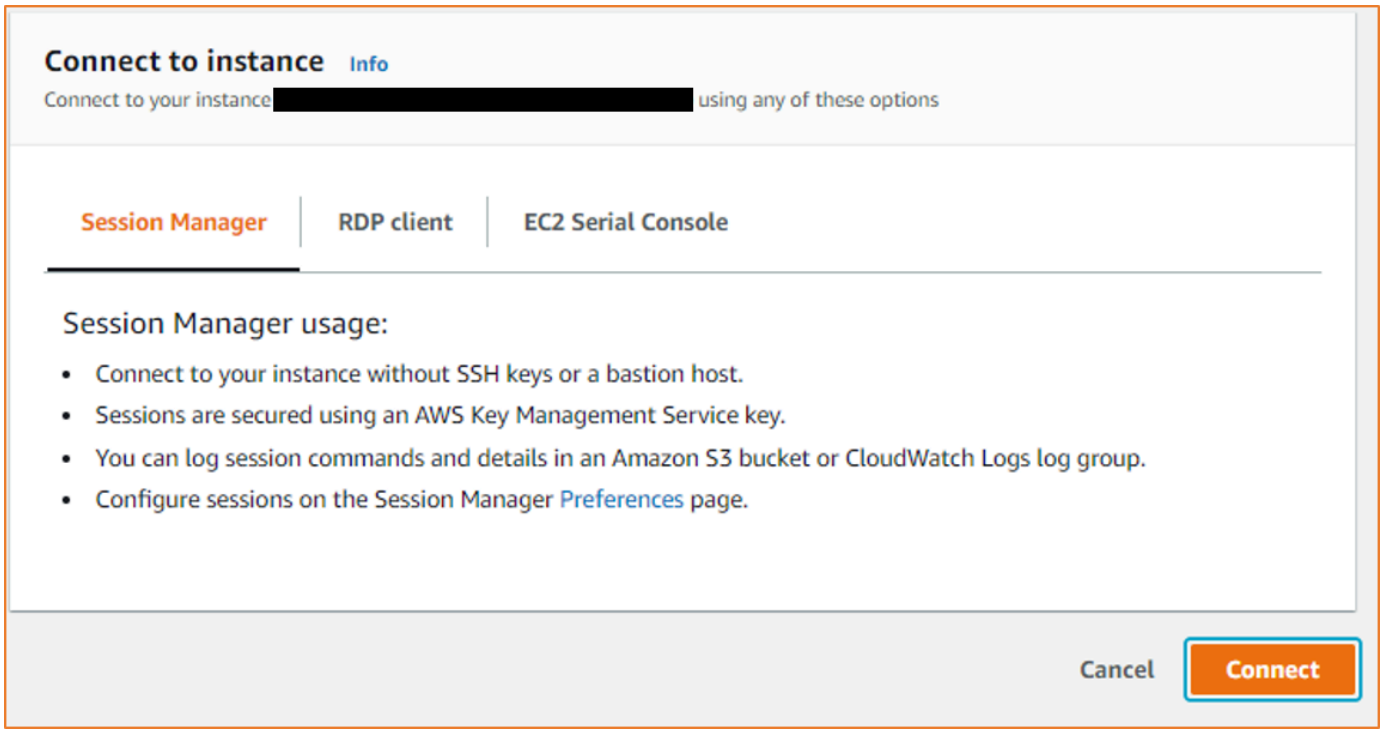
Herstellen einer Verbindung über Session Manager

Session Manager ist eine vollständig verwaltete AWS Systems Manager Funktion zur Verwaltung Ihrer Amazon EC2 EC2-Instances über eine interaktive, browserbasierte Shell mit einem Klick oder über die. AWS CLI Sie können Session Manager verwenden, um eine Sitzung mit einer Instance in Ihrem Konto zu starten. Nach dem Start der Sitzung können Sie interaktive Befehle auf der Instance ausführen, wie Sie es für jeden anderen Verbindungstyp tun würden. Weitere Informationen zum Session Manager finden Sie unter AWS Systems Manager Session Manager im AWS Systems Manager -Benutzerhandbuch.

Bevor Sie versuchen, eine Verbindung mit einer Instance mithilfe des Session Managers herzustellen, stellen Sie sicher, dass die erforderlichen Einrichtungsschritte abgeschlossen sind. Weitere Informationen finden Sie unter Einrichten von Session Manager.

So stellen Sie mithilfe von Session Manager auf der Amazon EC2 EC2-Konsole eine Verbindung zu einer Amazon EC2 EC2-Instance her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und Connect (Verbinden) aus.
4. Wählen Sie für Connection method (Verbindungsmethode) ´Session Manager.
5. Wählen Sie Connect (Verbinden) aus.



> **Tip**
>
> Wenn Sie die Fehlermeldung erhalten, dass Sie nicht berechtigt sind, eine oder mehrere Systems Manager-Aktionen auszuführen (`ssm:command-name`), müssen Sie Ihre Richtlinien aktualisieren, damit Sie Sitzungen über die Amazon EC2-Konsole starten können. Weitere Informationen und Anleitungen finden Sie unter Quick-Start Standard-IAM-Richtlinien für Session Manager im AWS Systems Manager -Benutzerhandbuch.

Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu Ihren Instances her

Mit EC2 Instance Connect Endpoint können Sie eine sichere Verbindung zu einer Instance aus dem Internet herstellen, ohne einen Bastion-Host zu verwenden oder zu benötigen, dass Ihre Virtual Private Cloud (VPC) über eine direkte Internetverbindung verfügt.

Vorteile

- Sie können eine Verbindung zu Ihren Instances herstellen, ohne dass die Instances über eine öffentliche IPv4-Adresse verfügen müssen. AWS Gebühren für alle öffentlichen IPv4-Adressen, einschließlich öffentlicher IPv4-Adressen, die mit laufenden Instances verknüpft sind, und Elastic IP-Adressen. Weitere Informationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite Preise für Amazon VPC.
- Sie können über das Internet eine Verbindung zu Ihren Instances herstellen, ohne dass Ihre VPC über ein Internet-Gateway direkt mit dem Internet verbunden sein muss.
- Sie können den Zugriff auf die Erstellung und Verwendung der EC2 Instance Connect-Endpoints steuern, um mithilfe von IAM-Richtlinien und -Berechtigungen eine Verbindung zu Instances herzustellen.
- Alle Versuche, eine Verbindung zu Ihren Instances herzustellen, sowohl erfolgreiche als auch erfolglose, werden protokolliert. CloudTrail

Preisgestaltung

Für die Nutzung von EC2 Instance Connect Endpoints fallen keine zusätzlichen Kosten an. Wenn Sie einen EC2 Instance Connect-Endpunkt verwenden, um eine Verbindung zu einer Instance in einer anderen Availability Zone herzustellen, fallen zusätzliche Gebühren für die Datenübertragung zwischen Availability Zones an.

Inhalt

- Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu einer Amazon EC2-Instance Connect
- Protokollverbindungen, die über EC2-Instance-Connect-Endpunkt hergestellt wurden
- Löschen Sie einen EC2 Instance Connect-Endpunkt
- Serviceverknüpfte Rolle für EC2-Instance-Connect-Endpunkt
- Kontingente für den EC2 Instance Connect-Endpunkt

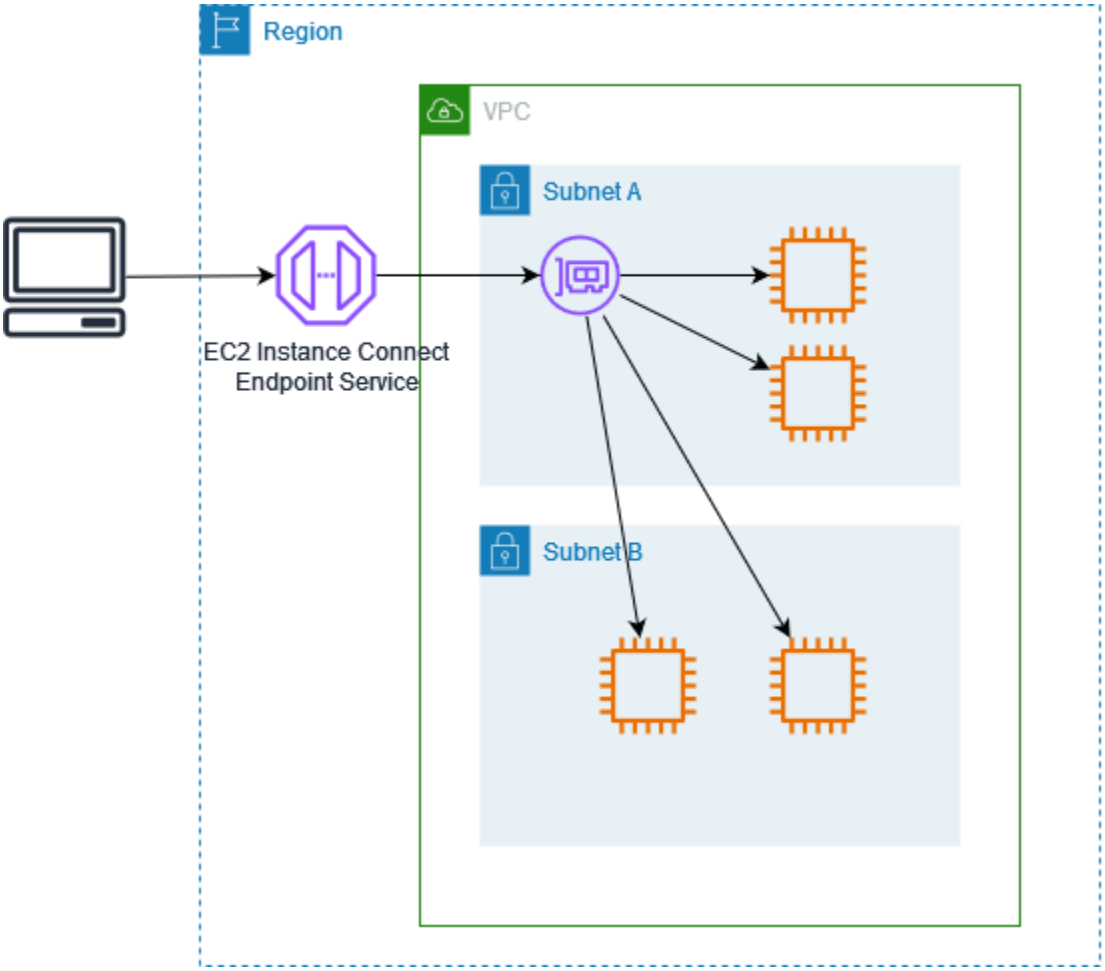
Funktionsweise

EC2 Instance Connect Endpoint ist ein identitätsbewusster TCP-Proxy. Der EC2 Instance Connect Endpoint Service richtet mithilfe der Anmeldeinformationen für Ihre IAM-Entität einen privaten Tunnel von Ihrem Computer zum Endpunkt ein. Der Datenverkehr wird authentifiziert und autorisiert, bevor er Ihre VPC erreicht.

Sie können zusätzliche Sicherheitsgruppenregeln konfigurieren, um den eingehenden Datenverkehr auf Ihre Instances zu beschränken. Sie können beispielsweise Regeln für eingehenden Datenverkehr verwenden, um Datenverkehr auf Management-Ports nur vom EC2 Instance Connect-Endpunkt aus zuzulassen.

Sie können Routentabellenregeln so konfigurieren, dass der Endpunkt eine Verbindung zu einer beliebigen Instanz in einem beliebigen Subnetz der VPC herstellen kann.

Das folgende Diagramm zeigt, wie ein Benutzer mithilfe eines EC2 Instance Connect-Endpunkts über das Internet eine Verbindung zu seinen Instances herstellen kann. Erstellen Sie zunächst einen EC2 Instance Connect-Endpunkt in Subnetz A. Wir erstellen eine Netzwerkschnittstelle für den Endpunkt im Subnetz, die als Einstiegspunkt für den Datenverkehr dient, der für Ihre Instances in der VPC bestimmt ist. Wenn die Routing-Tabelle für Subnetz B Datenverkehr von Subnetz A zulässt, können Sie den Endpunkt verwenden, um Instances in Subnetz B zu erreichen.



Überlegungen

Bevor Sie beginnen, sollten Sie Folgendes berücksichtigen.

- EC2 Instance Connect Endpoint ist speziell für Anwendungsfälle zur Verwaltung des Datenverkehrs vorgesehen, nicht für Datenübertragungen mit hohem Datenvolumen. Datenübertragungen mit hohem Datenvolumen werden gedrosselt.
- Ihre Instance muss eine IPv4-Adresse haben (entweder privat oder öffentlich). EC2 Instance Connect Endpoint unterstützt keine Verbindung zu Instances, die IPv6-Adressen verwenden.
- (Linux-Instances) Wenn Sie Ihr eigenes key pair verwenden, können Sie jedes Linux-AMI verwenden. Andernfalls muss auf Ihrer Instance EC2 Instance Connect installiert sein. Informationen darüber, welche AMIs EC2 Instance Connect enthalten und wie es auf anderen unterstützten AMIs installiert wird, finden Sie unterInstallieren Sie EC2 Instance Connect.
- Sie können einem EC2 Instance Connect-Endpoint eine Sicherheitsgruppe zuweisen, wenn Sie ihn erstellen. Andernfalls verwenden wir die Standardsicherheitsgruppe für die VPC. Die

Sicherheitsgruppe für einen EC2 Instance Connect-Endpunkt muss ausgehenden Datenverkehr zu den Ziel-Instances zulassen. Weitere Informationen finden Sie unter Sicherheitsgruppen für EC2-Instance-Connect-Endpunkt.

- Sie können einen EC2 Instance Connect-Endpunkt so konfigurieren, dass die Quell-IP-Adressen der Clients erhalten bleiben, wenn Anfragen an die Instances weitergeleitet werden. Andernfalls wird die IP-Adresse der Netzwerkschnittstelle zur Client-IP-Adresse für den gesamten eingehenden Datenverkehr.
  - Wenn Sie die Client-IP-Erhaltung aktivieren, müssen die Sicherheitsgruppen für die Instances den Datenverkehr von den Clients zulassen. Außerdem müssen sich die Instances in derselben VPC wie der EC2 Instance Connect-Endpunkt befinden.
  - Wenn Sie die Client-IP-Erhaltung deaktivieren, müssen die Sicherheitsgruppen für die Instances den Datenverkehr von der VPC zulassen. Dies ist die Standardeinstellung.
  - Die folgenden Instance-Typen unterstützen keine Client-IP-Erhaltung: C1, CG1, CG2, G1, HI1, M1, M2, M3 und T1. Wenn Sie die Client-IP-Erhaltung aktivieren und versuchen, mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu einer Instance mit einem dieser Instance-Typen herzustellen, schlägt die Verbindung fehl.
  - Die Beibehaltung der Client-IP wird nicht unterstützt, wenn der Datenverkehr über ein Transit-Gateway geleitet wird.
- Wenn Sie einen EC2 Instance Connect-Endpunkt erstellen, wird automatisch eine serviceverknüpfte Rolle für den Amazon EC2-Service in AWS Identity and Access Management (IAM) erstellt. Amazon EC2 verwendet die serviceverknüpfte Rolle, um Netzwerkschnittstellen in Ihrem Konto bereitzustellen, die beim Erstellen von EC2-Instance-Connect-Endpunkten erforderlich sind. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für EC2-Instance-Connect-Endpunkt.
- Jeder EC2-Instance-Connect-Endpunkt kann bis zu 20 gleichzeitige Verbindungen unterstützen.
- Die maximale Dauer für eine hergestellte TCP-Verbindung beträgt 1 Stunde (3.600 Sekunden). Sie können die maximal zulässige Dauer in einer IAM-Richtlinie angeben, die bis zu 3.600 Sekunden betragen kann. Weitere Informationen finden Sie unter Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instances.
- EC2 Instance Connect Endpoint wird in Canada West (Calgary) nicht unterstützt.

Erteilen Sie Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint

Standardmäßig sind IAM-Entitäten nicht berechtigt, EC2 Instance Connect-Endpoints zu erstellen, zu beschreiben oder zu ändern. Ein IAM-Administrator kann IAM-Richtlinien erstellen, die die für

die Ausführung bestimmter Aktionen mit den benötigten Ressourcen erforderlichen Berechtigungen gewähren.

Informationen zum Erstellen und Bearbeiten von IAM-Richtlinien finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Die folgenden Beispielrichtlinien zeigen, dass Sie die Berechtigungen steuern können, die Benutzer für EC2 Instance Connect Endpoints haben.

Beispiele

- Berechtigungen zum Erstellen, Beschreiben und Löschen von EC2 Instance Connect-Endpoints
- Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instances
- Berechtigungen, nur von einem bestimmten IP-Adressbereich aus eine Verbindung herzustellen

Berechtigungen zum Erstellen, Beschreiben und Löschen von EC2 Instance Connect-Endpoints

Um einen EC2-Instance-Connect-Endpunkt zu erstellen, benötigen Benutzer Berechtigungen für die folgenden Aktionen:

- `ec2:CreateInstanceConnectEndpoint`
- `ec2:CreateNetworkInterface`
- `ec2:CreateTags`
- `iam:CreateServiceLinkedRole`

Um einen EC2-Instance-Connect-Endpunkt zu erstellen, benötigen Benutzer Berechtigungen für die folgenden Aktionen:

- `ec2:DescribeInstanceConnectEndpoints`
- `ec2:DeleteInstanceConnectEndpoint`

Sie können eine Richtlinie erstellen, über die Berechtigungen zum Erstellen, Beschreiben und Löschen von EC2-Instance-Connect-Endpunkten in allen Subnetzen erteilt werden. Alternativ können Sie die Aktionen nur für bestimmte Subnetze einschränken, indem Sie die ARNs der Subnetze als zulässige `Resource` angeben oder den Bedingungsschlüssel `ec2:SubnetID` verwenden. Sie können den `aws:ResourceTag`-Bedingungsschlüssel auch verwenden, um die Erstellung von

Endpunkten mit bestimmten Tags explizit zuzulassen oder zu verweigern. Weitere Informationen finden Sie unter Richtlinien und Berechtigungen in IAM im -IAM-Benutzerhandbuch.

Beispiel für eine IAM-Richtlinie

In der folgenden Beispiel-IAM-Richtlinie erteilt der Abschnitt `Resource` die Berechtigung zum Erstellen und Löschen von Endpunkten in allen Subnetzen, die durch das Sternchen (*) angegeben sind. `ec2:Describe*`-API-Aktionen unterstützen keine Berechtigungen auf Ressourcenebene. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "GrantAllActionsInAllSubnets",
            "Action": [
                "ec2:CreateInstanceConnectEndpoint",
                "ec2:DeleteInstanceConnectEndpoint",
                "ec2:CreateNetworkInterface",
                "ec2:CreateTags",
                "iam:CreateServiceLinkedRole"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:subnet/*"
        },
        {
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:::security-group/*"
        },
        {
            "Sid": "DescribeInstanceConnectEndpoints",
            "Action": [
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instances

Die `ec2-instance-connect:OpenTunnel` Aktion erteilt die Berechtigung, eine TCP-Verbindung zu einer Instance herzustellen, um eine Verbindung über den EC2-Instance-Connect-Endpunkt herzustellen. Sie können den zu verwendenden EC2-Instance-Connect-Endpunkt angeben. Alternativ ermöglicht ein `Resource` mit einem Sternchen (`*`) versehenes Zeichen Benutzern, jeden verfügbaren EC2-Instance-Connect-Endpunkt zu verwenden. Sie können den Zugriff auf Instances auch einschränken, wenn Ressourcen-Tags als Bedingungsschlüssel vorhanden oder nicht vorhanden sind.

Bedingungen

- `ec2-instance-connect:remotePort`— Der Port auf der Instanz, der zum Herstellen einer TCP-Verbindung verwendet werden kann. Wenn dieser Bedingungsschlüssel verwendet wird, führt der Versuch, eine Verbindung zu einer Instance an einem anderen Port als dem in der Richtlinie angegebenen Port herzustellen, zu einem Fehler.
- `ec2-instance-connect:privateIpAddress`— Die private Ziel-IP-Adresse, die der Instance zugeordnet ist, mit der Sie eine TCP-Verbindung aufbauen möchten. Sie können eine einzelne IP-Adresse, z. B. `10.0.0.1/32` oder einen Bereich von IP-Adressen über CIDRs angeben, wie z. B. `10.0.1.0/28`. Wenn dieser Bedingungsschlüssel verwendet wird, führt der Versuch, eine Verbindung zu einer Instance mit einer anderen privaten IP-Adresse oder außerhalb des CIDR-Bereichs herzustellen, zu einem Fehler.
- `ec2-instance-connect:maxTunnelDuration`— Die maximale Dauer einer eingerichteten TCP-Verbindung. Die Einheit ist Sekunden und die Dauer reicht von mindestens 1 Sekunde bis maximal 3 600 Sekunden (1 Stunde). Wenn die Bedingung nicht angegeben ist, ist die Standarddauer auf 3 600 Sekunden (1 Stunde) festgelegt. Der Versuch, länger als die in der IAM-Richtlinie angegebene Dauer oder länger als das Standardmaximum eine Verbindung zu einer Instance herzustellen, führt zu einem Fehler. Die Verbindung wird nach Ablauf der angegebenen Dauer getrennt.

  Wenn `maxTunnelDuration` in der IAM-Richtlinie angegeben ist und der angegebene Wert weniger als 3 600 Sekunden beträgt (Standard), müssen Sie `--max-tunnel-duration` im Befehl angeben, wenn Sie eine Verbindung zu einer Instance herstellen. Weitere Information über das Verbinden mit einer Instance finden Sie unter Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu einer Amazon EC2-Instance Connect.

Sie können einem Benutzer auch Zugriff gewähren, um Verbindungen zu Instances herzustellen, die auf dem Vorhandensein von Ressourcen-Tags auf dem EC2 Instance Connect-Endpunkt basieren. Weitere Informationen finden Sie unter Richtlinien und Berechtigungen in IAM im -IAM-Benutzerhandbuch.

Bei Linux-Instances gewährt die `ec2-instance-connect:SendSSHPublicKey` Aktion die Erlaubnis, den öffentlichen Schlüssel an eine Instance weiterzuleiten. Die `ec2:osuser`-Bedingung gibt den Namen des Betriebssystembenutzers an, der den öffentlichen Schlüssel per Push an die Instance übertragen kann. Verwenden Sie den Standardbenutzernamen für das AMI, mit dem Sie die Instance gestartet haben. Weitere Informationen finden Sie unter Erteilen Sie IAM-Berechtigungen für EC2 Instance Connect.

Beispiel für eine IAM-Richtlinie

Die folgenden Beispiel-IAM-Richtlinien ermöglichen es einem IAM-Prinzipal, eine Connect zu einer Instance herzustellen, indem er nur den angegebenen EC2 Instance Connect-Endpunkt verwendet, der durch die angegebene Endpunkt-ID identifiziert wird. `eice-123456789abcdef` Die Verbindung wird nur erfolgreich hergestellt, wenn alle Bedingungen erfüllt sind.

> **Note**
>
> `ec2:Describe*`-API-Aktionen unterstützen keine Berechtigungen auf Ressourcenebene. Aus diesem Grund ist in der obigen Anweisung der `*`-Platzhalter im `Resource`-Element erforderlich.

Linux

In diesem Beispiel wird ausgewertet, ob die Verbindung zur Instanz auf Port 22 (SSH) hergestellt wurde, ob die private IP-Adresse der Instanz im Bereich von `10.0.1.0/31` (zwischen `10.0.1.0` und`10.0.1.1`) liegt und diese weniger als oder gleich Sekunden `maxTunnelDuration` ist. `3600` Die Verbindung wird nach `3600` Sekunden (1 Stunden) getrennt.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
```

```
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Windows

In diesem Beispiel wird ausgewertet, ob die Verbindung zur Instance auf Port 3389 (RDP) hergestellt wird, ob die private IP-Adresse der Instanz im Bereich von `10.0.1.0/31` (zwischen `10.0.1.0` und`10.0.1.1`) liegt und diese weniger als oder gleich `3600` Sekunden `maxTunnelDuration` ist. Die Verbindung wird nach `3600` Sekunden (1 Stunden) getrennt.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "EC2InstanceConnect",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Effect": "Allow",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "3389"
                },
                "IpAddress": {
                    "ec2-instance-connect:privateIpAddress": "10.0.1.0/31"
                },
                "NumericLessThanEquals": {
                    "ec2-instance-connect:maxTunnelDuration": "3600"
                }
            }
        },
        {
            "Sid": "Describe",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

Berechtigungen, nur von einem bestimmten IP-Adressbereich aus eine Verbindung herzustellen

Die folgende Beispiel-IAM-Richtlinie ermöglicht es einem IAM-Prinzipal, eine Verbindung zu einer Instance herzustellen, sofern er von einer IP-Adresse innerhalb des in der Richtlinie angegebenen IP-Adressbereichs aus eine Verbindung herstellt. Wenn der IAM-Prinzipal `OpenTunnel` von einer IP-Adresse aus anruft, die sich außerhalb des IP-Adressbereichs befindet `192.0.2.0/24` (der Beispiel-IP-Adressbereich in dieser Richtlinie), lautet `Access Denied` die Antwort. Weitere Informationen finden Sie unter `aws:SourceIp` im IAM-Benutzerhandbuch.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": "ec2-instance-connect:OpenTunnel",
            "Resource": "arn:aws:ec2:region:account-id:instance-connect-
endpoint/eice-123456789abcdef",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NumericEquals": {
                    "ec2-instance-connect:remotePort": "22"
                }
            }
        },
        {
            "Sid": "SSHPublicKey",
            "Effect": "Allow",
            "Action": "ec2-instance-connect:SendSSHPublicKey",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "ec2:osuser": "ami-username"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceConnectEndpoints"
            ],
            "Resource": "*"
        }
    ]
}
```

Sicherheitsgruppen für EC2-Instance-Connect-Endpunkt

Eine Sicherheitsgruppe steuert den Datenverkehr, der die Ressourcen erreichen und verlassen darf, mit denen er verknüpft ist. Beispielsweise verweigern wir den Datenverkehr zu und von einer

Amazon EC2 EC2-Instance, sofern er nicht ausdrücklich von den mit der Instance verknüpften Sicherheitsgruppen zugelassen wird.

Die folgenden Beispiele zeigen Ihnen, wie Sie die Sicherheitsgruppenregeln für den EC2 Instance Connect Endpoint und die Ziel-Instances konfigurieren.

Beispiele

- EC2 Instance Connect Endpoint Sicherheitsgruppenregeln
- Regeln für Sicherheitsgruppen der Zielinstanz

EC2 Instance Connect Endpoint Sicherheitsgruppenregeln

Die Sicherheitsgruppenregeln für einen EC2 Instance Connect-Endpunkt müssen zulassen, dass ausgehender Datenverkehr, der für die Ziel-Instances bestimmt ist, den Endpunkt verlässt. Sie können entweder die Instanz-Sicherheitsgruppe oder den IPv4-Adressbereich der VPC als Ziel angeben.

Der Datenverkehr zum Endpunkt stammt vom EC2 Instance Connect Endpoint Service und ist unabhängig von den Regeln für eingehende Nachrichten für die Endpunkt-Sicherheitsgruppe zulässig. Verwenden Sie eine IAM-Richtlinie, um zu steuern, wer EC2 Instance Connect Endpoint verwenden kann, um eine Verbindung zu einer Instance herzustellen. Weitere Informationen finden Sie unter Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instances.

Beispiel für eine ausgehende Regel: Referenzierung von Sicherheitsgruppen

Im folgenden Beispiel wird auf Sicherheitsgruppen verwiesen, was bedeutet, dass das Ziel eine Sicherheitsgruppe ist, die den Zielinstanzen zugeordnet ist. Diese Regel erlaubt ausgehenden Datenverkehr vom Endpunkt zu allen Instances, die diese Sicherheitsgruppe verwenden.

Protokoll	Bestimmungsort	Port-Bereich	Kommentar
TCP	*ID der Instanz-Sicherheitsgruppe*	22	Erlaubt ausgehenden SSH-Verkehr zu allen Instances, die der Instanz-Sicherheitsgruppe zugeordnet sind

Beispiel für eine ausgehende Regel: IPv4-Adressbereich

Das folgende Beispiel erlaubt ausgehenden Datenverkehr in den angegebenen IPv4-Adressbereich. Die IPv4-Adressen einer Instance werden von ihrem Subnetz aus zugewiesen, sodass Sie den IPv4-Adressbereich der VPC verwenden können.

Protokoll	Bestimmungsort	Port-Bereich	Kommentar
TCP	*VPC - IPv4 CIDR*	22	Erlaubt ausgehenden SSH-Verkehr zur VPC

Regeln für Sicherheitsgruppen der Zielinstanz

Die Sicherheitsgruppenregeln für Ziel-Instances müssen eingehenden Datenverkehr vom EC2 Instance Connect-Endpunkt zulassen. Sie können entweder die Endpunkt-Sicherheitsgruppe oder einen IPv4-Adressbereich als Quelle angeben. Wenn Sie einen IPv4-Adressbereich angeben, hängt die Quelle davon ab, ob die Client-IP-Aufbewahrung aus- oder aktiviert ist. Weitere Informationen finden Sie unter Überlegungen.

Da Sicherheitsgruppen statusbehaftet sind, darf der Antwortdatenverkehr die VPC unabhängig von den ausgehenden Regeln für die Instanz-Sicherheitsgruppe verlassen.

Beispiel für eine Regel für eingehenden Datenverkehr: Referenzierung von Sicherheitsgruppen

Im folgenden Beispiel wird auf Sicherheitsgruppen verwiesen, was bedeutet, dass die Quelle die Sicherheitsgruppe ist, die dem Endpunkt zugeordnet ist. Diese Regel erlaubt eingehenden SSH-Verkehr vom Endpunkt zu allen Instances, die diese Sicherheitsgruppe verwenden, unabhängig davon, ob die Client-IP-Erhaltung aktiviert oder deaktiviert ist. Wenn es keine anderen Regeln für eingehende Sicherheitsgruppen für SSH gibt, akzeptieren die Instances nur SSH-Verkehr vom Endpunkt.

Protokoll	Quelle	Port-Bereich	Kommentar
TCP	*ID der Endpunkt-Sicherheitsgruppe*	22	Lässt eingehenden SSH-Verkehr von den Ressourcen zu, die der Endpunktsicherheitsgruppe zugeordnet sind

Beispiel für eine Regel für eingehenden Datenverkehr: Client-IP-Erhaltung aus

Das folgende Beispiel erlaubt eingehenden SSH-Verkehr aus dem angegebenen IPv4-Adressbereich. Da die Client-IP-Erhaltung deaktiviert ist, ist die IPv4-Quelladresse die Adresse der Endpunkt-Netzwerkschnittstelle. Die Adresse der Endpunkt-Netzwerkschnittstelle wird von ihrem Subnetz aus zugewiesen, sodass Sie den IPv4-Adressbereich der VPC verwenden können, um Verbindungen zu allen Instances in der VPC zuzulassen.

Protokoll	Quelle	Port-Bereich	Kommentar
TCP	*VPC – IPv4 CIDR*	22	Lässt eingehenden SSH-Verkehr von der VPC zu

Beispiel für eine Regel für eingehenden Datenverkehr: Client-IP-Erhaltung aktiviert

Das folgende Beispiel erlaubt eingehenden SSH-Verkehr aus dem angegebenen IPv4-Adressbereich. Da die Client-IP-Erhaltung aktiviert ist, ist die IPv4-Quelladresse die Adresse des Clients.

Protokoll	Quelle	Port-Bereich	Kommentar
TCP	*Öffentlicher IPv4-Adressbereich*	22	Lässt eingehenden Datenverkehr aus dem angegebenen IPv4-Adressbereich des Clients zu

Erstellen Sie einen EC2-Instance-Connect-Endpunkt

Sie können einen EC2 Instance Connect-Endpunkt erstellen, um eine sichere Verbindung zu Ihren Instances zu ermöglichen.

Sie können einen EC2 Instance Connect-Endpunkt nicht mehr ändern, nachdem Sie ihn erstellt haben. Stattdessen müssen Sie den EC2 Instance Connect-Endpunkt löschen und einen neuen mit den benötigten Einstellungen erstellen.

Voraussetzungen

Sie müssen über die erforderlichen IAM-Berechtigungen verfügen, um einen EC2-Instance-Connect-Endpunkt zu erstellen. Weitere Informationen finden Sie unter Berechtigungen zum Erstellen, Beschreiben und Löschen von EC2 Instance Connect-Endpoints.

Gemeinsam genutzte Subnetze

Sie können einen EC2 Instance Connect-Endpunkt in einem Subnetz erstellen, das mit Ihnen gemeinsam genutzt wird. Sie können keinen EC2 Instance Connect-Endpoint verwenden, den der VPC-Besitzer in einem Subnetz erstellt hat, das mit Ihnen gemeinsam genutzt wird.

Erstellen Sie den Endpunkt mithilfe der Konsole

Gehen Sie wie folgt vor, um einen EC2 Instance Connect-Endpoint zu erstellen.

So erstellen Sie einen EC2-Instance-Connect-Endpunkt

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich die Option Endpoints (Endpunkte) aus.
3. Wählen Sie Create Endpoint aus und geben Sie dann die Endpunkteinstellungen wie folgt an:
   a. (Optional) Geben Sie unter Namens-Tag einen Namen für den Endpunkt ein.
   b. Wählen Sie als Servicekategorie EC2-Instance-Connect-Endpunkt aus.
   c. Wählen Sie für VPC die VPC mit den Ziel-Instances aus.
   d. (Optional) Um Client-IP-Adressen beizubehalten, erweitern Sie Zusätzliche Einstellungen und aktivieren Sie das Kontrollkästchen. Andernfalls wird standardmäßig die Netzwerkschnittstelle des Endpunkts als Client-IP-Adresse verwendet.
   e. (Optional) Wählen Sie für Sicherheitsgruppen die VPC-Sicherheitsgruppe aus, die der Option zugeordnet werden soll. Andernfalls wird standardmäßig die Standardsicherheitsgruppe für die VPC verwendet. Weitere Informationen finden Sie unter Sicherheitsgruppen für EC2-Instance-Connect-Endpunkt.
   f. Wählen Sie für Subnetz das Subnetz aus, in dem der Endpunkt erstellt werden soll.
   g. (Optional) Sie fügen ein Tag hinzu, indem Sie neuen Tag hinzufügen auswählen und den Schlüssel und den Wert für den Tag eingeben.
4. Überprüfen Sie Ihre Einstellungen und wählen Sie dann Endpunkt erstellen.

   Der ursprüngliche Status des Endpunkts lautet Ausstehend. Bevor Sie über diesen Endpunkt eine Verbindung zu einer Instance herstellen können, müssen Sie warten, bis der Endpunktstatus Verfügbar lautet. Dies kann einige Minuten dauern.
5. Informationen zum Herstellen einer Verbindung mit einer Instance, die Ihren Endpunkt verwendet, finden Sie unterHerstellen einer Verbindung zu einer -Instance.

Erstellen Sie den Endpunkt mit AWS CLI

Verwenden Sie den create-instance-connect-endpoint-Befehl. AWS CLI

Voraussetzungen

Installieren Sie AWS CLI Version 2 und konfigurieren Sie sie mit Ihren Anmeldeinformationen. Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von AWS CLI und Konfigurieren von AWS CLI im AWS Command Line Interface Benutzerhandbuch. Alternativ können Sie AWS CLI Befehle in der vorauthentifizierten Shell öffnen AWS CloudShell und ausführen.

So erstellen Sie den Endpunkt

Verwenden Sie den folgenden Befehl, um eine Endpunkt-Netzwerkschnittstelle für Ihren EC2 Instance Connect-Endpunkt im angegebenen Subnetz zu erstellen.

```
aws ec2 create-instance-connect-endpoint --subnet-id subnet-0123456789example
```

Es folgt eine Beispielausgabe.

```
 {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "create-complete",
        "StateMessage": "",
        "DnsName": "eice-0123456789example.0123abcd.ec2-instance-connect-endpoint.us-
east-1.amazonaws.com",
        "FipsDnsName": "eice-0123456789example.0123abcd.fips.ec2-instance-connect-
endpoint.us-east-1.amazonaws.com",
        "NetworkInterfaceIds": [
            "eni-0123abcd"
        ],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1a",
        "CreatedAt": "2023-04-07T15:43:53.000Z"
        "SubnetId": "subnet-0123abcd",
        "PreserveClientIp": false,
        "SecurityGroupIds": [
```

```
            "sg-0123abcd"
        ],
        "Tags": []
}
```

Um den Erstellungsstatus zu überwachen

Der Anfangswert für das `State`-Feld ist `create-in-progress`. Bevor Sie über diesen Endpunkt eine Verbindung zu einer Instance herstellen können, warten Sie, bis der Status `create-complete` lautet. Verwenden Sie den describe-instance-connect-endpoints AWS CLI Befehl, um den Status des EC2 Instance Connect-Endpunkts zu überwachen. Der Parameter --query filtert die Ergebnisse nach dem `State` Feld.

```
aws ec2 describe-instance-connect-endpoints --instance-connect-endpoint-
ids eice-0123456789example --query InstanceConnectEndpoints[*].State --output text
```

Es folgt eine Beispielausgabe.

```
create-complete
```

Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu einer Amazon EC2-Instance Connect

Sie können EC2 Instance Connect Endpoint verwenden, um eine Verbindung zu einer Amazon EC2 EC2-Instance herzustellen, die SSH oder RDP unterstützt.

Inhalt

Voraussetzungen

- Sie müssen über die erforderlichen IAM-Berechtigungen verfügen, um einen EC2-Instance-Connect-Endpunkt zu erstellen. Weitere Informationen finden Sie unter Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint zum Herstellen einer Verbindung zu Instances.
- Um eine Verbindung zu einer Instance herzustellen, muss der Endpunktstatus Verfügbar (Konsole) oder `create-complete` (AWS CLI) sein. Wenn Sie keinen EC2 Instance Connect-Endpunkt für

Ihre VPC haben, können Sie einen erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen EC2-Instance-Connect-Endpunkt.

- (Linux-Instances) Um die EC2-Konsole zu verwenden, um eine Verbindung zu Ihrer Instance herzustellen, oder um die CLI zu verwenden, um eine Verbindung herzustellen und EC2 Instance Connect den kurzlebigen Schlüssel verarbeiten zu lassen, muss auf Ihrer Instance EC2 Instance Connect installiert sein. Weitere Informationen finden Sie unter Installieren Sie EC2 Instance Connect.
- Stellen Sie sicher, dass die Sicherheitsgruppe der Instance eingehenden SSH-Verkehr vom EC2 Instance Connect-Endpunkt zulässt. Weitere Informationen finden Sie unter Regeln für Sicherheitsgruppen der Zielinstanz.

Verbinden Sie sich mit Ihrer Linux-Instance über die Amazon-EC2-Konsole

Sie können über die Amazon EC2 EC2-Konsole wie folgt eine Verbindung zu einer Instance herstellen.

So stellen Sie mithilfe des browserbasierten Clients eine Verbindung zu Ihrer Instance her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instanz aus und wählen Sie Connect.
4. Wählen Sie die Registerkarte EC2 Instance Connect aus.
5. Wählen Sie als Verbindungstyp Verbinden mit EC2-Instance-Connect-Endpunkt aus.
6. Wählen Sie für EC2 Instance Connect Endpoint die ID des EC2 Instance Connect-Endpunkts.
7. Wenn das AMI, das Sie zum Starten der Instance verwendet haben, einen anderen Benutzernamen als verwendet`ec2-user`, geben Sie unter Benutzername den richtigen Benutzernamen ein.
8. Geben Sie für Max. Tunneldauer (Sekunden) die maximal zulässige Dauer für die SSH-Verbindung ein.

   Die Dauer muss allen in der IAM-Richtlinie angegebenen `maxTunnelDuration` Bedingungen entsprechen. Wenn Sie keinen Zugriff auf die IAM-Richtlinie haben, wenden Sie sich an Ihren Administrator.
9. Wählen Sie Connect aus. Dadurch wird ein Terminalfenster für Ihre Instance geöffnet.

Herstellen einer Verbindung zu Ihrer Linux-Instance mit SSH

Sie können SSH verwenden, um eine Verbindung zu Ihrer Linux-Instance herzustellen, und den `open-tunnel`-Befehl verwenden, um einen privaten Tunnel einzurichten. Sie können `open-tunnel` im Einzelverbindungsmodus oder im Mehrfachverbindungsmodus verwenden.

Informationen zur Verwendung von AWS CLI , um über SSH eine Verbindung zu Ihrer Instance herzustellen, finden Sie unterConnect mit dem her AWS CLI.

Im folgenden Beispiel wird OpenSSH verwendet. Sie können jeden anderen SSH-Client verwenden, der einen Proxy-Modus unterstützt.

Einzelne -Verbindung

So erlauben Sie nur eine einzige Verbindung zu einer Instance über SSH und den Befehl **`open-tunnel`**

Verwenden Sie `ssh` und den open-tunnel AWS CLI Befehl wie folgt. Der `-o`-Proxy-Befehl umfasst den `open-tunnel`-Befehl, der den privaten Tunnel zur Instance erstellt.

```
ssh -i my-key-pair.pem ec2-user@i-0123456789example \
    -o ProxyCommand='aws ec2-instance-connect open-tunnel --instance-
id i-0123456789example'
```

Für:

- `-i` – Geben Sie das Schlüsselpaar an, das zum Starten der Instance verwendet wurde.
- *`ec2-user`*`@`*`i-0123456789example`* – Geben Sie den Benutzernamen des AMI an, das zum Starten der Instance verwendet wurde, und die Instance-ID.
- `--instance-id` – Geben Sie die ID der Instance, zu der eine Verbindung hergestellt werden soll, an. Alternativ können Sie auch `%h` angeben, wodurch die Instance-ID des Benutzers extrahiert wird.

Mehrfachverbindung

Um mehrere Verbindungen zu einer Instance zuzulassen, führen Sie zuerst den open-tunnel AWS CLI Befehl aus, um auf neue TCP-Verbindungen zu warten, und verwenden Sie ihn dann, `ssh` um eine neue TCP-Verbindung und einen privaten Tunnel zu Ihrer Instance zu erstellen.

So erlauben Sie mehrere Verbindungen zu Ihrer Instance mit SSH und dem Befehl **`open-tunnel`**

1. Führen Sie den folgenden Befehl aus, um auf Ihrem lokalen Computer auf neue TCP-Verbindungen am angegebenen Port zu horchen.

```
aws ec2-instance-connect open-tunnel \
    --instance-id i-0123456789example \
    --local-port 8888
```

   Erwartete Ausgabe

```
Listening for connections on port 8888.
```

2. Führen Sie in einem neuen Terminalfenster den folgenden `ssh`-Befehl aus, um eine neue TCP-Verbindung und einen privaten Tunnel zu Ihrer Instance zu erstellen.

```
ssh -i my-key-pair.pem ec2-user@localhost -p 8888
```

   Erwartete Ausgabe – Im ersten Terminalfenster sehen Sie Folgendes:

```
[1] Accepted new tcp connection, opening websocket tunnel.
```

   Möglicherweise wird auch Folgendes angezeigt:

```
[1] Closing tcp connection.
```

Connect zu Ihrer Linux-Instance her, indem Sie AWS CLI

Wenn Sie nur Ihre Instance-ID kennen, können Sie den AWS CLI Befehl ec2-instance-connect verwenden, um über einen SSH-Client eine Verbindung zu Ihrer Instance herzustellen. Weitere Hinweise zur Verwendung des Befehls ec2-instance-connect finden Sie unter. Connect mit dem her AWS CLI

Voraussetzungen

Installieren Sie AWS CLI Version 2 und konfigurieren Sie sie mit Ihren Anmeldeinformationen. Weitere Informationen finden Sie unter Installieren oder Aktualisieren auf die neueste Version von AWS CLI und Konfigurieren von AWS CLI im AWS Command Line Interface Benutzerhandbuch.

Alternativ können Sie AWS CLI Befehle in der vorauthentifizierten Shell öffnen AWS CloudShell und ausführen.

So stellen Sie eine Verbindung zu einer Instance über die Instance-ID und einen EC2-Instance-Connect-Endpunkt her

Wenn Sie nur die Instanz-ID kennen, verwenden Sie den CLI-Befehl ec2-instance-connect und geben Sie den `ssh` Befehl, die Instanz-ID und den `--connection-type` Parameter mit dem Wert an. `eice`

```
aws ec2-instance-connect ssh --instance-id i-1234567890example --connection-type eice
```

> **Tip**
>
> Wenn Sie bei der Verwendung dieses Befehls eine Fehlermeldung erhalten, stellen Sie sicher, dass Sie Version 2 verwenden. AWS CLI Der `ssh` Parameter ist nur in AWS CLI Version 2 verfügbar. Weitere Informationen finden Sie unter Über AWS CLI Version 2 im AWS Command Line Interface Benutzerhandbuch.

Stellen Sie mithilfe von EC2 Instance Connect Endpoint eine Verbindung zu Ihrer Windows-Instance her

Sie können Remote Desktop Protocol (RDP) über den EC2-Instance-Connect-Endpunkt verwenden, um eine Verbindung zu einer Windows-Instance ohne öffentliche IPv4-Adresse oder öffentlichen DNS-Namen herzustellen.

Verwenden Sie einen RDP Client, um sich mit Ihrer Windows-Instance zu verbinden.

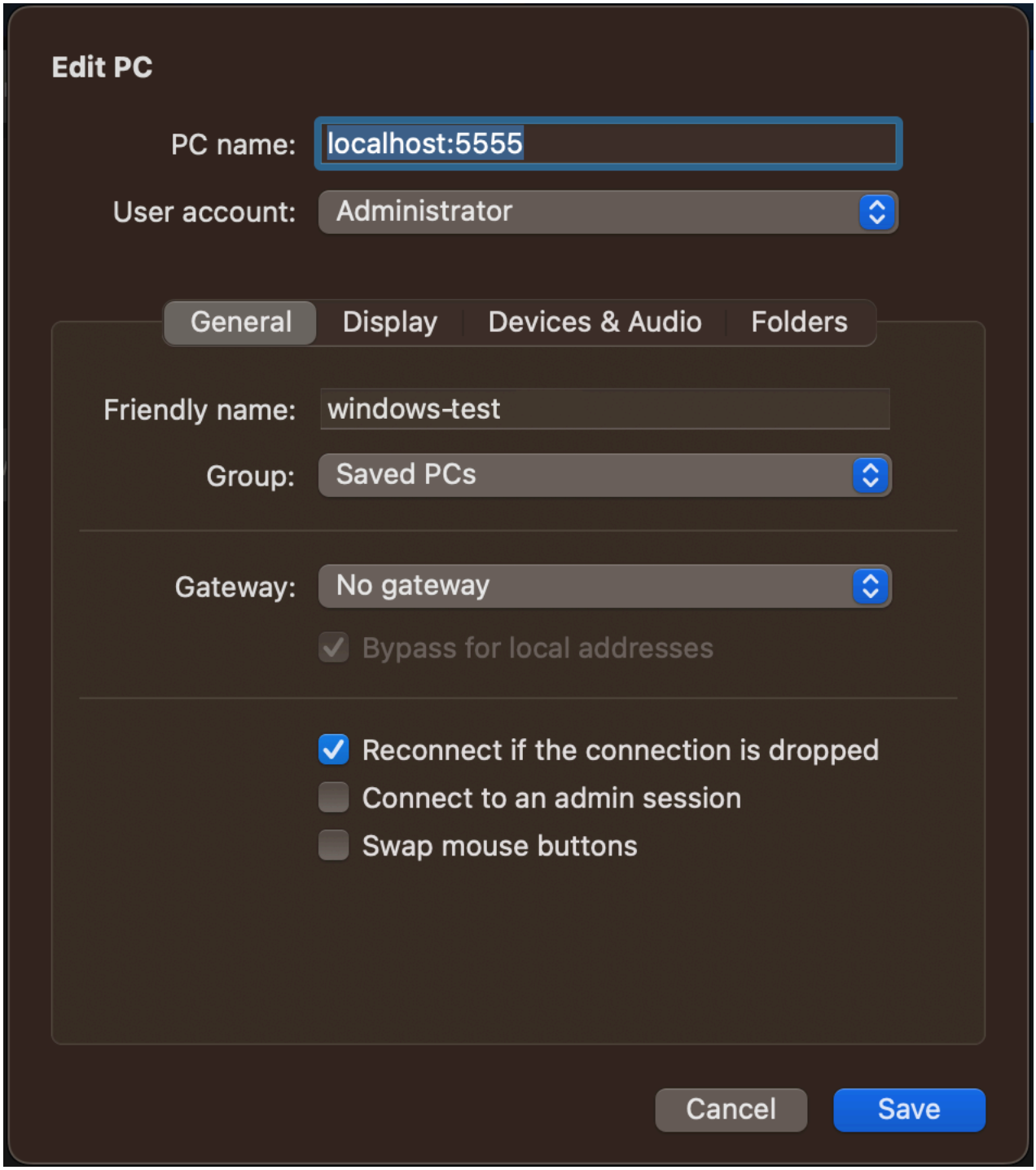
1. Führen Sie die Schritte 1 bis 8 unter Connect Ihrer Windows-Instanz mithilfe von RDP herstellen aus. Nachdem Sie die RDP-Desktop-Datei in Schritt 8 heruntergeladen haben, erhalten Sie die Meldung Es konnte keine Verbindung hergestellt werden. Dies ist zu erwarten, da Ihre Instanz keine öffentliche IP-Adresse hat.
2. Führen Sie den folgenden Befehl aus, um einen privaten Tunnel zu der VPC einzurichten, in der sich die Instance befindet. `--remote-port` muss `3389` sein, weil RDP standardmäßig Port 3389 verwendet.

   ```
   aws ec2-instance-connect open-tunnel \
   ```

```
    --instance-id i-0123456789example \
    --remote-port 3389 \
    --local-port any-port
```

3. Suchen Sie in Ihrem Downloads-Ordner nach der RDP-Desktop-Datei, die Sie heruntergeladen haben, und ziehen Sie sie in das RDP-Clientfenster.
4. Klicken Sie mit der rechten Maustaste auf die RDP-Datei und wählen Sie Bearbeiten aus.
5. Geben Sie im Fenster PC bearbeiten als PC-Namen (die Instanz, zu der eine Verbindung hergestellt werden soll) den Wert where `local-port` uses the same value ein`localhost:local-port`, den Sie in Schritt 2 angegeben haben, und wählen Sie dann Save aus.

   Beachten Sie, dass der folgende Screenshot des Fensters PC bearbeiten von Microsoft Remote Desktop auf einem Mac stammt. Wenn Sie einen Windows-Client verwenden, sieht das Fenster eventuell anders aus.



6. Klicken Sie im RDP-Client mit der rechten Maustaste auf den PC (den Sie gerade konfiguriert haben) und wählen Sie Verbinden, um eine Verbindung zu Ihrer Instance herzustellen.
7. Geben Sie an der Eingabeaufforderung das unverschlüsselte Passwort für das Administratorkonto ein.

Fehlerbehebung

Nutzen Sie die folgenden Informationen, um Probleme zu diagnostizieren und zu beheben, die auftreten können, wenn EC2-Instance-Connect-Endpunkt zum Herstellen von Verbindungen mit einer Instance verwendet wird.

Kann nicht zu Ihrer Instance verbinden

Nachfolgend finden Sie die häufigsten Gründe, warum Sie möglicherweise keine Verbindung zu Ihrer Instance herstellen können.

- Sicherheitsgruppen – Überprüfen Sie die Sicherheitsgruppen, die dem EC2-Instance-Connect-Endpunkt und Ihrer Instance zugewiesen sind. Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppen für EC2-Instance-Connect-Endpunkt.
- Instance-Status – Stellen Sie sicher, dass sich Ihre Instance im `running`-Status befindet.
- Schlüsselpaar – Wenn der Befehl, den Sie zum Herstellen einer Verbindung verwenden, einen privaten Schlüssel erfordert, stellen Sie sicher, dass Ihre Instance über einen öffentlichen Schlüssel verfügt und dass Sie über den entsprechenden privaten Schlüssel verfügen.
- IAM-Berechtigungen – Stellen Sie sicher, dass Sie über die erforderlichen IAM-Berechtigungen verfügen. Weitere Informationen finden Sie unter Erteilen Sie Berechtigungen zur Verwendung von EC2 Instance Connect Endpoint.

Weitere Tipps zur Fehlerbehebung für Linux-Instances finden Sie unterProblembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance. Tipps zur Problembehandlung für Windows-Instanzen finden Sie unterthe section called “Herstellen einer Verbindung mit Ihrer -Windows-Instance”.

ErrorCode: AccessDeniedException

Wenn Sie einen `AccessDeniedException`-Fehler erhalten und die `maxTunnelDuration`-Bedingung in der IAM-Richtlinie angegeben ist, geben Sie den `--max-tunnel-duration`-Parameter unbedingt an, wenn Sie eine Verbindung zu einer Instance herstellen. Weitere Informationen zu Parametern finden Sie unter open-tunnel in der AWS CLI - Befehlsreferenz.

Protokollverbindungen, die über EC2-Instance-Connect-Endpunkt hergestellt wurden

Sie können Ressourcenoperationen protokollieren und Verbindungen, die über den EC2 Instance Connect-Endpunkt hergestellt wurden, mit AWS CloudTrail Protokollen überprüfen.

Weitere Informationen zur Verwendung AWS CloudTrail mit Amazon EC2 finden Sie unterAmazon EC2 EC2-API-Aufrufe protokollieren mit AWS CloudTrail.

EC2 Instance Connect Endpoint API-Aufrufe protokollieren mit AWS CloudTrail

EC2 Instance Connect Endpoint-Ressourcenoperationen werden CloudTrail als Verwaltungsereignisse protokolliert. Wenn die folgenden API-Aufrufe getätigt werden, wird die Aktivität als CloudTrail Ereignis im Ereignisverlauf aufgezeichnet:

- `CreateInstanceConnectEndpoint`
- `DescribeInstanceConnectEndpoints`
- `DeleteInstanceConnectEndpoint`

Sie können aktuelle Ereignisse in Ihrem anzeigen, suchen und herunterladen AWS-Konto. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Verwenden Sie AWS CloudTrail , um Benutzer zu prüfen, die sich über den EC2-Instance-Connect-Endpunkt mit einer Instance verbinden

Verbindungsversuche zu Instances über den EC2 Instance Connect Endpoint werden CloudTrail im Ereignisverlauf protokolliert. Wenn eine Verbindung zu einer Instance über einen EC2 Instance Connect-Endpunkt initiiert wird, wird die Verbindung als CloudTrail Verwaltungsereignis mit dem Wert `eventName` of `OpenTunnel` protokolliert.

Sie können EventBridge Amazon-Regeln erstellen, die das CloudTrail Ereignis an ein Ziel weiterleiten. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Im Folgenden finden Sie ein Beispiel für ein `OpenTunnel` Verwaltungsereignis, das angemeldet wurde CloudTrail.


```
{
     "eventVersion": "1.08",
     "userIdentity": {
         "type": "IAMUser",
         "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
         "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
         "accountId": "123456789012",
         "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
         "userName": "IAM-friendly-name"
     },
```

```
     "eventTime": "2023-04-11T23:50:40Z",
     "eventSource": "ec2-instance-connect.amazonaws.com",
     "eventName": "OpenTunnel",
     "awsRegion": "us-east-1",
     "sourceIPAddress": "1.2.3.4",
     "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
     "requestParameters": {
         "instanceConnectEndpointId": "eici-0123456789EXAMPLE",
         "maxTunnelDuration": "3600",
         "remotePort": "22",
         "privateIpAddress": "10.0.1.1"
     },
     "responseElements": null,
     "requestID": "98deb2c6-3b3a-437c-a680-03c4207b6650",
     "eventID": "bbba272c-8777-43ad-91f6-c4ab1c7f96fd",
     "readOnly": false,
     "resources": [{
         "accountId": "123456789012",
         "type": "AWS::EC2::InstanceConnectEndpoint",
         "ARN": "arn:aws:ec2:us-east-1:123456789012:instance-connect-endpoint/
eici-0123456789EXAMPLE"
     }],
     "eventType": "AwsApiCall",
     "managementEvent": true,
     "recipientAccountId": "123456789012",
     "eventCategory": "Management"
}
```


Löschen Sie einen EC2 Instance Connect-Endpunkt

Wenn Sie mit einem EC2 Instance Connect-Endpoint fertig sind, können Sie ihn löschen.

Sie müssen über die erforderlichen IAM-Berechtigungen verfügen, um einen EC2-Instance-Connect-Endpunkt zu erstellen. Weitere Informationen finden Sie unter Berechtigungen zum Erstellen, Beschreiben und Löschen von EC2 Instance Connect-Endpoints.

Wenn Sie einen EC2 Instance Connect-Endpoint mithilfe der Konsole löschen, wechselt er in den Status Löschen. Wenn der Löschvorgang erfolgreich ist, wird der gelöschte Endpunkt nicht mehr angezeigt. Wenn das Löschen fehlschlägt, lautet der Status `delete-failed` und die Statusmeldung gibt den Grund für den Fehler an.

Wenn Sie einen EC2 Instance Connect-Endpoint mit dem löschen AWS CLI, wechselt er in den `delete-in-progress` Status. Wenn der Löschvorgang erfolgreich ist, wechselt er in den

`delete-complete` Status. Schlägt der Löschvorgang fehl, lautet der Status `delete-failed` und `StateMessage` gibt den Grund für den Fehler an.

Console

Wie Sie einen EC2-Instance-Connect-Endpunkt löschen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im linken Navigationsbereich die Option Endpoints (Endpunkte) aus.
3. Wählen Sie den Endpunkt.
4. Wählen Sie Actions (Aktionen), Delete VPC Endpoint (VPC-Endpunkte löschen).
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein.
6. Wählen Sie Löschen.

AWS CLI

Wie Sie einen EC2-Instance-Connect-Endpunkt löschen

Verwenden Sie den delete-instance-connect-endpoints AWS CLI Befehl und geben Sie die ID des zu löschenden EC2 Instance Connect-Endpunkts an.

```
aws ec2 delete-instance-connect-endpoint --instance-connect-endpoint-
id eice-03f5e49b83924bbc7
```

Beispielausgabe

```
{
    "InstanceConnectEndpoint": {
        "OwnerId": "111111111111",
        "InstanceConnectEndpointId": "eice-0123456789example",
        "InstanceConnectEndpointArn": "arn:aws:ec2:us-east-1:111111111111:instance-
connect-endpoint/eice-0123456789example",
        "State": "delete-in-progress",
        "StateMessage": "",
        "NetworkInterfaceIds": [],
        "VpcId": "vpc-0123abcd",
        "AvailabilityZone": "us-east-1d",
        "CreatedAt": "2023-02-07T12:05:37+00:00",
        "SubnetId": "subnet-0123abcd"
```

```
    }
}
```

Serviceverknüpfte Rolle für EC2-Instance-Connect-Endpunkt

Amazon EC2 verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon EC2 verknüpft ist. Servicebezogene Rollen sind von Amazon EC2 vordefiniert und enthalten alle erforderlichen Berechtigungen, damit Amazon EC2 andere AWS-Services in Ihrem Namen anrufen kann. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im -IAM-Benutzerhandbuch.

Dienstbezogene Rollenberechtigungen für EC2 Instance Connect Endpoint

Amazon EC2 verwendet AWSServiceRoleForEC2InstanceConnect, um Netzwerkschnittstellen in Ihrem Konto zu erstellen und zu verwalten, die für EC2 Instance Connect Endpoint erforderlich sind.

Die AWSServiceRoleForEC2InstanceConnectserviceverknüpfte Rolle vertraut darauf, dass die folgenden Dienste die Rolle übernehmen:

- `ec2-instance-connect.amazonaws.com`

Die AWSServiceRoleForEC2InstanceConnectdienstverknüpfte Rolle verwendet die verwaltete Richtlinie Ec2 Endpoint. InstanceConnect Die Berechtigungen für diese Richtlinie finden Sie unter Ec2 InstanceConnect Endpoint in der Referenz für AWS verwaltete Richtlinien.

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für den EC2 Instance Connect Endpoint erstellen

Sie müssen die serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie einen EC2 Instance Connect-Endpunkt erstellen, erstellt Amazon EC2 die serviceverknüpfte Rolle für Sie.

Bearbeiten Sie eine serviceverknüpfte Rolle für den EC2 Instance Connect Endpoint

Mit EC2 Instance Connect Endpoint können Sie die AWSServiceRoleForEC2InstanceConnectserviceverknüpfte Rolle nicht bearbeiten.

Löschen Sie eine serviceverknüpfte Rolle für den EC2 Instance Connect Endpoint

Wenn Sie EC2 Instance Connect Endpoint nicht mehr verwenden müssen, empfehlen wir Ihnen, die AWSServiceRoleForEC2InstanceConnectserviceverknüpfte Rolle zu löschen.

Sie müssen alle EC2 Instance Connect Endpoint-Ressourcen löschen, bevor Sie die serviceverknüpfte Rolle löschen können.

Informationen zum Löschen der serviceverknüpften Rolle finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Kontingente für den EC2 Instance Connect-Endpunkt

Ihr AWS-Konto hat Standardkontingente, früher als Limits bezeichnet, für jeden AWS Dienst. Wenn nicht anders angegeben, gilt jedes Kontingent spezifisch für eine Region.

Ihr AWS-Konto hat die folgenden Kontingente in Bezug auf den EC2 Instance Connect Endpoint.

Beschreibung	Kontingent
Maximale Anzahl von EC2 Instance Connect-Endpunkten pro AWS-Konto AWS-Region	5
Maximale Anzahl von EC2 Instance Connect Endpoints pro VPC	1
Maximale Anzahl von EC2 Instance Connect Endpoints pro Subnetz	1
Maximale Anzahl gleichzeitiger Verbindungen pro EC2 Instance Connect-Endpunkt	20

Verbinden Ihrer EC2-Instance mit einer AWS -Ressource

Nachdem Sie eine Instance gestartet haben, können Sie sie mit einer oder mehreren AWS Ressourcen verbinden.

In diesem Abschnitt wird beschrieben, wie Sie eine Amazon-EC2-Instance automatisch mit einer Amazon-RDS-Datenbank verbinden.

Automatisches Verbinden einer EC2-Instance mit einer RDS-Datenbank

Sie können die automatische Verbindungsfunktion in der Amazon-EC2-Konsole verwenden, um eine oder mehrere EC2-Instances schnell mit einer RDS-Datenbank zu verbinden, um Datenverkehr zwischen ihnen zuzulassen.

Weitere Informationen finden Sie unter So wird die Verbindung automatisch konfiguriert. Eine ausführliche exemplarische Vorgehensweise, die weitere Möglichkeiten zum Verbinden einer EC2-Instance und einer RDS-Datenbank enthält, finden Sie unter Tutorial: Verbinden einer Amazon-EC2-Instance mit einer Amazon-RDS-Datenbank.

Themen

Kosten

Es fallen zwar keine Gebühren für die automatische Verbindung Ihrer EC2-Instance mit einer RDS-Datenbank an, die zugrunde liegenden Services werden Ihnen jedoch in Rechnung gestellt. Datenübertragungsgebühren fallen an, wenn sich Ihre EC2-Instance und Ihre RDS-Datenbank in unterschiedlichen Availability Zones befinden. Weitere Informationen zu den Datenübertragungsgebühren finden Sie unter Datenübertragung auf der Seite Amazon-EC2-On-Demand-Preise.

Voraussetzungen

Bevor Sie eine EC2-Instance automatisch mit einer RDS-Datenbank verbinden können, überprüfen Sie Folgendes:

- Die EC2-Instances müssen sich im Status Running (Ausgeführt) befinden. Sie können eine EC2-Instance nicht verbinden, wenn sie sich in einem anderen Status befindet.
- Die EC2-Instances und die RDS-Datenbank müssen sich in derselben Virtual Private Cloud (VPC) befinden. Das automatische Verbindungsfeature wird nicht unterstützt, wenn sich eine EC2-Instance und eine RDS-Datenbank in unterschiedlichen VPCs befinden.

Automatisches Verbinden einer Instance und einer Datenbank

Sie können eine EC2-Instance sofort nach dem Start Ihrer Instance oder zu einem späteren Zeitpunkt automatisch mit einer RDS-Datenbank verbinden.

Automatisches Verbinden direkt nach dem Start

Führen Sie die folgenden Schritte aus, um eine EC2-Instance unmittelbar nach dem Start der EC2-Instance automatisch mit einer RDS-Datenbank zu verbinden.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Automatisches Verbinden einer neu gestarteten EC2-Instance mit einer RDS-Datenbank.

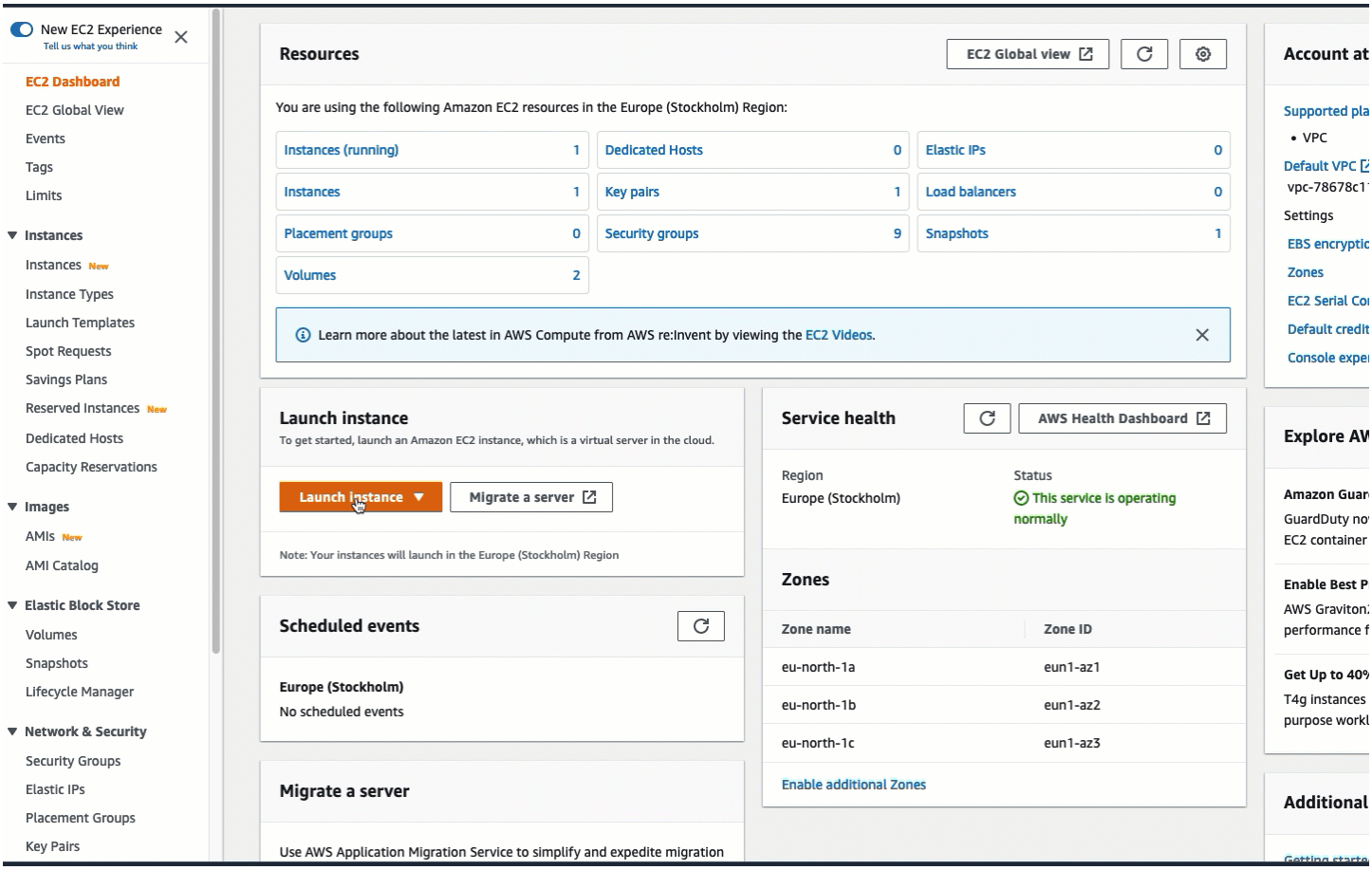
So verbinden Sie eine neu gestartete EC2-Instance automatisch mit einer RDS-Datenbank mithilfe der EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard der Konsole die Option Launch instances (Instances starten) und folgen Sie dann den Schritten zum Starten einer Instance.
3. Wählen Sie auf der Bestätigungsseite für den Start der Instance die Option Connect an RDS database (Eine RDS-Datenbank verbinden) aus.
4. Gehen Sie im Dialogfeld Connect RDS Database (RDS-Datenbank verbinden) wie folgt vor:
   a. Wählen Sie für Database role (Datenbankrolle) entweder Cluster oder Instance aus.
   b. Wählen Sie für die RDS database (RDS-Datenbank) eine Datenbank aus, zu der eine Verbindung hergestellt werden soll.

      > **Note**
      >
      > Die EC2-Instances und die RDS-Datenbank müssen sich in derselben VPC befinden, um eine Verbindung miteinander herzustellen.

   c. Wählen Sie Connect aus.

Animation anzeigen: Automatisches Verbinden einer neu gestarteten EC2-Instance mit einer RDS-Datenbank



Automatisches Verbinden einer bestehenden Instance

Führen Sie die folgenden Schritte aus, um eine vorhandene EC2-Instance automatisch mit einer RDS-Datenbank zu verbinden.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Automatisches Verbinden einer vorhandenen EC2-Instance mit einer RDS-Datenbank.

So verbinden Sie eine vorhandene EC2-Instance automatisch mit einer RDS-Datenbank mithilfe der EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine oder mehrere EC2-Instances aus, um eine Verbindung zu einer RDS-Datenbank herzustellen, und wählen Sie dann Actions (Aktionen), Networking (Netzwerk), Connect RDS database (RDS-Datenbank verbinden).

Wenn Connect RDS database (RDS-Datenbank verbinden) nicht verfügbar ist, überprüfen Sie, ob sich die EC2-Instances im Status Running (Ausgeführt) befinden und dass sie sich in der gleichen VPC befinden.

4. Gehen Sie im Dialogfeld Connect RDS Database (RDS-Datenbank verbinden) wie folgt vor:

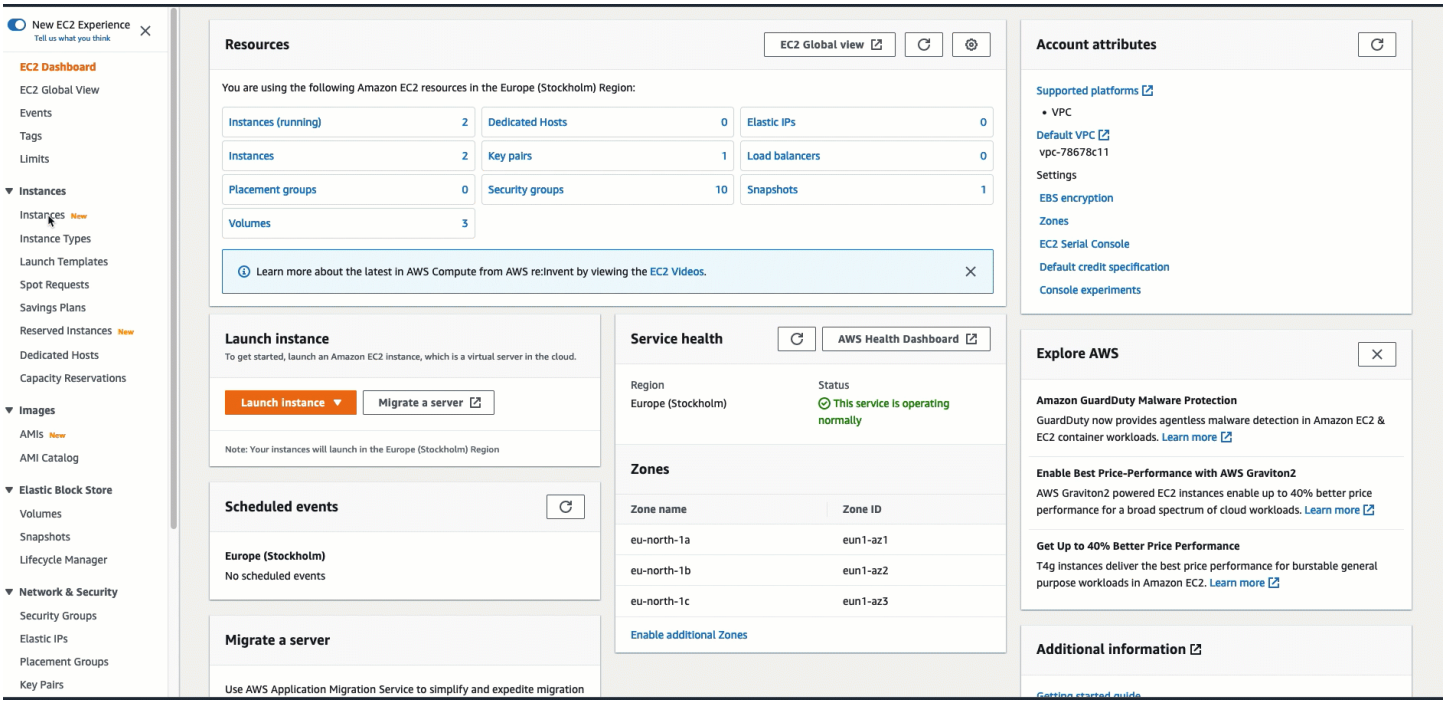
   a. Wählen Sie für Database role (Datenbankrolle) entweder Cluster oder Instance aus.

   b. Wählen Sie für die RDS database (RDS-Datenbank) eine Datenbank aus, zu der eine Verbindung hergestellt werden soll.

   > **Note**
   >
   > Die EC2-Instances und die RDS-Datenbank müssen sich in derselben VPC befinden, um eine Verbindung miteinander herzustellen.

   c. Wählen Sie Connect aus.

Animation anzeigen: Automatisches Verbinden einer vorhandenen EC2-Instance mit einer RDS-Datenbank



Informationen zur Verwendung der Amazon RDS-Konsole zum automatischen Verbinden einer EC2-Instance mit einer RDS-Datenbank finden Sie unter Konfigurieren der automatischen Netzwerkverbindung mit einer EC2-Instance im Amazon-RDS-Benutzerhandbuch.

So wird die Verbindung automatisch konfiguriert

Wenn Sie die EC2-Konsole verwenden, um die Verbindung zwischen einer EC2-Instance und einer RDS-Datenbank automatisch so zu konfigurieren, dass der Datenverkehr zwischen ihnen zugelassen wird, wird die Verbindung durch Sicherheitsgruppen konfiguriert.

Die Sicherheitsgruppen werden automatisch erstellt und der EC2-Instance und der RDS-Datenbank wie folgt hinzugefügt:

- Amazon EC2 erstellt eine Sicherheitsgruppe mit dem Namen ec2-rds-***x*** und fügt sie der EC2-Instance hinzu. Es verfügt über eine ausgehende Regel, die Datenverkehr zur Datenbank zulässt, indem rds-ec2-***x*** (die Datenbanksicherheitsgruppe) als Ziel angegeben wird.
- Amazon RDS erstellt eine Sicherheitsgruppe mit dem Namen rds-ec2-***x*** und fügt sie zur Datenbank hinzu. Es verfügt über eine eingehende Regel, die Datenverkehr von der EC2-Instance zulässt, indem ec2-rds-***x*** (die EC2-Instance-Sicherheitsgruppe) als Quelle angegeben wird.

Die Sicherheitsgruppen referenzieren sich gegenseitig als Ziel und Quelle und lassen nur Datenverkehr am Datenbankport zu. Sie können diese Sicherheitsgruppen wiederverwenden, sodass jede Datenbank mit der Sicherheitsgruppe rds-ec2-***x*** mit jeder EC2-Instance mit der Sicherheitsgruppe ec2-rds-***x*** kommunizieren kann.

Die Namen der Sicherheitsgruppen folgen einem Muster. Für die von Amazon EC2 erstellten Sicherheitsgruppen lautet das Muster ec2-rds-***x*** und für die von Amazon RDS erstellten Sicherheitsgruppen lautet das Muster ***rds-ec2-x***. ***x*** ist eine Zahl, die jedes Mal um 1 erhöht wird, wenn eine neue Sicherheitsgruppe automatisch erstellt wird.

Tutorial: Verbinden einer Amazon-EC2-Instance mit einer Amazon-RDS-Datenbank

Tutorial-Ziel

Ziel dieses Tutorials ist es, zu lernen, wie Sie eine sichere Verbindung zwischen einer Amazon-EC2-Instance und einer Amazon-RDS-Datenbank mithilfe der AWS Management Console konfigurieren.

Es gibt verschiedene Möglichkeiten, die Verbindung zu konfigurieren. In diesem Tutorial untersuchen wir die folgenden drei Optionen:

- Option 1: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank mithilfe der EC2-Konsole

  Verwenden Sie das automatische Verbindungsfeature in der EC2-Konsole, um die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank automatisch zu konfigurieren, um Datenverkehr zwischen der EC2-Instance und der RDS-Datenbank zuzulassen.

- Option 2: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank mithilfe der RDS-Konsole

  Verwenden Sie das automatische Verbindungsfeature in der RDS-Konsole, um die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank automatisch zu konfigurieren, um Datenverkehr zwischen der EC2-Instance und der RDS-Datenbank zuzulassen.

- Option 3: Manuelles Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank durch Nachahmung des automatischen Verbindungsfeatures

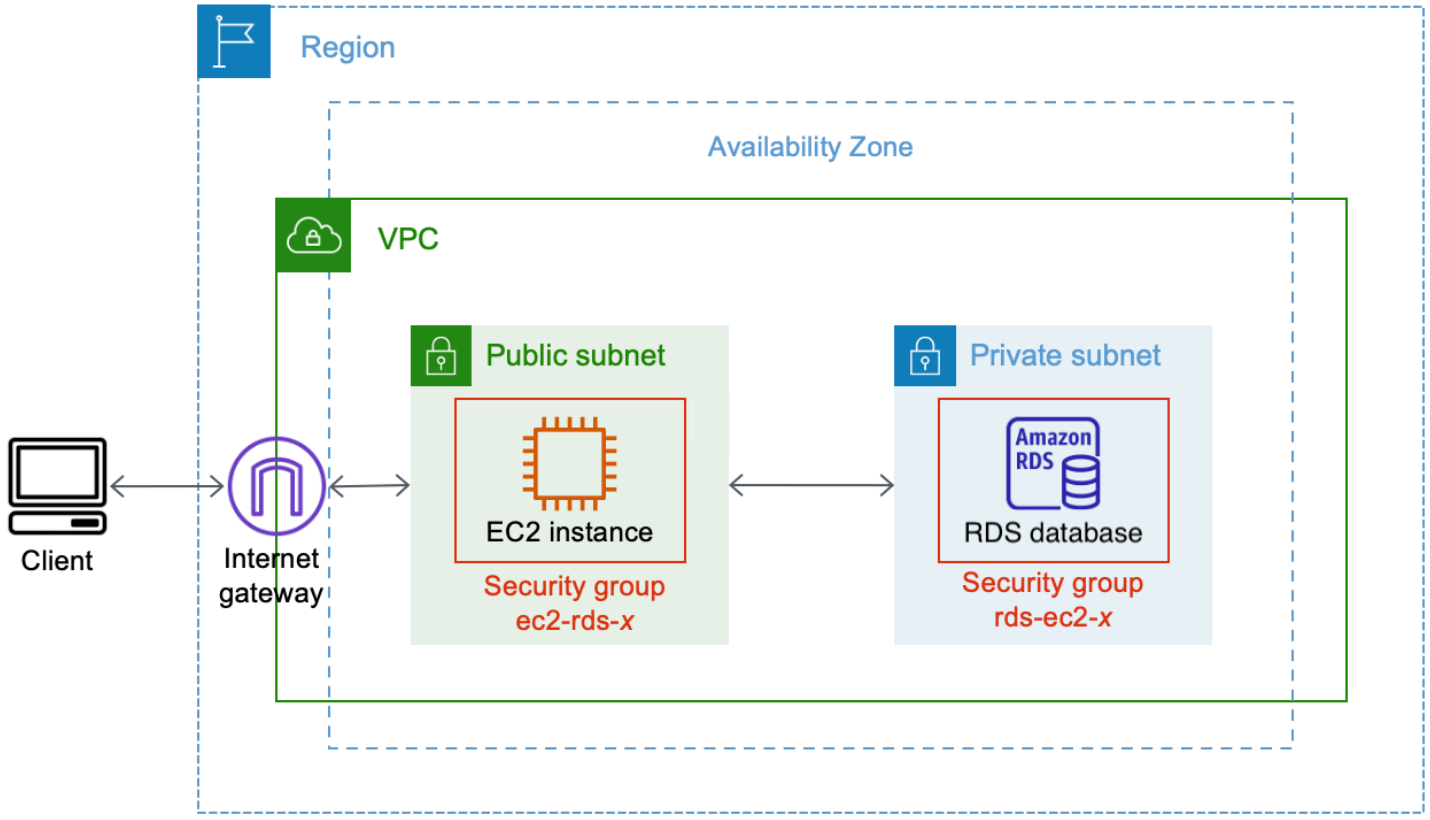
  Konfigurieren Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank, indem Sie die Sicherheitsgruppen manuell konfigurieren und zuweisen. Damit reproduzieren Sie die Konfiguration, die durch das automatische Verbindungsfeature in Option 1 und Option 2 automatisch erstellt wird.

Kontext

Als Kontext dafür, warum Sie eine Verbindung zwischen Ihrer EC2-Instance und einer RDS-Datenbank konfigurieren möchten, betrachten wir das folgende Szenario: Ihre Website zeigt Ihren Benutzern ein Formular zum Ausfüllen an. Sie müssen die Formulardaten in einer Datenbank erfassen. Sie können Ihre Website auf einer EC2-Instance hosten, die als Webserver konfiguriert wurde, und Sie können die Formulardaten in einer RDS-Datenbank erfassen. Die EC2-Instance und die RDS-Datenbank müssen miteinander verbunden sein, damit die Formulardaten von der EC2-Instance in die RDS-Datenbank übertragen werden können. In diesem Tutorial wird erklärt, wie Sie diese Verbindung konfigurieren. Beachten Sie, dass dies nur ein Beispiel für einen Anwendungsfall zum Verbinden einer EC2-Instance und einer RDS-Datenbank ist.

Architektur

Das folgende Diagramm zeigt die erstellten Ressourcen und die architektonische Konfiguration, die sich aus der Ausführung aller Schritte in diesem Tutorial ergibt.



Das Diagramm veranschaulicht die folgenden Ressourcen, die Sie erstellen werden:

- Sie erstellen eine EC2-Instance und eine RDS-Datenbank in derselben AWS-Region VPC und Availability Zone.
- Sie erstellen die EC2-Instance in einem öffentlichen Subnetz.
- Sie erstellen die RDS-Datenbank in einem privaten Subnetz.

  Wenn Sie die RDS-Konsole verwenden, um die RDS-Datenbank zu erstellen und die EC2-Instance automatisch zu verbinden, werden die VPC, die DB-Subnetzgruppe und die Einstellungen für den öffentlichen Zugriff für die Datenbank automatisch ausgewählt. Die RDS-Datenbank wird automatisch in einem privaten Subnetz innerhalb derselben VPC wie die EC2-Instance erstellt.
- Internetbenutzer können sich mithilfe von SSH oder HTTP/HTTPS über ein Internet-Gateway mit der EC2-Instance verbinden.
- Internetbenutzer können keine direkte Verbindung mit der RDS-Datenbank herstellen. Nur die EC2-Instance ist mit der RDS-Datenbank verbunden.
- Wenn Sie das automatische Verbindungsfeature verwenden, um Datenverkehr zwischen der EC2-Instance und der RDS-Datenbank zuzulassen, werden die folgenden Sicherheitsgruppen automatisch erstellt und hinzugefügt:

- Die Sicherheitsgruppe ec2-rds- ***x*** wird erstellt und der EC2-Instance hinzugefügt. Es verfügt über eine ausgehende Regel, die auf die Sicherheitsgruppe rds-ec2-***x*** als Ziel verweist. Dadurch kann der Datenverkehr von der EC2-Instance die RDS-Datenbank mit der Sicherheitsgruppe rds-ec2-***x*** erreichen.
- Die Sicherheitsgruppe rds-ec2-***x*** wird erstellt und der RDS-Datenbank hinzugefügt. Es verfügt über eine eingehende Regel, die auf die Sicherheitsgruppe ec2-rds-***x*** als Quelle verweist. Dadurch kann der Datenverkehr von der EC2-Instance mit der Sicherheitsgruppe ec2-rds-***x*** die RDS-Datenbank erreichen.

Durch die Verwendung getrennter Sicherheitsgruppen (eine für die EC2-Instance und eine für die RDS-Datenbank) haben Sie eine bessere Kontrolle über die Sicherheit der Instance und der Datenbank. Wenn Sie dieselbe Sicherheitsgruppe sowohl für die Instance als auch für die Datenbank verwenden und dann die Sicherheitsgruppe beispielsweise nur für die Datenbank anpassen würden, würde sich die Änderung sowohl auf die Instance als auch auf die Datenbank auswirken. Mit anderen Worten, wenn Sie eine Sicherheitsgruppe verwenden würden, könnten Sie unbeabsichtigt die Sicherheit einer Ressource (entweder der Instance oder der Datenbank) ändern, da Sie vergessen haben, dass die Sicherheitsgruppe an sie angefügt war.

Die Sicherheitsgruppen, die automatisch erstellt werden, respektieren auch die geringsten Berechtigungen, da sie nur die gegenseitige Verbindung für diesen Workload auf dem Datenbankport zulassen, indem sie ein Workload-spezifisches Sicherheitsgruppenpaar erstellen.

Überlegungen

Beachten Sie bei Durchführung der Aufgaben in diesem Tutorial Folgendes:

- Two consoles (Zwei Konsolen) – Sie werden die folgenden zwei Konsolen für dieses Tutorial verwenden:
  - Amazon-EC2-Konsole – Sie verwenden die EC2-Konsole zum Starten von Instances, zum automatischen Verbinden einer EC2-Instance mit einer RDS-Datenbank und für die manuelle Option zum Konfigurieren der Verbindung durch Erstellen der Sicherheitsgruppen.
  - Amazon-RDS-Konsole – Sie verwenden die RDS-Konsole, um eine RDS-Datenbank zu erstellen und eine EC2-Instance automatisch mit einer RDS-Datenbank zu verbinden.
- One VPC (Eine VPC) – Um das automatische Verbindungsfeature zu verwenden, müssen sich Ihre EC2-Instance und Ihre RDS-Datenbank in derselben VPC befinden.

Wenn Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank manuell konfigurieren, können Sie Ihre EC2-Instance in einer VPC und Ihre RDS-Datenbank in einer anderen VPC starten. Allerdings müssen Sie zusätzliches Routing und eine VPC-Konfiguration einrichten. Dieses Szenario wird in diesem Tutorial nicht behandelt.

- Erstens AWS-Region — Die EC2-Instance und die RDS-Datenbank müssen sich in derselben Region befinden.
- Two security groups (Zwei Sicherheitsgruppen) – Die Verbindung zwischen der EC2-Instance und der RDS-Datenbank wird durch zwei Sicherheitsgruppen konfiguriert – eine Sicherheitsgruppe für Ihre EC2-Instance und eine Sicherheitsgruppe für Ihre RDS-Datenbank.

  Wenn Sie das automatische Verbindungsfeature in der EC2-Konsole oder RDS-Konsole verwenden, um die Verbindung zu konfigurieren (Option 1 und Option 2 dieses Tutorials), werden die Sicherheitsgruppen automatisch erstellt und der EC2-Instance und RDS-Datenbank zugewiesen.

  Wenn Sie das automatische Verbindungsfeature nicht verwenden, müssen Sie die Sicherheitsgruppen manuell erstellen und zuweisen. Sie tun dies in Option 3 dieses Tutorials.

Zeit zur Absolvierung des Tutorials

30 Minuten

Sie können das gesamte Tutorial in einer Sitzung abschließen oder eine Aufgabe nach der anderen erledigen.

Kosten

Wenn Sie dieses Tutorial abschließen, können Ihnen Kosten für die von Ihnen erstellten AWS Ressourcen entstehen.

Sie können Amazon EC2 im Rahmen des kostenlosen Kontingents verwenden, sofern Ihr AWS Konto weniger als 12 Monate alt ist und Sie Ihre Ressourcen gemäß den Anforderungen des kostenlosen Kontingents konfigurieren.

Wenn sich Ihre EC2-Instance und Ihre RDS-Datenbank in unterschiedlichen Availability Zones befinden, fallen Datenübertragungsgebühren an. Um diese Gebühren zu vermeiden, müssen sich die EC2-Instance und die RDS-Datenbank in derselben Availability Zone befinden. Weitere Informationen zu den Datenübertragungsgebühren finden Sie unter Datenübertragung auf der Seite Amazon-EC2-On-Demand-Preise.

Um Kosten zu vermeiden, nachdem Sie das Tutorial abgeschlossen haben, löschen Sie die Ressourcen, wenn sie nicht mehr benötigt werden. Die Schritte zum Löschen der Ressourcen finden Sie unter Bereinigen.

Option 1: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank mithilfe der EC2-Konsole

Ziel

Das Ziel von Option 1 ist es, das automatische Verbindungsfeature in der EC2-Konsole zu erkunden, die die Verbindung zwischen Ihrer EC2-Instance und der RDS-Datenbank automatisch konfiguriert, damit Datenverkehr von der EC2-Instance zur RDS-Datenbank zugelassen wird. In Option 3 erfahren Sie, wie Sie die Verbindung manuell konfigurieren.

Bevor Sie beginnen

Sie benötigen Folgendes, um dieses Tutorial abzuschließen:

- Eine RDS-Datenbank, die sich in derselben VPC wie die EC2-Instance befindet. Sie können entweder eine vorhandene RDS-Datenbank verwenden oder die Schritte in Aufgabe 1 ausführen, um eine neue RDS-Datenbank zu erstellen.
- Eine EC2-Instance, die sich in derselben VPC wie die RDS-Datenbank befindet. Sie können entweder eine vorhandene EC2-Instance verwenden oder die Schritte in Aufgabe 2 ausführen, um eine neue EC2-Instance zu erstellen.
- Berechtigungen zum Aufrufen der folgenden Operationen:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`

- `ec2:RevokeSecurityGroupEgress`

Aufgaben zur Erledigung von Option 1

- Aufgabe 1: Erstellen einer RDS-Datenbank – optional
- Aufgabe 2: Starten einer EC2-Instance – optional
- Aufgabe 3: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank
- Aufgabe 4: Überprüfen der Verbindungskonfiguration

Aufgabe 1: Erstellen einer RDS-Datenbank – optional

> **Note**
>
> Das Erstellen einer Amazon-RDS-Datenbank steht nicht im Mittelpunkt dieses Tutorials. Wenn Sie bereits über eine RDS-Datenbank verfügen und diese für dieses Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.

Aufgabenziel

Ziel dieser Aufgabe ist es, eine RDS-Datenbank zu erstellen, damit Sie Aufgabe 3 abschließen können, in der Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank konfigurieren. Wenn Sie über eine RDS-Datenbank verfügen, die Sie verwenden können, können Sie diese Aufgabe überspringen.

> **Important**
>
> Wenn Sie eine vorhandene RDS-Datenbank verwenden, stellen Sie sicher, dass sie sich in derselben VPC wie Ihre EC2-Instance befindet, damit Sie das automatische Verbindungsfeature verwenden können.

Schritte zum Erstellen einer RDS-Datenbank

Führen Sie die folgenden Schritte aus, um eine RDS-Datenbank zu erstellen.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Erstellen einer RDS-Datenbank.

RDS-Datenbankkonfiguration

Mit den Schritten in dieser Aufgabe wird die RDS-Datenbank wie folgt konfiguriert:

- Engine-Typ: MySQL
- Vorlage: Kostenloses Kontingent
- DB-Instance-Kennung: **`tutorial-database-1`**
- DB-Instance-Klasse: `db.t3.micro`

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

So erstellen Sie eine MySQL-RDS-Datenbank

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der Regionsauswahl (oben rechts) eine AWS-Region aus. Die Datenbank und die EC2-Instance müssen sich in derselben Region befinden, um das automatische Verbindungsfeature in der EC2-Konsole verwenden zu können.
3. Wählen Sie im Dashboard Create database (Datenbank erstellen) aus.
4. Überprüfen Sie unter Choose a database creation method (Datenbankerstellungsmethode auswählen), ob Standard create (Standarderstellung) ausgewählt ist. Wenn Sie Easy create (Einfache Erstellung) wählen, ist der VPC-Selektor nicht verfügbar. Sie müssen sicherstellen, dass sich Ihre Datenbank in derselben VPC wie Ihre EC2-Instance befindet, um das automatische Verbindungsfeature in der EC2-Konsole verwenden zu können.
5. Wählen Sie unter Engine options (Engine-Optionen) für Engine type (Engine-Typ) die Option MySQL aus.
6. Wählen Sie unter Templates (Vorlagen) eine Beispielvorlage aus, die Ihren Anforderungen entspricht. Wählen Sie für dieses Tutorial die Option Free tier (Kostenloses Kontingent), um kostenlos eine Datenbank zu erstellen. Beachten Sie jedoch, dass das kostenlose Kontingent nur verfügbar ist, wenn Ihr Konto weniger als 12 Monate alt ist. Es gelten andere Einschränkungen. Sie können mehr darüber erfahren, indem Sie auf den Info-Link im Feld Free tier (Kostenloses Kontingent) klicken.

7. Führen Sie unter Settings (Einstellungen) die folgenden Schritte aus:

   a. Geben Sie unter DB instance identifier (DB-Instance-Kennung) einen Namen für die Datenbank ein. Geben Sie für dieses Tutorial **`tutorial-database-1`** ein.

   b. Behalten Sie für Master username (Master-Benutzername) den Standardnamen **`admin`** bei.

   c. Geben Sie unter Master password (Master-Passwort) ein Passwort ein, das Sie sich für dieses Tutorial merken können, und geben Sie dann unter Confirm password (Passwort bestätigen) das Passwort erneut ein.

8. Behalten Sie unter Instance configuration (Instance-Konfiguration) für die DB instance class (DB-Instance-Klasse) die Standardeinstellung db.t3.micro bei. Wenn Ihr Konto weniger als 12 Monate alt ist, können Sie diese Datenbankklasse kostenlos nutzen. Es gelten andere Einschränkungen. Weitere Informationen finden Sie unter Kostenloses Kontingent für AWS.

9. Wählen Sie unter Connectivity (Verbindung) für Compute resource (Rechenressource) die Option Don't connect to an EC2 compute resource (Keine Verbindung zu einer EC2-Rechenressource herstellen) aus, da Sie die EC2-Instance und die RDS-Datenbank später in Aufgabe 3 miteinander verbinden werden.

   (Später, in Option 2 dieses Tutorials, werden Sie das automatische Verbindungsfeature in der RDS-Konsole ausprobieren, indem Sie Connect to an EC2 compute resource (Mit einer EC2-Rechenressource verbinden) auswählen.)

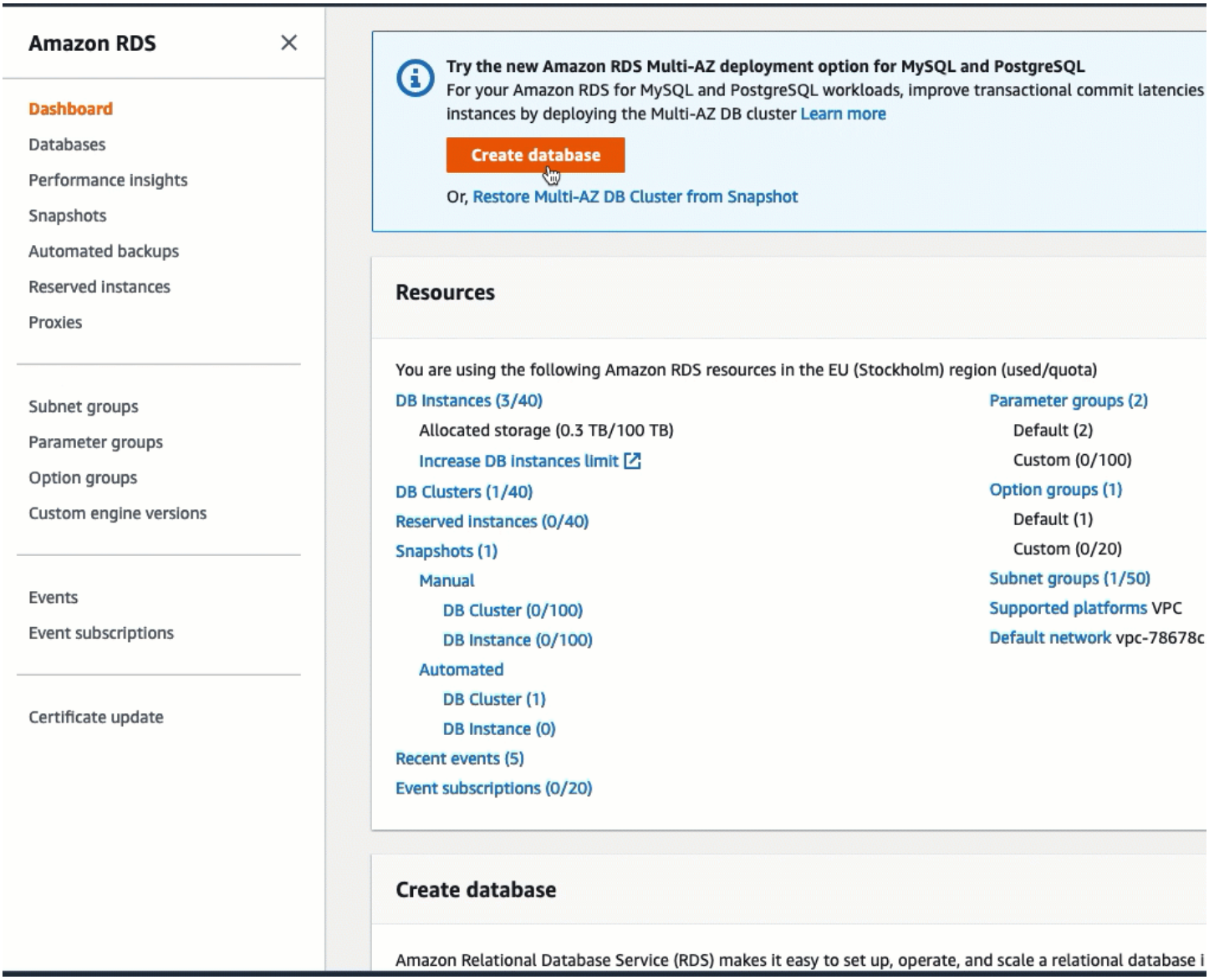
10. Wählen Sie unter Virtual Private Cloud (VPC) eine VPC aus. Die VPC muss über eine DB-Subnetzgruppe verfügen. Um das automatische Verbindungsfeature verwenden zu können, müssen sich Ihre EC2-Instance und die RDS-Datenbank in derselben VPC befinden.

11. Behalten Sie alle Standardwerte für die anderen Felder auf dieser Seite bei.

12. Wählen Sie Datenbank erstellen aus.

    Auf dem Bildschirm Databases (Datenbanken) lautet der Status der neuen Datenbank Creating (Wird erstellt), bis die Datenbank einsatzbereit ist. Wenn sich der Status in Available (Verfügbar) ändert, können Sie eine Verbindung zur Datenbank herstellen. Abhängig von der Klasse der Datenbank und vom verfügbaren Speicherplatz kann es bis zu 20 Minuten dauern, bis die neue Datenbank verfügbar ist.

Animation anzeigen: Erstellen einer RDS-Datenbank



Sie sind jetzt bereit für Aufgabe 2: Starten einer EC2-Instance – optional.

Aufgabe 2: Starten einer EC2-Instance – optional

> **Note**
>
> Das Starten einer Instance steht nicht im Mittelpunkt dieses Tutorials. Wenn Sie bereits über eine Amazon-EC2-Instance verfügen und diese in diesem Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.

Aufgabenziel

Ziel dieser Aufgabe ist es, eine EC2-Instance zu starten, damit Sie Aufgabe 3 abschließen können, in der Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer Amazon RDS-Datenbank konfigurieren. Wenn Sie über eine EC2-Instance verfügen, die Sie verwenden können, können Sie diese Aufgabe überspringen.

> **Important**
>
> Wenn Sie eine vorhandene EC2-Instance verwenden, stellen Sie sicher, dass sie sich in derselben VPC wie Ihre RDS-Datenbank befindet, damit Sie das automatische Verbindungsfeature verwenden können.

Schritte für das Starten einer EC2-Instance

Führen Sie die folgenden Schritte aus, um eine EC2-Instance für dieses Tutorial zu starten.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Starten einer EC2-Instance.

Konfigurieren der EC2-Instance

Mit den Schritten in dieser Aufgabe wird die EC2-Instance wie folgt konfiguriert:

- Instance-Name: **`tutorial-instance-1`**
- AMI: Amazon Linux 2
- Instance-Typ: `t2.micro`
- Öffentliche IP automatisch zuweisen: Aktiviert
- Sicherheitsgruppe mit den folgenden drei Regeln:
  - SSH von Ihrer IP-Adresse zulassen
  - HTTPS-Datenverkehr von überall zulassen
  - HTTP-Datenverkehr von überall zulassen

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

Starten Sie EC2-Instances wie folgt:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Regionsauswahl (oben rechts) eine AWS-Region aus. Die Datenbank und die EC2-Instance müssen sich in derselben Region befinden, um das automatische Verbindungsfeature in der EC2-Konsole verwenden zu können.
3. Wählen Sie im EC2-Dashboard die Option Launch Instance (Instance starten) aus.
4. Geben Sie unter Name and tags (Name und Tags) für Name einen Namen ein, um Ihre Instance zu identifizieren. Geben Sie für dieses Tutorial der Instance den Namen **`tutorial-instance-1`**. Der Instance-Name ist zwar nicht obligatorisch, aber wenn Sie Ihre Instance in der EC2-Konsole auswählen, können Sie sie anhand des Namens leicht identifizieren.
5. Wählen Sie unter Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus, das Ihren Webserver-Anforderungen entspricht. Dieses Tutorial verwendet Amazon Linux 2.
6. Wählen Sie unter Instance type (Instance-Typ) für Instance type (Instance-Typ) einen Instance-Typ aus, der Ihren Webserver-Anforderungen entspricht. In diesem Tutorial wird ein `t2.micro` verwendet.

   > **Note**
   >
   > Sie können Amazon EC2 im Rahmen des kostenlosen Kontingents verwenden, sofern Ihr AWS Konto weniger als 12 Monate alt ist und Sie einen `t2.micro` Instance-Typ wählen (oder `t3.micro` in Regionen, in denen dieser nicht verfügbar `t2.micro` ist).

7. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) für Key pair name (Schlüsselpaar-Name) Ihr Schlüsselpaar aus.
8. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:

   a. Wenn Sie für Network (Netzwerk) und Subnet (Subnetz) keine Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, können Sie die Standardeinstellungen beibehalten.

      Wenn Sie Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, überprüfen Sie Folgendes:

i. Die Instance muss sich in derselben VPC wie die RDS-Datenbank befinden, um das automatische Verbindungsfeature verwenden zu können. Standardmäßig haben Sie nur eine VPC.

ii. Die VPC, in der Sie Ihre Instance starten, muss mit einem Internet-Gateway verbunden sein, damit Sie über das Internet auf Ihren Webserver zugreifen können. Ihre Standard-VPC wird automatisch mit einem Internet-Gateway eingerichtet.

iii. Um sicherzustellen, dass Ihre Instance eine öffentliche IP-Adresse erhält, überprüfen Sie für Auto-assign public IP (Automatische Zuweisung öffentlicher IP), dass Enable (Aktivieren) ausgewählt ist. Wenn Disable (Deaktivieren) ausgewählt ist, wählen Sie Edit (Bearbeiten) (rechts neben Network Settings (Netzwerkeinstellungen)) und dann für Auto-assign public IP (Öffentliche IP automatisch zuweisen) die Option Enable (Aktivieren) aus.

b. Um mithilfe von SSH eine Verbindung zu Ihrer Instance herzustellen, benötigen Sie eine Sicherheitsgruppenregel, die SSH- (Linux) oder RDP-Datenverkehr (Windows) von der öffentlichen IPv4-Adresse Ihres Computers autorisiert. Wenn Sie eine Instance starten, wird standardmäßig eine neue Sicherheitsgruppe mit einer Regel erstellt, die eingehenden SSH-Datenverkehr von überall zulässt.

   Um sicherzustellen, dass nur Ihre IP-Adresse eine Verbindung zu Ihrer Instance herstellen kann, wählen Sie unter Firewall (security groups) (Firewall (Sicherheitsgruppen)) in der Dropdown-Liste neben dem Kontrollkästchen Allow SSH traffic from (SSH-Verkehr zulassen von) die Option My IP (Meine IP) aus.

c. Um Datenverkehr aus dem Internet zu Ihrer Instance zuzulassen, aktivieren Sie die folgenden Kontrollkästchen:

   - Allow HTTPs traffic from the internet (HTTPs-Datenverkehr aus dem Internet zulassen)
   - Allow HTTP traffic from the internet (HTTP-Datenverkehr aus dem Internet zulassen)

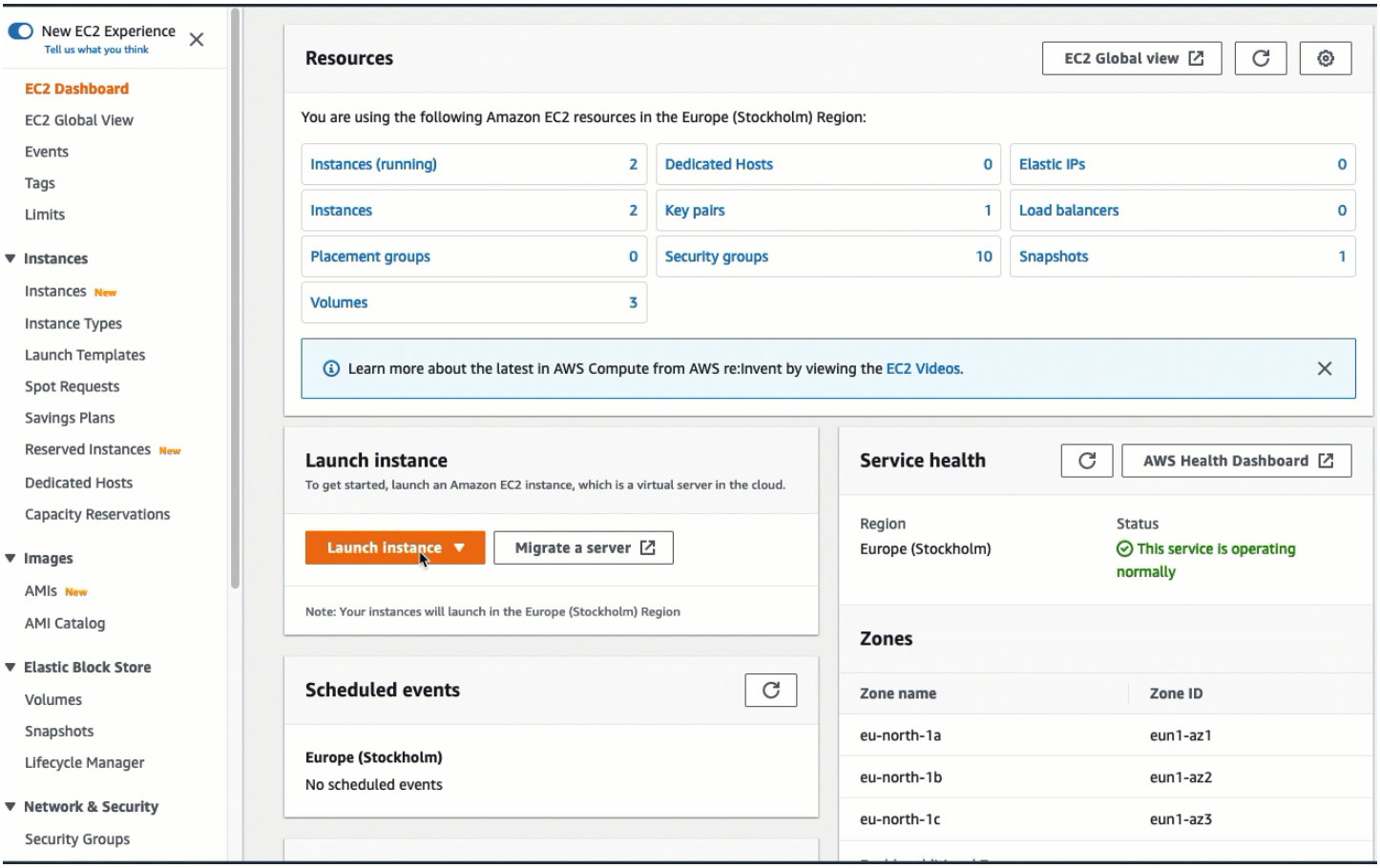
9. Überprüfen Sie im Bereich Summary (Übersicht) Ihre Instance-Konfiguration und wählen Sie dann Launch instance (Instance starten) aus.

10. Lassen Sie die Bestätigungsseite geöffnet. Sie benötigen es im nächsten Schritt, wenn Sie Ihre Instance automatisch mit Ihrer Datenbank verbinden.

    Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Weitere Informationen über das Starten einer Instance finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Animation anzeigen: Starten einer EC2-Instance



Sie sind jetzt bereit für Aufgabe 3: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank.

Aufgabe 3: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank

Aufgabenziel

Ziel dieser Aufgabe ist es, das automatische Verbindungsfeature in der EC2-Konsole zu verwenden, um die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank automatisch zu konfigurieren.

Schritte zum Verbinden Ihrer EC2-Instance und der RDS-Datenbank

Führen Sie die folgenden Schritte aus, um Ihre EC2-Instance und die RDS-Datenbank mithilfe des automatischen Features in der EC2-Konsole zu verbinden.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Automatisches Verbinden einer neu gestarteten EC2-Instance mit einer RDS-Datenbank.

So verbinden Sie eine EC2-Instance automatisch mit einer RDS-Datenbank mithilfe der EC2-Konsole

1. Wählen Sie auf der Bestätigungsseite für den Start der Instance (sie sollte von der vorherigen Aufgabe geöffnet sein) die Option Connect an RDS database (Mit einer RDS-Datenbank verbinden) aus.

   Wenn Sie die Bestätigungsseite geschlossen haben, gehen Sie wie folgt vor:

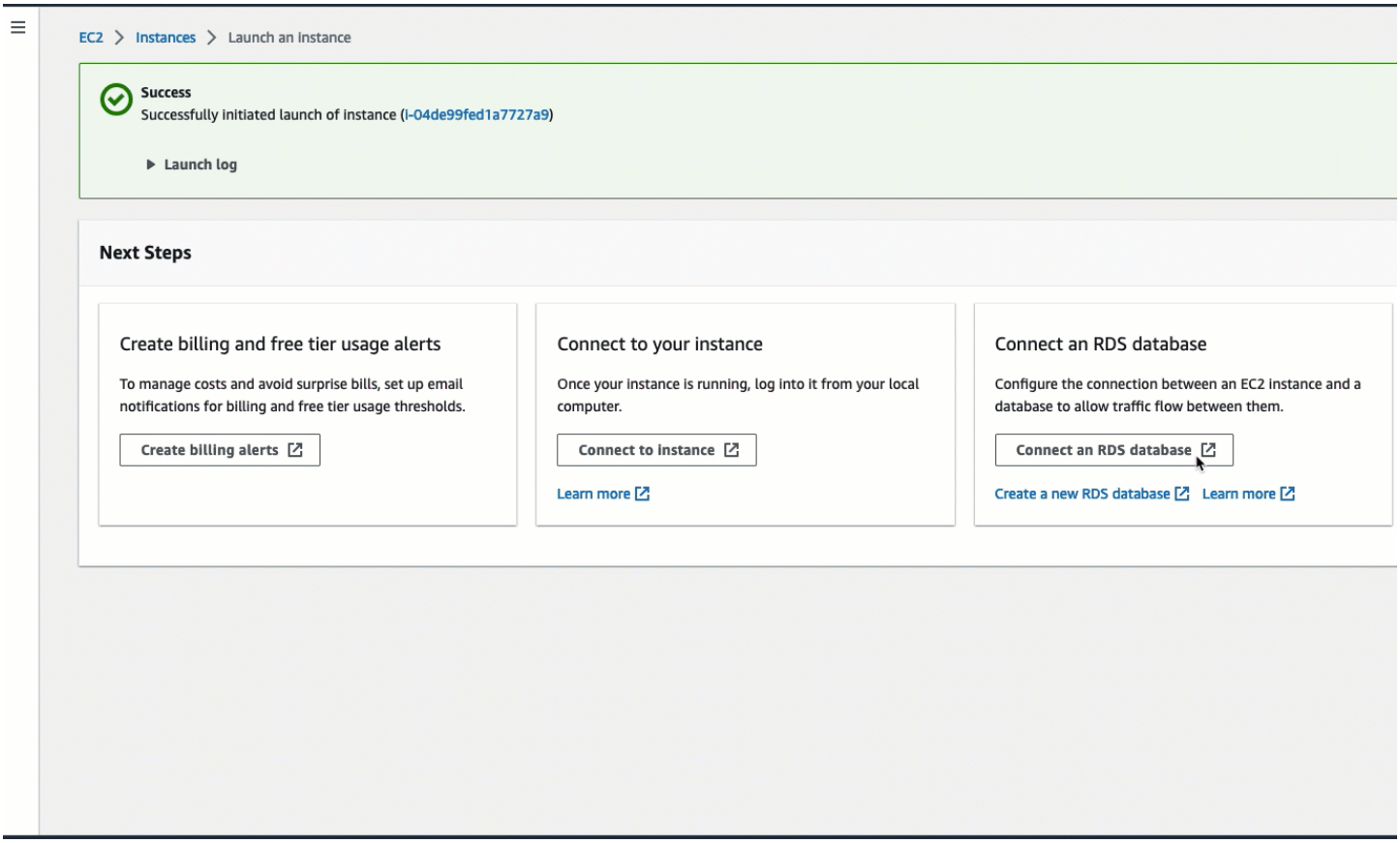
   a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie im Navigationsbereich Instances aus.
   c. Wählen Sie die EC2-Instance, die Sie gerade erstellt haben, und wählen Sie dann Actions (Aktionen), Networking (Netzwerk), Connect RDS database (RDS-Datenbank verbinden) aus.

      Wenn Connect RDS database (RDS-Datenbank verbinden) nicht verfügbar ist, überprüfen Sie, ob sich die EC2-Instance im Status Running (Ausgeführt) befindet.
2. Wählen Sie für Database role (Datenbankrolle) die Option Instance aus. Instance bezieht sich in diesem Fall auf die Datenbank-Instance.
3. Wählen Sie unter RDS database (RDS-Datenbank) die RDS-Datenbank aus, die Sie in Aufgabe 1 erstellt haben.

   > **Note**
   >
   > Die EC2-Instances und die RDS-Datenbank müssen sich in derselben VPC befinden, um eine Verbindung miteinander herzustellen.

4. Wählen Sie Connect aus.

Animation anzeigen: Automatisches Verbinden einer neu gestarteten EC2-Instance mit einer RDS-Datenbank



Sie sind jetzt bereit für Aufgabe 4: Überprüfen der Verbindungskonfiguration.

Aufgabe 4: Überprüfen der Verbindungskonfiguration

Aufgabenziel

Ziel dieser Aufgabe ist es, zu überprüfen, ob die beiden Sicherheitsgruppen erstellt und der Instance und Datenbank zugewiesen wurden.

Wenn Sie das automatische Verbindungsfeature in der EC2-Konsole verwenden, um die Verbindung zu konfigurieren, werden die Sicherheitsgruppen automatisch erstellt und der Instance und Datenbank wie folgt zugewiesen:

- Die Sicherheitsgruppe rds-ec2-*x*wird erstellt und der RDS-Datenbank hinzugefügt. Es verfügt über eine eingehende Regel, die auf die Sicherheitsgruppe ec2-rds-*x* als Quelle verweist. Dadurch kann der Datenverkehr von der EC2-Instance mit der Sicherheitsgruppe ec2-rds-*x* die RDS-Datenbank erreichen.

- Die Sicherheitsgruppe ec2-rds-*x* wird erstellt und der EC2-Instance hinzugefügt. Es verfügt über eine ausgehende Regel, die auf die Sicherheitsgruppe rds-ec2-*x* als Ziel verweist. Dadurch kann der Datenverkehr von der EC2-Instance die RDS-Datenbank mit der Sicherheitsgruppe rds-ec2-*x* erreichen.

Schritte zum Überprüfen der Verbindungskonfiguration

Führen Sie die folgenden Schritte aus, um die Verbindungskonfiguration zu überprüfen.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Überprüfen der Verbindungskonfiguration.

So überprüfen Sie die Verbindungskonfiguration mithilfe der Konsole

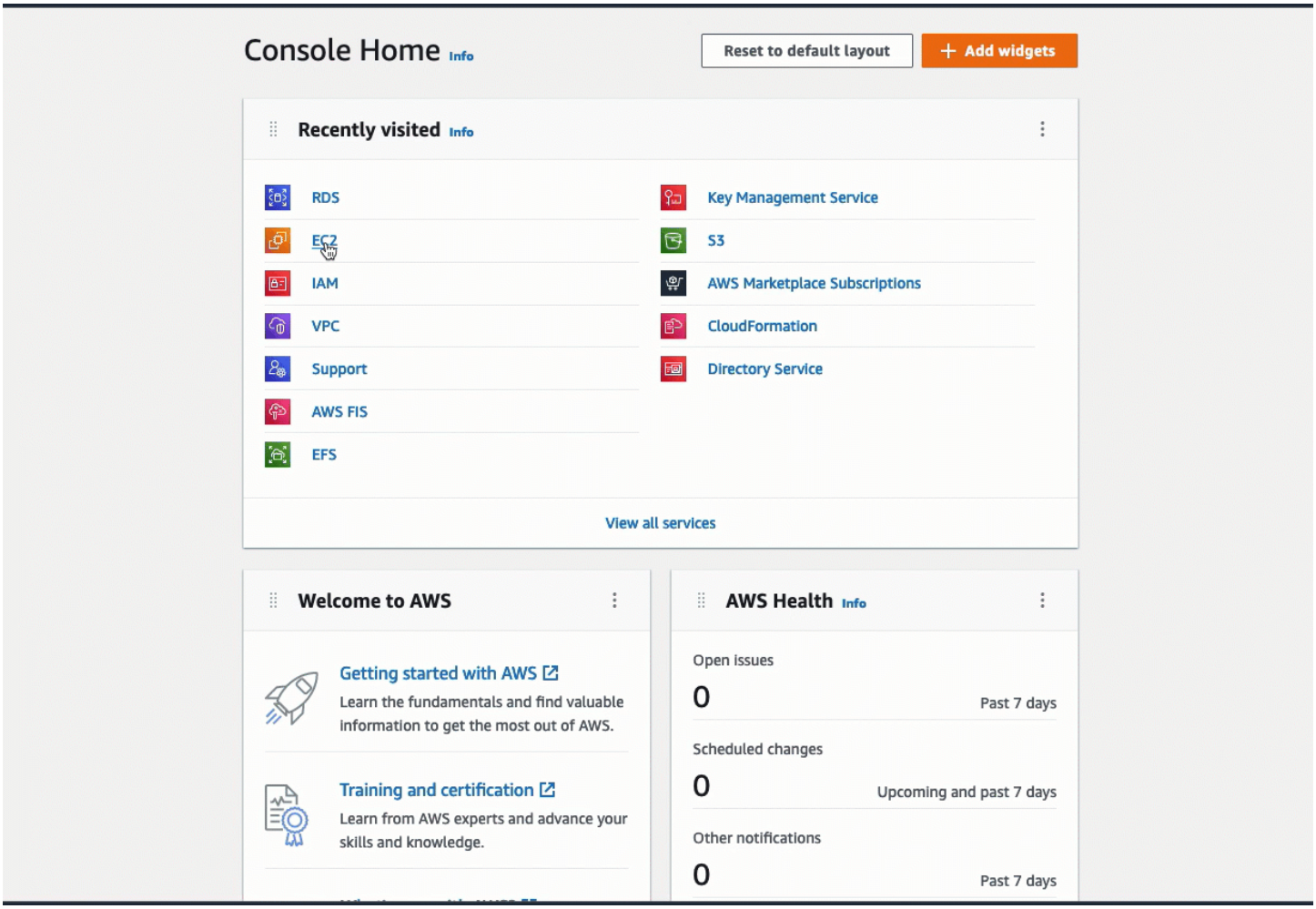
1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
3. Wählen Sie die RDS-Datenbank aus, die Sie für dieses Tutorial erstellt haben.
4. Überprüfen Sie auf der Registerkarte Connectivity & security (Verbindung und Sicherheit) unter Security (Sicherheit), VPC security groups (VPC-Sicherheitsgruppen), dass eine Sicherheitsgruppe mit dem Namen rds-ec2-*x* angezeigt wird.
5. Wählen Sie die Sicherheitsgruppe rds-ec2-*x* aus. Der Bildschirm Security Groups (Sicherheitsgruppen) in der EC2-Konsole wird geöffnet.
6. Wählen Sie die Sicherheitsgruppe rds-ec2-*x* aus, um sie zu öffnen.
7. Wählen Sie die Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) aus.
8. Stellen Sie wie folgt sicher, dass die folgende Sicherheitsgruppenregel vorhanden ist:
   - Typ: MYSQL/Aurora
   - Portbereich: 3306
   - Quelle: ***sg-0987654321example*** / ec2-rds-*x* – Dies ist die Sicherheitsgruppe, die der EC2-Instance zugewiesen ist, die Sie in den vorherigen Schritten überprüft haben.
   - Beschreibung: Rule to allow connections from EC2 instances with ***sg-1234567890example*** attached (Regel zum Zulassen von Verbindungen von EC2-Instances mit angefügtem sg-1234567890example)
9. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
10. Wählen Sie im Navigationsbereich Instances aus.

11. Wählen Sie die EC2-Instance aus, die Sie in der vorherigen Aufgabe für die Verbindung mit der RDS-Datenbank ausgewählt haben, und wählen Sie die Registerkarte Security (Sicherheit) aus.
12. Überprüfen Sie unter Security details (Sicherheitsdetails), Security groups (Sicherheitsgruppen), dass eine Sicherheitsgruppe mit dem Namen ec2-rds-*x* in der Liste enthalten ist. *x* ist eine Zahl.
13. Wählen Sie die Sicherheitsgruppe ec2-rds-*x*, um sie zu öffnen.
14. Wählen Sie die Registerkarte Outbound rules (Ausgehende Regeln).
15. Stellen Sie wie folgt sicher, dass die folgende Sicherheitsgruppenregel vorhanden ist:

    - Typ: MYSQL/Aurora
    - Portbereich: 3306
    - Ziel: *sg-1234567890example* / rds-ec2-*x*
    - Beschreibung: Regel zum Zulassen von Verbindungen zu **database-tutorial** von allen Instances, an denen diese Sicherheitsgruppe angefügt ist

Indem Sie überprüfen, ob diese Sicherheitsgruppen und Sicherheitsgruppenregeln vorhanden sind und ob sie der RDS-Datenbank und der EC2-Instance wie in diesem Verfahren beschrieben zugewiesen sind, können Sie überprüfen, ob die Verbindung automatisch konfiguriert wurde, indem Sie das automatische Verbindungsfeature verwenden.

Animation anzeigen: Überprüfen der Verbindungskonfiguration



Sie haben Option 1 dieses Tutorials abgeschlossen. Sie können nun entweder Option 2 abschließen, in der Sie lernen, wie Sie die RDS-Konsole verwenden, um eine EC2-Instance automatisch mit einer RDS-Datenbank zu verbinden oder Sie können Option 3 abschließen, in der Sie lernen, wie Sie die Sicherheitsgruppen, die in Option 1 automatisch erstellt wurden, manuell konfigurieren.

Option 2: Automatisches Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank mithilfe der RDS-Konsole

Ziel

Das Ziel von Option 2 ist es, das automatische Verbindungsfeature in der RDS-Konsole zu erkunden, die automatisch die Verbindung zwischen Ihrer EC2-Instance und der RDS-Datenbank konfiguriert, damit Datenverkehr von der EC2-Instance zur RDS-Datenbank zugelassen wird. In Option 3 erfahren Sie, wie Sie die Verbindung manuell konfigurieren.

Bevor Sie beginnen

Sie benötigen Folgendes, um dieses Tutorial abzuschließen:

- Eine EC2-Instance, die sich in derselben VPC wie die RDS-Datenbank befindet. Sie können entweder eine vorhandene EC2-Instance verwenden oder die Schritte in Aufgabe 1 ausführen, um eine neue Instance zu erstellen.
- Berechtigungen zum Aufrufen der folgenden Operationen:
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Aufgaben zur Erledigung von Option 2

- Aufgabe 1: Starten einer EC2-Instance – optional
- Aufgabe 2: Erstellen einer RDS-Datenbank und automatisches Verbinden mit Ihrer EC2-Instance
- Aufgabe 3: Überprüfen der Verbindungskonfiguration

Aufgabe 1: Starten einer EC2-Instance – optional

> **Note**
>
> Das Starten einer Instance steht nicht im Mittelpunkt dieses Tutorials. Wenn Sie bereits über eine Amazon-EC2-Instance verfügen und diese in diesem Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.

Aufgabenziel

Ziel dieser Aufgabe ist es, eine EC2-Instance zu starten, damit Sie Aufgabe 2 abschließen können, in der Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer Amazon RDS-Datenbank konfigurieren. Wenn Sie über eine EC2-Instance verfügen, die Sie verwenden können, können Sie diese Aufgabe überspringen.

Schritte für das Starten einer EC2-Instance

Führen Sie die folgenden Schritte aus, um eine EC2-Instance für dieses Tutorial zu starten.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Starten einer EC2-Instance.

Konfigurieren der EC2-Instance

Mit den Schritten in dieser Aufgabe wird die EC2-Instance wie folgt konfiguriert:

- Instance-Name: **`tutorial-instance-2`**
- AMI: Amazon Linux 2
- Instance-Typ: `t2.micro`
- Öffentliche IP automatisch zuweisen: Aktiviert
- Sicherheitsgruppe mit den folgenden drei Regeln:
  - SSH von Ihrer IP-Adresse zulassen
  - HTTPS-Datenverkehr von überall zulassen
  - HTTP-Datenverkehr von überall zulassen

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

Starten Sie EC2-Instances wie folgt:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im EC2-Dashboard die Option Launch Instance (Instance starten) aus.
3. Geben Sie unter Name and tags (Name und Tags) für Name einen Namen ein, um Ihre Instance zu identifizieren. Geben Sie für dieses Tutorial der Instance den Namen **`tutorial-`**

`instance-2`. Der Instance-Name ist zwar nicht obligatorisch, aber wenn Sie Ihre Instance in der RDS-Konsole auswählen, können Sie sie anhand des Namens leicht identifizieren.

4. Wählen Sie unter Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus, das Ihren Webserver-Anforderungen entspricht. Dieses Tutorial verwendet Amazon Linux.
5. Wählen Sie unter Instance type (Instance-Typ) für Instance type (Instance-Typ) einen Instance-Typ aus, der Ihren Webserver-Anforderungen entspricht. In diesem Tutorial wird ein `t2.micro` verwendet.

   > **Note**
   >
   > Sie können Amazon EC2 im Rahmen des kostenlosen Kontingents verwenden, sofern Ihr AWS Konto weniger als 12 Monate alt ist und Sie einen `t2.micro` Instance-Typ wählen (oder `t3.micro` in Regionen, in denen dieser nicht verfügbar `t2.micro` ist).

6. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) für Key pair name (Schlüsselpaar-Name) Ihr Schlüsselpaar aus.
7. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:

   a. Wenn Sie für Network (Netzwerk) und Subnet (Subnetz) keine Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, können Sie die Standardeinstellungen beibehalten.

      Wenn Sie Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, überprüfen Sie Folgendes:

      i. Die Instance muss sich in derselben VPC wie die RDS-Datenbank befinden, um die automatische Verbindungskonfiguration verwenden zu können. Standardmäßig haben Sie nur eine VPC.

      ii. Die VPC, in der Sie Ihre Instance starten, muss mit einem Internet-Gateway verbunden sein, damit Sie über das Internet auf Ihren Webserver zugreifen können. Ihre Standard-VPC wird automatisch mit einem Internet-Gateway eingerichtet.

      iii. Um sicherzustellen, dass Ihre Instance eine öffentliche IP-Adresse erhält, überprüfen Sie für Auto-assign public IP (Automatische Zuweisung öffentlicher IP), dass Enable (Aktivieren) ausgewählt ist. Wenn Disable (Deaktivieren) ausgewählt ist, wählen Sie Edit (Bearbeiten) (rechts neben Network Settings (Netzwerkeinstellungen)) und dann

für Auto-assign public IP (Öffentliche IP automatisch zuweisen) die Option Enable (Aktivieren) aus.

b. Um mithilfe von SSH eine Verbindung zu Ihrer Instance herzustellen, benötigen Sie eine Sicherheitsgruppenregel, die SSH- (Linux) oder RDP-Datenverkehr (Windows) von der öffentlichen IPv4-Adresse Ihres Computers autorisiert. Wenn Sie eine Instance starten, wird standardmäßig eine neue Sicherheitsgruppe mit einer Regel erstellt, die eingehenden SSH-Datenverkehr von überall zulässt.

   Um sicherzustellen, dass nur Ihre IP-Adresse eine Verbindung zu Ihrer Instance herstellen kann, wählen Sie unter Firewall (security groups) (Firewall (Sicherheitsgruppen)) in der Dropdown-Liste neben dem Kontrollkästchen Allow SSH traffic from (SSH-Verkehr zulassen von) die Option My IP (Meine IP) aus.

c. Um Datenverkehr aus dem Internet zu Ihrer Instance zuzulassen, aktivieren Sie die folgenden Kontrollkästchen:

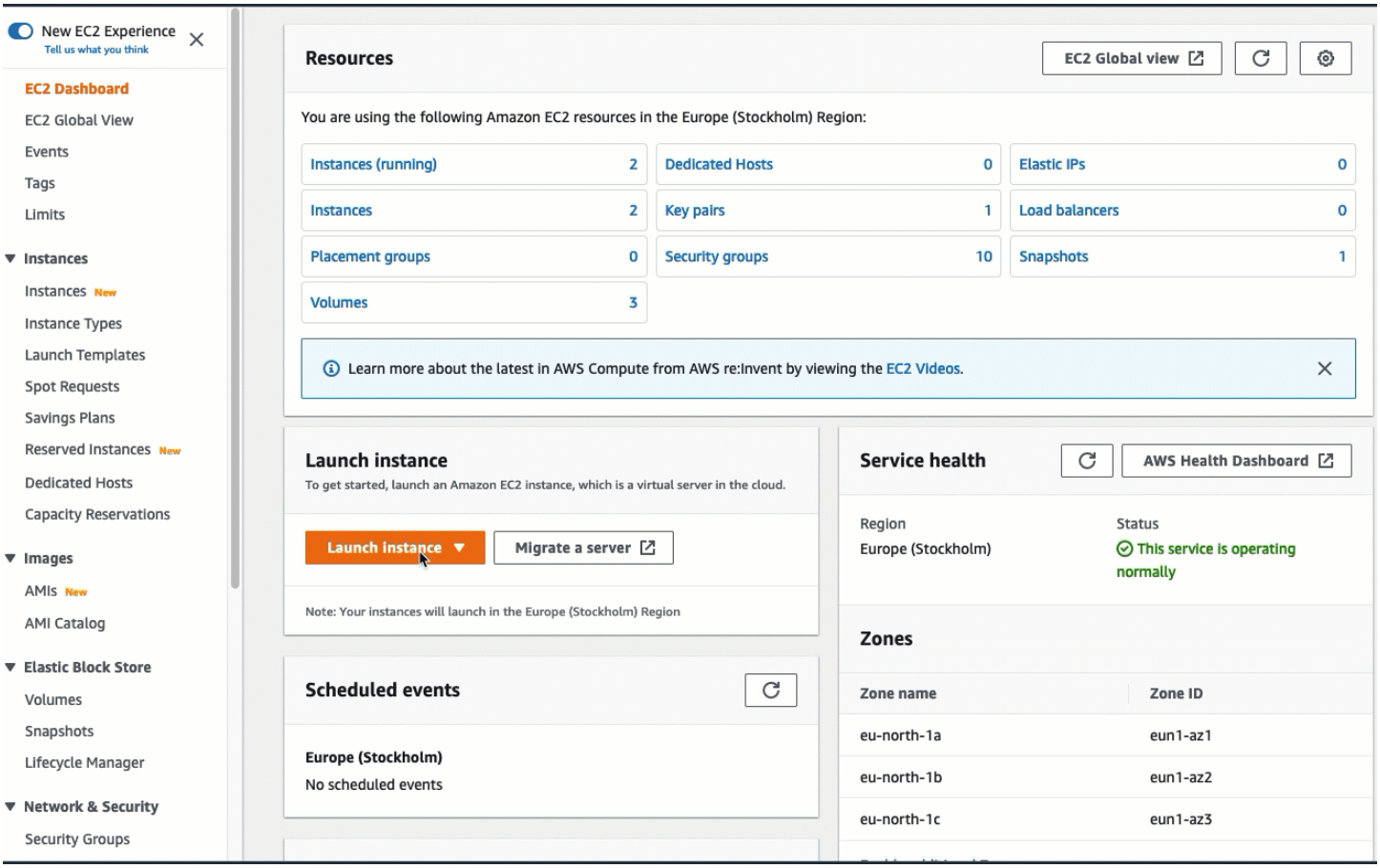
   - Allow HTTPs traffic from the internet (HTTPs-Datenverkehr aus dem Internet zulassen)
   - Allow HTTP traffic from the internet (HTTP-Datenverkehr aus dem Internet zulassen)

8. Überprüfen Sie im Bereich Summary (Übersicht) Ihre Instance-Konfiguration und wählen Sie dann Launch instance (Instance starten) aus.
9. Wählen Sie View all Instances (Alle Instances anzeigen) aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren. Ihre Instance befindet sich zunächst in einem `pending`-Status und wechselt dann in den `running`-Status.

   Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Weitere Informationen über das Starten einer Instance finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Animation anzeigen: Starten einer EC2-Instance



Sie sind jetzt bereit für Aufgabe 2: Erstellen einer RDS-Datenbank und automatisches Verbinden mit Ihrer EC2-Instance.

Aufgabe 2: Erstellen einer RDS-Datenbank und automatisches Verbinden mit Ihrer EC2-Instance

Aufgabenziel

Ziel dieser Aufgabe ist es, eine RDS-Datenbank zu erstellen und das automatische Verbindungsfeature in der RDS-Konsole zu verwenden, um die Verbindung zwischen Ihrer EC2-Instance und Ihrer RDS-Datenbank automatisch zu konfigurieren.

Schritte zum Erstellen einer RDS-Datenbank

Führen Sie die folgenden Schritte aus, um eine RDS-Datenbank zu erstellen und sie mithilfe des automatischen Features in der RDS-Konsole mit Ihrer EC2-Instance zu verbinden.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Erstellen einer RDS-Datenbank und automatisches Verbinden mit einer EC2-Instance.

DB-Instance-Konfiguration

Mit den Schritten in dieser Aufgabe wird die DB-Instance wie folgt konfiguriert:

- Engine-Typ: MySQL
- Vorlage: Kostenloses Kontingent
- DB-Instance-Kennung: **`tutorial-database`**
- DB-Instance-Klasse: `db.t3.micro`

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

So erstellen Sie eine RDS-Datenbank und verbinden sie automatisch mit einer EC2-Instance

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der Regionsauswahl (oben rechts) die aus, AWS-Region in der Sie die EC2-Instance erstellt haben. Die EC2-Instance und die RDS-Datenbank müssen sich in der gleichen Region befinden.
3. Wählen Sie im Dashboard Create database (Datenbank erstellen) aus.
4. Überprüfen Sie unter Choose a database creation method (Datenbankerstellungsmethode auswählen), ob Standard create (Standarderstellung) ausgewählt ist. Wenn Sie Easy create (Einfache Erstellung) wählen, ist das automatische Verbindungsfeature nicht verfügbar.
5. Wählen Sie unter Engine options (Engine-Optionen) für Engine type (Engine-Typ) die Option MySQL aus.
6. Wählen Sie unter Templates (Vorlagen) eine Beispielvorlage aus, die Ihren Anforderungen entspricht. Wählen Sie für dieses Tutorial die Option Free tier (Kostenloses Kontingent), um kostenlos eine Datenbank zu erstellen. Beachten Sie jedoch, dass das kostenlose Kontingent nur verfügbar ist, wenn Ihr Konto weniger als 12 Monate alt ist. Es gelten andere Einschränkungen. Sie können mehr darüber erfahren, indem Sie auf den Info-Link im Feld Free tier (Kostenloses Kontingent) klicken.
7. Führen Sie unter Settings (Einstellungen) die folgenden Schritte aus:

a. Geben Sie unter DB instance identifier (DB-Instance-Kennung) einen Namen für die Datenbank ein. Geben Sie für dieses Tutorial **`tutorial-database`** ein.

b. Behalten Sie für Master username (Master-Benutzername) den Standardnamen **`admin`** bei.

c. Geben Sie unter Master password (Master-Passwort) ein Passwort ein, das Sie sich für dieses Tutorial merken können, und geben Sie dann unter Confirm password (Passwort bestätigen) das Passwort erneut ein.

8. Behalten Sie unter Instance configuration (Instance-Konfiguration) für die DB instance class (DB-Instance-Klasse) die Standardeinstellung db.t3.micro bei. Wenn Ihr Konto weniger als 12 Monate alt ist, können Sie diese Instance kostenlos verwenden. Es gelten andere Einschränkungen. Weitere Informationen finden Sie unter Kostenloses Kontingent für AWS.

9. Wählen Sie unter Connectivity (Verbindung) für Compute resource (Rechenressource) die Option Connect to an EC2 compute resource (Mit einer EC2-Rechenressource verbinden) aus. Dies ist das automatische Verbindungsfeature in der RDS-Konsole.

10. Wählen Sie für die EC2 instance (EC2-Instance), die EC2-Instance aus, zu der Sie eine Verbindung herstellen möchten. Für die Zwecke dieses Tutorials können Sie entweder die Instance wählen, die Sie in der vorherigen Aufgabe erstellt haben und die Sie **`tutorial-instance`** genannt haben oder eine andere bereits vorhandene Instance wählen. Wenn Ihre Instance nicht in der Liste angezeigt wird, wählen Sie das Aktualisierungssymbol rechts neben Connectivity (Verbindung) aus.

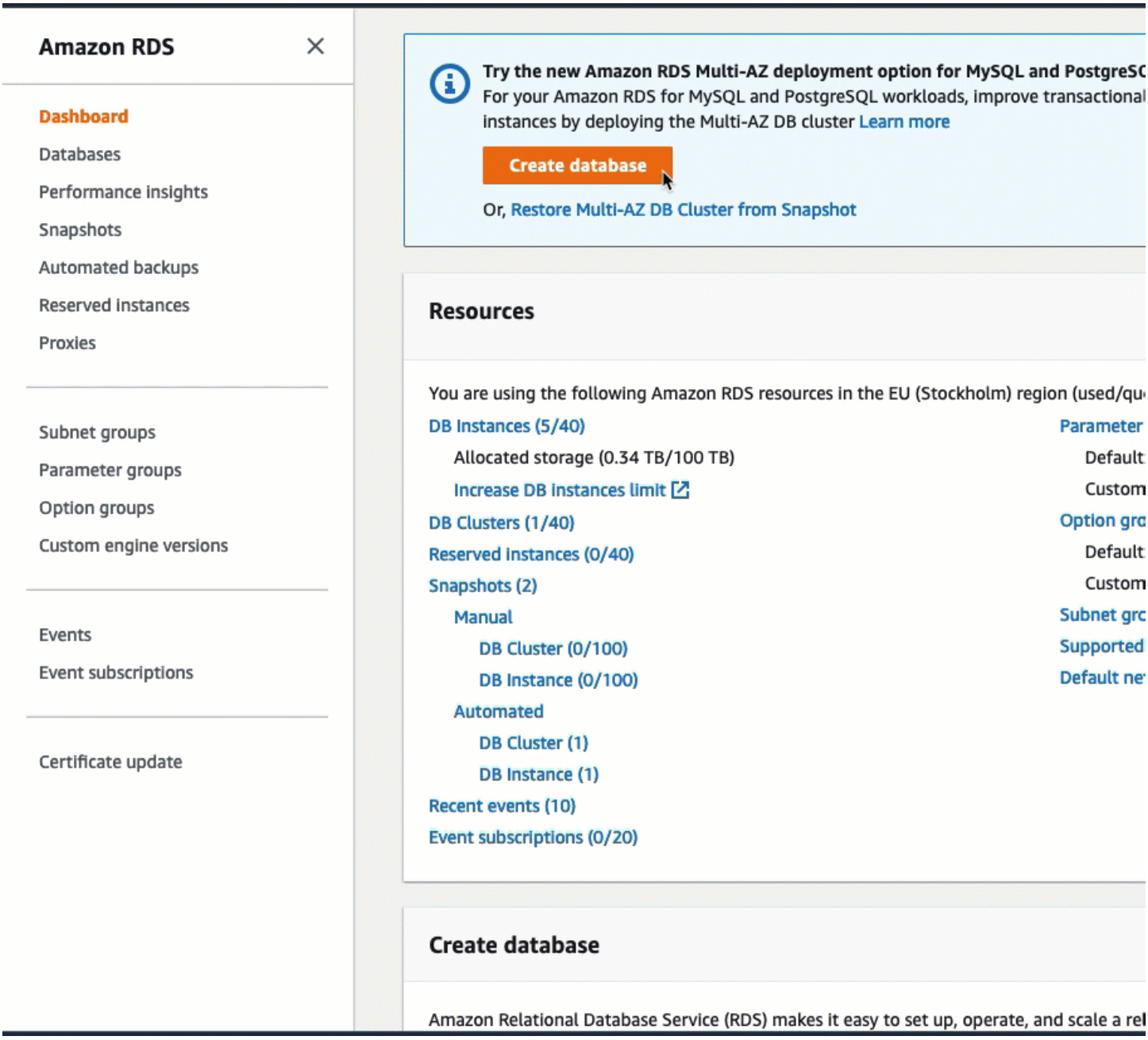
    Wenn Sie das automatische Verbindungsfeature verwenden, wird dieser EC2-Instance eine Sicherheitsgruppe hinzugefügt, und der RDS-Datenbank wird eine weitere Sicherheitsgruppe hinzugefügt. Die Sicherheitsgruppen werden automatisch so konfiguriert, dass der Datenverkehr zwischen der EC2-Instance und der RDS-Datenbank zugelassen wird. In der nächsten Aufgabe überprüfen Sie, ob die Sicherheitsgruppen erstellt und der EC2-Instance und der RDS-Datenbank zugewiesen wurden.

11. Wählen Sie Datenbank erstellen aus.

    Auf dem Bildschirm Databases (Datenbanken) lautet der Status der neuen Datenbank Creating (Wird erstellt), bis die Datenbank einsatzbereit ist. Wenn sich der Status in Available (Verfügbar) ändert, können Sie eine Verbindung zur Datenbank herstellen. Abhängig von der Klasse der Datenbank und vom verfügbaren Speicherplatz kann es bis zu 20 Minuten dauern, bis die neue Datenbank verfügbar ist.

Weitere Informationen finden Sie unter Konfigurieren der automatischen Netzwerkverbindung mit einer EC2-Instance im Amazon-RDS-Benutzerhandbuch.

Animation anzeigen: Erstellen einer RDS-Datenbank und automatisches Verbinden mit einer EC2-Instance



Sie sind jetzt bereit für Aufgabe 3: Überprüfen der Verbindungskonfiguration.

Aufgabe 3: Überprüfen der Verbindungskonfiguration

Aufgabenziel

Ziel dieser Aufgabe ist es, zu überprüfen, ob die beiden Sicherheitsgruppen erstellt und der Instance und der Datenbank zugewiesen wurden.

Wenn Sie das automatische Verbindungsfeature in der RDS-Konsole verwenden, um die Verbindung zu konfigurieren, werden die Sicherheitsgruppen automatisch erstellt und der Instance und Datenbank wie folgt zugewiesen:

- Die Sicherheitsgruppe rds-ec2-***x*** wird erstellt und der RDS-Datenbank hinzugefügt. Es verfügt über eine eingehende Regel, die auf die Sicherheitsgruppe ec2-rds-***x*** als Quelle verweist. Dadurch kann der Datenverkehr von der EC2-Instance mit der Sicherheitsgruppe ec2-rds-***x*** die RDS-Datenbank erreichen.
- Die Sicherheitsgruppe ec2-rds-***x*** wird erstellt und der EC2-Instance hinzugefügt. Es verfügt über eine ausgehende Regel, die auf die Sicherheitsgruppe rds-ec2-***x*** als Ziel verweist. Dadurch kann der Datenverkehr von der EC2-Instance die RDS-Datenbank mit der Sicherheitsgruppe rds-ec2-***x*** erreichen.

Schritte zum Überprüfen der Verbindungskonfiguration

Führen Sie die folgenden Schritte aus, um die Verbindungskonfiguration zu überprüfen.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Überprüfen der Verbindungskonfiguration.

So überprüfen Sie die Verbindungskonfiguration mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die EC2-Instance aus, die Sie in der vorherigen Aufgabe für die Verbindung mit der RDS-Datenbank ausgewählt haben, und wählen Sie die Registerkarte Security (Sicherheit) aus.
4. Überprüfen Sie unter Security details (Sicherheitsdetails), Security groups (Sicherheitsgruppen), dass eine Sicherheitsgruppe mit dem Namen ec2-rds-***x*** in der Liste enthalten ist. *x* ist eine Zahl.
5. Wählen Sie die Sicherheitsgruppe ec2-rds-***x***, um sie zu öffnen.
6. Wählen Sie die Registerkarte Outbound rules (Ausgehende Regeln).

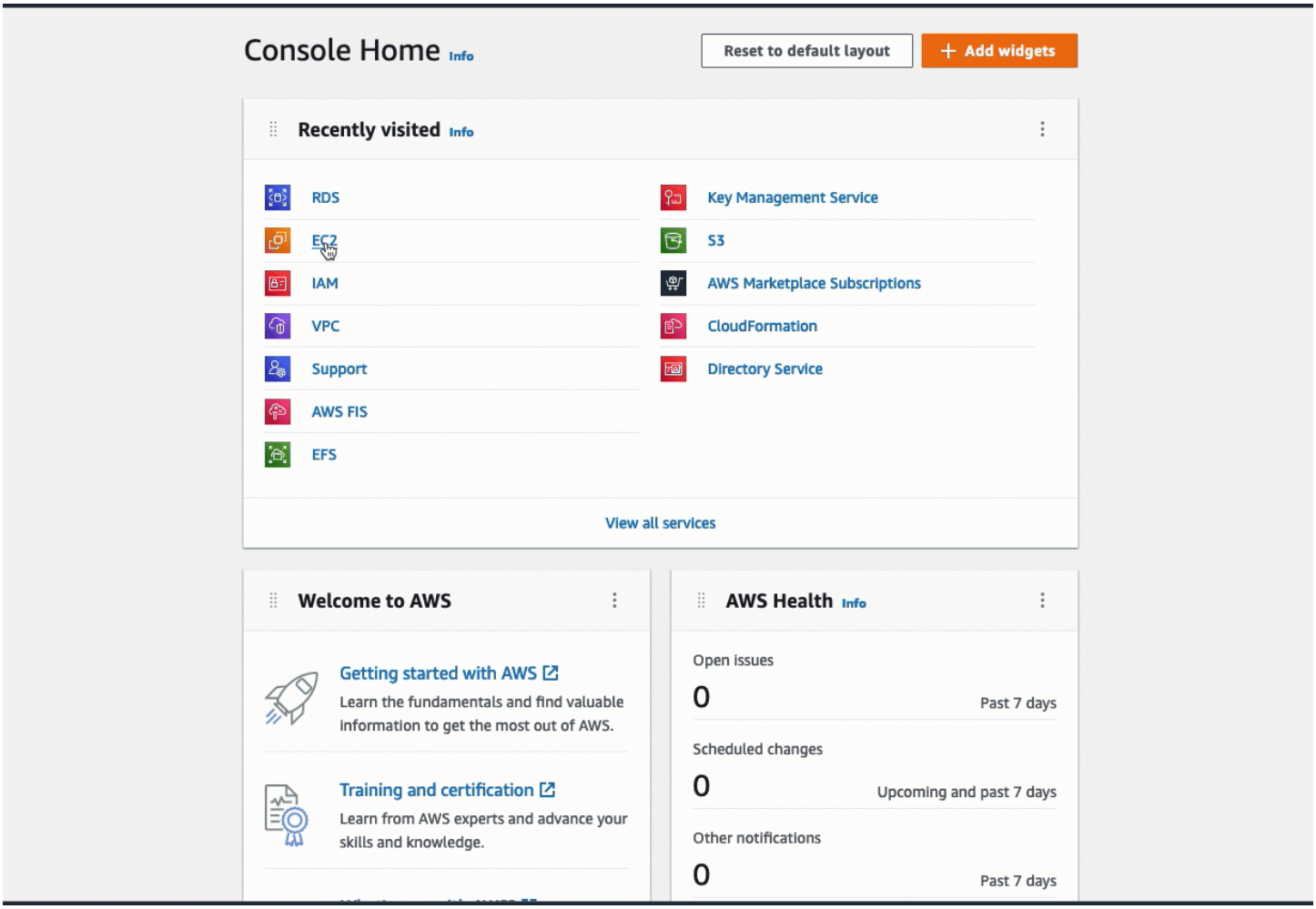
7. Stellen Sie wie folgt sicher, dass die folgende Sicherheitsgruppenregel vorhanden ist:

   - Typ: MYSQL/Aurora
   - Portbereich: 3306
   - Ziel: ***sg-1234567890example*** / rds-ec2-***x***
   - Beschreibung: Regel zum Zulassen von Verbindungen zu **`database-tutorial`** von allen Instances, an denen diese Sicherheitsgruppe angefügt ist
8. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
9. Wählen Sie im Navigationsbereich Databases (Datenbanken) aus.
10. Wählen Sie die RDS-Datenbank aus, die Sie für dieses Tutorial erstellt haben.
11. Überprüfen Sie auf der Registerkarte Connectivity & security (Verbindung und Sicherheit) unter Security (Sicherheit), VPC security groups (VPC-Sicherheitsgruppen), dass eine Sicherheitsgruppe mit dem Namen rds-ec2-***x*** angezeigt wird.
12. Wählen Sie die Sicherheitsgruppe rds-ec2-***x*** aus. Der Bildschirm Security Groups (Sicherheitsgruppen) in der EC2-Konsole wird geöffnet.
13. Wählen Sie die Sicherheitsgruppe rds-ec2-***x*** aus und öffnen Sie sie.
14. Wählen Sie die Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) aus.
15. Stellen Sie wie folgt sicher, dass die folgende Sicherheitsgruppenregel vorhanden ist:

    - Typ: MYSQL/Aurora
    - Portbereich: 3306
    - Quelle: ***sg-0987654321example*** / ec2-rds-***x*** – Dies ist die Sicherheitsgruppe, die der EC2-Instance zugewiesen ist, die Sie in den vorherigen Schritten überprüft haben.
    - Beschreibung: Rule to allow connections from EC2 instances with ***sg-1234567890example*** attached (Regel zum Zulassen von Verbindungen von EC2-Instances mit angefügtem sg-1234567890example)

    Indem Sie überprüfen, ob diese Sicherheitsgruppen und Sicherheitsgruppenregeln vorhanden sind und ob sie der RDS-Datenbank und der EC2-Instance wie in diesem Verfahren beschrieben zugewiesen sind, können Sie überprüfen, ob die Verbindung automatisch konfiguriert wurde, indem Sie das automatische Verbindungsfeature verwenden.

Animation anzeigen: Überprüfen der Verbindungskonfiguration



Sie haben Option 2 dieses Tutorials abgeschlossen. Sie können jetzt Option 3 abschließen, in der Sie erfahren, wie Sie die Sicherheitsgruppen, die automatisch in Option 2 erstellt wurden, manuell konfigurieren.

Option 3: Manuelles Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank durch Nachahmung des automatischen Verbindungsfeatures

Ziel

Das Ziel von Option 3 besteht darin, zu lernen, wie die Verbindung zwischen einer EC2-Instance und einer RDS-Datenbank manuell konfiguriert wird, indem die Konfiguration des automatischen Verbindungsfeatures manuell reproduziert wird.

Bevor Sie beginnen

Sie benötigen Folgendes, um dieses Tutorial abzuschließen:

- Eine EC2-Instance, die sich in derselben VPC wie die RDS-Datenbank befindet. Sie können entweder eine vorhandene EC2-Instance verwenden oder die Schritte in Aufgabe 1 ausführen, um eine neue Instance zu erstellen.
- Eine RDS-Datenbank, die sich in derselben VPC wie die EC2-Instance befindet. Sie können entweder eine vorhandene RDS-Datenbank verwenden oder die Schritte in Aufgabe 2 ausführen, um eine neue Datenbank zu erstellen.
- Berechtigungen zum Aufrufen der folgenden Operationen. Wenn Sie Option 1 dieses Tutorials abgeschlossen haben, verfügen Sie bereits über diese Berechtigungen.
  - `ec2:AssociateRouteTable`
  - `ec2:AuthorizeSecurityGroupEgress`
  - `ec2:CreateRouteTable`
  - `ec2:CreateSecurityGroup`
  - `ec2:CreateSubnet`
  - `ec2:DescribeInstances`
  - `ec2:DescribeNetworkInterfaces`
  - `ec2:DescribeRouteTables`
  - `ec2:DescribeSecurityGroups`
  - `ec2:DescribeSubnets`
  - `ec2:ModifyNetworkInterfaceAttribute`
  - `ec2:RevokeSecurityGroupEgress`

Aufgaben zur Erledigung von Option 3

- Aufgabe 1: Starten einer EC2-Instance – optional
- Aufgabe 2: Erstellen einer RDS-Datenbank – optional
- Aufgabe 3: Manuelles Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank, durch Erstellen von Sicherheitsgruppen und deren Zuweisung zu den Instances

Aufgabe 1: Starten einer EC2-Instance – optional

> **Note**
>
> Das Starten einer Instance steht nicht im Mittelpunkt dieses Tutorials. Wenn Sie bereits über eine Amazon-EC2-Instance verfügen und diese in diesem Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.

Aufgabenziel

Ziel dieser Aufgabe ist es, eine EC2-Instance zu starten, damit Sie Aufgabe 3 abschließen können, in der Sie die Verbindung zwischen Ihrer EC2-Instance und Ihrer Amazon RDS-Datenbank konfigurieren.

Schritte für das Starten einer EC2-Instance

Führen Sie die folgenden Schritte aus, um eine EC2-Instance für dieses Tutorial zu starten.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Starten einer EC2-Instance.

Konfigurieren der EC2-Instance

Mit den Schritten in dieser Aufgabe wird die EC2-Instance wie folgt konfiguriert:

- Instance-Name: **`tutorial-instance`**
- AMI: Amazon Linux 2
- Instance-Typ: `t2.micro`
- Öffentliche IP automatisch zuweisen: Aktiviert
- Sicherheitsgruppe mit den folgenden drei Regeln:
  - SSH von Ihrer IP-Adresse zulassen
  - HTTPS-Datenverkehr von überall zulassen
  - HTTP-Datenverkehr von überall zulassen

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

Starten Sie EC2-Instances wie folgt:

1. Melden Sie sich bei der Amazon EC2 EC2-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im EC2-Dashboard die Option Launch Instance (Instance starten) aus.
3. Geben Sie unter Name and tags (Name und Tags) für Name einen Namen ein, um Ihre Instance zu identifizieren. Geben Sie für dieses Tutorial der Instance den Namen **`tutorial-instance-manual-1`**. Der Instance-Name ist zwar nicht obligatorisch, aber er hilft Ihnen bei der Identifizierung.
4. Wählen Sie unter Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI aus, das Ihren Webserver-Anforderungen entspricht. Dieses Tutorial verwendet Amazon Linux.
5. Wählen Sie unter Instance type (Instance-Typ) für Instance type (Instance-Typ) einen Instance-Typ aus, der Ihren Webserver-Anforderungen entspricht. In diesem Tutorial wird ein `t2.micro` verwendet.

   > **Note**
   >
   > Sie können Amazon EC2 im Rahmen des kostenlosen Kontingents verwenden, sofern Ihr AWS Konto weniger als 12 Monate alt ist und Sie einen `t2.micro` Instance-Typ wählen (oder `t3.micro` in Regionen, in denen dieser nicht verfügbar `t2.micro` ist).

6. Wählen Sie unter Key pair (login) (Schlüsselpaar (Anmeldung)) für Key pair name (Schlüsselpaar-Name) Ihr Schlüsselpaar aus.
7. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:

   a. Wenn Sie für Network (Netzwerk) und Subnet (Subnetz) keine Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, können Sie die Standardeinstellungen beibehalten.

      Wenn Sie Änderungen an Ihrer Standard-VPC oder Ihren Subnetzen vorgenommen haben, überprüfen Sie Folgendes:

      i. Die Instance muss sich in derselben VPC befinden wie die RDS-Datenbank. Standardmäßig haben Sie nur eine VPC.

ii. Die VPC, in der Sie Ihre Instance starten, muss mit einem Internet-Gateway verbunden sein, damit Sie über das Internet auf Ihren Webserver zugreifen können. Ihre Standard-VPC wird automatisch mit einem Internet-Gateway eingerichtet.

iii. Um sicherzustellen, dass Ihre Instance eine öffentliche IP-Adresse erhält, überprüfen Sie für Auto-assign public IP (Automatische Zuweisung öffentlicher IP), dass Enable (Aktivieren) ausgewählt ist. Wenn Disable (Deaktivieren) ausgewählt ist, wählen Sie Edit (Bearbeiten) (rechts neben Network Settings (Netzwerkeinstellungen)) und dann für Auto-assign public IP (Öffentliche IP automatisch zuweisen) die Option Enable (Aktivieren) aus.

b. Um mithilfe von SSH eine Verbindung zu Ihrer Instance herzustellen, benötigen Sie eine Sicherheitsgruppenregel, die SSH- (Linux) oder RDP-Datenverkehr (Windows) von der öffentlichen IPv4-Adresse Ihres Computers autorisiert. Wenn Sie eine Instance starten, wird standardmäßig eine neue Sicherheitsgruppe mit einer Regel erstellt, die eingehenden SSH-Datenverkehr von überall zulässt.

   Um sicherzustellen, dass nur Ihre IP-Adresse eine Verbindung zu Ihrer Instance herstellen kann, wählen Sie unter Firewall (security groups) (Firewall (Sicherheitsgruppen)) in der Dropdown-Liste neben dem Kontrollkästchen Allow SSH traffic from (SSH-Verkehr zulassen von) die Option My IP (Meine IP) aus.

c. Um Datenverkehr aus dem Internet zu Ihrer Instance zuzulassen, aktivieren Sie die folgenden Kontrollkästchen:

   - Allow HTTPs traffic from the internet (HTTPs-Datenverkehr aus dem Internet zulassen)
   - Allow HTTP traffic from the internet (HTTP-Datenverkehr aus dem Internet zulassen)

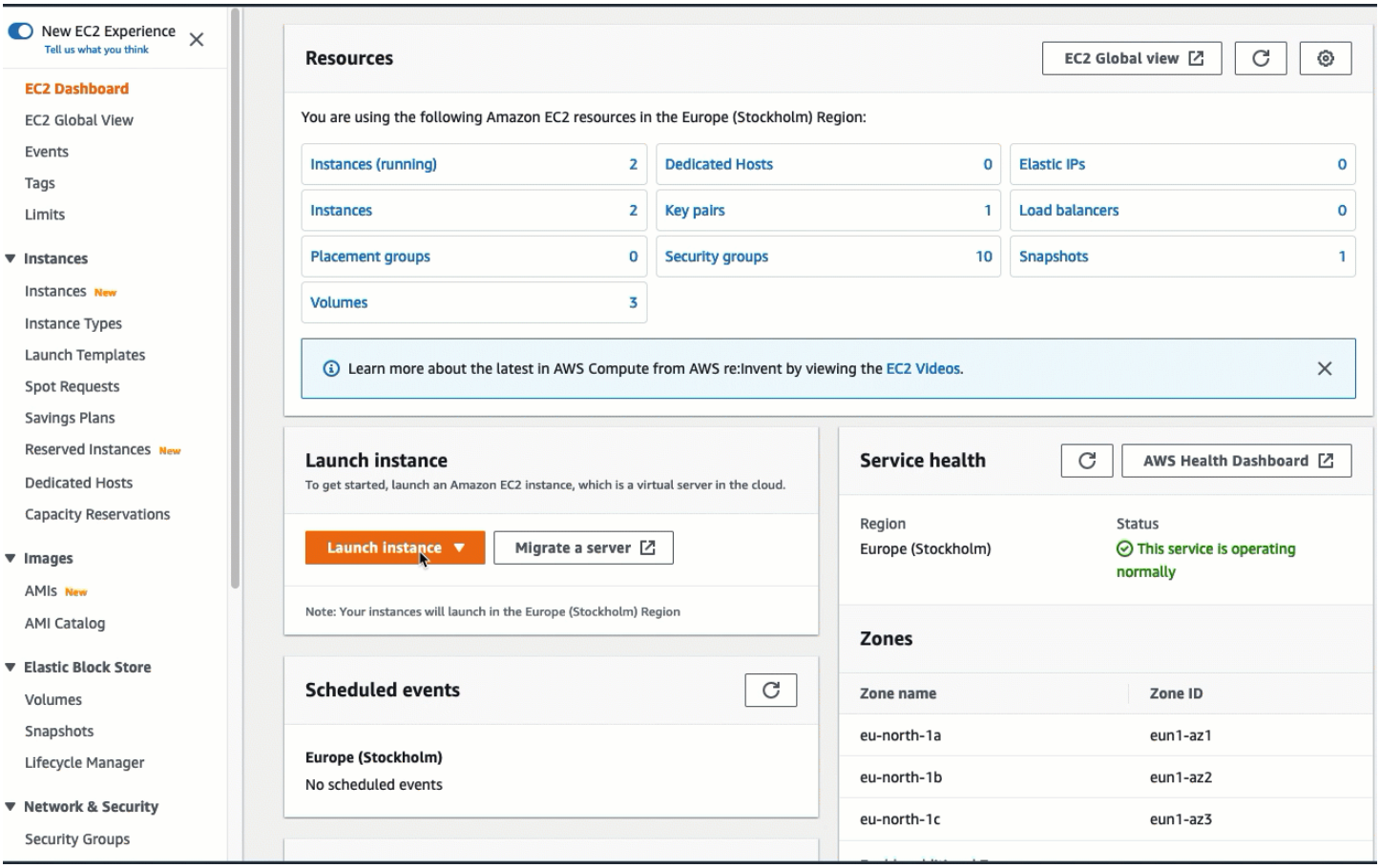
8. Überprüfen Sie im Bereich Summary (Übersicht) Ihre Instance-Konfiguration und wählen Sie dann Launch instance (Instance starten) aus.

9. Wählen Sie View all Instances (Alle Instances anzeigen) aus, um die Bestätigungsseite zu schließen und zur Konsole zurückzukehren. Ihre Instance befindet sich zunächst in einem `pending`-Status und wechselt dann in den `running`-Status.

   Wenn die Instance nicht gestartet wird oder der Status sofort `terminated` statt `running` anzeigt, finden Sie weitere Informationen unter Beheben von Problemen beim Starten von Instances.

Weitere Informationen über das Starten einer Instance finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Animation anzeigen: Starten einer EC2-Instance



Sie sind nun bereit für Aufgabe 2: Erstellen einer RDS-Datenbank – optional.

Aufgabe 2: Erstellen einer RDS-Datenbank – optional

> **Note**
>
> Das Erstellen einer RDS-Datenbank steht in diesem Teil des Tutorials nicht im Mittelpunkt. Wenn Sie bereits über eine RDS-Datenbank verfügen und diese für dieses Tutorial verwenden möchten, können Sie diese Aufgabe überspringen.

Aufgabenziel

Ziel dieser Aufgabe ist es, eine RDS-Datenbank zu erstellen. Sie verwenden diese Instance in Aufgabe 3, wenn Sie sie mit Ihrer EC2-Instance verbinden.

Schritte zum Erstellen einer RDS-Datenbank

Führen Sie die folgenden Schritte aus, um eine RDS-Datenbank für Option 3 dieses Tutorials zu erstellen.

Eine Animation dieser Schritte finden Sie unter Animation anzeigen: Erstellen einer DB-Instance.

RDS-Datenbankkonfiguration

Mit den Schritten in dieser Aufgabe wird die RDS-Datenbank wie folgt konfiguriert:

- Engine-Typ: MySQL
- Vorlage: Kostenloses Kontingent
- DB-Instance-Kennung: **`tutorial-database-manual`**
- DB-Instance-Klasse: `db.t3.micro`

> **Important**
>
> In einer Produktionsumgebung sollten Sie Ihre Instance so konfigurieren, dass sie Ihren speziellen Anforderungen entspricht.

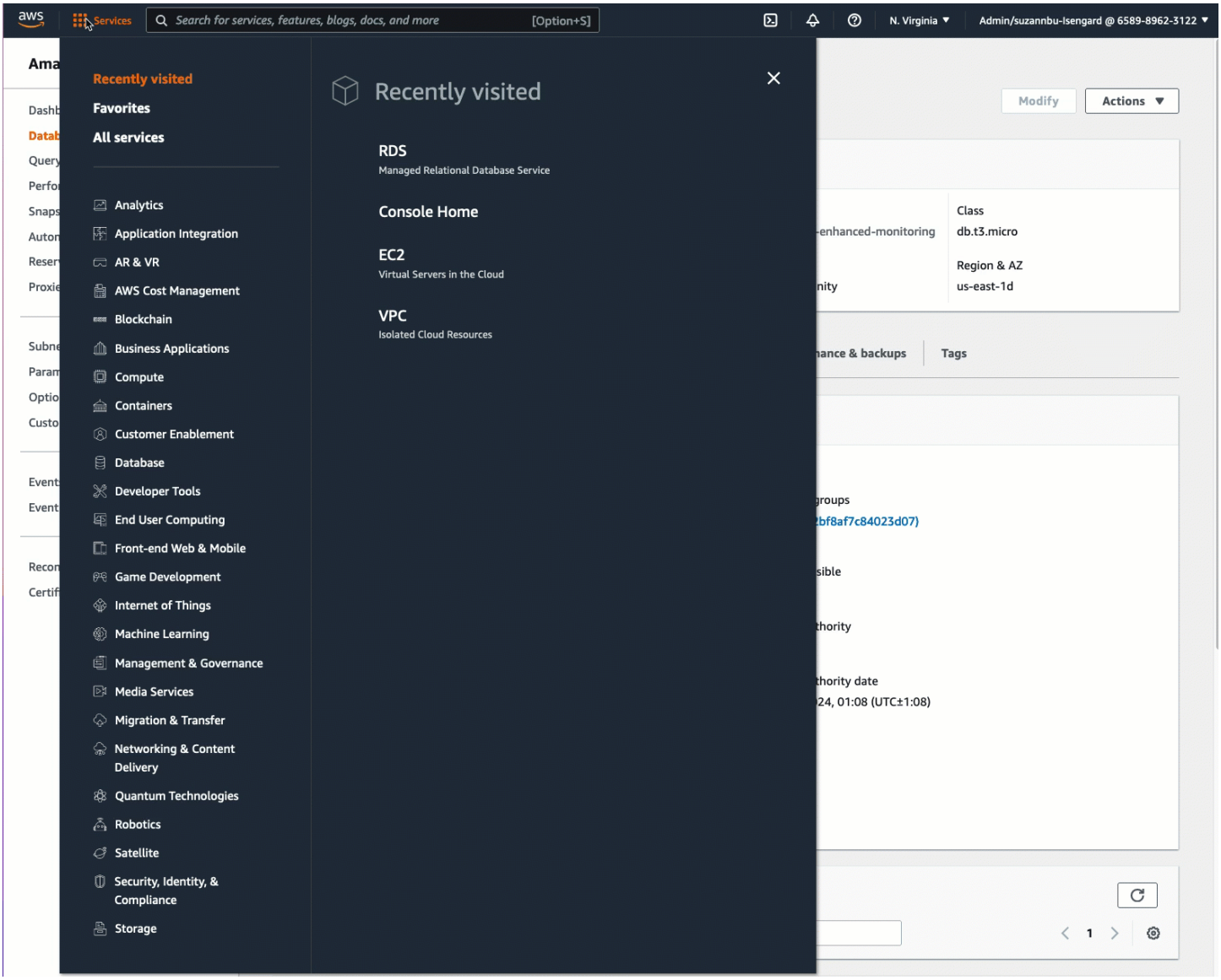
So erstellen Sie eine MySQL-DB-Instance

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie in der Regionsauswahl (oben rechts) die aus, AWS-Region in der Sie die EC2-Instance erstellt haben. Die EC2-Instance und die DB-Instance müssen sich in derselben Region befinden.
3. Wählen Sie im Dashboard Create database (Datenbank erstellen) aus.
4. Wählen Sie unter Choose a database creation method (Eine Datenbankerstellungsmethode auswählen) die Option Easy create (Einfache Erstellung) aus. Wenn Sie diese Option wählen, ist das automatische Verbindungsfeature zum automatischen Konfigurieren der Verbindung nicht verfügbar.
5. Wählen Sie unter Engine options (Engine-Optionen) für Engine type (Engine-Typ) die Option MySQL aus.
6. Wählen Sie in DB-Instance-Größe die Option Kostenloses Kontingent aus.

7. Geben Sie unter DB instance identifier (DB-Instance-Kennung) einen Namen für die Datenbank ein. Geben Sie für dieses Tutorial **`tutorial-database-manual`** ein.
8. Behalten Sie für Master username (Master-Benutzername) den Standardnamen **`admin`** bei.
9. Geben Sie unter Master password (Master-Passwort) ein Passwort ein, das Sie sich für dieses Tutorial merken können, und geben Sie dann unter Confirm password (Passwort bestätigen) das Passwort erneut ein.
10. Wählen Sie Datenbank erstellen aus.

    Auf dem Bildschirm Databases (Datenbanken) lautet der Status der neuen DB-Instance Creating (Wird erstellt), bis die DB-Instance einsatzbereit ist. Wenn sich der Status in Available (Verfügbar) ändert, können Sie die Verbindung zur DB-Instance herstellen. Abhängig von der Klasse der DB-Instance und vom verfügbaren Speicherplatz kann es bis zu 20 Minuten dauern, bis die neue DB-Instance verfügbar ist.

Animation anzeigen: Erstellen einer DB-Instance



Sie sind nun bereit für [Aufgabe 3: Manuelles Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank, durch Erstellen von Sicherheitsgruppen und deren Zuweisung zu den Instances](#).

Aufgabe 3: Manuelles Verbinden Ihrer EC2-Instance mit Ihrer RDS-Datenbank, durch Erstellen von Sicherheitsgruppen und deren Zuweisung zu den Instances

Aufgabenziel

Ziel dieser Aufgabe ist es, die Verbindungskonfiguration des automatischen Verbindungsfeatures zu reproduzieren, indem Sie Folgendes manuell ausführen: Sie erstellen zwei neue Sicherheitsgruppen und fügen dann jeweils eine Sicherheitsgruppe zur EC2-Instance und zur RDS-Datenbank hinzu.

Schritte zum Erstellen neuer Sicherheitsgruppen und Hinzufügen dieser zu den Instances

Führen Sie die folgenden Schritte aus, um eine EC2-Instance mit Ihrer RDS-Datenbank zu verbinden, indem Sie zwei neue Sicherheitsgruppen erstellen. Anschließend fügen Sie der EC2-Instance und der RDS-Datenbank jeweils eine Sicherheitsgruppe hinzu.

So erstellen Sie zwei neue Sicherheitsgruppen und weisen jeweils eine der EC2-Instance und der RDS-Datenbank zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Erstellen Sie zuerst die Sicherheitsgruppe, die der EC2-Instance hinzugefügt werden soll, wie folgt:
   a. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
   b. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
   c. Geben Sie unter Security group name (Name der Sicherheitsgruppe) einen aussagekräftigen Namen für die Sicherheitsgruppe ein. Geben Sie für dieses Tutorial **`ec2-rds-manual-configuration`** ein.
   d. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung ein. Geben Sie für dieses Tutorial **`EC2 instance security group to allow EC2 instance to securely connect to RDS database`** ein.
   e. Wählen Sie Sicherheitsgruppe erstellen aus. Sie kehren zu dieser Sicherheitsgruppe zurück, um eine ausgehende Regel hinzuzufügen, nachdem Sie die Sicherheitsgruppe der RDS-Datenbank erstellt haben.
3. Erstellen Sie nun die Sicherheitsgruppe, die Sie der RDS-Datenbank hinzufügen möchten, wie folgt:
   a. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
   b. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
   c. Geben Sie unter Security group name (Name der Sicherheitsgruppe) einen aussagekräftigen Namen für die Sicherheitsgruppe ein. Geben Sie für dieses Tutorial **`rds-ec2-manual-configuration`** ein.
   d. Geben Sie unter Description (Beschreibung) eine kurze Beschreibung ein. Geben Sie für dieses Tutorial **`RDS database security group to allow EC2 instance to securely connect to RDS database`** ein.

e. Wählen Sie unter Inbound rules (Eingehende Regeln) die Option Add rule (Regel hinzufügen) aus und gehen Sie wie folgt vor:

   i. Wählen Sie für Type (Typ) die Option MySQL/Aurora.

   ii. Wählen Sie als Source (Quelle) die EC2-Instance-Sicherheitsgruppe ec2-rds-manual-configuration aus, die Sie in Schritt 2 dieses Verfahrens erstellt haben.

f. Wählen Sie Sicherheitsgruppe erstellen aus.

4. Bearbeiten Sie die EC2-Instance-Sicherheitsgruppe wie folgt, um eine Regel für ausgehenden Datenverkehr hinzuzufügen:

   a. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.

   b. Wählen Sie die EC2-Instance-Sicherheitsgruppe (Sie haben sie **`ec2-rds-manual-configuration`** benannt) und wählen Sie die Registerkarte Outbound rules (Ausgehende Regeln) aus.

   c. Wählen Sie Edit outbound rules (Ausgehende Regeln bearbeiten).

   d. Wählen Sie Add rule (Regel hinzufügen) und gehen Sie wie folgt vor:

      i. Wählen Sie für Type (Typ) die Option MySQL/Aurora.

      ii. Wählen Sie als Source (Quelle) die RDS-Datenbank-Sicherheitsgruppe rds-ec2-manual-configuration, die Sie in Schritt 3 dieses Verfahrens erstellt haben

      iii. Wählen Sie Save rules (Regeln speichern) aus.

5. Fügen Sie die EC2-Instance-Sicherheitsgruppe wie folgt zur EC2-Instance hinzu:

   a. Wählen Sie im Navigationsbereich Instances aus.

   b. Wählen Sie Ihre EC2-Instance aus und wählen Sie Actions (Aktionen), Security (Sicherheit), Change security groups (Sicherheitsgruppen ändern) aus.

   c. Wählen Sie unter Associated security groups (Zugeordnete Sicherheitsgruppen) das Feld Select security groups (Sicherheitsgruppen auswählen), wählen Sie ec2-rds-manual-configuration aus, die Sie zuvor erstellt haben, und wählen Sie dann Add security group (Sicherheitsgruppe hinzufügen) aus.

   d. Wählen Sie Speichern.

6. Fügen Sie die RDS-Datenbanksicherheitsgruppe wie folgt zur RDS-Datenbank hinzu:

   a. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.

b. Wählen Sie im Navigationsbereich Databases (Datenbanken) und wählen Sie Ihre Datenbank aus.

c. Wählen Sie Ändern aus.

d. Wählen Sie unter Connectivity (Verbindung) für die Security group (Sicherheitsgruppe), rds-ec2-manual-configuration aus, die Sie zuvor erstellt haben, und wählen Sie dann Continue (Fortfahren) aus.

e. Wählen Sie unter Scheduling of modifications (Planung von Änderungen) die Option Apply immediately (Sofort anwenden) aus.

f. Wählen Sie Modify DB Instance (DB-Instance ändern) aus.

Sie haben jetzt die manuellen Schritte abgeschlossen, die die automatischen Schritte nachahmen, die bei der Verwendung des automatischen Verbindungsfeatures ausgeführt werden.

Sie haben Option 3 dieses Tutorials abgeschlossen. Wenn Sie die Optionen 1, 2 und 3 abgeschlossen haben und die in diesem Tutorial erstellten Ressourcen nicht mehr benötigen, sollten Sie sie löschen, um unnötige Kosten zu vermeiden. Weitere Informationen finden Sie unter Bereinigen.

Bereinigen

Nachdem Sie das Tutorial abgeschlossen haben, empfiehlt es sich, alle Ressourcen zu bereinigen (zu löschen), die Sie nicht mehr verwenden möchten. Durch die Bereinigung von AWS Ressourcen wird verhindert, dass für Ihr Konto weitere Gebühren anfallen.

Themen

- Beenden Ihrer EC2-Instance
- Löschen Ihre RDS-Datenbank

Beenden Ihrer EC2-Instance

Wenn Sie eine EC2-Instance speziell für dieses Tutorial gestartet haben, können Sie sie beenden, damit keine damit verbundenen Gebühren anfallen.

Um eine Instance mithilfe der Konsole zu beenden

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Instance state (Instance-Status), Terminate instance (Instance beenden) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Beenden aus.

Löschen Ihre RDS-Datenbank

Wenn Sie eine RDS-Datenbank speziell für dieses Tutorial erstellt haben, können Sie sie löschen, damit keine damit verbundenen Gebühren anfallen.

Löschen einer RDS-Datenbank mithilfe der Konsole

1. Öffnen Sie die Amazon-RDS-Konsole unter https://console.aws.amazon.com/rds/.
2. Wählen Sie im Navigationsbereich Datenbanken aus.
3. Wählen Sie die RDS-Datenbank aus, die Sie für dieses Tutorial erstellt haben, und wählen Sie Actions (Aktionen), Delete (Löschen) aus.
4. Geben Sie **`delete me`** in das Feld ein und wählen Sie dann Delete (Löschen).

Identifizieren Sie Ihre EC2-Instances

Möglicherweise müssen Sie feststellen, ob Ihre Anwendung auf einer EC2-Instance ausgeführt wird, insbesondere wenn Sie eine gemischte Computerumgebung haben. Jede Instanz verfügt über ein signiertes Identitätsdokument für die Instanz, das Sie kryptografisch überprüfen können. Sie finden diese Dokumente unter der folgenden lokalen, nicht routbaren Adresse. `http://169.254.169.254/latest/dynamic/instance-identity/` Weitere Informationen finden Sie unter Instance-Identitätsdokumente.

Überprüfen des System-UUID

Sie können die System-UUID abrufen und im ersten Oktett der UUID danach suchen `EC2` (unter Linux kann das ein Kleinbuchstabe sein). `ec2` Diese Methode ist schnell, aber möglicherweise ungenau, da die Wahrscheinlichkeit gering ist, dass ein System, das keine EC2-Instanz ist, eine UUID hat, die mit diesen Zeichen beginnt. Darüber hinaus verwenden einige Versionen von SMBIOS das Little-Endian-Format, bei dem die UUID nicht am Anfang steht. `EC2` Dies kann bei EC2-Instances

der Fall sein, die SMBIOS 2.4 für Windows verwenden, oder bei anderen Linux-Distributionen als Amazon Linux 2, die über eine eigene Implementierung von SMBIOS verfügen.

Linux-Beispiel: Rufen Sie die UUID von DMI ab (nur HVM-AMIs)

Verwenden Sie den folgenden Befehl, um die UUID mit dem Desktop Management Interface (DMI) abzurufen:

```
[ec2-user ~]$ sudo dmidecode --string system-uuid
```

In der folgenden Beispielausgabe beginnt die UUID mit „EC2“. Es handelt sich daher wahrscheinlich um eine EC2 Instance.

```
EC2E1916-9099-7CAF-FD21-012345ABCDEF
```

In der folgenden Beispielausgabe ist die UUID im Little-Endian-Format dargestellt.

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Alternativ können Sie für Instances, die auf dem Nitro-System basieren, den folgenden Befehl verwenden:

```
[ec2-user ~]$ cat /sys/devices/virtual/dmi/id/board_asset_tag
```

Wenn die Ausgabe eine Instance-ID ist, ist das System als folgende Beispielausgabe eine EC2-Instance:

```
i-0af01c0123456789a
```

Linux-Beispiel: Holen Sie sich die UUID vom Hypervisor (nur PV-AMIs)

Verwenden Sie den folgenden Befehl, um die UUID vom Hypervisor zu erhalten:

```
[ec2-user ~]$ cat /sys/hypervisor/uuid
```

In der folgenden Beispielausgabe beginnt die UUID mit „ec2“. Es handelt sich daher wahrscheinlich um eine EC2 Instance.

```
ec2e1916-9099-7caf-fd21-012345abcdef
```

Windows-Beispiel: Rufen Sie die UUID mithilfe von WMI oder Windows ab PowerShell

Verwenden Sie die Windows-Verwaltungsinstrumentation-Befehlszeile (WMIC) wie folgt:

```
wmic path win32_computersystemproduct get uuid
```

Wenn Sie Windows verwenden, verwenden Sie das PowerShell Get-WmiObject Cmdlet alternativ wie folgt:

```
PS C:\> Get-WmiObject -query "select uuid from Win32_ComputerSystemProduct" | Select
 UUID
```

In der folgenden Beispielausgabe beginnt die UUID mit „EC2“. Es handelt sich daher wahrscheinlich um eine EC2 Instance.

```
EC2AE145-D1DC-13B2-94ED-012345ABCDEF
```

Bei Instances mit SMBIOS 2.4 kann die UUID im Little-Endian-Format angegeben werden, zum Beispiel:

```
45E12AEC-DCD1-B213-94ED-012345ABCDEF
```

Überprüfen der System-ID zur Generierung der virtuellen Maschine

Eine ID zur Generierung virtueller Maschinen besteht aus einem eindeutigen Puffer von 128 Bit, der als kryptografische, zufällige Ganzzahl-ID interpretiert wird. Sie können die ID zur Generierung der virtuellen Maschine abrufen, um Ihre Amazon-Elastic-Compute-Cloud-Instance zu identifizieren. Die Generierungs-ID wird im Gastbetriebssystem der Instance durch einen ACPI-Tabelleneintrag verfügbar gemacht. Der Wert ändert sich, wenn Ihre Maschine geklont, kopiert oder in AWS importiert wird, z. B. mit VM Import/Export.

Beispiel: Rufen Sie die Generierungs-ID der virtuellen Maschine von Linux ab

Sie können die folgenden Befehle verwenden, um die ID zur Generierung der virtuellen Maschine von Ihren Instances abzurufen, auf denen Linux ausgeführt wird.

Amazon Linux 2

1. Aktualisieren Sie Ihre vorhandenen Softwarepakete bei Bedarf mit dem folgenden Befehl:

```
sudo yum update
```

2. Wenn nötig, beziehen Sie das busybox-Paket mit dem folgenden Befehl:

```
sudo curl https://www.rpmfind.net/linux/epel/next/8/Everything/x86_64/Packages/
b/busybox-1.35.0-2.el8.next.x86_64.rpm --output busybox.rpm
```

3. Installieren Sie ggf. die Voraussetzungspakete mit dem folgenden Befehl:

```
sudo yum install busybox.rpm iasl -y
```

4. Führen Sie den folgenden `iasl`-Befehl aus, um eine Ausgabe aus der ACPI-Tabelle zu erzeugen:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

5. Führen Sie den folgenden Befehl aus, um die Ausgabe des `iasl`-Befehls zu prüfen:

```
cat SSDT2.dsl
```

Die Ausgabe sollte den Adressraum liefern, der zum Abrufen der ID zur Generierung der virtuellen Maschine erforderlich ist:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
```

```
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

6. (Optional) Erweitern Sie Ihre Terminalberechtigungen für die verbleibenden Schritte mit dem folgenden Befehl:

```
sudo -s
```

7. Verwenden Sie den folgenden Befehl, um den zuvor erfassten Adressraum zu speichern:

```
VMGN_ADDR=0xFED01000
```

8. Verwenden Sie den folgenden Befehl, um den Adressraum zu durchlaufen und die ID zur Generierung der virtuellen Maschine zu erstellen:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

9. Rufen Sie die ID zur Generierung der virtuellen Maschine mit dem folgenden Befehl aus der Ausgabedatei ab:

```
cat vmgenid ; echo
```

Die Ausgabe sollte in etwa wie folgt aussehen:

```
EC2F335D979132C4165896753E72BD1C
```

Ubuntu

1. Aktualisieren Sie Ihre vorhandenen Softwarepakete bei Bedarf mit dem folgenden Befehl:

```
sudo apt update
```

2. Installieren Sie ggf. die Voraussetzungspakete mit dem folgenden Befehl:

```
sudo apt install busybox iasl -y
```

3. Führen Sie den folgenden `iasl`-Befehl aus, um eine Ausgabe aus der ACPI-Tabelle zu erzeugen:

```
sudo iasl -p ./SSDT2 -d /sys/firmware/acpi/tables/SSDT2
```

4. Führen Sie den folgenden Befehl aus, um die Ausgabe des `iasl`-Befehls zu prüfen:

```
cat SSDT2.dsl
```

Die Ausgabe sollte den Adressraum liefern, der zum Abrufen der ID zur Generierung der virtuellen Maschine erforderlich ist:

```
Intel ACPI Component Architecture
ASL+ Optimizing Compiler/Disassembler version 20190509
Copyright (c) 2000 - 2019 Intel Corporation

File appears to be binary: found 32 non-ASCII characters, disassembling
Binary file appears to be a valid ACPI table, disassembling
Input file /sys/firmware/acpi/tables/SSDT2, Length 0x7B (123) bytes
ACPI: SSDT 0x0000000000000000 00007B (v01 AMAZON AMZNSSDT 00000001 AMZN
 00000001)
Pass 1 parse of [SSDT]
Pass 2 parse of [SSDT]
Parsing Deferred Opcodes (Methods/Buffers/Packages/Regions)

Parsing completed
Disassembly completed
ASL Output:    ./SSDT2.dsl - 1065 bytes
$
/*
* Intel ACPI Component Architecture
* AML/ASL+ Disassembler version 20190509 (64-bit version)
* Copyright (c) 2000 - 2019 Intel Corporation
*
* Disassembling to symbolic ASL+ operators
*
* Disassembly of /sys/firmware/acpi/tables/SSDT2, Tue Mar 29 16:15:14 2022
*
* Original Table Header:
*     Signature        "SSDT"
*     Length           0x0000007B (123)
*     Revision         0x01
*     Checksum         0xB8
*     OEM ID           "AMAZON"
*     OEM Table ID     "AMZNSSDT"
*     OEM Revision     0x00000001 (1)
*     Compiler ID      "AMZN"
*     Compiler Version 0x00000001 (1)
*/
DefinitionBlock ("", "SSDT", 1, "AMAZON", "AMZNSSDT", 0x00000001)
{
Scope (\_SB)
{
    Device (VMGN)
    {
```

```
        Name (_CID, "VM_Gen_Counter")  // _CID: Compatible ID
        Name (_DDN, "VM_Gen_Counter")  // _DDN: DOS Device Name
        Name (_HID, "AMZN0000")  // _HID: Hardware ID
        Name (ADDR, Package (0x02)
        {
            0xFED01000,
            Zero
        })
    }
}
}
```

5. (Optional) Erweitern Sie Ihre Terminalberechtigungen für die verbleibenden Schritte mit dem folgenden Befehl:

```
sudo -s
```

6. Verwenden Sie die folgenden Befehle, um den zuvor erfassten Adressraum zu speichern:

```
VMGN_ADDR=0xFED01000
```

7. Verwenden Sie den folgenden Befehl, um den Adressraum zu durchlaufen und die ID zur Generierung der virtuellen Maschine zu erstellen:

```
for offset in 0x0 0x4 0x8 0xc; do busybox devmem $(($VMGN_ADDR + $offset)) | sed
 's/0x//' | sed -z '$ s/\n$//' >> vmgenid; done
```

8. Rufen Sie die ID zur Generierung der virtuellen Maschine mit dem folgenden Befehl aus der Ausgabedatei ab:

```
cat vmgenid ; echo
```

   Die Ausgabe sollte in etwa wie folgt aussehen:

```
EC2F335D979132C4165896753E72BD1C
```

Beispiel: Rufen Sie die Generierungs-ID der virtuellen Maschine von Windows ab

Sie können eine Beispielanwendung erstellen, um die ID zur Generierung der virtuellen Maschine von Ihren Instances abzurufen, auf denen Windows ausgeführt wird. Weitere Informationen finden Sie unter Erhalten der ID zur Generierung der virtuellen Maschine in der Microsoft-Dokumentation.

Systemeinstellungen für Ihre Amazon EC2 EC2-Instance verwalten

Nachdem Sie Ihre Instance gestartet haben, können Sie sich als Administrator anmelden, um Änderungen vorzunehmen. Dieser Abschnitt konzentriert sich auf die Verwaltung der Systemeinstellungen für Ihre Instance.

Inhalt

Stellen Sie die Zeit für Ihre Amazon EC2 EC2-Instance ein

Eine konsistente und genaue Zeitreferenz auf Ihrer Amazon EC2 EC2-Instance ist für viele Serveraufgaben und -prozesse von entscheidender Bedeutung. Zeitstempel in Systemprotokollen sind wichtig, um den Zeitpunkt, zu dem Probleme aufgetreten sind, sowie die chronologische Reihenfolge von Ereignissen zu ermitteln. Wenn Sie das AWS CLI oder ein AWS SDK verwenden, um Anfragen von Ihrer Instance aus zu stellen, signieren diese Tools Anfragen in Ihrem Namen. Wenn die Datums- und Uhrzeiteinstellungen Ihrer Instance falsch sind, kann dies zu einer Diskrepanz zwischen dem Datum in der Signatur und dem Datum der Anfrage führen, was zur AWS Ablehnung Ihrer Anfragen führen kann.

Für diesen wichtigen Aspekt stellt Amazon den Amazon Time Sync Service bereit, der über alle EC2-Instances zugänglich ist und von verschiedenen AWS-Services verwendet. Der Service verwendet jeweils eine Flotte von satellitengestützten und atomaren Referenzuhren, AWS-Region um genaue und aktuelle Zeitwerte des globalen Standards Coordinated Universal Time (UTC) zu liefern.

Der Amazon Time Sync Service verwendet entweder das Network Time Protocol (NTP) oder stellt in unterstützten Instances eine lokale Precision Time Protocol (PTP)-Hardware-Uhr bereit. Die PTP-Hardware-Uhr unterstützt entweder NTP oder eine direkte PTP-Verbindung. Die NTP-Verbindung und die direkte PTP-Verbindung verwenden zwar die gleiche hochpräzise Zeitquelle, die direkte PTP-Verbindung ist jedoch genauer als die NTP-Verbindung. Die NTP-Verbindung mit dem Amazon Time Sync Service unterstützt „Leap Smearing“ (Aufteilung von Schaltsekunden). Bei der PTP-Verbindung mit der PTP-Hardware-Uhr gibt es dagegen keine zeitliche Verwischung. Weitere Informationen finden Sie unter Schaltsekunden.

Für eine optimale Leistung empfehlen wir, den lokalen Amazon Time Sync Service auf Ihren EC2-Instances zu verwenden. Für ein Backup zum lokalen Amazon Time Sync Service auf Ihren Instances und um Ressourcen außerhalb von Amazon EC2 mit dem Amazon Time Sync Service zu verbinden, können Sie den öffentlichen Amazon Time Sync Service verwenden, der sich unter `time.aws.com` befindet. Der öffentliche Amazon Time Sync Service teilt genau wie der lokale Amazon Time Sync Service automatisch alle Schaltsekunden auf, die der UTC hinzugefügt werden. Der öffentliche Amazon Time Sync Service wird weltweit durch unsere Flotte von satellitengestützten und atomaren Referenzuhren unterstützt. AWS-Region

Themen

Festlegen der Nutzung des lokalen Amazon Time Sync Service für Ihre Instance

Ihre Instances können wie folgt auf den lokalen Amazon Time Sync Service zugreifen:

- Über NTP an folgenden IP-Adressendpunkten:
  - IPv4: `169.254.169.123`
  - IPv6: `fd00:ec2::123` (Nur für Instances zugänglich, die auf dem Nitro-System basieren.) AWS
- (Nur Linux) Über eine direkte PTP-Verbindung zur Verbindung mit einer lokalen PTP-Hardware-Uhr:

- PHC0

Amazon Linux-AMIs, Windows-AMIs und die meisten Partner-AMIs konfigurieren Ihre Instance so, dass sie standardmäßig den NTP-IPv4-Endpunkt verwendet. Dies ist die empfohlene Einstellung für die meisten Kunden-Workloads. Für Instances, die von diesen AMIs aus gestartet werden, ist keine weitere Konfiguration erforderlich, es sei denn, Sie möchten den IPv6-Endpunkt verwenden oder eine direkte Verbindung mit der PTP-Hardware-Uhr herstellen.

Für NTP- und PTP-Verbindungen müssen keine VPC-Konfigurationsänderungen vorgenommen werden und Ihre Instance benötigt keinen Zugriff auf das Internet.

> **Note**
>
> Nur Linux-Instances können eine direkte PTP-Verbindung verwenden, um eine Verbindung zur lokalen PTP-Hardwareuhr herzustellen. Windows-Instanzen verwenden NTP, um eine Verbindung zur lokalen PTP-Hardwareuhr herzustellen.

Themen

Eine Verbindung mit dem IPv4-Endpunkt des Amazon Time Sync Service herstellen

In diesem Abschnitt erfahren Sie, wie Sie Ihre Instance für die Verwendung des lokalen Amazon Time Sync Service über den IPv4-Endpunkt konfigurieren.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance.

Linux

AL2023 und die neuesten Versionen von Amazon Linux 2 und Amazon Linux AMIs sind so konfiguriert, dass sie standardmäßig den Amazon Time Sync Service IPv4-Endpunkt verwenden. Für Instances, die von diesen AMIs aus gestartet werden, ist keine weitere Konfiguration erforderlich, und Sie können das folgende Verfahren überspringen.

Verwenden Sie eines der folgenden Verfahren, um den Amazon Time Sync Service in Ihrer Instance mithilfe des `chrony`-Clients zu konfigurieren, wenn Sie eine AMI verwenden, für die der Amazon Time Sync Service nicht standardmäßig konfiguriert ist. Hierzu muss der `chrony`-Konfigurationsdatei ein Servereintrag für den Amazon Time Sync Service hinzugefügt werden.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance.

Amazon Linux

So stellen Sie unter Amazon Linux mithilfe von chrony eine Verbindung mit dem IPv4-Endpunkt des Amazon Time Sync Service her

1. Stellen Sie eine Verbindung mit Ihrer Instance her und deinstallieren Sie den NTP-Service.

```
[ec2-user ~]$ sudo yum erase 'ntp*'
```

2. Installieren Sie das Paket `chrony`.

```
[ec2-user ~]$ sudo yum install chrony
```

3. Öffnen Sie die Datei `/etc/chrony.conf` mit einem Texteditor Ihrer Wahl, z. B. vim oder nano. Überprüfen Sie, ob die Datei die folgende Zeile enthält:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

   Wenn die Zeile vorhanden ist, ist der Amazon Time Sync Service bereits für die Verwendung des IPv4-Endpunkts des Amazon Time Sync Service konfiguriert und Sie können mit dem nächsten Schritt fortfahren. Fügen Sie andernfalls die Zeile nach beliebigen anderen `server`- oder `pool`-Anweisungen ein, die bereits in der Datei vorhanden sind. Speichern Sie Ihre Änderungen.

4. Starten Sie den `chrony`-Daemon (`chronyd`) neu.

```
[ec2-user ~]$ sudo service chronyd restart
```

```
Starting chronyd:                                          [  OK  ]
```

> **Note**
>
> Auf RHEL und CentOS (bis zu Version 6) lautet der Servicename `chrony` anstatt `chronyd`.

5. Mithilfe des Befehls `chkconfig` können Sie konfigurieren, dass `chronyd` bei jedem Systemstart gestartet werden soll.

```
[ec2-user ~]$ sudo chkconfig chronyd on
```

6. Vergewissern Sie sich, dass `chrony` den IPv4-Endpunkt `169.254.169.123` für die Zeitsynchronisierung verwendet.

```
[ec2-user ~]$ chronyc sources -v
```

```
210 Number of sources = 7

  .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
 / .- Source state '*' = current synced, '+' = combined , '-' = not
combined,
| /   '?' = unreachable, 'x' = time may be in error, '~' = time too
variable.
||                                                 .- xxxx [ yyyy ] +/-
zzzz
||      Reachability register (octal) -.           |  xxxx = adjusted
offset,
||      Log2(Polling interval) --.      |          |  yyyy = measured
offset,
||                                \     |          |  zzzz = estimated
error.
||                                 |    |           \
MS Name/IP address         Stratum Poll Reach LastRx Last sample


===============================================================================
^* 169.254.169.123               3   6    17    43    -30us[ -226us] +/-
 287us
^- ec2-12-34-231-12.eu-west>     2   6    17    43   -388us[ -388us] +/-
  11ms
```

```
        ^- tshirt.heanet.ie              1   6    17    44   +178us[  +25us] +/-
 1959us
        ^? tbag.heanet.ie                0   6     0     -     +0ns[   +0ns] +/-
    0ns
        ^? bray.walcz.net                0   6     0     -     +0ns[   +0ns] +/-
    0ns
        ^? 2a05:d018:c43:e312:ce77:>     0   6     0     -     +0ns[   +0ns] +/-
    0ns
        ^? 2a05:d018:dab:2701:b70:b>     0   6     0     -     +0ns[   +0ns] +/-
    0ns
```

In der zurückgegebenen Ausgabe gibt ^* die bevorzugte Zeitquelle an.

7. Überprüfen Sie die von chrony gemeldeten Zeitsynchronisierungsmetriken.

```
[ec2-user ~]$ chronyc tracking
```

```
Reference ID    : A9FEA97B (169.254.169.123)
        Stratum         : 4
        Ref time (UTC)  : Wed Nov 22 13:18:34 2017
        System time     : 0.000000626 seconds slow of NTP time
        Last offset     : +0.002852759 seconds
        RMS offset      : 0.002852759 seconds
        Frequency       : 1.187 ppm fast
        Residual freq   : +0.020 ppm
        Skew            : 24.388 ppm
        Root delay      : 0.000504752 seconds
        Root dispersion : 0.001112565 seconds
        Update interval : 64.4 seconds
        Leap status     : Normal
```

Ubuntu

So stellen Sie unter Ubuntu mithilfe von chrony eine Verbindung mit dem IPv4-Endpunkt des Amazon Time Sync Service her

1. Stellen Sie eine Verbindung mit Ihrer Instance her und installieren Sie mit apt das chrony-Paket.

```
ubuntu:~$ sudo apt install chrony
```

> **Note**
>
> Sofern erforderlich, aktualisieren Sie Ihre Instance, indem Sie zuerst `sudo apt update` ausführen.

2. Öffnen Sie die Datei `/etc/chrony/chrony.conf` mit einem Texteditor Ihrer Wahl, z. B. vim oder nano. Fügen Sie die folgende Zeile vor beliebigen anderen `server`- oder `pool`-Anweisungen ein, die bereits in der Datei vorhanden sind. Speichern Sie dann Ihre Änderungen:

```
server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
```

3. Den Service `chrony` neu starten.

```
ubuntu:~$ sudo /etc/init.d/chrony restart
```

```
Restarting chrony (via systemctl): chrony.service.
```

4. Vergewissern Sie sich, dass `chrony` den IPv4-Endpunkt `169.254.169.123` für die Zeitsynchronisierung verwendet.

```
ubuntu:~$ chronyc sources -v
```

```
210 Number of sources = 7

             .-- Source mode  '^' = server, '=' = peer, '#' = local clock.
            / .- Source state '*' = current synced, '+' = combined , '-' = not
 combined,
           | /   '?' = unreachable, 'x' = time may be in error, '~' = time too
 variable.
           ||                                                 .- xxxx [ yyyy ]
 +/- zzzz
           ||      Reachability register (octal) -.           |  xxxx =
 adjusted offset,
           ||      Log2(Polling interval) --.      |          |  yyyy =
 measured offset,
           ||                                \     |          |  zzzz =
 estimated error.
           ||                                 |    |           \
```

```
            MS Name/IP address         Stratum Poll Reach LastRx Last sample

 ===============================================================================
            ^* 169.254.169.123               3   6    17    12    +15us[  +57us]
 +/-  320us
            ^- tbag.heanet.ie                1   6    17    13  -3488us[-3446us]
 +/- 1779us
            ^- ec2-12-34-231-12.eu-west-     2   6    17    13   +893us[ +935us]
 +/- 7710us
            ^? 2a05:d018:c43:e312:ce77:6     0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
            ^? 2a05:d018:d34:9000:d8c6:5     0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
            ^? tshirt.heanet.ie              0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
            ^? bray.walcz.net                0   6     0   10y     +0ns[   +0ns]
 +/-    0ns
```

In der Ausgabe, die zurückgegeben wird, steht in der Zeile, die mit ^* beginnt, die bevorzugte Zeitquelle.

5. Überprüfen Sie die von chrony gemeldeten Zeitsynchronisierungsmetriken.

```
ubuntu:~$ chronyc tracking
```

```
Reference ID    : 169.254.169.123 (169.254.169.123)
            Stratum         : 4
            Ref time (UTC)  : Wed Nov 29 07:41:57 2017
            System time     : 0.000000011 seconds slow of NTP time
            Last offset     : +0.000041659 seconds
            RMS offset      : 0.000041659 seconds
            Frequency       : 10.141 ppm slow
            Residual freq   : +7.557 ppm
            Skew            : 2.329 ppm
            Root delay      : 0.000544 seconds
            Root dispersion : 0.000631 seconds
            Update interval : 2.0 seconds
            Leap status     : Normal
```

SUSE Linux

Ab SUSE Linux Enterprise Server 15 ist `chrony` die Standardimplementierung von NTP.

So stellen Sie unter SUSE Linux mithilfe von chrony eine Verbindung mit dem IPv4-Endpunkt des Amazon Time Sync Service her

1. Öffnen Sie die Datei `/etc/chrony.conf` mit einem Texteditor Ihrer Wahl, z. B. vim oder nano.
2. Überprüfen Sie, ob die Datei die folgende Zeile enthält:

   ```
   server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
   ```

   Wenn diese Zeile nicht vorhanden ist, fügen Sie sie hinzu.
3. Kommentieren Sie alle anderen Server- oder Pool-Zeilen aus.
4. Öffnen Sie yaST und aktivieren Sie den chrony-Service.

Windows

Aber der Version von August 2018 nutzen Windows-AMIs den Amazon Time Sync Service standardmäßig. Für Instances, die von diesen AMIs aus gestartet werden, ist keine weitere Konfiguration erforderlich und Sie können die folgenden Verfahren überspringen.

Wenn Sie ein AMI verwenden, für das der Amazon Time Sync Service nicht standardmäßig konfiguriert ist, überprüfen Sie zunächst Ihre aktuelle NTP-Konfiguration. Wenn Ihre Instance bereits den IPv4-Endpunkt des Amazon Time Sync Service verwendet, ist keine weitere Konfiguration erforderlich. Wenn Ihre Instance den Amazon Time Sync Service nicht verwendet, schließen Sie das Verfahren ab, um den NTP-Server so zu ändern, dass er den Amazon Time Sync Service verwendet.

So überprüfen Sie die NTP-Konfiguration

1. Öffnen Sie in Ihrer Instance ein Eingabeaufforderungsfenster.
2. Mit folgendem Befehl zeigen Sie die derzeitige NTP-Konfiguration an:

   ```
   w32tm /query /configuration
   ```

   Dieser Befehl gibt die aktuellen Konfigurationseinstellungen für die Windows-Instance zurück und zeigt, ob eine Verbindung mit dem Amazon Time Sync Service besteht.

3. Mit folgendem Befehl wird der Status der derzeitigen Konfiguration angezeigt (optional):

```
w32tm /query /status
```

   Dieser Befehl gibt Informationen wie den Zeitpunkt der letzten Synchronisierung der Instance mit dem NTP-Server und das Abrufintervall zurück.

So stellen Sie den NTP-Server auf die Verwendung des Amazon Time Sync Service ein

1. Führen Sie über das Eingabeaufforderungsfenster den folgenden Befehl aus:

```
w32tm /config /manualpeerlist:169.254.169.123 /syncfromflags:manual /update
```

2. Mit folgendem Befehl überprüfen Sie Ihre neuen Einstellungen:

```
w32tm /query /configuration
```

   Vergewissern Sie sich in der zurückgegebenen Ausgabe, dass für `NtpServer` der IPv4-Endpunkt `169.254.169.123` angezeigt wird.

Standardmäßige Network Time Protocol (NTP)-Einstellungen für Amazon Windows-AMIs

Amazon Machine Images (AMIs) halten sich im Allgemeinen an die out-of-the-box Standardeinstellungen, außer in Fällen, in denen Änderungen erforderlich sind, um in der EC2-Infrastruktur zu funktionieren. Die folgenden Einstellungen funktionieren in einer virtualisierten Umgebung erwiesenermaßen gut. Zudem weicht die Uhrzeit nie um mehr als eine Sekunde ab:

- Aktualisierungsintervall — Legt fest, wie oft der Zeitservice die Systemzeit an die Genauigkeit anpasst. AWS konfiguriert das Aktualisierungsintervall so, dass es alle zwei Minuten erfolgt.
- NTP-Server: Ab dem Release vom August 2018 verwenden AMIs standardmäßig den Amazon Time Sync Service. Dieser Zeitdienst ist von jedem IPv4-Endpunkt aus zugänglich, der AWS-Region sich am 169.254.169.123 befindet. Zudem gibt das Flag 0x9 an, dass der Zeitdienst als Client fungiert und dass `SpecialPollInterval` verwendet werden soll, um zu ermitteln, wie häufig der Abgleich mit dem konfigurierten Zeitserver erfolgen soll.
- Typ – „NTP“ bedeutet, dass der Service als eigenständiger NTP-Client und nicht als Teil einer Domain fungiert.

- Aktiviert und InputProvider — Der Zeitdienst ist aktiviert und stellt dem Betriebssystem Zeit zur Verfügung.
- Spezielles Abfrageintervall — Prüft alle 900 Sekunden (15 Minuten) den konfigurierten NTP-Server.

Registry-Pfad	Tastenname	Daten
HKL M:\System\ CurrentCo ntrol Set\ services\ w32time\ Config	UpdateInterval	120
HKL M:\System\ CurrentCo ntrol Set\ services\ w32time\ Parameters	NtpServer	169.254.169.123,0x9
HKL M:\System\ CurrentCo ntrol Set\ services\ w32time\ Parameters	Typ	NTP
HKL M:\System\ CurrentCo ntrol Set\ services\ w32time\\ TimeProviders NtpClient	Aktiviert	1
HKL M:\System\ CurrentCo ntrol Set\ services\ w32time\\ TimeProviders NtpClient	InputProvider	1
HKL M:\System\ CurrentCo ntrol Set\ services\ w32time\\ TimeProviders NtpClient	SpecialPollIntervall	900

Herstellen einer Verbindung mit dem IPv6-Endpunkt des Amazon Time Sync Service

In diesem Abschnitt erfahren Sie, inwiefern sich die unter Eine Verbindung mit dem IPv4-Endpunkt des Amazon Time Sync Service herstellen beschriebenen Schritte unterscheiden, wenn Sie Ihre Instance für die Verwendung des lokalen Amazon Time Sync Service über den IPv6-Endpunkt konfigurieren. Es wird nicht der gesamte Konfigurationsprozess des Amazon Time Sync Service erklärt.

Der IPv6-Endpunkt ist nur auf Instanzen zugänglich, die auf dem AWS Nitro-System basieren.

> **Note**
>
> Wir empfehlen nicht, sowohl die IPv4- als auch die IPv6-Endpunkteinträge zusammen zu verwenden. Die IPv4- und IPv6-NTP-Pakete stammen von demselben lokalen Server für Ihre Instance. Das gleichzeitige Konfigurieren von IPv4- und IPv6-Endpunkten ist unnötig und führt nicht zu einer höheren Zeitgenauigkeit in Ihrer Instance.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance.

Linux

Je nachdem, welche Linux-Distribution Sie verwenden, verwenden Sie, wenn Sie den Schritt zur Bearbeitung der Datei chrony.conf erreichen, den IPv6-Endpunkt des Amazon Time Sync Service (`fd00:ec2::123`) und nicht den IPv4-Endpunkt (): `169.254.169.123`

```
server fd00:ec2::123 prefer iburst minpoll 4 maxpoll 4
```

Speichern Sie die Datei und vergewissern Sie sich, dass `chrony` den IPv6-Endpunkt `fd00:ec2::123` für die Zeitsynchronisierung verwendet:

```
[ec2-user ~]$ chronyc sources -v
```

Wenn die Ausgabe den IPv6-Endpunkt `fd00:ec2::123` enthält, ist die Konfiguration abgeschlossen.

Windows

Wenn Sie den Schritt erreicht haben, den NTP-Server so zu ändern, dass er den Amazon Time Sync Service verwendet, verwenden Sie den IPv6-Endpunkt des Amazon Time Sync Service (`fd00:ec2::123`) und nicht den IPv4-Endpunkt (): `169.254.169.123`

```
w32tm /config /manualpeerlist:fd00:ec2::123 /syncfromflags:manual /update
```

Stellen Sie sicher, dass Ihre neuen Einstellungen den `fd00:ec2::123` IPv6-Endpunkt zur Zeitsynchronisierung verwenden:

```
w32tm /query /configuration
```

Vergewissern Sie sich, dass in der Ausgabe der `fd00:ec2::123` IPv6-Endpunkt `NtpServer` angezeigt wird.

Herstellen einer Verbindung mit der PTP-Hardware-Uhr

Die PTP-Hardware-Uhr ist Teil des AWS Nitro-Systems. Daher kann in unterstützten Bare-Metal- und virtualisierten EC2-Instances direkt darauf zugegriffen werden, ohne Kundenressourcen zu beanspruchen.

Die NTP-Endpunkte für die PTP-Hardware-Uhr sind die gleichen wie bei der regulären Amazon Time Sync Service-Verbindung über IPv4 oder IPv6. Wenn Ihre Software für den NTP-Endpunkt konfiguriert ist und in einer Instance mit einer PTP-Hardware-Uhr ausgeführt wird, wird automatisch eine NTP-Verbindung mit der PTP-Hardware-Uhr hergestellt.

Voraussetzungen

Die PTP-Hardware-Uhr ist in einer Instance verfügbar, wenn die folgenden Anforderungen erfüllt sind:

- Unterstützt AWS-Regionen: USA Ost (Nord-Virginia) und Asien-Pazifik (Tokio)
- Unterstützte Instance-Familien:
  - Allgemeiner Zweck: M7a, M7g, M7GD, M7i
  - Computeroptimiert: C7a, C7gd, C7i
  - Speicheroptimiert: R7a, R7g, R7gd, R7i
- (Nur Linux) Die ENA-Treiberversion 2.10.0 oder höher ist auf einem unterstützten Betriebssystem installiert. Weitere Informationen zu unterstützten Betriebssystemen finden Sie in den Treibervoraussetzungen unter GitHub.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance.

Linux

In diesem Abschnitt erfahren Sie, wie Sie Ihre Instance für die Verwendung des lokalen Amazon Time Sync Service über die PTP-Hardware-Uhr konfigurieren und dabei eine direkte PTP-Verbindung verwenden. Dazu muss der `chrony`-Konfigurationsdatei ein Servereintrag für die PTP-Hardware-Uhr hinzugefügt werden.

Wenn Ihre Instance über eine PTP-Hardware-Uhr verfügt und Sie die NTP-Verbindung (entweder mit dem IPv4- oder mit dem IPv6-Endpunkt) konfiguriert haben, wird Ihre Instance-Zeit automatisch

von der PTP-Hardware-Uhr abgerufen. Mit den folgenden Schritten wird die direkte PTP-Verbindung konfiguriert, um eine präzisere Uhrzeit zu erhalten als bei der NTP-Verbindung.

So stellen Sie eine Verbindung mit der PTP-Hardware-Uhr her

1. Stellen Sie eine Verbindung mit Ihrer Instance her und installieren Sie den Linux-Kernel-Treiber für die Elastic Network Adapter (ENA)-Version 2.10.0 (oder höher). Die Installationsanweisungen finden Sie unter Linux-Kernel-Treiber für die Elastic Network Adapter (ENA) -Familie auf GitHub.
2. Vergewissern Sie sich, dass das Gerät `/dev/ptp0` in Ihrer Instance angezeigt wird.

   ```
   [ec2-user ~]$ ls /dev/ptp0
   ```

   Folgendes ist die erwartete Ausgabe: Sollte `/dev/ptp0` nicht in der Ausgabe enthalten sein, wurde der ENA-Treiber nicht korrekt installiert. Informationen zum Installieren des Treibers finden Sie in Schritt 1 dieses Verfahrens.

   ```
   /dev/ptp0
   ```

3. Bearbeiten Sie `/etc/chrony.conf` mithilfe eines Text-Editors und fügen Sie an einer beliebigen Stelle in der Datei die folgende Zeile hinzu.

   ```
   refclock PHC /dev/ptp0 poll 0 delay 0.000010 prefer
   ```

4. Starten Sie chrony mithilfe des folgenden Befehls neu.

   ```
   [ec2-user ~]$ sudo systemctl restart chronyd
   ```

5. Vergewissern Sie sich, dass chrony die PTP-Hardware-Uhr für die Zeitsynchronisierung in dieser Instance verwendet.

   ```
   [ec2-user ~]$ chronyc sources
   ```

   Erwartete Ausgabe

   ```
   MS Name/IP address         Stratum Poll Reach LastRx Last sample
   ===============================================================================
   #* PHC0                          0   0    377    1   +2ns[ +1ns] +/-   5031ns
   ```

In der zurückgegebenen Ausgabe gibt * die bevorzugte Zeitquelle an. `PHC0` entspricht der PTP-Hardware-Uhr. Nach dem Neustart von chrony dauert es möglicherweise einige Sekunden, bis das Sternchen angezeigt wird.

Windows

Windows-Instances unterstützen nur eine NTP-Verbindung zur lokalen PTP-Hardwareuhr.

Die NTP-Endpunkte für die PTP-Hardware-Uhr sind die gleichen wie bei der regulären Amazon Time Sync Service-Verbindung über IPv4 oder IPv6. Wenn Ihre Software für die Verbindungsherstellung mit einem NTP-Endpunkt konfiguriert ist und in einer Instance mit einer PTP-Hardware-Uhr ausgeführt wird, wird automatisch eine NTP-Verbindung mit der PTP-Hardware-Uhr hergestellt.

Festlegen der Verwendung des öffentlichen Amazon Time Sync Service für Ihre Instance oder für ein beliebiges Gerät mit Internetverbindung

Sie können Ihre Instance oder ein beliebiges Gerät mit Internetverbindung (etwa Ihren lokalen Computer oder einen lokalen Server) für die Verwendung des öffentlichen Amazon Time Sync Service konfigurieren, der im Internet unter `time.aws.com` zur Verfügung steht. Sie können den öffentlichen Amazon Time Sync Service als Backup für den lokalen Amazon Time Sync Service verwenden und um Ressourcen außerhalb des Amazon Time Sync Service AWS zu verbinden.

> **Note**
>
> Für eine optimale Leistung empfehlen wir, den lokalen Amazon Time Sync Service auf Ihren Instances zu verwenden und nur den öffentlichen Amazon Time Sync Service als Backup zu verwenden.

Verwenden Sie die Anweisungen für das Betriebssystem Ihrer Instance oder Ihres Geräts.

Linux

So konfigurieren Sie Ihre Linux-Instance oder Ihr Linux-Gerät mithilfe von chrony oder ntpd für die Verwendung des öffentlichen Amazon Time Sync Service

1. Bearbeiten Sie `/etc/chrony.conf` (bei Verwendung von chrony) oder `/etc/ntp.conf` (bei Verwendung von ntpd) mithilfe eines Text-Editors wie folgt:

a. Entfernen Sie Zeilen, die mit `server` beginnen, oder kommentieren Sie sie aus (mit Ausnahme ggf. vorhandener Verbindungen mit dem lokalen Amazon Time Sync Service), damit Ihre Instance oder Ihr Gerät nicht versucht, Server mit und ohne Time Smearing gemeinsam zu verwenden.

> **Important**
>
> Wenn Sie Ihre EC2-Instance so konfigurieren, dass sie eine Verbindung mit dem öffentlichen Amazon Time Sync Service herstellt, darf die folgende Zeile, die Ihre Instance für die Verbindungsherstellung mit dem lokalen Amazon Time Sync Service konfiguriert, nicht entfernt werden. Der lokale Amazon Time Sync Service stellt eine direktere Verbindung dar und bietet eine höhere Zeitgenauigkeit. Der öffentliche Amazon Time Sync Service sollte nur als Ausweichlösung verwendet werden.
>
> ```
> server 169.254.169.123 prefer iburst minpoll 4 maxpoll 4
> ```

b. Fügen Sie die folgende Zeile hinzu, um eine Verbindung mit dem öffentlichen Amazon Time Sync Service herzustellen.

```
pool time.aws.com iburst
```

2. Starten Sie den Daemon mithilfe eines der folgenden Befehle neu.

   - chrony

     ```
     sudo service chronyd force-reload
     ```

   - ntpd

     ```
     sudo service ntp reload
     ```

macOS

So konfigurieren Sie Ihre macOS-Instance oder Ihr macOS-Gerät für die Verwendung des öffentlichen Amazon Time Sync Service

1. Öffnen Sie Systemeinstellungen.

2. Wählen Sie Date & Time (Datum und Uhrzeit) und dann die Registerkarte Date & Time (Datum und Uhrzeit).
3. Um Änderungen vorzunehmen, wählen Sie das Schlosssymbol und geben Sie Ihr Passwort ein, wenn Sie dazu aufgefordert werden.
4. Geben Sie für Set date and time automatically (Datum und Uhrzeit automatisch festlegen) den Wert **`time.aws.com`** ein.

Windows

So konfigurieren Sie Ihre Windows-Instance oder Ihr Windows-Gerät für die Verwendung des öffentlichen Amazon Time Sync Service

1. Öffnen Sie das Control Panel (Bedienfeld).
2. Wählen Sie das Symbol für Date and Time (Datum und Uhrzeit).
3. Wählen Sie die Registerkarte Internet Time (Internetzeit). Diese Registerkarte ist nicht verfügbar, wenn Ihr PC in eine Domain eingebunden ist. In diesem Fall synchronisiert er die Zeit mit dem Domain-Controller. Sie können den Controller für die Verwendung des öffentlichen Amazon Time Sync Service konfigurieren.
4. Wählen Sie Change settings (Einstellungen ändern).
5. Aktivieren Sie das Kontrollkästchen für Synchronize with an Internet time server (Mit einem Internet-Zeitserver synchronisieren).
6. Geben Sie neben Server **`time.aws.com`** ein.

So konfigurieren Sie Ihre Windows Server-Instance oder Ihr Windows Server-Gerät für die Verwendung des öffentlichen Amazon Time Sync Service

- Folgen Sie den Anweisungen von Microsoft, um Ihre Registry zu aktualisieren.

Vergleichen Sie die Zeitstempel für Ihre Linux-Instances

Wenn Sie den Amazon Time Sync Service verwenden, können Sie die Zeitstempel auf Ihren Amazon EC2 EC2-Linux-Instances mit vergleichen, ClockBound um den tatsächlichen Zeitpunkt eines Ereignisses zu ermitteln. ClockBound misst die Taktgenauigkeit Ihrer EC2-Instance und ermöglicht es Ihnen, zu überprüfen, ob ein bestimmter Zeitstempel in der Vergangenheit oder future in Bezug auf die aktuelle Uhr Ihrer Instance liegt. Diese Informationen sind wertvoll, um die Reihenfolge

und Konsistenz von Ereignissen und Transaktionen über EC2-Instances hinweg unabhängig vom geografischen Standort jeder Instance zu bestimmen.

ClockBound ist ein Open-Source-Daemon und eine Open-Source-Bibliothek. Weitere Informationen ClockBound, einschließlich Installationsanweisungen, finden Sie ClockBoundunter GitHub.

ClockBound wird nur für Linux-Instances unterstützt.

Bei Verwendung der direkten PTP-Verbindung mit der PTP-Hardware-Uhr unterschätzt Ihr Zeit-Daemon (beispielsweise chrony) die Zeitfehlergrenze. Das liegt daran, dass eine PTP-Hardware-Uhr im Gegensatz zu NTP nicht die richtigen Informationen zur Fehlergrenze an chrony übergibt. Folglich geht Ihr Daemon für die Zeitsynchronisierung davon aus, dass die UTC-Zeit der Uhr korrekt ist, und verwendet daher eine Fehlergrenze von `0`. Um die vollständige Fehlergrenze zu messen, berechnet das Nitro-System die Fehlergrenze der PTP-Hardware-Uhr und stellt sie Ihrer EC2-Instance über das ENA-Treiberdateisystem zur Verfügung. `sysfs` Sie können dies direkt als Wert in Nanosekunden ablesen.

Um den PTP-Hardware-Taktfehler abzurufen

1. Rufen Sie zunächst mithilfe eines der folgenden Befehle den korrekten Standort der PTP-Hardware-Uhr ab. Der Pfad im Befehl unterscheidet sich je nach dem AMI, das zum Starten der Instance verwendet wurde.

   - Für Amazon Linux 2:

     ```
     cat /sys/class/net/eth0/device/uevent | grep PCI_SLOT_NAME
     ```

   - Für Amazon Linux 2023:

     ```
     cat /sys/class/net/ens5/device/uevent | grep PCI_SLOT_NAME
     ```

   Die Ausgabe ist der Name des PCI-Steckplatzes, der den Standort der PTP-Hardware-Uhr angibt. In diesem Beispiel lautet `0000:00:03.0` der Standort.

   ```
   PCI_SLOT_NAME=0000:00:03.0
   ```

2. Führen Sie den folgenden Befehl aus, um den PTP-Hardware-Uhrfehler abzurufen. Geben Sie den Namen des PCI-Steckplatzes aus dem vorherigen Schritt an.

```
cat /sys/bus/pci/devices/0000:00:03.0/phc_error_bound
```

Die Ausgabe gibt die Zeitfehlergrenze der PTP-Hardware-Uhr in Nanosekunden an.

Um bei Verwendung der direkten PTP-Verbindung zur PTP-Hardwareuhr den korrekten Taktfehler zu berechnen, müssen Sie den Zeitfehler hinzufügen, der von oder zu dem Zeitpunkt, zu dem die PTP-Hardwareuhr abgerufen wird, stammt chrony oder zu dem Zeitpunkt liegt, ClockBound zu dem die chrony PTP-Hardwareuhr abgerufen wird. Weitere Informationen zur Messung und Überwachung der Uhrgenauigkeit finden Sie unter Verwalten der Uhrgenauigkeit von Amazon EC2 EC2-Instances mithilfe von Amazon Time Sync Service und Amazon CloudWatch — Teil 1.

Ändern Sie die Zeitzone Ihrer Instance

Amazon EC2 EC2-Instances sind standardmäßig auf die Zeitzone UTC (Coordinated Universal Time) eingestellt. Sie können die Zeit für eine Instance auf die lokale Zeitzone oder auf eine andere Zeitzone in Ihrem Netzwerk festlegen.

Verwenden Sie die Anleitung für das Betriebssystem Ihrer Instance.

Linux

> **Important**
>
> Diese Informationen gelten für Amazon Linux. Weitere Informationen zu anderen Verteilungen finden Sie in der jeweiligen Dokumentation.

So ändern Sie die Zeitzone auf einer AL2023- oder Amazon Linux 2-Instance

1. Zeigen Sie die aktuelle Zeitzoneneinstellung des Systems an.

   ```
   [ec2-user ~]$ timedatectl
   ```

2. Listen Sie die verfügbaren Zeitzonen auf.

   ```
   [ec2-user ~]$ timedatectl list-timezones
   ```

3. Legen Sie die ausgewählte Zeitzone fest.

```
[ec2-user ~]$ sudo timedatectl set-timezone America/Vancouver
```

4. (Optional) Bestätigen Sie durch erneutes Ausführen des Befehls timedatectl, dass die aktuelle Zeitzone auf die neue Zeitzone geändert wird.

```
[ec2-user ~]$ timedatectl
```

So ändern Sie die Zeitzone in einer Amazon-Linux-Instance

1. Ermitteln Sie die Zeitzone, die in Ihrer Instance verwendet wird. Das Verzeichnis `/usr/share/zoneinfo` enthält eine Hierarchie von Zeitzonendateien. Durchsuchen Sie die Verzeichnisstruktur an dieser Stelle, um eine Datei für Ihre Zeitzone zu finden.

```
[ec2-user ~]$ ls /usr/share/zoneinfo
Africa      Chile    GB         Indian       Mideast   posixrules  US
America     CST6CDT  GB-Eire    Iran         MST       PRC         UTC
Antarctica  Cuba     GMT        iso3166.tab  MST7MDT   PST8PDT     WET
Arctic      EET      GMT0       Israel       Navajo    right       W-SU
...
```

   Einige Einträge an dieser Stelle sind Verzeichnisse (z. B. `America`). Diese enthalten Zeitzonendateien für einzelne Städte. Suchen Sie nach der Stadt, in der Sie sich befinden (oder einer Stadt in Ihrer Zeitzone), um die Instance auf die entsprechende Zeitzone einzustellen.

2. Aktualisieren Sie die Datei `/etc/sysconfig/clock` mit der neuen Zeitzone. In diesem Beispiel verwenden wir die Zeitzonendatendatei für Los Angeles, `/usr/share/zoneinfo/America/Los_Angeles`.

   a. Öffnen Sie die Datei `/etc/sysconfig/clock` mit einem Text-Editor (z. B. vim oder nano). Sie müssen sudo mit dem Editor verwenden, da die Datei `/etc/sysconfig/clock` Eigentum von `root` ist.

   ```
   [ec2-user ~]$ sudo nano /etc/sysconfig/clock
   ```

   b. Suchen Sie den Eintrag `ZONE` und geben Sie die Zeitzonendatei an (ohne den folgenden Teil des Pfads: `/usr/share/zoneinfo`). Ändern Sie den Eintrag `ZONE` beispielsweise wie folgt, um die Zeitzone „Los Angeles“ einzustellen:

```
ZONE="America/Los_Angeles"
```

> **Note**
>
> Ändern Sie den Eintrag `UTC=true` NICHT. Dieser Eintrag gehört zur Hardware-Uhr und muss nicht geändert werden, um für eine Instance eine andere Zeitzone einzustellen.

c. Speichern Sie die Datei und schließen Sie den Texteditor.

3. Erstellen Sie eine symbolische Verknüpfung zwischen `/etc/localtime` und der Zeitzonendatei, damit die Instance die Zeitzonendatei beim Abrufen der Ortszeit findet.

```
[ec2-user ~]$ sudo ln -sf /usr/share/zoneinfo/America/Los_Angeles /etc/localtime
```

4. Starten Sie das System neu, damit alle Services und Anwendungen die neuen Zeitzoneninformationen erhalten.

```
[ec2-user ~]$ sudo reboot
```

5. (Optional) Bestätigen Sie mit dem Befehl date, dass die aktuelle Zeitzone auf die neue Zeitzone aktualisiert wird. Die aktuelle Zeitzone wird in der Ausgabe angezeigt. Im folgenden Beispiel ist die aktuelle Zeitzone PDT, die sich auf die Zeitzone Los Angeles bezieht.

```
[ec2-user ~]$ date
Sun Aug 16 05:45:16 PDT 2020
```

Windows

So ändern Sie die Zeitzone für eine Windows-Instance

1. Öffnen Sie in Ihrer Instance ein Eingabeaufforderungsfenster.
2. Ermitteln Sie die Zeitzone, die in Ihrer Instance verwendet wird. Mit dem folgenden Befehl zeigen Sie eine Liste aller Zeitzonen an:

```
tzutil /l
```

Dieser Befehl gibt eine Liste mit allen verfügbaren Zeitzonen im folgenden Format zurück:

```
display name
time zone ID
```

3. Ermitteln Sie die ID der Zeitzone, die Sie der Instance zuordnen möchten.
4. Verwenden Sie für die Zuweisung zu einer anderen Zeitzone den folgenden Befehl:

```
tzutil /s "Pacific Standard Time"
```

Die neue Zeitzone sollte sofort übernommen werden.

> **Note**
>
> Die UTC-Zeitzone können Sie mithilfe des folgenden Befehls zuweisen:
>
> ```
> tzutil /s "UTC"
> ```

Um zu verhindern, dass sich Ihre Zeitzone ändert, nachdem Sie sie für Windows Server festgelegt haben

Wenn Sie die Zeitzone für eine Windows-Instance ändern, müssen Sie sicherstellen, dass die Zeitzone bei Systemneustarts erhalten bleibt. Andernfalls ändert sich die Zeit beim Neustart einer Instance wieder in UTC. Sie können Ihre Zeitzoneneinstellung beibehalten, indem Sie einen RealTimeIsUniversal Registrierungsschlüssel hinzufügen. Dieser Schlüssel wird standardmäßig für alle Instances der aktuellen Generation festgelegt. Informationen zum Überprüfen, ob der Registrierungsschlüssel RealTimeIsUniversal festgelegt ist, finden Sie im folgenden Verfahren unter Schritt 4. Ist der Schlüssel nicht festgelegt, führen Sie die folgenden Schritte von Anfang an aus.

Um den RealTimeIsUniversal Registrierungsschlüssel festzulegen

1. Öffnen Sie in der Instance ein Eingabeaufforderungsfenster.
2. Verwenden Sie den folgenden Befehl, um den Registrierungsschlüssel hinzuzufügen:

```
reg add "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation" /
v RealTimeIsUniversal /d 1 /t REG_DWORD /f
```

3. Wenn Sie ein Windows Server 2008-AMI (nicht Windows Server 2008 R2) verwenden, das vor dem 22. Februar 2013 erstellt wurde, empfehlen wir, auf das neueste AWS Windows-AMI zu aktualisieren. Wenn Sie ein AMI auf einem Windows Server 2008 R2 ausführen (nicht Windows Server 2008), stellen Sie sicher, dass der Microsoft-Hotfix KB2922223 installiert ist. Wenn dieser Hotfix nicht installiert ist, empfehlen wir, auf das neueste AWS Windows-AMI zu aktualisieren.
4. Stellen Sie sicher, dass die Instance den Schlüssel erfolgreich gespeichert hat, bevor Sie folgenden Befehl ausführen (optional):

```
reg query "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control
\TimeZoneInformation" /s
```

Dieser Befehl gibt die Unterschlüssel für den Registrierungsschlüssel TimeZoneInformation zurück. Die Ausgabe des RealTimeIsUniversal-Schlüssels am Ende der Liste sollte ähnlich dem folgenden Beispiel aussehen:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TimeZoneInformation
    Bias                            REG_DWORD     0x1e0
    DaylightBias                    REG_DWORD     0xffffffc4
    DaylightName                    REG_SZ        @tzres.dll,-211
    DaylightStart                   REG_BINARY    00000300020002000000000000000000
    StandardBias                    REG_DWORD     0x0
    StandardName                    REG_SZ        @tzres.dll,-212
    StandardStart                   REG_BINARY    00000B0001000200000000000000000
    TimeZoneKeyName                 REG_SZ        Pacific Standard Time
    DynamicDaylightTimeDisabled     REG_DWORD     0x0
    ActiveTimeBias                  REG_DWORD     0x1a4
    RealTimeIsUniversal             REG_DWORD     0x1
```

Schaltsekunden

Schaltsekunden wurden 1972 eingeführt. Sie sind gelegentliche einsekündige Anpassungen der UTC-Zeit, um Unregelmäßigkeiten bei der Erdrotation sowie Abweichungen zwischen der Internationalen Atomzeit (TAI) und der Sonnenzeit (Ut1) Rechnung zu tragen. Um Schaltsekunden für unsere Kunden zu verwalten, haben wir die Schaltsekundenaufteilung im Rahmen des Amazon Time Sync Service entwickelt. Weitere Informationen finden Sie unter Augen auf bei der Verwendung von Schaltsekunden: Die nächste Schaltsekunde und AWS.

Schaltsekunden werden abgeschafft und wir stehen voll und ganz hinter der bei der 27. General Conference on Weights and Measures getroffenen Entscheidung, Schaltsekunden bis spätestens 2035 abzuschaffen.

Um diese Umstellung zu unterstützen, planen wir, während eines Schaltsekundenereignisses weiterhin Time Smearing einzusetzen, wenn auf den Amazon Time Sync Service über die lokale NTP-Verbindung oder über unsere öffentlichen NTP-Pools (`time.aws.com`) zugegriffen wird. Die PTP-Hardware-Uhr bietet jedoch keine Time Smearing-Option. Im Falle einer Schaltsekunde fügt die PTP-Hardware-Uhr die Schaltsekunde gemäß den UTC-Standards hinzu. Zeitquellen mit Leap Smearing und Zeitquellen mit Schaltsekunden sind in den meisten Fällen gleich. Da sie sich jedoch während eines Schaltsekundenereignisses unterscheiden, raten wir davon ab, während eines Schaltsekundenereignisses sowohl Zeitquellen mit Time Smearing als auch Zeitquellen ohne Time Smearing in Ihrer Zeit-Client-Konfiguration zu verwenden.

Zugehörige Ressourcen

- AWS Compute-Blog: Es ist an der Zeit: Mikrosekundengenaue Uhren auf Amazon EC2 EC2-Instances
- (Linux) https://chrony-project.org/
- (Windows) So funktioniert der Windows-Zeitdienst (Microsoft)
- (Windows) W32tm (Microsoft)
- (Windows) So behandelt der Windows-Zeitdienst eine Schaltsekunde (Microsoft)
- (Windows) Die Geschichte rund um Leap Seconds und Windows: Es ist wahrscheinlich nicht Y2K (Microsoft)

Kontrolle des Prozessorstatus für Ihre Amazon EC2 EC2-Linux-Instance

Über den C-Zustand werden die Ruhezustandsebenen gesteuert, in denen sich ein Core im Leerlauf befinden kann. C-Zustände sind von C0 (Arbeitszustand, in dem der Core „wach“ ist und Anweisungen ausführt) bis C6 („tiefster“ Leerlaufzustand, in dem ein Core ausgeschaltet ist) nummeriert.

Mit P-Zuständen wird die gewünschte Performance für einen Core gesteuert (nach CPU-Frequenz). P-Zustände sind ab P0 (höchste Performancestufe, in der Intel Turbo Boost-Technologie für den Core eingesetzt werden kann, um ggf. die Frequenz zu erhöhen) über P1 (in diesem P-Zustand wird die maximale Basisfrequenz angefordert) bis P15 (geringstmögliche Frequenz) nummeriert.

C-Staaten und P-Staaten

Bei den folgenden Instance-Typen besteht für ein Betriebssystem die Möglichkeit, den C- und P-Zustand von Prozessoren zu steuern:

- Allgemeiner Zweck: `m4.10xlarge` | `m4.16xlarge` | `m5.metal` | | `m5d.metal` | `m5n.metal` | `m5zn.metal` | `m6i.metal` | | `m6id.metal` | `m7a.metal-48xl` | `m7i.metal-24xl` `m7i.metal-48xl`
- Für Datenverarbeitung optimiert: `c4.8xlarge` | `c5.metal` | `c5an.metal` | `c5adn.metal` | `c5n.metal` | `c6i.metal` | `c6id.metal` | `c7a.metal-48xl` | `c7i.metal-24xl` | `c7i.metal-48xl`
- Speicheroptimiert: `r4.8xlarge` | `r4.16xlarge` | `r5.metal` | | `r5b.metal` | `r5d.metal` | `r6i.metal` | `r7a.metal-48xl` | `r7i.metal-24xl` | `r7i.metal-48xl` | `r7iz.metal-16xl` | `r7iz.metal-32xl` | `u-6tb1.metal` | `u-9tb1.metal` | `u-12tb1.metal` | `u-18tb1.metal` | | `u-24tb1.metal` | `x1.16xlarge` | `x1.32xlarge` | `x1e.8xlarge` | `x1e.16xlarge` | `x1e.32xlarge` | `z1d.metal`
- Speicheroptimiert: `d2.8xlarge` | `d3.metal` | `d3en.metal` | `i3.8xlarge` | `i3.16xlarge` | `i3.metal` | `i3en.metal` | `h1.8xlarge` | `h1.16xlarge`
- Beschleunigtes Computing: `f1.16xlarge` | `g3.16xlarge` | `g4dn.metal` | `p2.16xlarge` | `p3.16xlarge`

Nur C-Staaten

Bei den folgenden Instance-Typen besteht für ein Betriebssystem die Möglichkeit, den C-Zustand von Prozessoren zu steuern:

- Allgemeiner Zweck: `m5.12xlarge` `m5.24xlarge` | `m5d.12xlarge` | `m5d.24xlarge` | `m5n.12xlarge` | `m5n.24xlarge` | `m5dn.12xlarge` | `m5dn.24xlarge` | `m6a.24xlarge` | `m6a.48xlarge` | `m6ad.metal` | `m6i.16xlarge` | `m6i.32xlarge` | `m7a.medium` | `m7a.large` | | `m7a.xlarge` | `m7a.2xlarge` | `m7a.4xlarge` | `m7a.8xlarge` | `m7a.12xlarge` | `m7a.16xlarge` | `m7a.24xlarge` | `m7a.32xlarge` | `m7a.48xlarge` | `m7i.large` | `m7i.xlarge` | `m7i.2xlarge` | `m7i.4xlarge` | `m7i.8xlarge` | `m7i.12xlarge` | `m7i.16xlarge` | `m7i.24xlarge` | `m7i.48xlarge`
- Für Datenverarbeitung optimiert: `c5.9xlarge` | `c5.12xlarge` | `c5.18xlarge` | `c5.24xlarge` | `c5a.24xlarge` | `c5ad.24xlarge` | `c5d.9xlarge` | | `c5d.12xlarge` | `c5d.18xlarge` | `c5d.24xlarge` | `c5n.9xlarge` | `c5n.18xlarge` | `c6a.24xlarge` | | `c6a.32xlarge` |

c6a.48xlarge | c6i.16xlarge | c6i.32xlarge | c7a.medium | c7a.large | c7a.xlarge || c7a.2xlarge | c7a.4xlarge | c7a.8xlarge | c7a.12xlarge | c7a.16xlarge | c7a.24xlarge || c7a.32xlarge | c7a.48xlarge | c7i.large | c7i.xlarge | c7i.2xlarge | c7i.4xlarge | c7i.8xlarge || c7i.12xlarge | c7i.16xlarge | c7i.24xlarge | c7i.48xlarge

- Speicheroptimiert: r5.12xlarge | r5.24xlarge | r5d.12xlarge r5d.24xlarge | r5n.12xlarge | r5n.24xlarge | r5dn.12xlarge | r5dn.24xlarge | r6a.24xlarge | r6a.48xlarge | r6i.16xlarge | r6i.32xlarge | r6id.32xlarge | r6in.32xlarge | r7a.medium | r7a.large r7a.xlarge | r7a.2xlarge | r7a.4xlarge | r7a.8xlarge | r7a.12xlarge | r7a.16xlarge | r7a.24xlarge | r7a.32xlarge | r7a.48xlarge | r7i.large | r7i.xlarge | r7i.2xlarge | r7i.4xlarge | r7i.8xlarge r7i.12xlarge | r7i.16xlarge | r7i.24xlarge | r7i.48xlarge | r7iz.large | r7iz.xlarge | r7iz.2xlarge | r7iz.4xlarge| r7iz.8xlarge | r7iz.12xlarge || r7iz.16xlarge | r7iz.32xlarge | u-6tb1.56xlarge | u-6tb1.112xlarge | u-9tb1.112xlarge || u-12tb1.112xlarge | u-18tb1.112xlarge | u-24tb1.112xlarge | u7i-12tb.224xlarge | u7in-16tb.224xlarge || u7in-24tb.224xlarge | u7in-32tb.224xlarge | z1d.6xlarge | z1d.12xlarge
- Speicheroptimiert: d3en.12xlarge | dl1.24xlarge | i3en.12xlarge | i3en.24xlarge | i4i.metal | r5b.12xlarge | r5b.24xlarge | i4i.16xlarge
- Beschleunigtes Rechnen: dl1.24xlarge g5.24xlarge g5.48xlarge || g6.24xlarge | g6.48xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | vt1.24xlarge

AWS Graviton-Prozessoren verfügen über integrierte Energiesparmodi und arbeiten mit einer festen Frequenz. Daher bieten sie dem Betriebssystem nicht die Möglichkeit, C-States und P-States zu überwachen.

Es kann ratsam sein, die Einstellungen für den C- bzw. P-Zustand zu ändern, um die Konsistenz der Prozessorleistung zu erhöhen, die Latenz zu reduzieren oder Ihre Instance für einen bestimmten Workload zu optimieren. Die Standardeinstellungen für den C- und P-Zustand sind auf maximale Performance ausgelegt. Dies ist für die meisten Workloads optimal. Erwägen Sie jedoch, mit den für diese Instances verfügbaren Einstellungen für den C- oder P-Zustand zu experimentieren, wenn Ihre Anwendung von einer verringerten Latenz auf Kosten von höheren Single- oder Dual-Core-Frequenzen oder von einer konsistenten Performance bei niedrigeren Frequenzen (im Gegensatz zu diskontinuierlichen Turbo Boost-Frequenzen) profitieren würde.

Informationen zu verschiedenen Prozessorkonfigurationen und zur Überwachung der Auswirkungen Ihrer Konfiguration für Amazon Linux finden Sie unter Processor State Control for Amazon EC2 Amazon Linux-Instance im Amazon Linux 2-Benutzerhandbuch. Diese Verfahren wurden für Amazon Linux geschrieben und gelten für Amazon Linux. Sie könnten jedoch auch für andere Linux-Distributionen mit einem Linux-Kernel von 3.9 oder neuer funktionieren. Weitere Informationen zu anderen Linux-Distributionen und zur Steuerung des Prozessorzustands erhalten Sie jeweils in der Dokumentation Ihres Systems.

CPU-Optionen optimieren

Viele Amazon-EC2-Instances unterstützen simultanes Multithreading, was die gleichzeitige Ausführung mehrerer Threads auf einem einzelnen CPU-Kern ermöglicht. Jeder Thread wird als virtuelle CPU (vCPU) auf der Instance dargestellt. Eine Instance hat eine Standardanzahl von CPU-Kernen, die je nach Instance-Typ variiert. Zum Beispiel hat ein `m5.xlarge`-Instance-Typ standardmäßig zwei CPU-Kerne und zwei —Threads pro Kern, also insgesamt vier vCPUs.

> **Note**
>
> Jede vCPU ist ein Thread eines CPU-Kerns, außer bei T2-Instances, M7a-Instances, Apple-Silicon-Mac-Instances und 64-Bit-ARM-Plattformen wie Instances, die von AWS Graviton-Prozessoren betrieben werden.

In den meisten Fällen gibt es einen Amazon EC2-Instance-Typ, der eine Kombination aus Speicher und Anzahl der vCPUs hat, die Ihren Workloads entspricht. Sie können jedoch die folgenden CPU-Optionen angeben, um Ihre Instance für bestimmte Workloads oder Geschäftsanforderungen zu optimieren:

- Anzahl der CPU-Kerne: Sie können die Anzahl der CPU-Kerne für die Instance anpassen. Sie könnten dies tun, um die Lizenzkosten Ihrer Software mit einer Instance zu optimieren, die genügend RAM für speicherintensive Workloads, aber weniger CPU-Kerne hat.
- Threads pro Kern: Sie können Multithreading deaktivieren, indem Sie einen einzelnen Thread pro CPU-Kern angeben. Sie können dies für bestimmte Workloads tun, z. B. für High Performance Computing (HPC)-Workloads.

Sie können diese CPU-Optionen beim Start der Instance angeben. Es gibt keine zusätzlichen oder reduzierten Kosten für die Angabe von CPU-Optionen. Sie werden genauso berechnet wie Instances, die mit Standard-CPU-Optionen gestartet werden.

Inhalt

Regeln für die Angabe von CPU-Optionen

Um die CPU-Optionen für Ihre Instance festzulegen, beachten Sie die folgenden Regeln:

- Für Bare-Metal-Instances können Sie keine CPU-Optionen angeben.
- CPU-Optionen können nur beim Start der Instance angegeben werden und können nach dem Start nicht mehr geändert werden.
- Wenn Sie eine Instance starten, müssen Sie sowohl die Anzahl der CPU-Kerne als auch die Anzahl der Threads pro Kern in der Anforderung angeben. Beispielanforderungen finden Sie unter CPU-Optionen für Ihre Instance festlegen.
- Die Zahl der vCPUs für die Instance ist die Anzahl der CPU-Kerne multipliziert mit den Threads pro Kern. Um eine benutzerdefinierte Anzahl von vCPUs anzugeben, müssen Sie eine gültige Anzahl von CPU-Kernen und Threads pro Kern für den Instance-Typ angeben. Sie können die Standardanzahl der vCPUs für die Instance nicht überschreiten. Weitere Informationen finden Sie unter CPU-Kerne und Threads pro CPU-Kern pro Instance-Typ.
- Um Multithreading zu deaktivieren, geben Sie einen Thread pro Kern an.
- Wenn Sie den Instance-Typ einer existierenden Instance ändern, werden die CPU-Optionen automatisch in die Standard-CPU-Optionen für den neuen Instance-Typ geändert.
- Die CPU-Optionen, die Sie angeben, bleiben nach dem Stoppen, Starten oder Neustarten einer Instance erhalten.

CPU-Kerne und Threads pro CPU-Kern pro Instance-Typ

Die folgenden Tabellen listen die Instance-Typen auf, die die Angabe von CPU-Optionen unterstützen.

Inhalt

Instances für allgemeine Zwecke

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m2.xlarge	2	2	1	1, 2	1
m2.2xlarge	4	4	1	1, 2, 3, 4	1
m2.4xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m3.large	2	1	2	1	1, 2
m3.xlarge	4	2	2	1, 2	1, 2
m3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m4.large	2	1	2	1	1, 2
m4.xlarge	4	2	2	1, 2	1, 2
m4.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m4.10xlarge	40	20	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20	1, 2
m4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5.large	2	1	2	1	1, 2
m5.xlarge	4	2	2	2	1, 2
m5.2xlarge	8	4	2	2, 4	1, 2
m5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5a.large	2	1	2	1	1, 2
m5a.xlarge	4	2	2	2	1, 2
m5a.2xlarge	8	4	2	2, 4	1, 2
m5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5ad.large	2	1	2	1	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5ad.xlarge	4	2	2	2	1, 2
m5ad.2xlarge	8	4	2	2, 4	1, 2
m5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
m5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
m5d.large	2	1	2	1	1, 2
m5d.xlarge	4	2	2	2	1, 2
m5d.2xlarge	8	4	2	2, 4	1, 2
m5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5dn.large	2	1	2	1	1, 2
m5dn.xlarge	4	2	2	1, 2	1, 2
m5dn.2xlarge	8	4	2	2, 4	1, 2
m5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5n.large	2	1	2	1	1, 2
m5n.xlarge	4	2	2	1, 2	1, 2
m5n.2xlarge	8	4	2	2, 4	1, 2
m5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m5zn.large	2	1	2	1	1, 2
m5zn.xlarge	4	2	2	1, 2	1, 2
m5zn.2xlarge	8	4	2	2, 4	1, 2
m5zn.3xlarge	12	6	2	2, 4, 6	1, 2
m5zn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m5zn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6a.large	2	1	2	1	1, 2
m6a.xlarge	4	2	2	1, 2	1, 2
m6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
m6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
m6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
m6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
m6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
m6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6g.large	2	2	1	1, 2	1
m6g.xlarge	4	4	1	1, 2, 3, 4	1
m6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6gd.large	2	2	1	1, 2	1
m6gd.xlarge	4	4	1	1, 2, 3, 4	1
m6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m6i.large	2	1	2	1	1, 2
m6i.xlarge	4	2	2	1, 2	1, 2
m6i.2xlarge	8	4	2	2, 4	1, 2
m6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
m6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6id.large	2	1	2	1	1, 2
m6id.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6id.2xlarge	8	4	2	2, 4	1, 2
m6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
m6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
m6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
m6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
m6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6idn.large	2	1	2	1	1, 2
m6idn.xlarge	4	2	2	1, 2	1, 2
m6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m6in.large	2	1	2	1	1, 2
m6in.xlarge	4	2	2	1, 2	1, 2
m6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
m6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
m7a.large	2	2	1	1, 2	1
m7a.xlarge	4	4	1	1, 2, 3, 4	1
m7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
m7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
m7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
m7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
m7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
m7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
m7g.large	2	2	1	1, 2	1
m7g.xlarge	4	4	1	1, 2, 3, 4	1
m7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
m7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7gd.large	2	2	1	1, 2	1
m7gd.xlarge	4	4	1	1, 2, 3, 4	1
m7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
m7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
m7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
m7i.large	2	1	2	1	1, 2
m7i.xlarge	4	2	2	1, 2	1, 2
m7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
m7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
m7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
m7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
m7i-flex.large	2	1	2	1	1, 2
m7i-flex.xlarge	4	2	2	1, 2	1, 2
m7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
m7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
m7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
t3.nano	2	1	2	1	1, 2
t3.micro	2	1	2	1	1, 2
t3.small	2	1	2	1	1, 2
t3.medium	2	1	2	1	1, 2
t3.large	2	1	2	1	1, 2
t3.xlarge	4	2	2	2	1, 2
t3.2xlarge	8	4	2	2, 4	1, 2
t3a.nano	2	1	2	1	1, 2
t3a.micro	2	1	2	1	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
t3a.small	2	1	2	1	1, 2
t3a.medium	2	1	2	1	1, 2
t3a.large	2	1	2	1	1, 2
t3a.xlarge	4	2	2	2	1, 2
t3a.2xlarge	8	4	2	2, 4	1, 2
t4g.nano	2	2	1	1, 2	1
t4g.micro	2	2	1	1, 2	1
t4g.small	2	2	1	1, 2	1
t4g.medium	2	2	1	1, 2	1
t4g.large	2	2	1	1, 2	1
t4g.xlarge	4	4	1	1, 2, 3, 4	1
t4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Für Datenverarbeitung optimierte Instances

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c3.large	2	1	2	1	1, 2
c3.xlarge	4	2	2	1, 2	1, 2
c3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c4.large	2	1	2	1	1, 2
c4.xlarge	4	2	2	1, 2	1, 2
c4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c4.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.large	2	1	2	1	1, 2
c5.xlarge	4	2	2	2	1, 2
c5.2xlarge	8	4	2	2, 4	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c5.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c5.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5a.large	2	1	2	1	1, 2
c5a.xlarge	4	2	2	1, 2	1, 2
c5a.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5a.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c5a.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5a.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2
c5a.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5a.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5ad.large	2	1	2	1	1, 2
c5ad.xlarge	4	2	2	1, 2	1, 2
c5ad.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c5ad.4xlarge	16	8	2	1, 2, 3, 4, 8	1, 2
c5ad.8xlarge	32	16	2	1, 2, 3, 4, 8, 12, 16	1, 2
c5ad.12xlarge	48	24	2	1, 2, 3, 4, 8, 12, 16, 20, 24	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c5ad.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
c5ad.24xlarge	96	48	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48	1, 2
c5d.large	2	1	2	1	1, 2
c5d.xlarge	4	2	2	2	1, 2
c5d.2xlarge	8	4	2	2, 4	1, 2
c5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5d.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c5d.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c5d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c5n.large	2	1	2	1	1, 2
c5n.xlarge	4	2	2	2	1, 2
c5n.2xlarge	8	4	2	2, 4	1, 2
c5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c5n.9xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
c5n.18xlarge	72	36	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36	1, 2
c6a.large	2	1	2	1	1, 2
c6a.xlarge	4	2	2	1, 2	1, 2
c6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
c6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
c6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
c6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
c6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
c6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
c6g.large	2	2	1	1, 2	1
c6g.xlarge	4	4	1	1, 2, 3, 4	1
c6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gd.large	2	2	1	1, 2	1
c6gd.xlarge	4	4	1	1, 2, 3, 4	1
c6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6gn.medium	1	1	1	1	1
c6gn.large	2	2	1	1, 2	1
c6gn.xlarge	4	4	1	1, 2, 3, 4	1
c6gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c6gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c6gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c6i.large	2	1	2	1	1, 2
c6i.xlarge	4	2	2	1, 2	1, 2
c6i.2xlarge	8	4	2	2, 4	1, 2
c6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
c6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6id.large	2	1	2	1	1, 2
c6id.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6id.2xlarge	8	4	2	2, 4	1, 2
c6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
c6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
c6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
c6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
c6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c6in.large	2	1	2	1	1, 2
c6in.xlarge	4	2	2	1, 2	1, 2
c6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
c6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
c7a.large	2	2	1	1, 2	1
c7a.xlarge	4	4	1	1, 2, 3, 4	1
c7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
c7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
c7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
c7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
c7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
c7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1
c7g.large	2	2	1	1, 2	1
c7g.xlarge	4	4	1	1, 2, 3, 4	1
c7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
c7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gd.large	2	2	1	1, 2	1
c7gd.xlarge	4	4	1	1, 2, 3, 4	1
c7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7gn.large	2	2	1	1, 2	1
c7gn.xlarge	4	4	1	1, 2, 3, 4	1
c7gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
c7gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
c7gn.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
c7i.large	2	1	2	1	1, 2
c7i.xlarge	4	2	2	1, 2	1, 2
c7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
c7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
c7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
c7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
c7i-flex.large	2	1	2	1	1, 2
c7i-flex.xlarge	4	2	2	1, 2	1, 2
c7i-flex.2xlarge	8	4	2	1, 2, 3, 4	1, 2
c7i-flex.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
c7i-flex.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2

RAM-optimierte Instances

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r3.large	2	1	2	1	1, 2
r3.xlarge	4	2	2	1, 2	1, 2
r3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r4.large	2	1	2	1	1, 2
r4.xlarge	4	2	2	1, 2	1, 2
r4.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r4.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r4.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r4.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.large	2	1	2	1	1, 2
r5.xlarge	4	2	2	2	1, 2
r5.2xlarge	8	4	2	2, 4	1, 2
r5.4xlarge	16	8	2	2, 4, 6, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5a.large	2	1	2	1	1, 2
r5a.xlarge	4	2	2	2	1, 2
r5a.2xlarge	8	4	2	2, 4	1, 2
r5a.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5a.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5a.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5a.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5ad.large	2	1	2	1	1, 2
r5ad.xlarge	4	2	2	2	1, 2
r5ad.2xlarge	8	4	2	2, 4	1, 2
r5ad.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5ad.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r5ad.12xlarge	48	24	2	6, 12, 18, 24	1, 2
r5ad.16xlarge	64	32	2	8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5ad.24xlarge	96	48	2	12, 18, 24, 36, 48	1, 2
r5b.large	2	1	2	1	1, 2
r5b.xlarge	4	2	2	1, 2	1, 2
r5b.2xlarge	8	4	2	2, 4	1, 2
r5b.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5b.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5b.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5b.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5b.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5d.large	2	1	2	1	1, 2
r5d.xlarge	4	2	2	2	1, 2
r5d.2xlarge	8	4	2	2, 4	1, 2
r5d.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5d.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5d.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5d.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5d.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5dn.large	2	1	2	1	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5dn.xlarge	4	2	2	1, 2	1, 2
r5dn.2xlarge	8	4	2	2, 4	1, 2
r5dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5dn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r5n.large	2	1	2	1	1, 2
r5n.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r5n.2xlarge	8	4	2	2, 4	1, 2
r5n.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r5n.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r5n.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r5n.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r5n.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6a.large	2	1	2	1	1, 2
r6a.xlarge	4	2	2	1, 2	1, 2
r6a.2xlarge	8	4	2	1, 2, 3, 4	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6a.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6a.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
r6a.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 16, 24	1, 2
r6a.16xlarge	64	32	2	4, 6, 8, 10, 12, 14, 16, 32	1, 2
r6a.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
r6a.32xlarge	128	64	2	8, 12, 16, 20, 24, 28, 32, 64	1, 2
r6a.48xlarge	192	96	2	8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
r6g.large	2	2	1	1, 2	1
r6g.xlarge	4	4	1	1, 2, 3, 4	1
r6g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r6g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6gd.large	2	2	1	1, 2	1
r6gd.xlarge	4	4	1	1, 2, 3, 4	1
r6gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r6gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r6gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r6i.large	2	1	2	1	1, 2
r6i.xlarge	4	2	2	1, 2	1, 2
r6i.2xlarge	8	4	2	2, 4	1, 2
r6i.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6i.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6i.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
r6i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6idn.large	2	1	2	1	1, 2
r6idn.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6idn.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6idn.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r6idn.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6idn.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6idn.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6idn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6idn.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6in.large	2	1	2	1	1, 2
r6in.xlarge	4	2	2	1, 2	1, 2
r6in.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r6in.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6in.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r6in.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r6in.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2
r6in.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6in.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r6id.large	2	1	2	1	1, 2
r6id.xlarge	4	2	2	1, 2	1, 2
r6id.2xlarge	8	4	2	2, 4	1, 2
r6id.4xlarge	16	8	2	2, 4, 6, 8	1, 2
r6id.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
r6id.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r6id.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
r6id.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
r6id.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
r7a.large	2	2	1	1, 2	1
r7a.xlarge	4	4	1	1, 2, 3, 4	1
r7a.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7a.4xlarge	16	16	1	1, 2, 4, 6, 8, 10, 12, 14, 16	1
r7a.8xlarge	32	32	1	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1
r7a.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1
r7a.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 16, 24, 32, 40, 48, 56, 64	1
r7a.24xlarge	96	96	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 24, 36, 48, 60, 72, 84, 96	1
r7a.32xlarge	128	128	1	4, 6, 8, 10, 12, 14, 16, 32, 48, 64, 80, 96, 112, 128	1
r7a.48xlarge	192	192	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 48, 72, 96, 120, 144, 168, 192	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7g.large	2	2	1	1, 2	1
r7g.xlarge	4	4	1	1, 2, 3, 4	1
r7g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
r7g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7g.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7gd.large	2	2	1	1, 2	1
r7gd.xlarge	4	4	1	1, 2, 3, 4	1
r7gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
r7gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1
r7gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
r7i.large	2	1	2	1	1, 2
r7i.xlarge	4	2	2	1, 2	1, 2
r7i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7i.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7i.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1, 2
r7i.48xlarge	192	96	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7iz.large	2	1	2	1	1, 2
r7iz.xlarge	4	2	2	1, 2	1, 2
r7iz.2xlarge	8	4	2	1, 2, 3, 4	1, 2
r7iz.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
r7iz.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
r7iz.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
r7iz.16xlarge	64	32	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
r7iz.32xlarge	128	64	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
u-3tb1.56xlarge	224	112	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112	1, 2
u-6tb1.56xlarge	224	224	1	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u-6tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-9tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u-12tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2
u-18tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u-24tb1.112xlarge	448	224	2	8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7i-12tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7in-16tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7in-24tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
u7in-32tb.224xlarge	896	448	2	16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120, 128, 136, 144, 152, 160, 168, 176, 184, 192, 200, 208, 216, 224, 232, 240, 248, 256, 264, 272, 280, 288, 296, 304, 312, 320, 328, 336, 344, 352, 360, 368, 376, 384, 392, 400, 408, 416, 424, 432, 440, 448	1, 2
x1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x1.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
x2gd.large	2	2	1	1, 2	1
x2gd.xlarge	4	4	1	1, 2, 3, 4	1
x2gd.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
x2gd.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
x2gd.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2gd.12xlarge	48	48	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2gd.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
x2idn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2idn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2idn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iedn.xlarge	4	2	2	1, 2	1, 2
x2iedn.2xlarge	8	4	2	2, 4	1, 2
x2iedn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iedn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2iedn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x2iedn.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
x2iedn.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
x2iezn.2xlarge	8	4	2	2, 4	1, 2
x2iezn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
x2iezn.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
x2iezn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
x2iezn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
x1e.xlarge	4	2	2	1, 2	1, 2
x1e.2xlarge	8	4	2	1, 2, 3, 4	1, 2
x1e.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
x1e.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
x1e.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
x1e.32xlarge	128	64	2	4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64	1, 2
z1d.large	2	1	2	1	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
z1d.xlarge	4	2	2	1, 2	1, 2
z1d.2xlarge	8	4	2	2, 4	1, 2
z1d.3xlarge	12	6	2	2, 4, 6	1, 2
z1d.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
z1d.12xlarge	48	24	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Speicheroptimierte Instances

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
d2.xlarge	4	2	2	1, 2	1, 2
d2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
d2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
d2.8xlarge	36	18	2	2, 4, 6, 8, 10, 12, 14, 16, 18	1, 2
d3.xlarge	4	2	2	1, 2	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
d3.2xlarge	8	4	2	2, 4	1, 2
d3.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.xlarge	4	2	2	1, 2	1, 2
d3en.2xlarge	8	4	2	2, 4	1, 2
d3en.4xlarge	16	8	2	2, 4, 6, 8	1, 2
d3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
d3en.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
d3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
h1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
h1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
h1.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
h1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i2.xlarge	4	2	2	1, 2	1, 2
i2.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i2.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
i2.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
i3.large	2	1	2	1	1, 2
i3.xlarge	4	2	2	1, 2	1, 2
i3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i3en.large	2	1	2	1	1, 2
i3en.xlarge	4	2	2	1, 2	1, 2
i3en.2xlarge	8	4	2	2, 4	1, 2
i3en.3xlarge	12	6	2	2, 4, 6	1, 2
i3en.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2
i3en.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i3en.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
i4g.large	2	2	1	1, 2	1
i4g.xlarge	4	4	1	1, 2, 3, 4	1
i4g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
i4g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
i4g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i4g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
i4i.large	2	1	2	1	1, 2
i4i.xlarge	4	2	2	1, 2	1, 2
i4i.2xlarge	8	4	2	1, 2, 3, 4	1, 2
i4i.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i4i.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
i4i.12xlarge	48	24	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24	1, 2
i4i.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
i4i.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
i4i.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
im4gn.large	2	2	1	1, 2	1
im4gn.xlarge	4	4	1	1, 2, 3, 4	1
im4gn.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
im4gn.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
im4gn.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
im4gn.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
is4gen.medium	1	1	1	1	1
is4gen.large	2	2	1	1, 2	1
is4gen.xlarge	4	4	1	1, 2, 3, 4	1
is4gen.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
is4gen.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
is4gen.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Beschleunigte Computing-Instances

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
dl1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
dl2q.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28,	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				30, 32, 34, 36, 38, 40, 42, 44, 46, 48	
f1.2xlarge	8	4	2	1, 2, 3, 4	1, 2
f1.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
f1.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g3.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
g3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g4ad.xlarge	4	2	2	2	1, 2
g4ad.2xlarge	8	4	2	2, 4	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g4ad.4xlarge	16	8	2	2, 4, 8	1, 2
g4ad.8xlarge	32	16	2	2, 4, 8, 16	1, 2
g4ad.16xlarge	64	32	2	2, 4, 8, 16, 32	1, 2
g4dn.xlarge	4	2	2	2	1, 2
g4dn.2xlarge	8	4	2	2, 4	1, 2
g4dn.4xlarge	16	8	2	2, 4, 6, 8	1, 2
g4dn.8xlarge	32	16	2	2, 4, 6, 8, 10, 12, 14, 16	1, 2
g4dn.12xlarge	48	24	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24	1, 2
g4dn.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
g5g.xlarge	4	4	1	1, 2, 3, 4	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g5g.2xlarge	8	8	1	1, 2, 3, 4, 5, 6, 7, 8	1
g5g.4xlarge	16	16	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1
g5g.8xlarge	32	32	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g5g.16xlarge	64	64	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64	1
g6.xlarge	4	2	2	1, 2	1, 2
g6.2xlarge	8	4	2	1, 2, 3, 4	1, 2
g6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
g6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
g6.12xlarge	48	24	2	1, 2, 3, 6, 9, 12, 15, 18, 21, 24	1, 2
g6.16xlarge	64	32	2	1, 2, 3, 4, 8, 12, 16, 20, 24, 28, 32	1, 2
g6.24xlarge	96	48	2	1, 2, 3, 4, 5, 6, 12, 18, 24, 30, 36, 42, 48	1, 2
g6.48xlarge	192	96	2	4, 6, 8, 10, 12, 24, 36, 48, 60, 72, 84, 96	1, 2
gr6.4xlarge	16	8	2	1, 2, 3, 4, 5, 6, 7, 8	1, 2
gr6.8xlarge	32	16	2	1, 2, 4, 6, 8, 10, 12, 14, 16	1, 2
inf1.xlarge	4	2	2	2	1, 2
inf1.2xlarge	8	4	2	2, 4	1, 2
inf1.6xlarge	24	12	2	2, 4, 6, 8, 10, 12	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
inf1.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
inf2.xlarge	4	2	2	1, 2	1, 2
inf2.8xlarge	32	16	2	4, 6, 8, 10, 12, 14, 16	1, 2
inf2.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 32, 48	1, 2
inf2.48xlarge	192	96	2	4, 8, 12, 16, 20, 24, 28, 32, 64, 96	1, 2
p2.xlarge	4	2	2	1, 2	1, 2
p2.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p2.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
p3.2xlarge	8	4	2	1, 2, 3, 4	1, 2
p3.8xlarge	32	16	2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16	1, 2
p3.16xlarge	64	32	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32	1, 2
p3dn.24xlarge	96	48	2	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p4d.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
p4de.24xlarge	96	48	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48	1, 2
p5.48xlarge	192	96	2	12, 24, 36, 48, 60, 72, 84, 96	1, 2
trn1.2xlarge	8	4	2	2, 4	1, 2
trn1.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
trn1n.32xlarge	128	64	2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64	1, 2
vt1.3xlarge	12	6	2	6	1, 2
vt1.6xlarge	24	12	2	6, 12	1, 2
vt1.24xlarge	96	48	2	6, 12, 48	1, 2

Instances für Datenverarbeitung in Hochleistung

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
hpc6id.32xlarge	64	64	1	4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46,	1

Instance-Typ	Standard vCPUs	Standard-CPU-Kerne	Standard-Threads pro Kern	Gültige CPU-Kerne	Gültige Threads pro Kern
				48, 50, 52, 54, 56, 58, 60, 62, 64	

CPU-Optionen für Ihre Instance festlegen

Sie können CPU-Optionen beim Start der Instance angeben.

In den folgenden Beispielen wird beschrieben, wie Sie die CPU-Optionen angeben, wenn Sie den Launch-Instance-Assistenten in der EC2-Konsole und den AWS CLI Befehl run-instances sowie die Seite create launch template in der EC2-Konsole und den AWS CLI Befehl create-launch-template verwenden. Für eine EC2-Flotte oder Spot-Flotte müssen Sie die CPU-Optionen in einer Startvorlage angeben.

Die folgenden Beispiele sind für einen `r5.4xlarge`-Instance-Typ, der folgende Vorgabewerte aufweist:

- Standard-CPU-Kerne: 8
- Standard-Threads pro Kern: 2
- Standard vCPUs: 16 (8 * 2)
- Gültige Anzahl von CPU-Kernen: 2, 4, 6, 8
- Gültige Fadenzahl pro Kern: 1, 2

Deaktivieren des Multithreading

Um Multithreading zu deaktivieren, geben Sie 1 Thread pro Kern an.

New console

So deaktivieren Sie Multithreading während des Instance-Starts

1. Befolgen Sie das Starten Sie schnell eine Instance-Verfahren und konfigurieren Sie Ihre Instance nach Bedarf.

2. Erweitern Sie Erweiterte Details und aktivieren Sie das Kontrollkästchen CPU-Optionen festlegen.
3. Wählen Sie für Core count (Anzahl Kerne) die Anzahl der benötigten CPU-Kerne aus. Um in diesem Beispiel die Standard-CPU-Kernanzahl für einer`5.4xlarge`-Instance festzulegen, wählen Sie 8 aus.
4. Um Multithreading für Threads per core (Threads pro Kern) zu deaktivieren, wählen Sie 1.
5. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Old console

So deaktivieren Sie Multithreading während des Instance-Starts

1. Folgen Sie dem Verfahren unter Starten einer Instance mit dem alten Launch Instance Wizard.
2. Wählen Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) für CPU options (CPU-Optionen) die Option Specify CPU options (CPU-Optionen festlegen) aus.
3. Wählen Sie für Core count (Anzahl Kerne) die Anzahl der benötigten CPU-Kerne aus. Um in diesem Beispiel die Standard-CPU-Kernanzahl für einer`5.4xlarge`-Instance festzulegen, wählen Sie 8 aus.
4. Um Multithreading für Threads per core (Threads pro Kern) zu deaktivieren, wählen Sie 1.
5. Fahren Sie den Aufforderungen des Assistenten entsprechend fort. Wählen Sie nach dem Überprüfen Ihrer Optionen auf der Seite Review Instance Launch (Instance-Start überprüfen) die Option Launch (Starten). Weitere Informationen finden Sie unter Starten einer Instance mit dem alten Launch Instance Wizard.

AWS CLI

So deaktivieren Sie Multithreading während des Instance-Starts

Verwenden Sie den AWS CLI -Befehl run-instances, und geben Sie einen Wert von 1 für `ThreadsPerCore` beim `--cpu-options`-Parameter an. Geben Sie für `CoreCount` die Anzahl der CPU-Kerne an. Um in diesem Beispiel die standardmäßige CPU-Kernanzahl für eine `r5.4xlarge`-Instance festzulegen, geben Sie den Wert 8 an.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=8,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Legen Sie eine benutzerdefinierte Anzahl von vCPUs fest

Sie können die Anzahl der CPU-Kerne und -Threads pro Kern für die Instance anpassen.

Im folgenden Beispiel wird eine `r5.4xlarge` Instanz mit 4 vCPUs gestartet.

New console

So legen Sie eine benutzerdefinierte Anzahl von vCPUs beim Instance-Start fest

1. Befolgen Sie das Starten Sie schnell eine Instance-Verfahren und konfigurieren Sie Ihre Instance nach Bedarf.
2. Erweitern Sie Erweiterte Details und aktivieren Sie das Kontrollkästchen CPU-Optionen festlegen.
3. Um 4 vCPUs zu erhalten, geben Sie 2 CPU-Kerne und 2 Threads pro Kern wie folgt an:
   - Wählen Sie für Anzahl der Kerne den Wert 2 aus.
   - Wählen Sie für Threads per core (Threads pro Kern) wählen Sie 2 aus.
4. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Old console

So legen Sie eine benutzerdefinierte Anzahl von vCPUs beim Instance-Start fest

1. Folgen Sie dem Verfahren unter Starten einer Instance mit dem alten Launch Instance Wizard.
2. Wählen Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) für CPU options (CPU-Optionen) die Option Specify CPU options (CPU-Optionen festlegen) aus.
3. Um 4 vCPUs zu erhalten, geben Sie 2 CPU-Kerne und 2 Threads pro Kern wie folgt an:

- Wählen Sie für Anzahl der Kerne den Wert 2 aus.
- Wählen Sie für Threads per core (Threads pro Kern) wählen Sie 2 aus.

4. Fahren Sie den Aufforderungen des Assistenten entsprechend fort. Wählen Sie nach dem Überprüfen Ihrer Optionen auf der Seite Review Instance Launch (Instance-Start überprüfen) die Option Launch (Starten). Weitere Informationen finden Sie unter Starten einer Instance mit dem alten Launch Instance Wizard.

AWS CLI

So legen Sie eine benutzerdefinierte Anzahl von vCPUs beim Instance-Start fest

Verwenden Sie den AWS CLI Befehl run-instances und geben Sie die Anzahl der CPU-Kerne und die Anzahl der Threads im `--cpu-options` Parameter an. Sie können 2 CPU-Kerne und 2 Threads pro Kern angeben, um 4 vCPUs zu erhalten.

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=2,ThreadsPerCore=2" \
    --key-name MyKeyPair
```

Geben Sie alternativ 4 CPU-Kerne und 1 Thread pro Kern an (Multithreading deaktivieren), um 4 vCPUs zu erhalten:

```
aws ec2 run-instances \
    --image-id ami-1a2b3c4d \
    --instance-type r5.4xlarge \
    --cpu-options "CoreCount=4,ThreadsPerCore=1" \
    --key-name MyKeyPair
```

Legen Sie eine benutzerdefinierte Anzahl von vCPUs in einer Startvorlage fest

Sie können die Anzahl der CPU-Kerne und -Threads pro Kern für die Instance in einer Startvorlage anpassen.

Im folgenden Beispiel wird eine Startvorlage erstellt, die die Konfiguration für eine `r5.4xlarge` Instanz mit 4 vCPUs angibt.

Console

Wie Sie eine benutzerdefinierte Anzahl von vCPUs in einer Startvorlage festlegen

1. Befolgen Sie das Erstellen Sie eine Startvorlage aus Parametern-Verfahren und konfigurieren Sie Ihre Startvorlage nach Bedarf.
2. Erweitern Sie Erweiterte Details und aktivieren Sie das Kontrollkästchen CPU-Optionen festlegen.
3. Um 4 vCPUs zu erhalten, geben Sie 2 CPU-Kerne und 2 Threads pro Kern wie folgt an:
   - Wählen Sie für Anzahl der Kerne den Wert 2 aus.
   - Wählen Sie für Threads per core (Threads pro Kern) wählen Sie 2 aus.
4. Überprüfen Sie im Bereich Zusammenfassung die Konfiguration Ihrer Instance und wählen Sie dann Startvorlage erstellen aus. Weitere Informationen finden Sie unter Starten einer Instance über eine Startvorlage.

AWS CLI

Wie Sie eine benutzerdefinierte Anzahl von vCPUs in einer Startvorlage festlegen

Verwenden Sie den AWS CLI Befehl create-launch-template und geben Sie die Anzahl der CPU-Kerne und die Anzahl der Threads im Parameter an. `CpuOptions` Sie können 2 CPU-Kerne und 2 Threads pro Kern angeben, um 4 vCPUs zu erhalten.

```
aws ec2 create-launch-template \
    --launch-template-name TemplateForCPUOptions \
    --version-description CPUOptionsVersion1 \
    --launch-template-data file://template-data.json
```

Nachfolgend finden Sie eine JSON-Beispieldatei, die die Startvorlagedaten, einschließlich der CPU-Optionen, für die Konfiguration der Instance für dieses Beispiel enthält.

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
```

```
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":2,
        "ThreadsPerCore":2
    }
}
```

Geben Sie alternativ 4 CPU-Kerne und 1 Thread pro Kern an (Multithreading deaktivieren), um 4 vCPUs zu erhalten:

```
{
    "NetworkInterfaces": [{
        "AssociatePublicIpAddress": true,
        "DeviceIndex": 0,
        "Ipv6AddressCount": 1,
        "SubnetId": "subnet-7b16de0c"
    }],
    "ImageId": "ami-8c1be5f6",
    "InstanceType": "r5.4xlarge",
    "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
            "Key":"Name",
            "Value":"webserver"
        }]
    }],
    "CpuOptions": {
        "CoreCount":4,
        "ThreadsPerCore":1
    }
}
```

Anzeigen der CPU-Optionen für Ihre Instance

Sie können die CPU-Optionen für eine vorhandene Instance in der Amazon-EC2-Konsole einsehen oder die Instance mit der AWS CLI beschreiben.

Console

So zeigen Sie die CPU-Optionen für eine Instance über die Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im linken Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Suchen Sie auf der Registerkarte Details unter Host und Platzierungsgruppe nach der Option Anzahl der vCPUs.

AWS CLI

So zeigen Sie die CPU-Optionen für eine Instance an (AWS CLI)

Verwenden Sie den Befehl describe-instances.

```
aws ec2 describe-instances --instance-ids i-123456789abcde123
```

```
...
    "Instances": [
        {
            "Monitoring": {
                "State": "disabled"
            },
            "PublicDnsName": "ec2-198-51-100-5.eu-central-1.compute.amazonaws.com",
            "State": {
                "Code": 16,
                "Name": "running"
            },
            "EbsOptimized": false,
            "LaunchTime": "2018-05-08T13:40:33.000Z",
            "PublicIpAddress": "198.51.100.5",
            "PrivateIpAddress": "172.31.2.206",
            "ProductCodes": [],
            "VpcId": "vpc-1a2b3c4d",
            "CpuOptions": {
```

```
                "CoreCount": 34,
                "ThreadsPerCore": 1
            },
            "StateTransitionReason": "",
            ...
        }
    ]
...
```

In der Ausgabe, die zurückgegeben wird, gibt die Option `CoreCount` die Anzahl der Kerne für die Instance an. Das Feld `ThreadsPerCore` gibt die Anzahl der Threads pro Kern an.

Um CPU-Informationen anzuzeigen, können Sie alternativ eine Verbindung zu Ihrer Instance herstellen und eines der folgenden Systemtools verwenden:

- Windows `Task Manager` auf Ihrer Windows-Instanz
- Der lscpu Befehl auf Ihrer Linux-Instanz

Sie können ihn verwenden, AWS Config um Konfigurationsänderungen für Instances, einschließlich beendeter Instances, aufzuzeichnen, zu bewerten, zu prüfen und auszuwerten. Weitere Informationen finden Sie unter Erste Schritte mit AWS Config im AWS Config -Developerhandbuch.

AMD SEV-SNP auf Amazon EC2

AMD Secure Encrypted Virtualization-Secure Nested Paging (AMD SEV-SNP) ist ein CPU-Feature, das die folgenden Eigenschaften bietet:

- Bescheinigung – Mit AMD SEV-SNP können Sie einen signierten Bescheinigungsbericht abrufen, der eine kryptografische Maßnahme enthält, mit welcher der Status und die Identität der Instance sowie die Ausführung auf echter AMD-Hardware überprüft werden kann. Weitere Informationen finden Sie unter Bescheinigung mit AMD SEV-SNP.
- Speicherverschlüsselung — Ab den Prozessoren AMD EPYC (Milan), AWS Graviton2 und Intel Xeon Scalable (Ice Lake) ist der Instance-Speicher immer verschlüsselt. Für AMD SEV-SNP aktivierte Instances verwenden einen Instance-spezifischen Schlüssel für ihre Speicherverschlüsselung.

Konzepte und Terminologie

Bevor Sie mit AMD SEV-SNP beginnen, sollten Sie mit den folgenden Konzepten und Begriffen vertraut sein:

Bescheinigungsbericht von AMD SEV-SNP

Der Bescheinigungsbericht von AMD SEV-SNP ist ein Dokument, das eine Instance von der CPU anfordern kann. Der Bescheinigungsbericht von AMD SEV-SNP kann verwendet werden, um den Status und die Identität einer Instance zu überprüfen und sicherzustellen, ob sie in einer genehmigten AMD-Umgebung ausgeführt wird. Der Bericht enthält eine Startmessung, bei der es sich um einen kryptografischen Hash des anfänglichen Startstatus einer Instance handelt, einschließlich des ursprünglichen Speicherinhalts der Instance und des Anfangsstatus der vCPUs. Der Bescheinigungsbericht von AMD SEV-SNP ist mit einer VLEK-Signatur signiert, die auf eine AMD-Stammvertrauenstellung zurückgeht.

VLEK

Der VLEK (Versioned Loaded Endorsement Key) ist ein Signaturschlüssel mit Versionsverwaltung, der von AMD zertifiziert ist und von der AMD-CPU zum Signieren der Bescheinigungsberichte von AMD SEV-SNP verwendet wird. VLEK-Signaturen können mit den von AMD bereitgestellten Zertifikaten validiert werden.

OVMF-Binärdatei

OVMF (Open Virtual Machine Firmware) ist der Frühstartcode, der verwendet wird, um eine UEFI-Umgebung für die Instance bereitzustellen. Der Frühstartcode wird ausgeführt, bevor der Code im AMI gestartet wird. Die OVMF findet und führt auch das im AMI bereitgestellte Startladeprogramm aus. Weitere Informationen finden Sie im OMVF-Repository.

Voraussetzungen

Zur Verwendung von AMD SEV-SNP müssen Sie folgende Voraussetzungen erfüllen:

- Verwenden Sie einen der folgenden unterstützten Instance-Typen:
  - Universell: `m6a.large` | `m6a.xlarge` | `m6a.2xlarge` | `m6a.4xlarge` | `m6a.8xlarge`
  - Für Datenverarbeitung optimiert: `c6a.large` | `c6a.xlarge` | `c6a.2xlarge` | `c6a.4xlarge` | `c6a.8xlarge` | `c6a.12xlarge` | `c6a.16xlarge`
  - Speicheroptimiert: `r6a.large` | `r6a.xlarge` | `r6a.2xlarge` | `r6a.4xlarge`

- Starten Sie Ihre Instance in einer unterstützten Version. AWS-Region Derzeit werden nur USA Ost (Ohio) und Europa (Irland) unterstützt.
- Verwenden Sie ein AMI mit dem Startmodus `uefi` oder`uefi-preferred` und einem Betriebssystem, das AMD SEV-SNP unterstützt. Weitere Informationen zur Unterstützung von AMD SEV-SNP unter Ihrem Betriebssystem finden Sie in der Dokumentation des jeweiligen Betriebssystems. Denn AWS AMD SEV-SNP wird auf AL2023, RHEL 9.3, SLES 15 SP4 und Ubuntu 23.04 und höher unterstützt.

Überlegungen

Sie können AMD SEV-SNP nur aktivieren, wenn Sie eine Instance starten. Wenn AMD SEV-SNP für den Start Ihrer Instance aktiviert ist, gelten die folgenden Regeln.

- AMD SEV-SNP kann nicht ausgeschaltet werden. Es bleibt während des gesamten Instance-Lebenszyklus aktiviert.
- Sie können den Instance-Typ nur in einen anderen Instance-Typ ändern, der AMD SEV-SNP unterstützt.
- Hibernation und Nitro Enclaves werden nicht unterstützt.
- Dedicated Hosts werden nicht unterstützt.
- Wenn für den Host, der Ihrer Instance zugrunde liegt, eine Wartung geplant ist, erhalten Sie 14 Tage vor dem Ereignis eine Benachrichtigung über ein geplantes Ereignis. Sie müssen Ihre Instance manuell stoppen oder neu starten, um sie auf einen neuen Host zu verschieben.

Preisgestaltung

Wenn Sie eine Amazon-EC2-Instance mit aktiviertem AMD SEV-SNP starten, wird Ihnen eine zusätzliche stündliche Nutzungsgebühr in Höhe von 10 Prozent des On-Demand-Stundensatzes des ausgewählten Instance-Typs berechnet.

Diese Nutzungsgebühr für AMD SEV-SNP ist eine separate Gebühr für die Nutzung Ihrer Amazon-EC2-Instance. Reserved Instances, Savings Plans und die Nutzung des Betriebssystems haben keinen Einfluss auf diese Gebühr.

Wenn Sie eine Spot Instance konfigurieren, mit aktiviertem AMD SEV-SNP zu starten, wird Ihnen eine zusätzliche stündliche Nutzungsgebühr in Höhe von 10 % des On-Demand-Stundensatzes des ausgewählten Instance-Typs berechnet. Wenn die Zuweisungsstrategie den Preis als Eingabewert

verwendet, berücksichtigt die Spot-Flotte diese zusätzliche Gebühr nicht. Es wird nur der Spot-Preis verwendet.

Arbeiten Sie mit AMD SEV-SNP auf Amazon EC2

Führen Sie die folgenden Aufgaben aus, um mit AMD SEV-SNP auf Amazon EC2 zu arbeiten.

Aufgaben

- Unterstützte Instance-Typen finden
- AMD SEV-SNP beim Start einschalten
- Status von AMD SEV-SNP überprüfen

Unterstützte Instance-Typen finden

Sie können den verwenden, um Instance-Typen AWS CLI zu finden, die AMD SEV-SNP unterstützen.

Verwenden Sie den folgenden Befehl, um die Instance-Typen zu finden, die AMD SEV-SNP unterstützen, indem Sie den AWS CLI folgenden Befehl verwenden. describe-instance-types

```
$ C:\> aws ec2 describe-instance-types \
--filters Name=processor-info.supported-features,Values=amd-sev-snp \
--query 'InstanceTypes[*].InstanceType'
```

Beispielausgabe.

```
[
 "r6a.2xlarge",
 "m6a.large",
 "m6a.2xlarge",
 "r6a.xlarge",
 "c6a.16xlarge",
 "c6a.8xlarge",
 "m6a.4xlarge",
 "c6a.12xlarge",
 "r6a.4xlarge",
 "c6a.xlarge",
 "c6a.4xlarge",
 "c6a.2xlarge",
 "m6a.xlarge",
 "c6a.large",
```

```
 "r6a.large",
 "m6a.8xlarge"
]
```

AMD SEV-SNP beim Start einschalten

Sie können den verwenden, AWS CLI um eine Instance mit aktiviertem AMD SEV-SNP zu starten.

Um eine Instance mit aktiviertem AMD SEV-SNP mit dem zu starten AWS CLI, verwenden Sie den Befehl und fügen Sie die Option hinzu. run-instances`--cpu-options AmdSevSnp=enabled` Geben Sie für `--image-id` ein AMI mit dem Startmodus `uefi` oder `uefi-prefered` und ein Betriebssystem an, das AMD SEV-SNP unterstützt. Für `--instance-type` geben Sie einen unterstützten Instance-Typ an.

```
$ C:\> aws ec2 run-instances \
--image-id supported_ami_id \
--instance-type supported_instance_type \
--key-name key_pair_name \
--subnet-id subnet_id \
--cpu-options AmdSevSnp=enabled
```

Status von AMD SEV-SNP überprüfen

Sie können eine der folgenden Methoden verwenden, um den Status von AMD SEV-SNP zu überprüfen.

AWS CLI

Verwenden Sie den Befehl, um zu überprüfen, ob AMD SEV-SNP für eine Instance aktiviert ist, die den verwendet. AWS CLIdescribe-instances Geben Sie für `--instance-ids` die ID der zu prüfenden Instance an.

```
$ C:\> aws ec2 describe-instances --instance-ids instance_id
```

In der Befehlsausgabe zeigt der Wert für `AmdSevSnp` in `CpuOptions` an, ob AMD SEV-SNP aktiviert oder deaktiviert ist.

AWS CloudTrail

Im AWS CloudTrail Fall der Anfrage zum Starten der Instance `"cpuOptions": {"AmdSevSnp": enabled}` gibt der Wert von an, dass AMD SEV-SNP für die Instance aktiviert ist.

Bescheinigung mit AMD SEV-SNP

Die Bescheinigung ist ein Prozess, mit dem Ihre Instance ihren Status und ihre Identität nachweisen kann. Wenn Sie AMD SEV-SNP für Ihre Instance aktivieren, können Sie vom zugrunde liegenden Prozessor einen AMD-SEV-SNP-Bescheinigungsbericht anfordern. Der AMD-SEV-SNP-Bescheinigungsbericht enthält einen kryptografischen Hash, die sogenannte Startmessung, die den anfänglichen Inhalt des Gastspeichers und den anfänglichen vCPU-Status anzeigt. Der Bescheinigungsbericht ist mit einer VLEK-Signatur signiert, die auf eine AMD-Stammvertrauenstellung zurückgeht. Sie können anhand der im Bescheinigungsbericht enthaltenen Startmessung überprüfen, ob die Instance in einer echten AMD-Umgebung ausgeführt wird, und den anfänglichen Startcode überprüfen, der zum Starten der Instance verwendet wurde.

Führen Sie die folgenden Schritte aus, um die Bescheiningung mit AMD SEV-SNP durchzuführen:

Schritt 1: Abrufen des Bescheinigungsberichts

In diesem Schritt installieren und erstellen Sie das `snpguest` Utility und verwenden es dann, um den AMD SEV-SNP-Bestätigungsbericht und die Zertifikate anzufordern.

1. Führen Sie die folgenden Befehle aus, um das Hilfsprogramm aus dem zu erstellen. `snpguest` snpguest repository

   ```
   $ C:\> git clone https://github.com/virtee/snpguest.git
   $ C:\> cd snpguest
   $ C:\> cargo build -r
   $ C:\> cd target/release
   ```

2. Generieren Sie eine Anfrage für den Bestätigungsbericht. Das Hilfsprogramm fordert den Bestätigungsbericht vom Host an und schreibt ihn mit den bereitgestellten Anforderungsdaten in eine Binärdatei.

   Das folgende Beispiel erstellt eine zufällige Anforderungszeichenfolge und verwendet sie als Anforderungsdatei ()`request-file.txt`. Wenn der Befehl den Bestätigungsbericht zurückgibt, wird er in dem von Ihnen angegebenen Dateipfad gespeichert ()`report.bin`. In diesem Fall speichert das Hilfsprogramm den Bericht im aktuellen Verzeichnis.

   ```
   $ C:\> ./snpguest report report.bin request-file.txt --random
   ```

3. Fordern Sie die Zertifikate aus dem Hostspeicher an und speichern Sie sie als PEM-Dateien. Im folgenden Beispiel werden die Dateien im selben Verzeichnis wie das `snpguest` Hilfsprogramm

gespeichert. Wenn im angegebenen Verzeichnis bereits Zertifikate vorhanden sind, werden diese Zertifikate überschrieben.

```
$ C:\> ./snpguest certificates PEM ./
```

Schritt 2: Überprüfen Sie die Signatur des Bestätigungsberichts

Der Bestätigungsbericht ist mit einem Zertifikat signiert, dem sogenannten Versioned Loaded Endorsement Key (VLEK), das von AMD ausgestellt wurde für. AWS In diesem Schritt können Sie überprüfen, ob das VLEK-Zertifikat von AMD ausgestellt wurde und ob der Bestätigungsbericht mit diesem VLEK-Zertifikat signiert ist.

1. Laden Sie die VLEK-Vertrauenszertifikate von der offiziellen AMD-Website in das aktuelle Verzeichnis herunter.

   ```
   $ C:\> sudo curl --proto '=https' --tlsv1.2 -sSf https://kdsintf.amd.com/vlek/v1/
   Milan/cert_chain -o ./cert_chain.pem
   ```

2. Verwenden Sie `openssl`, um zu überprüfen, ob das VLEK-Zertifikat von den Zertifikaten der AMD-Stammvertrauenstellung signiert ist.

   ```
   $ C:\> sudo openssl verify --CAfile ./cert_chain.pem vlek.pem
   ```

   Erwartete Ausgabe:

   ```
   certs/vcek.pem: OK
   ```

3. Verwenden Sie das Dienstprogramm `snpguest`, um zu überprüfen, ob der Bescheinigungsbericht mit dem VLEK-Zertifikat signiert ist.

   ```
   $ C:\> ./snpguest verify attestation ./ report.bin
   ```

   Erwartete Ausgabe.

   ```
   Reported TCB Boot Loader from certificate matches the attestation report.
   Reported TCB TEE from certificate matches the attestation report.
   Reported TCB SNP from certificate matches the attestation report.
   Reported TCB Microcode from certificate matches the attestation report.
   ```

```
VEK signed the Attestation Report!
```

Fügen Sie Windows-Systemkomponenten mithilfe von Installationsmedien hinzu

Windows Server-Betriebssysteme enthalten viele optionale Komponenten. Es ist nicht sinnvoll, alle optionalen Komponenten auf jedem Amazon EC2-Windows Server-AMI vorzuhalten. Stattdessen stellen wir Ihnen EBS-Snapshots als Installationsmedien zur Verfügung, die die erforderlichen Dateien zum Konfigurieren bzw. Installieren von Komponenten auf Ihrer Windows-Instance enthalten.

Zum Zugreifen auf und Installieren der optionalen Komponenten müssen Sie den richtigen EBS-Snapshot für Ihre Version von Windows Server ermitteln, aus dem Snapshot ein Volume erstellen und das Volume an Ihre Instance anfügen.

Bevor Sie beginnen

Verwenden Sie das Befehlszeilentool AWS Management Console oder, um die Instanz-ID und die Availability Zone Ihrer Instanz abzurufen. Sie müssen Ihr EBS-Volume in derselben Availability Zone wie Ihre Instance erstellen.

Hinzufügen von Windows-Komponenten mit der Konsole

Gehen Sie wie folgt vor AWS Management Console , um Ihrer Instanz Windows-Komponenten hinzuzufügen.

So fügen Sie Ihrer Instance mit der Konsole Windows-Komponenten hinzu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Snapshots.
3. Wählen Sie in der Leiste Filter die Option Public Snapshots (Öffentliche Snapshots).
4. Fügen Sie den Filter Owner Alias (Benutzeralias) hinzu und wählen Sie die Option Amazon.
5. Fügen Sie den Filter Description (Beschreibung) hinzu und geben Sie **`Windows`** ein.
6. Drücken Sie die Eingabetaste
7. Wählen Sie den Snapshot aus, der mit Ihrer Systemarchitektur und Sprachauswahl übereinstimmt. Wählen Sie beispielsweise Windows 2019 English Installation Media, wenn auf Ihrer Instance Windows Server 2019 ausgeführt wird.

8. Wählen Sie Actions (Aktionen, Create volume from snapshot (Volume aus Snapshot erstellen) aus.
9. Wählen Sie unter Availability Zone die Availability Zone aus, die Ihrer Windows-Instance entspricht. Wählen Sie Add tag (Tag hinzufügen) und geben Sie für den Tag-Schlüssel **`Name`** und einen beschreibenden Namen für den Tag-Wert an. Wählen Sie Create Volume (Volume erstellen) aus.
10. Wählen Sie in der Meldung Volume Successfully Created (Volume erfolgreich erstellt), die als grünes Banner angezeigt wird, das eben erstellte Volume aus.
11. Wählen Sie Actions (Aktionen) und Attach Volume (Volume anfügen).
12. Wählen Sie unter Instance die Instance-ID aus.
13. Geben Sie unter Device name (Gerätename) den Namen des Geräts ein, das angefügt werden soll. Wenn Sie Hilfe zum Gerätenamen benötigen, finden Sie weitere Informationen unter Gerätenamen auf Amazon EC2 EC2-Instances.
14. Wählen Sie Attach volume (Volume anfügen) aus.
15. Stellen Sie eine Verbindung mit Ihrer Instance her und machen Sie das Volume verfügbar. Weitere Informationen finden Sie unter Bereitstellen eines Amazon EBS-Volumes zur Verwendung im Amazon EBS-Benutzerhandbuch.

    > **Important**
    >
    > Initialisieren Sie das Volume nicht.

16. Öffnen Sie die Systemsteuerung und dann Programme und Features. Wählen Sie die Option Windows-Features aktivieren oder deaktivieren. Geben Sie das EBS-Volume mit den Installationsmedien an, wenn die entsprechende Aufforderung angezeigt wird.
17. (Optional) Wenn Sie mit dem Installationsmedium fertig sind, können Sie die Zuordnung des Volumes aufheben. Nachdem Sie die Zuordnung des Volumes aufgehoben haben, können Sie es löschen.

Fügen Sie Windows-Komponenten mithilfe der Tools für Windows hinzu PowerShell

Gehen Sie wie folgt vor, um mithilfe der Tools für Windows PowerShell Windows-Komponenten zu Ihrer Instanz hinzuzufügen.

Fügen Sie Ihrer Instanz mithilfe der Tools für Windows Windows-Komponenten hinzu PowerShell

1. Verwenden Sie das Get-EC2SnapshotCmdlet mit den `description` Filtern `Owner` und, um eine Liste der verfügbaren Snapshots der Installationsmedien abzurufen.

```
PS C:\> Get-EC2Snapshot -Owner amazon -Filter @{ Name="description";
 Values="Windows*" }
```

2. Beachten Sie in der Ausgabe die ID des Snapshots, der mit Ihrer Systemarchitektur und Sprachauswahl übereinstimmt. Beispielsweise:

```
...
DataEncryptionKeyId :
Description         : Windows 2019 English Installation Media
Encrypted           : False
KmsKeyId            :
OwnerAlias          : amazon
OwnerId             : 123456789012
Progress            : 100%
SnapshotId          : snap-22da283e
StartTime           : 10/25/2019 8:00:47 PM
State               : completed
StateMessage        :
Tags                : {}
VolumeId            : vol-be5eafcb
VolumeSize          : 6
...
```

3. Verwenden Sie das New-EC2VolumeCmdlet, um aus dem Snapshot ein Volume zu erstellen. Geben Sie dieselbe Availability Zone wie für Ihre Instance an.

```
PS C:\> New-EC2Volume -AvailabilityZone us-east-1a -VolumeType gp2 -
SnapshotId snap-22da283e
```

4. Notieren Sie sich in der Ausgabe die Volume-ID.

```
Attachments      : {}
AvailabilityZone : us-east-1a
CreateTime       : 4/18/2017 10:50:25 AM
Encrypted        : False
Iops             : 100
KmsKeyId         :
```

```
Size              : 6
SnapshotId        : snap-22da283e
State             : creating
Tags              : {}
VolumeId          : vol-06aa9e1fbf8b82ed1
VolumeType        : gp2
```

5. Verwenden Sie das Add-EC2VolumeCmdlet, um das Volume an Ihre Instance anzuhängen.

```
PS C:\> Add-EC2Volume -InstanceId i-087711ddaf98f9489 -
VolumeId vol-06aa9e1fbf8b82ed1 -Device xvdh
```

6. Stellen Sie eine Verbindung mit Ihrer Instance her und machen Sie das Volume verfügbar. Weitere Informationen finden Sie unter Bereitstellen eines Amazon EBS-Volumes zur Verwendung im Amazon EBS-Benutzerhandbuch.

> **Important**
>
> Initialisieren Sie das Volume nicht.

7. Öffnen Sie die Systemsteuerung und dann Programme und Features. Wählen Sie die Option Windows-Features aktivieren oder deaktivieren. Geben Sie das EBS-Volume mit den Installationsmedien an, wenn die entsprechende Aufforderung angezeigt wird.
8. (Optional) Wenn Sie mit dem Installationsmedium fertig sind, verwenden Sie das Dismount-EC2VolumeCmdlet, um das Volume von Ihrer Instance zu trennen. Nachdem Sie das Volume getrennt haben, können Sie das Volume mit dem Remove-EC2VolumeCmdlet löschen.

Fügen Sie Windows-Komponenten hinzu, indem Sie AWS CLI

Gehen Sie wie folgt vor, AWS CLI um Windows-Komponenten zu Ihrer Instanz hinzuzufügen.

Um Ihrer Instanz Windows-Komponenten hinzuzufügen, verwenden Sie den AWS CLI

1. Verwenden Sie den Befehl describe-snapshots mit dem Parameter `owner-ids` und dem Filter `description`, um eine Liste mit den verfügbaren Installationsmedien-Snapshots abzurufen.

```
aws ec2 describe-snapshots --owner-ids amazon --filters
 Name=description,Values=Windows*
```

2. Beachten Sie in der Ausgabe die ID des Snapshots, der mit Ihrer Systemarchitektur und Sprachauswahl übereinstimmt. Beispiel:

```
{
    "Snapshots": [
    ...
        {
            "OwnerAlias": "amazon",
            "Description": "Windows 2019 English Installation Media",
            "Encrypted": false,
            "VolumeId": "vol-be5eafcb",
            "State": "completed",
            "VolumeSize": 6,
            "Progress": "100%",
            "StartTime": "2019-10-25T20:00:47.000Z",
            "SnapshotId": "snap-22da283e",
            "OwnerId": "123456789012"
        },
    ...
   ]
}
```

3. Verwenden Sie den Befehl create-volume, um aus dem Snapshot ein Volume zu erstellen. Geben Sie dieselbe Availability Zone wie für Ihre Instance an.

```
aws ec2 create-volume --snapshot-id snap-22da283e --volume-type gp2 --availability-
zone us-east-1a
```

4. Notieren Sie sich in der Ausgabe die Volume-ID.

```
{
    "AvailabilityZone": "us-east-1a",
    "Encrypted": false,
    "VolumeType": "gp2",
    "VolumeId": "vol-0c98b37f30bcbc290",
    "State": "creating",
    "Iops": 100,
    "SnapshotId": "snap-22da283e",
    "CreateTime": "2017-04-18T10:33:10.940Z",
    "Size": 6
}
```

5. Verwenden Sie den Befehl attach-volume, um das Volume an Ihre Instance anzufügen.

```
aws ec2 attach-volume --volume-id vol-0c98b37f30bcbc290 --instance-
id i-01474ef662b89480 --device xvdg
```

6. Stellen Sie eine Verbindung mit Ihrer Instance her und machen Sie das Volume verfügbar. Weitere Informationen finden Sie unter Bereitstellen eines Amazon EBS-Volumes zur Verwendung im Amazon EBS-Benutzerhandbuch.

   Important

   Initialisieren Sie das Volume nicht.

7. Öffnen Sie die Systemsteuerung und dann Programme und Features. Wählen Sie die Option Windows-Features aktivieren oder deaktivieren. Geben Sie das EBS-Volume mit den Installationsmedien an, wenn die entsprechende Aufforderung angezeigt wird.
8. (Optional) Wenn Sie mit dem Installationsmedium fertig sind, heben Sie mit dem Befehl detach-volume die Zuordnung des Volumes zur Instance auf. Nachdem Sie die Zuordnung des Volumes aufgehoben haben, können Sie das Volume mit dem Befehl delete-volume löschen.

Verwalten Sie Systembenutzer auf Ihrer Linux-Instance

Jede Linux-Instance wird mit einem Standardbenutzer des Linux-Systems gestartet. Sie können Benutzer zu Ihrer Instance hinzufügen und Benutzer löschen.

Für den Standardbenutzer wird der Standardbenutzername durch das AMI bestimmt, das beim Starten der Instance angegeben wurde.

Note

Standardmäßig sind die Passwortauthentifizierung und die Root-Anmeldung deaktiviert und sudo ist aktiviert. Um sich bei Ihrer Instance anzumelden, müssen Sie ein Schlüsselpaar verwenden. Weitere Informationen zum Anmelden finden Sie unter Herstellen einer Verbindung zur Linux-Instance.
Sie können die Passwortauthentifizierung und die Root-Anmeldung für Ihre Instance zulassen. Weitere Informationen finden Sie in der Dokumentation für das Betriebssystem Ihrer Instance.

> **Note**
>
> Linux-Systembenutzer sollten nicht mit IAM-Benutzern verwechselt werden. Weitere Informationen finden Sie unter IAM-Benutzer im IAM-Benutzerhandbuch.

Inhalt

Standardbenutzernamen

Der Standardbenutzername für Ihre EC2-Instance wird durch das AMI bestimmt, das beim Starten der Instance angegeben wurde.

Die Standardbenutzernamen lauten:

- Bei AL2023, Amazon Linux 2 oder dem Amazon-Linux-AMI lautet der Benutzername `ec2-user`.
- Bei einem CentOS-AMI lautet der Benutzername `centos` oder `ec2-user`.
- Für ein Debian-AMI lautet der Benutzername `admin`.
- Bei einem Fedora-AMI lautet der Benutzername `fedora` oder `ec2-user`.
- Bei einem RHEL-AMI lautet der Benutzername `ec2-user` oder `root`.
- Bei einem SUSE-AMI lautet der Benutzername `ec2-user` oder `root`.
- Für ein Ubuntu-AMI lautet der Benutzername `ubuntu`.
- Bei einem Oracle-AMI lautet der Benutzername `ec2-user`.
- Für ein Bitnami-AMI lautet der Benutzername `bitnami`.

> **Note**
>
> Um den Standardbenutzernamen für andere Linux-Distributionen zu finden, wenden Sie sich an den AMI-Anbieter.

Überlegungen

Die Verwendung des Standardbenutzers ist für viele Anwendungen ausreichend. Sie können jedoch auch Benutzer hinzufügen, damit jeder seine eigenen Dateien und Workspaces haben kann. Darüber hinaus ist das Erstellen von Benutzern für neue Benutzer viel sicherer, als mehreren (möglicherweise unerfahrenen) Benutzern Zugriff auf den Standardbenutzer zu gewähren, da der Standardbenutzer bei unsachgemäßer Verwendung großen Schaden an einem System anrichten kann. Weitere Informationen finden Sie unter Tips for Securing Your EC2 Instance.

Um Benutzern den SSH-Zugriff auf Ihre EC2-Instance mithilfe eines Linux-Systembenutzers zu gewähren, müssen Sie den SSH-Schlüssel für den Benutzer freigeben. Alternativ können Sie mit EC2 Instance Connect Benutzern Zugriff erteilen, ohne SSH-Schlüssel freigeben und verwalten zu müssen. Weitere Informationen finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance mit EC2 Instance Connect.

Erstellen eines Benutzers

Erstellen Sie zuerst den Benutzer und fügen Sie dann den öffentlichen SSH-Schlüssel hinzu, der es dem Benutzer ermöglicht, eine Verbindung mit der Instance herzustellen und sich bei ihr anzumelden.

So erstellen Sie einen Benutzer

1. Erstellen Sie ein neues Schlüsselpaar. Sie müssen die `.pem`-Datei dem Benutzer bereitstellen, für den Sie den Benutzer erstellen. Er muss diese Datei verwenden, um eine Verbindung mit der Instance herzustellen.
2. Rufen Sie den öffentlichen Schlüssel aus dem Schlüsselpaar ab, das Sie im vorherigen Schritt erstellt haben.

   ```
   $ C:\>  ssh-keygen -y -f /path_to_key_pair/key-pair-name.pem
   ```

   Der Befehl gibt den öffentlichen Schlüssel zurück, wie im folgenden Beispiel gezeigt.

   ```
   ssh-rsa
    AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6Vhz2ItxCih
   +PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/
   d6RJhJOI0iBXrlsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/
   i8SeJtjnV3iAoG/cQk+0FzZqaeJAAHco
   +CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi
   +z7wB3RbBQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
   ```

3. Stellen Sie eine Verbindung zur Instance her.
4. Verwenden Sie den adduser-Befehl, um den Benutzer zu erstellen und ihn dem System hinzuzufügen (mit einem Eintrag in der `/etc/passwd`-Datei). Der Befehl erstellt außerdem eine Gruppe und ein Basisverzeichnis für den Benutzer. In diesem Beispiel lautet der Benutzer *`newuser`*.

   - Amazon Linux und Amazon Linux 2

     Bei Amazon Linux und Amazon Linux 2 wird der Benutzer standardmäßig mit deaktivierter Kennwortauthentifizierung erstellt.

     ```
     [ec2-user ~]$ sudo adduser newuser
     ```

   - Ubuntu

     Schließen Sie den `--disabled-password`-Parameter ein, um den Benutzer mit deaktivierter Kennwortauthentifizierung zu erstellen.

     ```
     [ubuntu ~]$ sudo adduser newuser --disabled-password
     ```

5. Wechseln Sie zum neuen Benutzer, damit das Verzeichnis und die Datei, die Sie erstellen, die richtigen Eigentumsrechte erhalten.

   ```
   [ec2-user ~]$ sudo su - newuser
   ```

   Die Eingabeaufforderung wechselt von `ec2-user` zu *`newuser`*, um anzuzeigen, dass Sie die Shell-Sitzung auf den neuen Benutzer umgestellt haben.
6. Fügen Sie dem Benutzer den öffentlichen SSH-Schlüssel hinzu. Erstellen Sie zuerst im Stammverzeichnis des Benutzers ein Verzeichnis für die SSH-Schlüsseldatei. Erstellen Sie dann die Schlüsseldatei und fügen Sie abschließend den öffentlichen Schlüssel in die Schlüsseldatei ein, wie in den folgenden Unterschritten beschrieben.

   a. Erstellen Sie ein Verzeichnis `.ssh` im Stammverzeichnis von *`newuser`* und ändern Sie seine Dateiberechtigungen in `700` (nur der Eigentümer kann das Verzeichnis öffnen, lesen oder darin schreiben).

      ```
      [newuser ~]$ mkdir .ssh
      ```

```
[newuser ~]$ chmod 700 .ssh
```

> **Important**
>
> Ohne diese Dateiberechtigungen kann sich der Benutzer nicht anmelden.

b. Erstellen Sie eine Datei namens `authorized_keys` im Verzeichnis `.ssh` und ändern Sie seine Dateiberechtigungen in `600` (nur der Eigentümer kann diese Datei lesen oder darin schreiben).

```
[newuser ~]$ touch .ssh/authorized_keys
```

```
[newuser ~]$ chmod 600 .ssh/authorized_keys
```

> **Important**
>
> Ohne diese Dateiberechtigungen kann sich der Benutzer nicht anmelden.

c. Öffnen Sie die Datei `authorized_keys` mit einem Texteditor Ihrer Wahl, z. B. vim oder nano.

```
[newuser ~]$ nano .ssh/authorized_keys
```

Fügen Sie den öffentlichen Schlüssel, den Sie in Schritt 2 abgerufen haben, in die Datei ein, und speichern Sie die Änderungen.

> **Important**
>
> Stellen Sie sicher, dass Sie den öffentlichen Schlüssel in eine durchgehende Zeile einfügen. Der öffentliche Schlüssel darf nicht auf mehrere Zeilen aufgeteilt werden.

Der Benutzer sollte sich nun bei dem *`newuser`*-Benutzer auf Ihrer Instance mit dem privaten Schlüssel anmelden können, der dem öffentlichen Schlüssel entspricht, den Sie der `authorized_keys`-Datei hinzugefügt haben. Weitere Informationen zu den verschiedenen

Methoden zum herstellen einer Verbindung mit einer Linux-Instance finden Sie unter Herstellen einer Verbindung zur Linux-Instance.

Entfernen eines Benutzers

Wenn ein Benutzer nicht mehr benötigt wird, können Sie ihn entfernen, damit er nicht mehr verwendet werden kann.

Verwenden Sie den userdel-Befehl, um den Benutzer aus dem System zu entfernen. Wenn Sie den Parameter `-r` angeben, werden das Stammverzeichnis und die Mail Spool gelöscht. Lassen Sie den Parameter `-r` weg, um das Stammverzeichnis und die Mail Spool nicht zu löschen.

```
[ec2-user ~]$ sudo userdel -r olduser
```

Legen Sie das Windows-Administratorkennwort für Ihre Instance fest

Wenn Sie eine Verbindung zu einer Windows-Instance herstellen, müssen Sie ein Benutzerkonto und Passwort angeben, das für den Zugriff auf die Instance berechtigt ist. Bei der ersten Anmeldung bei einer Instance werden Sie aufgefordert, das Administratorkonto und das Standard-Passwort anzugeben.

Bei AWS Windows-AMIs für Windows Server 2012 R2 und früher Konfigurieren Sie eine Windows-Instanz mithilfe des EC2Config-Dienstes (Legacy) generiert der das Standardkennwort. Konfigurieren einer Windows-Instance mithilfe von EC2LaunchGeneriert bei AWS Windows-AMIs für Windows Server 2016 und 2019 das Standardkennwort. Konfigurieren einer Windows-Instance mithilfe von EC2Launch v2Generiert bei AWS Windows-AMIs für Windows Server 2022 und höher das Standardkennwort.

> **Note**
>
> Bei Windows Server 2016 und höher ist `Password never expires` für den lokalen Administrator deaktiviert. Bei Windows Server 2012 R2 und früher ist `Password never expires` für den lokalen Administrator aktiviert.

Ändern des Administratorpassworts nach dem Verbinden

Bei der ersten Anmeldung bei einer Instance empfehlen wir Ihnen, den Standardwert des Administratorpassworts zu ändern. Mithilfe des folgenden Verfahrens können Sie das Administratorpasswort für Ihre Windows-Instance ändern.

> **Important**
>
> Speichern Sie das neue Passwort an einem sicheren Ort. Sie können das neue Passwort über die Amazon EC2-Konsole nicht abrufen. Sie können nur das Standard-Passwort über die Konsole abrufen. Wenn Sie versuchen, sich nach der Änderung des Passworts mithilfe des Standard-Passworts mit der Instance zu verbinden, erhalten Sie einen Fehler "Ihre Anmeldeinformationen sind nicht korrekt".

Um das lokale Administratorpasswort zu ändern

1. Stellen Sie eine Verbindung mit der Instance her und öffnen Sie ein Eingabeaufforderungsfenster.
2. Führen Sie den folgenden Befehl aus. Wenn Ihr neues Passwort Sonderzeichen enthält, muss das Passwort zwischen doppelten Anführungszeichen stehen:

   ```
   net user Administrator "new_password"
   ```
3. Speichern Sie das neue Passwort an einem sicheren Ort.

Ändern eines verlorenen oder abgelaufenen Passworts

Wenn Sie Ihr Passwort verlieren oder es abläuft, können Sie ein neues Passwort generieren. Informationen zu den Verfahren zum Zurücksetzen des Passworts erhalten Sie unter Zurücksetzen eines Windows-Administratorpassworts, das verloren oder abgelaufen ist.

Gerätetreiber für Ihre Amazon EC2 EC2-Instance verwalten

Einige Treiber sind auf dem EC2-AMI, von dem aus Sie starten, nicht vorinstalliert. Andere benötigen möglicherweise Updates, um die erweiterten Funktionen nutzen zu können. Die folgenden Themen behandeln Installation, Updates und Konfiguration für einige der Gerätetreiber, die an Ihre EC2-Instances angehängt sind.

Inhalt

Installieren Sie NVIDIA-Treiber auf Ihrer Amazon EC2 EC2-Instance

Auf Instances mit einer angeschlossenen NVIDIA-GPU, z. B. P3- oder G4dn-Instances, muss der entsprechende NVIDIA-Treiber installiert sein. Abhängig vom Instance-Typ können Sie entweder einen öffentlichen NVIDIA-Treiber herunterladen, einen Treiber von Amazon S3 herunterladen, der nur für AWS -Kunden verfügbar ist oder ein AMI verwenden, auf dem der Treiber vorinstalliert ist.

Informationen zur Installation von AMD-Treibern auf einer Instance mit einer angeschlossenen AMD-GPU, z. B. einer G4ad-Instance, finden Sie unter. Installieren Sie AMD-Treiber Informationen zur Installation von NVIDIA-Treibern finden Sie unter. Installieren Sie NVIDIA-Treiber

Inhalt

Typen von NVIDIA-Treibern

Im Folgenden finden Sie die wichtigsten Typen von NVIDIA-Treibern, die mit GPU-basierten Instances verwendet werden können.

Tesla-Treiber

Diese Treiber sind in erster Linie für Datenverarbeitungs-Workloads gedacht, die GPUs für Rechenaufgaben wie parallelisierte Gleitkommaberechnungen für Machine Learning und schnelle Fourier-Transformationen für High Performance Computing-Anwendungen verwenden.

GRID-Treiber

Diese Treiber wurden dafür zertifiziert, dass sie optimale Leistung für professionelle Visualisierungsanwendungen bieten, die Inhalte wie 3D-Modelle oder hochauflösende Videos rendern. Sie können GRID-Treiber zum Support zweier Modi konfigurieren. Quadro Virtual Workstations bieten pro GPU Zugriff auf vier 4K-Displays. GRID vApps bieten RDSH-App-Hosting-Funktionen.

Gaming-Treiber

Diese Treiber enthalten Optimierungen für Spiele und werden häufig aktualisiert, um Leistungsverbesserungen zu bieten. Sie unterstützen ein einzelnes 4K-Display pro GPU.

Konfigurierter Modus

Unter Windows sind die Tesla-Treiber so konfiguriert, dass sie im TCC-Modus (Tesla Compute Cluster) ausgeführt werden. Die GRID- und Gaming-Treiber sind für die Ausführung im WDDM-Modus (Windows Display Driver Model) konfiguriert. Im TCC-Modus ist die Karte für Datenverarbeitungs-Workloads bestimmt. Im WDDM-Modus unterstützt die Karte sowohl Datenverarbeitungs- als auch Grafik-Workloads.

NVIDIA-Steuerfeld

Das NVIDIA-Steuerfeld wird mit GRID und Gaming-Treibern unterstützt. Es wird nicht mit Tesla-Treibern unterstützt.

Unterstützte APIs für Tesla-, GRID- und Gaming-Treiber

- OpenCL, OpenGL und Vulkan
- NVIDIA CUDA und verwandte Bibliotheken (z. B. cuDNN, TensorRT, nvJPEG und cuBLAS)
- NVENC für Videocodierung und NVDEC für Videodecodierung
- Nur Windows-APIs: DirectX, Direct2D, DirectX-Videobeschleunigung, DirectX Raytracing

Verfügbare Treiber nach Instance-Typ

In der folgenden Tabelle werden die unterstützten NVIDIA-Treiber für jeden GPU-Instance-Typ zusammengefasst.

Instance-Typ	Tesla-Treiber	GRID-Treiber	Gaming-Treiber
G3	Ja	Ja	Nein
G4dn	Ja	Ja	Ja
G5	Ja	Ja	Ja
G5g	Ja[1]	Nein	Nein
G6	Ja	Ja	Nein
Gr 6	Ja	Ja	Nein
P2	Ja	Nein	Nein
P3	Ja	Nein	Nein
P4d	Ja	Nein	Nein
P4de	Ja	Nein	Nein

[1] Dieser Tesla-Treiber unterstützt auch optimierte Grafikanwendungen, die für die ARM64-Plattform spezifisch sind.

[2] Nur mit Marketplace-AMIs.

Installationsoptionen

Verwenden Sie eine der folgenden Optionen, um die für Ihre GPU-Instance erforderlichen NVIDIA-Treiber abzurufen.

Optionen

- Option 1: AMIs mit installierten NVIDIA-Treibern
- Option 2: Öffentliche NVIDIA-Treiber

- Option 3: GRID-Treiber (G6-, Gr6-, G5-, G4dn- und G3-Instanzen)
- Option 4: NVIDIA-Gaming-Treiber (G5- und G4dn-Instances)

Option 1: AMIs mit installierten NVIDIA-Treibern

AWS und NVIDIA bieten verschiedene Amazon Machine Images (AMI) an, auf denen die NVIDIA-Treiber installiert sind.

- Marketplace-Angebote mit dem Tesla-Treiber
- Marketplace-Angebote mit dem GRID-Treiber
- Marketplace-Angebote mit dem Gaming-Treiber

Um die Überlegungen zu überprüfen, die von Ihrer Betriebssystemplattform (OS) abhängen, wählen Sie die Registerkarte, die für Ihr AMI gilt.

Linux

Um die mit einem dieser AMIs installierte Treiberversion zu aktualisieren, müssen Sie die NVIDIA-Pakete von Ihrer Instance deinstallieren, um Versionskonflikte zu vermeiden. Verwenden Sie den folgenden Befehl, um die NVIDIA-Pakete zu deinstallieren:

```
[ec2-user ~]$ sudo yum erase nvidia cuda
```

Das CUDA-Toolkit-Paket weist Abhängigkeiten zu den NVIDIA-Treibern auf. Durch die Deinstallation der NVIDIA-Pakete wird das CUDA-Toolkit gelöscht. Sie müssen das CUDA-Toolkit nach der Installation des NVIDIA-Treibers erneut installieren.

Windows

Wenn Sie mit einem der AWS Marketplace Angebote ein benutzerdefiniertes Windows-AMI erstellen, muss es sich bei dem AMI um ein standardisiertes Image handeln, das mit Windows Sysprep erstellt wurde, um sicherzustellen, dass der GRID-Treiber funktioniert. Weitere Informationen finden Sie unter Erstellen Sie ein AMI mit Windows Sysprep.

Option 2: Öffentliche NVIDIA-Treiber

Die von angebotenen Optionen werden mit der erforderlichen Lizenz für den Treiber AWS geliefert. Alternativ können Sie die öffentlichen Treiber installieren und Ihre eigene Lizenz verwenden. Um

einen öffentlichen Treiber zu installieren, laden Sie ihn wie hier beschrieben von der NVIDIA-Website herunter.

Alternativ können Sie AWS anstelle der öffentlichen Treiber die von angebotenen Optionen verwenden. Um einen GRID-Treiber auf einer P3-Instance zu verwenden, verwenden Sie die AWS Marketplace AMIs wie in Option 1 beschrieben. Um einen GRID-Treiber auf einer G6-, Gr6-, G5-, G4dn- oder G3-Instance zu verwenden, verwenden Sie die AWS Marketplace AMIs wie in Option 1 beschrieben oder installieren Sie die NVIDIA-Treiber von, wie unter beschrieben. AWS Option 3: GRID-Treiber (G6-, Gr6-, G5-, G4dn- und G3-Instanzen)

So laden Sie einen öffentlichen NVIDIA-Treiber herunter:

Melden Sie sich bei Ihrer Instance an und laden Sie den 64-Bit-NVIDIA-Treiber, der für den Instance-Typ geeignet ist, von http://www.nvidia.com/Download/Find.aspx herunter. Verwenden Sie für Produkttyp Produktserie und Produkt die Optionen in der folgenden Tabelle.

Instance	Produkttyp	Produktserie	Produkt
G3	Tesla	M-Klasse	M60
G4dn	Tesla	T-Series	T4
G5[1]	Tesla	A-Serie	A10
G5g[2]	Tesla	T-Series	NVIDIA T4G
G6 [3]	Tesla	L-Serie	L4
Gr6 [3]	Tesla	L-Serie	L4
P2	Tesla	K-Serie	K80
P3	Tesla	V-Serie	V100
P4d	Tesla	A-Serie	A100
P4de	Tesla	A-Serie	A100
P 54	Tesla	H-Serie	H100

[1] G5-Instances erfordern die Treiberversion 470.00 oder höher.

[2] G5g-Instances erfordern die Treiberversion 470.82.01 oder höher. Das Betriebssystem ist Linux aarch64.

[3] G6- und Gr6-Instanzen benötigen die Treiberversion 525.0 oder höher.

Für [4] P5-Instanzen ist die Treiberversion 530 oder höher erforderlich.

Informationen zur Installation des NVIDIA-Treibers auf Linux-Betriebssystemen finden Sie in der Schnellstartanleitung zur NVIDIA-Treiberinstallation.

Gehen Sie wie folgt vor, um den NVIDIA-Treiber unter Windows zu installieren:

1. Öffnen Sie das Verzeichnis, in das Sie den Treiber heruntergeladen haben, und starten Sie die Installationsdatei. Befolgen Sie die Anweisungen, um den Treiber zu installieren, und starten Sie die Instance neu, wenn Sie dazu aufgefordert werden.
2. Deaktivieren Sie im Geräte-Manager den Displayadapter mit dem Namen Microsoft Basic Display Adapter, der mit einem Warnsymbol gekennzeichnet ist. Installieren Sie die folgenden Windows-Features: Media Foundation und Quality Windows Audio Video Experience.

   > **Important**
   >
   > Deaktivieren Sie nicht den Displayadapter mit dem Namen Microsoft Remote Display Adapter. Wenn der Microsoft Remote Display Adapter deaktiviert ist, wird Ihre Verbindung möglicherweise unterbrochen und Versuche, nach dem Neustart eine Verbindung zur Instance herzustellen, schlagen möglicherweise fehl.

3. Prüfen Sie im Geräte-Manager, ob die GPU korrekt funktioniert.
4. Führen Sie die Optimierungsschritte unter Optimieren Sie die GPU-Einstellungen auf Amazon EC2 EC2-Instances aus, um die beste Leistung für Ihre GPU zu erzielen.

Option 3: GRID-Treiber (G6-, Gr6-, G5-, G4dn- und G3-Instanzen)

Diese Downloads stehen nur Kunden zur Verfügung. AWS Durch das Herunterladen erklären Sie sich damit einverstanden, die heruntergeladene Software nur zur Entwicklung von AMIs für die NVIDIA L4-, NVIDIA A10G-, NVIDIA Tesla T4- oder NVIDIA Tesla M60-Hardware zu verwenden, um die Anforderungen der AWS Lösung zu erfüllen, auf die in der NVIDIA GRID Cloud Endbenutzer-Lizenzvereinbarung (EULA) verwiesen wird. Durch die Installation der Software stimmen Sie den

Bedingungen in der Endbenutzer-Lizenzvereinbarung für NVIDIA GRID Cloud zu. Informationen zur Version des NVIDIA GRID-Treibers für Ihr Betriebssystem finden Sie in der NVIDIA® Virtual GPU (vGPU)-Softwaredokumentation auf der NVIDIA-Website.

Überlegungen

- G6- und Gr6-Instances benötigen GRID 17 oder höher.
- G5-Instances erfordern GRID 13.1 oder höher (oder GRID 12.4 oder höher).
- G3-Instances benötigen die AWS bereitgestellte DNS-Auflösung, damit die GRID-Lizenzierung funktioniert.
- IMDSv2 wird nur mit NVIDIA-Treiberversion 14.0 oder höher unterstützt.
- Wenn Sie Ihre Instance für Windows-Instances von einem benutzerdefinierten Windows-AMI aus starten, muss das AMI ein standardisiertes Image sein, das mit Windows Sysprep erstellt wurde, um sicherzustellen, dass der GRID-Treiber funktioniert. Weitere Informationen finden Sie unter Erstellen Sie ein AMI mit Windows Sysprep.
- GRID 17.0 und höher unterstützen Windows Server 2019 nicht.
- GRID 14.2 und höher unterstützen Windows Server 2016 nicht.
- GRID 17.0 und höher wird mit G3-Instanzen nicht unterstützt.

Amazon Linux und Amazon Linux 2

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Herstellen einer Verbindung mit Ihrer Linux-Instance.
2. Installieren Sie die AWS CLI auf Ihrer Linux-Instanz und konfigurieren Sie Standardanmeldedaten. Weitere Informationen finden Sie unter Installieren der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.

   > **Important**
   >
   > Ihrem Benutzer oder Ihrer Rolle müssen die Berechtigungen erteilt worden sein, die die ReadOnlyAmazonS3-Zugriffsrichtlinie enthalten. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonS3 ReadOnly Access im Amazon Simple Storage Service-Benutzerhandbuch.

3. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install gcc make
```

4. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

5. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

6. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
7. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

8. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

9. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

10. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Zum Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Wenn Sie Amazon Linux 2 mit Kernelversion 5.10 verwenden, installieren Sie den GRID-Treiber mithilfe des folgenden Befehls.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

11. Vergewissern Sie sich, dass der Treiber funktioniert. In der Ausgabe des folgenden Befehls werden die installierte Version des NVIDIA-Treibers und Informationen über die GPUs angezeigt.

```
[ec2-user ~]$ nvidia-smi -q | head
```

12. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

14. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 EC2-GPU-basierten Instances aus.

CentOS 7 und Red Hat Enterprise Linux 7

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

   ```
   [ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
   ```

6. Deaktivieren Sie den Open-Source-Treiber `nouveau` für NVIDIA-Grafikkarten.

   a. Fügen Sie der Negativliste in der Datei `nouveau` den Eintrag `/etc/modprobe.d/blacklist.conf` hinzu. Kopieren Sie den folgenden Codeblock und fügen Sie ihn in ein Terminalfenster ein.

   ```
   [ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   b. Bearbeiten Sie die Datei `/etc/default/grub` und fügen Sie folgende Zeile hinzu.

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   c. Erstellen Sie die neue Grub-Konfiguration.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

8. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

9. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

10. Vergewissern Sie sich, dass der Treiber funktioniert. In der Ausgabe des folgenden Befehls werden die installierte Version des NVIDIA-Treibers und Informationen über die GPUs angezeigt.

```
[ec2-user ~]$ nvidia-smi -q | head
```

11. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

12. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

13. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 EC2-GPU-basierten Instances aus.

    c. Installieren Sie das GUI-Desktop-/Workstation-Paket.

    ```
    [ec2-user ~]$ sudo yum groupinstall -y "Server with GUI"
    ```

CentOS Stream 8 und Red Hat Enterprise Linux 8

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

   ```
   [ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel
    kernel-devel-$(uname -r)
   ```

6. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

   Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

   Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

9. Vergewissern Sie sich, dass der Treiber funktioniert. In der Ausgabe des folgenden Befehls werden die installierte Version des NVIDIA-Treibers und Informationen über die GPUs angezeigt.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

12. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 EC2-GPU-basierten Instances aus.

    c. Installieren Sie das GUI-Workstation-Paket.

```
[ec2-user ~]$ sudo dnf groupinstall -y workstation
```

Rocky Linux 8

So installieren Sie den NVIDIA GRID-Treiber auf einer Linux-Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

```
[ec2-user ~]$ sudo dnf install -y make gcc elfutils-libelf-devel libglvnd-devel
 kernel-devel-$(uname -r)
```

6. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
```

Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

```
[ec2-user ~]$ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
```

7. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

```
[ec2-user ~]$ chmod +x NVIDIA-Linux-x86_64*.run
```

8. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
[ec2-user ~]$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

9. Vergewissern Sie sich, dass der Treiber funktioniert. In der Ausgabe des folgenden Befehls werden die installierte Version des NVIDIA-Treibers und Informationen über die GPUs angezeigt.

```
[ec2-user ~]$ nvidia-smi -q | head
```

10. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

11. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

12. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 EC2-GPU-basierten Instances aus.

Ubuntu und Debian

So installieren Sie den NVIDIA-GRID-Treiber auf Ihrer Instance:

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
$ sudo apt-get update -y
```

3. (Ubuntu) Führen Sie ein Upgrade des `linux-aws`-Pakets durch, um die aktuelle Version zu erhalten.

```
$ sudo apt-get upgrade -y linux-aws
```

   (Debian) Führen Sie ein Upgrade des Pakets durch, um die aktuelle Version zu erhalten.

```
$ sudo apt-get upgrade -y
```

4. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
$ sudo reboot
```

5. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
6. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

7. Deaktivieren Sie den Open-Source-Treiber nouveau für NVIDIA-Grafikkarten.

   a. Fügen Sie der Negativliste in der Datei nouveau den Eintrag /etc/modprobe.d/blacklist.conf hinzu. Kopieren Sie den folgenden Codeblock und fügen Sie ihn in ein Terminalfenster ein.

   ```
   $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
   blacklist vga16fb
   blacklist nouveau
   blacklist rivafb
   blacklist nvidiafb
   blacklist rivatv
   EOF
   ```

   b. Bearbeiten Sie die Datei /etc/default/grub und fügen Sie folgende Zeile hinzu.

   ```
   GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
   ```

   c. Erstellen Sie die neue Grub-Konfiguration.

   ```
   $ sudo update-grub
   ```

8. Laden Sie das GRID-Treiberinstallationsprogramm anhand des folgenden Befehls herunter:

   ```
   $ aws s3 cp --recursive s3://ec2-linux-nvidia-drivers/latest/ .
   ```

   Mehrere Versionen des GRID-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen.

   ```
   $ aws s3 ls --recursive s3://ec2-linux-nvidia-drivers/
   ```

9. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiberinstallationsprogramms hinzu.

   ```
   $ chmod +x NVIDIA-Linux-x86_64*.run
   ```

10. Führen Sie das Selbstinstallationsskript wie folgt aus, um den heruntergeladenen GRID-Treiber zu installieren. Beispiel:

```
$ sudo /bin/sh ./NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

11. Vergewissern Sie sich, dass der Treiber funktioniert. In der Ausgabe des folgenden Befehls werden die installierte Version des NVIDIA-Treibers und Informationen über die GPUs angezeigt.

```
$ nvidia-smi -q | head
```

12. Wenn Sie die NVIDIA-vGPU-Software Version 14.x oder höher auf den G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

13. Starten Sie die Instance neu.

```
$ sudo reboot
```

14. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

    a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

    b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 EC2-GPU-basierten Instances aus.

    c. Installieren Sie das GUI-Desktop-/Workstation-Paket.

```
$ sudo apt-get install -y lightdm ubuntu-desktop
```

Windows-Betriebssysteme

So installieren Sie den NVIDIA GRID-Treiber auf einer Windows-Instance

1. Connect zu Ihrer Windows-Instanz her und öffnen Sie ein PowerShell Fenster.
2. Konfigurieren Sie Standardanmeldedaten für die AWS Tools for Windows PowerShell auf Ihrer Windows-Instanz. Weitere Informationen finden Sie unter Erste Schritte in AWS Tools for Windows PowerShell im AWS Tools for Windows PowerShell -Benutzerhandbuch.

   > **Important**
   >
   > Ihrem Benutzer oder Ihrer Rolle müssen die Berechtigungen erteilt worden sein, die die AmazonS3 ReadOnly Access-Richtlinie enthalten. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonS3 ReadOnly Access im Amazon Simple Storage Service-Benutzerhandbuch.

3. Laden Sie die Treiber und die NVIDIA GRID Cloud-Endbenutzer-Lizenzvereinbarung mit den folgenden PowerShell Befehlen von Amazon S3 auf Ihren Desktop herunter.

```
$Bucket = "ec2-windows-nvidia-drivers"
$KeyPrefix = "latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

   Mehrere Versionen des NVIDIA GRID-Treibers werden in diesem Bucket gespeichert. Sie können alle verfügbaren Windows-Versionen im Bucket herunterladen, indem Sie die `-KeyPrefix $KeyPrefix`-Option entfernen. Informationen zur Version des NVIDIA GRID-Treibers für Ihr Betriebssystem finden Sie in der NVIDIA® Virtual GPU (vGPU)-Softwaredokumentation auf der NVIDIA-Website.

Ab GRID-Version 11.0 können Sie die Treiber unter `latest` für G3- und für G4dn-Instances verwenden. Wir werden keine Versionen nach 11.0 zu `g4/latest` hinzufügen, aber die Version 11.0 und die früheren für G4dn spezifischen Versionen unter `g4/latest` beibehalten.

G5-Instances erfordern GRID 13.1 oder höher (oder GRID 12.4 oder höher).

4. Navigieren Sie zu Ihrem Desktop und doppelklicken Sie auf die Installationsdatei, um sie auszuführen (wählen Sie die Treiberversion für das Betriebssystem Ihrer Instance aus). Befolgen Sie die Anweisungen, um den Treiber zu installieren, und starten Sie die Instance neu, wenn Sie dazu aufgefordert werden. Sie können prüfen, ob die GPU richtig funktioniert, indem Sie den Geräte-Manager verwenden.
5. (Optional) Verwenden Sie den folgenden Befehl, um die Lizenzierungsseite in der Systemsteuerung zu deaktivieren und damit zu verhindern, dass Benutzer versehentlich den Produkttyp ändern (NVIDIA GRID Virtual Workstation ist standardmäßig aktiviert). Weitere Informationen finden Sie im GRID-Lizenzierungs-Benutzerhandbuch.

   PowerShell

   Führen Sie die folgenden PowerShell Befehle aus, um den Registrierungswert für die Deaktivierung der Lizenzierungsseite im Kontrollpanel zu erstellen. Die AMIs AWS Tools for PowerShell in AWS Windows verwenden standardmäßig die 32-Bit-Version, und dieser Befehl schlägt fehl. Verwenden Sie stattdessen die 64-Bit-Version von, die im Betriebssystem PowerShell enthalten ist.

   ```
   New-Item -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name GridLicensing
   New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" -
   Name "NvCplDisableManageLicensePage" -PropertyType "DWord" -Value "1"
   ```

   Eingabeaufforderung

   Führen Sie den folgenden Registry-Befehl aus, um den Registrierungswert zum Deaktivieren der Lizenzierungsseite in der Systemsteuerung zu erstellen. Sie können es über das Befehlszeilenfenster oder eine 64-Bit-Version von ausführenPowerShell.

   ```
   reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global\GridLicensing" /v
    NvCplDisableManageLicensePage /t REG_DWORD /d 1
   ```
6. (Optional) Je nach Anwendungsfall können Sie die folgenden optionalen Schritte ausführen. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diese Schritte nicht aus.

a. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

b. Der NVIDIA Quadro Virtual Workstation-Modus ist standardmäßig aktiviert. Um die Hosting-Funktionen von GRID Virtual Applications for RDSH Application zu aktivieren, führen Sie die Aktivierungsschritte für GRID Virtual Application in Aktivieren Sie virtuelle NVIDIA GRID-Anwendungen auf Ihren Amazon EC2 EC2-GPU-basierten Instances aus.

Option 4: NVIDIA-Gaming-Treiber (G5- und G4dn-Instances)

Diese Treiber sind nur für AWS Kunden verfügbar. Durch das Herunterladen erklären Sie sich damit einverstanden, die heruntergeladene Software nur zur Entwicklung von AMIs für die NVIDIA A10G- und NVIDIA Tesla T4-Hardware zu verwenden. Durch die Installation der Software stimmen Sie den Bedingungen in der Endbenutzer-Lizenzvereinbarung für NVIDIA GRID Cloud zu.

Überlegungen

- G3-Instances benötigen die AWS bereitgestellte DNS-Auflösung, damit die GRID-Lizenzierung funktioniert.
- IMDSv2 wird nur mit NVIDIA-Treiberversion 495.x oder höher unterstützt.

Amazon Linux und Amazon Linux 2

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance.
2. Installieren Sie die AWS CLI auf Ihrer Linux-Instanz und konfigurieren Sie Standardanmeldedaten. Weitere Informationen finden Sie unter Installieren der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.

   > **Important**
   >
   > Ihrem Benutzer oder Ihrer Rolle müssen die Berechtigungen erteilt worden sein, die die ReadOnlyAmazonS3-Zugriffsrichtlinie enthalten. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonS3 ReadOnly Access im Amazon Simple Storage Service-Benutzerhandbuch.

3. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

```
[ec2-user ~]$ sudo yum install gcc make
```

4. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

5. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

6. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
7. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

```
[ec2-user ~]$ sudo yum install -y gcc kernel-devel-$(uname -r)
```

8. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
[ec2-user ~]$ unzip latest-driver-name.zip -d nvidia-drivers
```

10. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/NVIDIA-Linux-x86_64*-grid.run
```

11. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo ./nvidia-drivers/NVIDIA-Linux-x86_64*.run
```

> **Note**
>
> Wenn Sie Amazon Linux 2 mit der Kernel-Version 5.10 verwenden, installieren Sie die NVIDIA-Gaming-Treiber mit dem folgenden Befehl.
>
> ```
> [ec2-user ~]$ sudo CC=/usr/bin/gcc10-cc ./NVIDIA-Linux-x86_64*.run
> ```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

12. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.

    - Für Version 460.39 oder höher:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Für Version 440.68 bis 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Für frühere Versionen:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

14. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

15. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

16. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

CentOS 7 und Red Hat Enterprise Linux 7

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

```
[ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
```

6. Deaktivieren Sie den Open-Source-Treiber `nouveau` für NVIDIA-Grafikkarten.

   a. Fügen Sie der Negativliste in der Datei `nouveau` den Eintrag `/etc/modprobe.d/blacklist.conf` hinzu. Kopieren Sie den folgenden Codeblock und fügen Sie ihn in ein Terminalfenster ein.

```
[ec2-user ~]$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

b. Bearbeiten Sie die Datei `/etc/default/grub` und fügen Sie folgende Zeile hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

c. Erstellen Sie die neue Grub-Konfiguration.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

8. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

9. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

10. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

11. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

12. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.
    - Für Version 460.39 oder höher:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Für Version 440.68 bis 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Für frühere Versionen:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

13. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
```

14. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

15. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diesen Schritt nicht aus.

CentOS Stream 8 und Red Hat Enterprise Linux 8

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

   ```
   [ec2-user ~]$ sudo yum update -y
   ```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

   ```
   [ec2-user ~]$ sudo reboot
   ```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

   ```
   [ec2-user ~]$ sudo yum install -y unzip gcc kernel-devel-$(uname -r)
   ```

6. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

   ```
   [ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
   ```

   Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

   ```
   [ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
   ```

7. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

   Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

10. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.

    - Für Version 460.39 oder höher:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
```

    - Für Version 440.68 bis 445.48:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
```

    - Für frühere Versionen:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
[ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
[ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /
etc/modprobe.d/nvidia.conf
```

13. Starten Sie die Instance neu.

```
[ec2-user ~]$ sudo reboot
```

14. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

Rocky Linux 8

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

```
[ec2-user ~]$ sudo yum update -y
```

3. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

```
[ec2-user ~]$ sudo reboot
```

4. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.
5. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

```
[ec2-user ~]$ sudo dnf install -y unzip gcc make elfutils-libelf-devel libglvnd-
devel kernel-devel-$(uname -r)
```

6. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
[ec2-user ~]$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
[ec2-user ~]$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

7. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
[ec2-user ~]$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

8. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
[ec2-user ~]$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

9. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
[ec2-user ~]$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

   Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

10. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
[ec2-user ~]$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

11. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.
    - Für Version 460.39 oder höher:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Für Version 440.68 bis 445.48:

      ```
      [ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Für frühere Versionen:

```
[ec2-user ~]$ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
```

12. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

    ```
    [ec2-user ~]$ sudo touch /etc/modprobe.d/nvidia.conf
    ```

    ```
    [ec2-user ~]$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/modprobe.d/nvidia.conf
    ```

13. Starten Sie die Instance neu.

    ```
    [ec2-user ~]$ sudo reboot
    ```

14. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

Ubuntu und Debian

So installieren Sie den NVIDIA-Gaming-Treiber auf Ihrer Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance. Installieren Sie gcc und make, falls sie noch nicht installiert sind.
2. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

    ```
    $ sudo apt-get update -y
    ```

3. Führen Sie ein Upgrade des `linux-aws`-Pakets durch, um die aktuelle Version zu erhalten.

    ```
    $ sudo apt-get upgrade -y linux-aws
    ```

4. Starten Sie Ihre Instance neu, um die neueste Kernelversion zu laden.

    ```
    $ sudo reboot
    ```

5. Stellen Sie nach dem Neustart eine neue Verbindung zu Ihrer Instance her.

6. Installieren Sie den gcc-Compiler und das Kernel-Header-Paket für die aktuell ausgeführte Kernel-Version.

```
$ sudo apt-get install -y unzip gcc make linux-headers-$(uname -r)
```

7. Deaktivieren Sie den Open-Source-Treiber `nouveau` für NVIDIA-Grafikkarten.

   a. Fügen Sie der Negativliste in der Datei `nouveau` den Eintrag `/etc/modprobe.d/blacklist.conf` hinzu. Kopieren Sie den folgenden Codeblock und fügen Sie ihn in ein Terminalfenster ein.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   b. Bearbeiten Sie die Datei `/etc/default/grub` und fügen Sie folgende Zeile hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   c. Erstellen Sie die neue Grub-Konfiguration.

```
$ sudo update-grub
```

8. Laden Sie das Installationsprogramm für den Gaming-Treiber anhand des folgenden Befehls herunter:

```
$ aws s3 cp --recursive s3://nvidia-gaming/linux/latest/ .
```

   Mehrere Versionen des Gaming-Treibers werden in diesem Bucket gespeichert. Mit dem folgenden Befehl können Sie alle verfügbaren Versionen anzeigen:

```
$ aws s3 ls --recursive s3://nvidia-gaming/linux/
```

9. Extrahieren Sie das Installationsprogramm für den Gaming-Treiber aus dem heruntergeladenen `.zip`-Archiv.

```
$ unzip vGPUSW-*vGaming-Linux-Guest-Drivers.zip -d nvidia-drivers
```

10. Fügen Sie mit dem folgenden Befehl Berechtigungen für die Ausführung des Treiber-Installationsprogramms hinzu:

```
$ chmod +x nvidia-drivers/Linux/NVIDIA-Linux-x86_64*-grid.run
```

11. Führen Sie das Installationsprogramm über den folgenden Befehl aus:

```
$ sudo ./nvidia-drivers/Linux/NVIDIA-Linux-x86_64*.run
```

    Akzeptieren Sie bei Aufforderung die Lizenzvereinbarung und geben Sie nach Bedarf die Installationsoptionen an (Sie können die Standardoptionen akzeptieren).

12. Verwenden Sie den folgenden Befehl zum Erstellen der benötigten Konfigurationsdatei.

```
$ cat << EOF | sudo tee -a /etc/nvidia/gridd.conf
vGamingMarketplace=2
EOF
```

13. Laden Sie die Zertifizierungsdatei mit dem folgenden Befehl herunter und benennen Sie sie um.

    - Für Version 460.39 oder höher:

      ```
      $ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCertLinux_2023_9_22.cert"
      ```

    - Für Version 440.68 bis 445.48:

      ```
      $ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2020_04.cert"
      ```

    - Für frühere Versionen:

      ```
      $ sudo curl -o /etc/nvidia/GridSwCert.txt "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-Archive/GridSwCert-Linux_2019_09.cert"
      ```

14. Wenn Sie NVIDIA-Treiberversion 510.x oder höher für die G4dn-, G5- oder G5g-Instances verwenden, deaktivieren Sie GSP mit den folgenden Befehlen. Weitere Informationen darüber, warum dies erforderlich ist, finden Sie unter NVIDIAs Dokumentation.

```
$ sudo touch /etc/modprobe.d/nvidia.conf
```

```
$ echo "options nvidia NVreg_EnableGpuFirmware=0" | sudo tee --append /etc/
modprobe.d/nvidia.conf
```

15. Starten Sie die Instance neu.

```
$ sudo reboot
```

16. (Optional) Um die Vorteile einer Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diesen Schritt nicht aus.

Windows-Betriebssysteme

Bevor Sie einen NVIDIA-Gaming-Treiber auf Ihrer Instanz installieren, müssen Sie sicherstellen, dass zusätzlich zu den für alle Spieletreiber genannten Überlegungen die folgenden Voraussetzungen erfüllt sind.

- Wenn Sie Ihre Windows-Instance mit einem benutzerdefinierten Windows-AMI starten, muss es sich bei dem AMI um ein standardisiertes Image handeln, das mit Windows Sysprep erstellt wurde, um sicherzustellen, dass der Spieletreiber funktioniert. Weitere Informationen finden Sie unter Erstellen Sie ein AMI mit Windows Sysprep.
- Konfigurieren Sie Standardanmeldedaten für die AWS Tools for Windows PowerShell auf Ihrer Windows-Instance. Weitere Informationen finden Sie unter Erste Schritte in AWS Tools for Windows PowerShell im AWS Tools for Windows PowerShell -Benutzerhandbuch.
- Ihren Benutzern oder Rollen müssen die Berechtigungen erteilt worden sein, die die AmazonS3 ReadOnly Access-Richtlinie enthalten. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonS3 ReadOnly Access im Amazon Simple Storage Service-Benutzerhandbuch.

So installieren Sie den NVIDIA-Gaming-Treiber auf einer Windows-Instance

1. Connect zu Ihrer Windows-Instanz her und öffnen Sie ein PowerShell Fenster.
2. Laden Sie den Gaming-Treiber mit den folgenden PowerShell Befehlen herunter und installieren Sie ihn.

```
$Bucket = "nvidia-gaming"
$KeyPrefix = "windows/latest"
$LocalPath = "$home\Desktop\NVIDIA"
$Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
foreach ($Object in $Objects) {
$LocalFileName = $Object.Key
if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
    $LocalFilePath = Join-Path $LocalPath $LocalFileName
    Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
Region us-east-1
}
}
```

Mehrere Versionen des NVIDIA GRID-Treibers werden in diesem S3-Bucket gespeichert. Sie können alle verfügbaren Versionen im Bucket herunterladen, wenn Sie den Wert der `$KeyPrefix`-Variablen von „windows/latest“ auf „windows“ ändern.

3. Navigieren Sie zu Ihrem Desktop und doppelklicken Sie auf die Installationsdatei, um sie auszuführen (wählen Sie die Treiberversion für das Betriebssystem Ihrer Instance aus). Befolgen Sie die Anweisungen, um den Treiber zu installieren, und starten Sie die Instance neu, wenn Sie dazu aufgefordert werden. Sie können prüfen, ob die GPU richtig funktioniert, indem Sie den Geräte-Manager verwenden.
4. Verwenden Sie eine der folgenden Methoden, um den Treiber zu registrieren.

   Version 527.27 or above

   Erstellen Sie den folgenden Registrierungsschlüssel mit der 64-Bit-Version von PowerShell oder im Befehlszeilenfenster.

   Schlüssel: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global`

   Name: vGamingMarketplace

   Typ: DWord

   Wert: 2

   PowerShell

Führen Sie den folgenden PowerShell Befehl aus, um diesen Registrierungswert zu erstellen. Die AMIs AWS Tools for PowerShell in AWS Windows verwenden standardmäßig die 32-Bit-Version, und dieser Befehl schlägt fehl. Verwenden Sie stattdessen die 64-Bit-Version von, die im Betriebssystem PowerShell enthalten ist.

```
New-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global"
 -Name "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Eingabeaufforderung

Führen Sie den folgenden Registrierungsbefehl aus, um diesen Registrierungswert zu erstellen. Sie können es über das Befehlszeilenfenster oder eine 64-Bit-Version von ausführen PowerShell.

```
reg add "HKLM\SYSTEM\CurrentControlSet\Services\nvlddmkm\Global" /v
 vGamingMarketplace /t REG_DWORD /d 2
```

Earlier versions

Erstellen Sie den folgenden Registrierungsschlüssel mit der 64-Bit-Version von PowerShell oder dem Befehlszeilenfenster.

Schlüssel: `HKEY_LOCAL_MACHINE\SOFTWARE\NVIDIA Corporation\Global`

Name: vGamingMarketplace

Typ: DWord

Wert: 2

PowerShell

Führen Sie den folgenden PowerShell Befehl aus, um diesen Registrierungswert zu erstellen. Die AMIs AWS Tools for PowerShell in AWS Windows verwenden standardmäßig die 32-Bit-Version, und dieser Befehl schlägt fehl. Verwenden Sie stattdessen die 64-Bit-Version von, die im Betriebssystem PowerShell enthalten ist.

```
New-ItemProperty -Path "HKLM:\SOFTWARE\NVIDIA Corporation\Global" -Name
 "vGamingMarketplace" -PropertyType "DWord" -Value "2"
```

Eingabeaufforderung

Führen Sie den folgenden Registrierungsbefehl aus, um diesen Registrierungsschlüssel im Eingabeaufforderungsfenster zu erstellen. Sie können diesen Befehl auch in der 64-Bit-Version von verwendenPowerShell.

```
reg add "HKLM\SOFTWARE\NVIDIA Corporation\Global" /v vGamingMarketplace /t
 REG_DWORD /d 2
```

5. Führen Sie den folgenden Befehl in aus PowerShell. Dadurch wird die Zertifizierungsdatei heruntergeladen, die Datei in `GridSwCert.txt` umbenannt und in den Ordner „Öffentliche Dokumente“ auf dem Systemlaufwerk verschoben. In der Regel lautet der Ordnerpfad `C:\Users\Public\Documents`.

   - Für Version 461.40 oder höher:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCertWindows_2023_9_22.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Für Version 445.87:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCert-Windows_2020_04.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   - Für frühere Versionen:

     ```
     Invoke-WebRequest -Uri "https://nvidia-gaming.s3.amazonaws.com/GridSwCert-
     Archive/GridSwCert-Windows_2019_09.cert" -OutFile "$Env:PUBLIC\Documents
     \GridSwCert.txt"
     ```

   > **Note**
   >
   > Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:

```
[Net.ServicePointManager]::SecurityProtocol =
 [Net.SecurityProtocolType]::Tls12
```

6. Starten Sie Ihre Instance neu.
7. Verifizieren Sie die NVIDIA Gaming-Lizenz mit dem folgenden Befehl:

```
C:\Windows\System32\DriverStore\FileRepository\nv_dispswi.inf_*\nvidia-smi.exe -q
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen.

```
vGPU Software Licensed Product
Product Name              : NVIDIA Cloud Gaming
License Status            : Licensed (Expiry: N/A)
```

8. (Optional) Um die Vorteile der Einzelanzeige mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein. Wenn Sie diese Funktionalität nicht benötigen, führen Sie diesen Schritt nicht aus.

Installieren einer zusätzlichen Version von CUDA

Nachdem Sie einen NVIDIA-Grafiktreiber auf Ihrer Instance installiert haben, können Sie eine andere Version von CUDA als die mit dem Grafiktreiber gebündelte Version installieren. Das folgende Verfahren veranschaulicht, wie mehrere CUDA-Versionen für die Instance konfiguriert werden.

Installieren Sie das CUDA-Toolkit unter Linux

Gehen Sie wie folgt vor, um das CUDA-Toolkit unter Linux zu installieren:

1. Herstellen einer Verbindung mit Ihrer Linux-Instance.
2. Öffnen Sie die NVIDIA-Website und wählen Sie die gewünschte CUDA-Version aus.
3. Wählen Sie die Architektur, Verteilung und Version für das Betriebssystem auf Ihrer Instance aus. Wählen Sie unter Installationstyp die Option runfile (local) (runfile (lokal))aus.
4. Folgen Sie den Anweisungen, um das Installationsskript herunterzuladen.
5. Fügen Sie dem Installationsskript, das Sie heruntergeladen haben, Ausführungsberechtigungen mit dem folgenden Befehl hinzu.

```
[ec2-user ~]$ chmod +x downloaded_installer_file
```

6. Führen Sie das Installationsskript wie folgt aus, um das CUDA-Toolkit zu installieren und dem Toolkit-Pfad die CUDA-Versionsnummer hinzuzufügen.

```
[ec2-user ~]$ sudo sh downloaded_installer_file --silent --override --toolkit --
samples --toolkitpath=/usr/local/cuda-version --samplespath=/usr/local/cuda --no-
opengl-libs
```

7. (Optional) Legen Sie die CUDA-Standardversion wie folgt fest.

```
[ec2-user ~]$ sudo ln -s /usr/local/cuda-version /usr/local/cuda
```

Installieren Sie das CUDA-Toolkit unter Windows

Gehen Sie wie folgt vor, um das CUDA-Toolkit unter Windows zu installieren:

So installieren Sie das CUDA-Toolkit

1. Herstellen einer Verbindung mit Ihrer Windows-Instance.
2. Öffnen Sie die NVIDIA-Website und wählen Sie die gewünschte CUDA-Version aus.
3. Wählen Sie unter Installer Type (Installationstyp) die Option exe (lokal) aus und klicken Sie anschließend auf Herunterladen.
4. Führen Sie die heruntergeladene Installationsdatei mit Ihrem Browser aus. Folgen Sie den Anweisungen zur Installation des CUDA-Toolkits. Möglicherweise müssen Sie die Instance neu starten.

Installieren Sie AMD-Treiber auf Ihrer Amazon EC2 EC2-Instance

Auf Instances mit einer angeschlossenen AMD-GPU, z. B. einer G4ad-Instance, muss der entsprechende AMD-Treiber installiert sein. Je nach Ihren Anforderungen können Sie entweder ein AMI mit vorinstalliertem Treiber verwenden oder einen Treiber Amazon S3 von herunterladen.

Informationen zum Installieren von NVIDIA-Treibern auf einer Instance mit einer angeschlossenen NVIDIA-GPU, z. B. einer G4DN-Instance, finden Sie stattdessen unter Installieren Sie NVIDIA-Treiber.

Inhalt

AMD Radeon Pro Software für Enterprise Driver

Die AMD Radeon Pro Software for Enterprise Driver wurde entwickelt, um Support für professionelle Grafik-Anwendungsfälle zu bieten. Mit dem Treiber können Sie Ihre Instances mit zwei 4K-Displays pro GPU konfigurieren.

Unterstützte APIs

- OpenGL, OpenCL
- Vulkan
- AMD Advanced Media Framework
- Video Acceleration API
- DirectX 9 und höher
- Microsoft Hardware Media Foundation Transformation

AMIs mit installiertem AMD-Treiber

AWS bietet verschiedene Amazon Machine Images (AMI) an, die mit den installierten AMD-Treibern geliefert werden. Öffnen Sie Marketplace-Angebote mit AMD-Treiber.

AMD-Treiber-Download

Wenn Sie kein AMI mit dem installierten AMD-Treiber verwenden, können Sie den AMD-Treiber herunterladen und auf Ihrer Instance installieren. Nur die folgenden Betriebssystemversionen unterstützen AMD-Treiber:

- Amazon Linux 2 mit Kernelversion 4.14

> **Note**
>
> Die AMD-Treiberversion amdgpu-pro-20.20-1184451 und neuere Treiberversionen erfordern Kernelversion 5.15 oder höher.

- Windows Server 2016
- Windows Server 2019

Diese Downloads stehen nur AWS Kunden zur Verfügung. Wenn Sie die Software herunterladen, stimmen Sie zu, diese nur für die Entwicklung von AMIs für den Einsatz auf AMD-Radeon-Pro-V520-Hardware zu verwenden. Durch die Installation der Software stimmen Sie den Bedingungen in der Endbenutzer-Lizenzvereinbarung für AMD-Software zu.

Installieren Sie den AMD-Treiber auf Ihrer Linux-Instance

1. Herstellen einer Verbindung mit Ihrer Linux-Instance.
2. Installieren Sie den AWS CLI auf Ihrer Linux-Instanz und konfigurieren Sie Standardanmeldedaten. Weitere Informationen finden Sie unter Installieren der AWS CLI im AWS Command Line Interface -Benutzerhandbuch.

   > **Important**
   >
   > Ihrem Benutzer oder Ihrer Rolle müssen die Berechtigungen erteilt worden sein, die die ReadOnlyAmazonS3-Zugriffsrichtlinie enthalten. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonS3 ReadOnly Access im Amazon Simple Storage Service-Benutzerhandbuch.

3. Installieren Sie gcc und make, falls sie noch nicht installiert sind.

   ```
   $ sudo yum install gcc make
   ```

4. Aktualisieren Sie den Cache der Paketverwaltung und laden Sie die Paketaktualisierungen für Ihre Instance herunter.

   - Für Amazon Linux 2:

     ```
     $ sudo amazon-linux-extras install epel -y
     ```

```
$ sudo yum update -y
```

- Für Ubuntu 22.04:

```
$ wget https://repo.radeon.com/.preview/a0e4ef1dffbc95b4abb54e891f265e61/amdgpu-install/5.5.02.05.2/ubuntu/jammy/amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo apt install ./amdgpu-install_5.5.02.05.50502-1_all.deb
$ sudo sed -i 's#repo.radeon.com#&/.preview/a0e4ef1dffbc95b4abb54e891f265e61#' /etc/apt/sources.list.d/{amdgpu.list,rocm.list,amdgpu-proprietary.list}
```

- Für andere Ubuntu-Versionen:

```
$ sudo dpkg --add-architecture i386
$ sudo apt-get update -y && sudo apt upgrade -y
```

- Für CentOS:

```
$ sudo yum install epel-release -y
$ sudo yum update -y
```

5. Starten Sie die Instance neu.

```
$ sudo reboot
```

6. Stellen Sie nach dem Neustart erneut eine Verbindung mit der Instance her.
7. Laden Sie den neuesten AMD-Treiber herunter.

> **Note**
>
> Überspringen Sie diesen Schritt für Ubuntu 22.04.

```
$ aws s3 cp --recursive s3://ec2-amd-linux-drivers/latest/ .
```

8. Extrahieren Sie die Datei.

- Für Amazon Linux 2 und CentOS:

```
$ tar -xf amdgpu-pro-*rhel*.tar.xz
```

- Für Ubuntu:

> **Note**
>
> Überspringen Sie diesen Schritt für Ubuntu 22.04.

```
$ tar -xf amdgpu-pro*ubuntu*.xz
```

9. Wechseln Sie in den Ordner für den extrahierten Treiber.
10. Fügen Sie die fehlenden Module für die Treiberinstallation hinzu.

    - Für Amazon Linux 2 und CentOS:

      Überspringen Sie diesen Schritt.

    - Für Ubuntu:

      > **Note**
      >
      > Überspringen Sie diesen Schritt für Ubuntu 22.04.

      ```
      $ sudo apt install linux-modules-extra-$(uname -r) -y
      ```

11. Führen Sie das Selbstinstallationsskript aus, um den vollständigen Grafik-Stack zu installieren.

    - Für Ubuntu 22.04:

      ```
      $ sudo amdgpu-install --usecase=workstation --vulkan=pro --opencl=rocr,legacy -y
      ```

    - Für Amazon Linux 2 und CentOS und andere Ubuntu-Versionen:

      ```
      $ ./amdgpu-pro-install -y --opencl=pal,legacy
      ```

12. Starten Sie die Instance neu.

    ```
    $ sudo reboot
    ```

13. Vergewissern Sie sich, dass der Treiber funktioniert.

```
$ dmesg | grep amdgpu
```

Die Antwort sollte wie folgt aussehen:

```
Initialized amdgpu
```

Installieren Sie den AMD-Treiber auf Ihrer Windows-Instanz

1. Connect zu Ihrer Windows-Instanz her und öffnen Sie ein PowerShell Fenster.
2. Konfigurieren Sie Standardanmeldedaten für die AWS Tools for Windows PowerShell auf Ihrer Windows-Instanz. Weitere Informationen finden Sie unter Erste Schritte in AWS Tools for Windows PowerShell im AWS Tools for Windows PowerShell -Benutzerhandbuch.

   > **Important**
   >
   > Ihrem Benutzer oder Ihrer Rolle müssen die Berechtigungen erteilt worden sein, die die AmazonS3 ReadOnly Access-Richtlinie enthalten. Weitere Informationen finden Sie unter AWS verwaltete Richtlinie: AmazonS3 ReadOnly Access im Amazon Simple Storage Service-Benutzerhandbuch.

3. Laden Sie die Treiber mit den folgenden PowerShell Befehlen von Amazon S3 auf Ihren Desktop herunter.

   ```
   $Bucket = "ec2-amd-windows-drivers"
   $KeyPrefix = "latest" # use "archives" for Windows Server 2016
   $LocalPath = "$home\Desktop\AMD"
   $Objects = Get-S3Object -BucketName $Bucket -KeyPrefix $KeyPrefix -Region us-east-1
   foreach ($Object in $Objects) {
   $LocalFileName = $Object.Key
   if ($LocalFileName -ne '' -and $Object.Size -ne 0) {
       $LocalFilePath = Join-Path $LocalPath $LocalFileName
       Copy-S3Object -BucketName $Bucket -Key $Object.Key -LocalFile $LocalFilePath -
   Region us-east-1
   }
   }
   ```

4. Entpacken Sie die heruntergeladene Treiberdatei und führen Sie das Installationsprogramm mit den folgenden PowerShell Befehlen aus.

```
Expand-Archive $LocalFilePath -DestinationPath "$home\Desktop\AMD\$KeyPrefix" -
Verbose
```

Prüfen Sie als Nächstes den Inhalt des neuen Verzeichnisses. Der Verzeichnisname kann mit dem `Get-ChildItem` PowerShell Befehl abgerufen werden.

```
Get-ChildItem "$home\Desktop\AMD\$KeyPrefix"
```

Die Ausgabe sollte folgendermaßen oder ähnlich aussehen:

```
Directory: C:\Users\Administrator\Desktop\AMD\latest

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----       10/13/2021  12:52 AM                210414a-365562C-Retail_End_User.2
```

Installieren der Treiber:

```
pnputil /add-driver $home\Desktop\AMD\$KeyPrefix\*.inf /install /subdirs
```

5. Befolgen Sie die Anweisungen, um den Treiber zu installieren, und starten Sie die Instance neu, wenn Sie dazu aufgefordert werden.
6. Sie können prüfen, ob die GPU richtig funktioniert, indem Sie den Geräte-Manager verwenden. Sie sollten "AMD Radeon Pro V520 MxGPU" als Grafikkarte aufgeführt sehen.
7. Um die Vorteile der vier Displays mit einer Auflösung von bis zu 4K zu nutzen, richten Sie das leistungsstarke Anzeigeprotokoll NICE DCV ein.

Richten Sie einen interaktiven Desktop für Linux ein

Nachdem Sie bestätigt haben, dass auf Ihrer Linux-Instanz der AMD-GPU-Treiber installiert ist und AMDGPU verwendet wird, können Sie einen interaktiven Desktop-Manager installieren. Wir empfehlen die MATE-Desktop-Umgebung für die beste Kompatibilität und Leistung.

Voraussetzung

Öffnen Sie einen Texteditor und speichern Sie Folgendes als eine Datei mit dem Namen `xorg.conf`. Sie benötigen diese Datei auf Ihrer Instance.

```
Section "ServerLayout"
Identifier     "Layout0"
Screen          0 "Screen0"
InputDevice     "Keyboard0" "CoreKeyboard"
InputDevice     "Mouse0" "CorePointer"
EndSection
Section "Files"
ModulePath "/opt/amdgpu/lib64/xorg/modules/drivers"
ModulePath "/opt/amdgpu/lib/xorg/modules"
ModulePath "/opt/amdgpu-pro/lib/xorg/modules/extensions"
ModulePath "/opt/amdgpu-pro/lib64/xorg/modules/extensions"
ModulePath "/usr/lib64/xorg/modules"
ModulePath "/usr/lib/xorg/modules"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Mouse0"
Driver         "mouse"
Option         "Protocol" "auto"
Option         "Device" "/dev/psaux"
Option         "Emulate3Buttons" "no"
Option         "ZAxisMapping" "4 5"
EndSection
Section "InputDevice"
# generated from default
Identifier     "Keyboard0"
Driver         "kbd"
EndSection
Section "Monitor"
Identifier     "Monitor0"
VendorName     "Unknown"
ModelName      "Unknown"
EndSection
Section "Device"
Identifier     "Device0"
Driver         "amdgpu"
VendorName     "AMD"
BoardName      "Radeon MxGPU V520"
BusID          "PCI:0:30:0"
EndSection
Section "Extensions"
Option         "DPMS" "Disable"
EndSection
```

```
Section "Screen"
Identifier     "Screen0"
Device         "Device0"
Monitor        "Monitor0"
DefaultDepth   24
Option         "AllowEmptyInitialConfiguration" "True"
SubSection "Display"
    Virtual    3840 2160
    Depth      32
EndSubSection
EndSection
```

Einrichten eines interaktiven Desktops auf Amazon Linux 2

1. Installieren Sie das EPEL-Repository.

```
$ C:\> sudo amazon-linux-extras install epel -y
```

2. Installieren Sie den MATE-Desktop.

```
$ C:\> sudo amazon-linux-extras install mate-desktop1.x -y
$ C:\> sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Kopieren Sie die `xorg.conf`-Datei nach `/etc/X11/xorg.conf`.
4. Starten Sie die Instance neu.

```
$ C:\> sudo reboot
```

5. (Optional) Install the NICE DCV server (Installieren Sie den NICE-DCV-Server), um NICE DCV als leistungsstarkes Anzeigeprotokoll zu verwenden, und connect to a NICE DCV session (stellen Sie dann eine NICE-DCV-Sitzung) mit Ihrem bevorzugten Client her.

Einrichten eines interaktiven Desktops auf Ubuntu

1. Installieren Sie den MATE-Desktop.

```
$ sudo apt install xorg-dev ubuntu-mate-desktop -y
$ C:\> sudo apt purge ifupdown -y
```

2. Kopieren Sie die `xorg.conf`-Datei nach `/etc/X11/xorg.conf`.

3. Starten Sie die Instance neu.

```
$ sudo reboot
```

4. Installieren Sie den AMF-Encoder für die entsprechende Version von Ubuntu.

```
$ sudo apt install ./amdgpu-pro-20.20-*/amf-amdgpu-pro_20.20-*_amd64.deb
```

5. (Optional) Install the NICE DCV server (Installieren Sie den NICE-DCV-Server), um NICE DCV als leistungsstarkes Anzeigeprotokoll zu verwenden, und connect to a NICE DCV session (stellen Sie dann eine NICE-DCV-Sitzung) mit Ihrem bevorzugten Client her.
6. Geben Sie nach der DCV-Installation dem DCV-Benutzer Videoberechtigungen ein:

```
$ sudo usermod -aG video dcv
```

Einrichten eines interaktiven Desktops auf CentOS

1. Installieren Sie das EPEL-Repository.

```
$ sudo yum update -y
$ C:\> sudo yum install epel-release -y
```

2. Installieren Sie den MATE-Desktop.

```
$ sudo yum groupinstall "MATE Desktop" -y
$ C:\> sudo systemctl disable firewalld
```

3. Kopieren Sie die `xorg.conf`-Datei nach `/etc/X11/xorg.conf`.
4. Starten Sie die Instance neu.

```
$ sudo reboot
```

5. (Optional) Install the NICE DCV server (Installieren Sie den NICE-DCV-Server), um NICE DCV als leistungsstarkes Anzeigeprotokoll zu verwenden, und connect to a NICE DCV session (stellen Sie dann eine NICE-DCV-Sitzung) mit Ihrem bevorzugten Client her.

Paravirtual-Treiber für Windows-Instances

Windows-AMIs enthalten eine Reihe von Treibern, die den Zugriff auf virtualisierte Hardware ermöglichen. Diese Treiber werden von Amazon EC2 verwendet, um Instance-Speicher und Amazon EBS-Volumes den jeweiligen Geräte zuzuordnen. Die folgende Tabelle zeigt die wichtigsten Unterschiede zwischen den verschiedenen Treibern.

	RedHat PV	Citrix PV	AWS PV
Instance-Typ	Wird nicht für alle Instance-Typen unterstützt. Wenn Sie einen nicht unterstützten Instance-Typ angeben, ist die Instance beeinträchtigt.	Wird für Xen-Instance-Typen unterstützt.	Wird für Xen-Instance-Typen unterstützt.
Zugeordnete Volumes	Unterstützt bis zu 16 zugeordnete Volumes	Unterstützt mehr als 16 zugeordnete Volumes	Unterstützt mehr als 16 zugeordnete Volumes
Netzwerk	Bekannte Probleme mit dem Treiber: Die Netzwerkverbindung wird bei hohen Workloads zurückgesetzt, z. B bei schneller Datenübertragung über FTP.		Der Treiber konfiguriert automatisch Jumbo-Frames auf dem Netzwerkadapter, wenn er sich in einem kompatiblen Instance-Typ befindet. Wenn sich die Instance in einer Cluster-Placement-

	RedHat PV	Citrix PV	AWS PV
			Gruppe befindet, bietet dies eine bessere Netzwerkl eistung zwischen Instances, die sich in der Cluster-Placement-Gruppe befinden. Weitere Informati onen finden Sie unter Placement-Gruppen.

Die folgende Tabelle zeigt, welche PV-Treiber Sie unter den einzelnen Versionen von Windows Server in Amazon EC2 verwenden sollten;.

Windows Server Version	PV-Treiber Version
Windows Server 2022	AWS PV, neueste Version
Windows Server 2019	AWS PV neueste Version
Windows Server 2016	AWS PV neueste Version
Windows Server 2012 R2	AWS PV neueste Version
Windows Server 2012	AWS PV neueste Version

Windows Server Version	PV-Treiber Version
Windows Server 2008 R2	AWS PV-Version 8.3.5
Windows Server 2008	Citrix PV 5.9
Windows Server 2003	Citrix PV 5.9

Inhalt

AWS PV-Treiber

Die AWS PV-Treiber werden im `%ProgramFiles%\Amazon\Xentools` Verzeichnis gespeichert. Dieses Verzeichnis enthält auch öffentliche Symbole und ein Befehlszeilentool,`xenstore_client.exe`, mit dem Sie auf Einträge in zugreifen können XenStore. Der folgende PowerShell Befehl gibt beispielsweise die aktuelle Uhrzeit vom Hypervisor zurück:

```
PS C:\> [DateTime]::FromFileTimeUTC((gwmi -n root\wmi -cl
 AWSXenStoreBase).XenTime).ToString("hh:mm:ss")
11:17:00
```

Die AWS PV-Treiberkomponenten sind in der Windows-Registrierung unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` aufgeführt. Diese Treiberkomponenten umfassen im Einzelnen: xenbus, xeniface, xennet, xenvbd und xenvif.

AWS PV-Treiber haben auch einen Windows-Dienst namens LiteAgent, der im Benutzermodus ausgeführt wird. Er verarbeitet Aufgaben wie das Herunterfahren und Neustarten von AWS APIs auf Instanzen der Xen-Generation. Sie können auf Services zugreifen und diese verwalten, indem Sie `Services.msc` in der Befehlszeile ausführen. Bei der Ausführung auf Instances der Nitro-Generation werden die AWS PV-Treiber nicht verwendet und der LiteAgent Dienst wird ab der

Treiberversion 8.2.4 automatisch beendet. Die Aktualisierung auf den neuesten AWS PV-Treiber aktualisiert auch den LiteAgent und verbessert die Zuverlässigkeit aller Instance-Generationen.

Installieren Sie die neuesten AWS PV-Treiber

Amazon Windows-AMIs enthalten eine Reihe von Treibern, die den Zugriff auf virtualisierte Hardware ermöglichen. Diese Treiber werden von Amazon EC2 verwendet, um Instance-Speicher und Amazon EBS-Volumes den jeweiligen Geräte zuzuordnen. Wir empfehlen, die aktuellen Treiber zu installieren, um die Stabilität und Leistung Ihrer EC2 Instances unter Windows zu verbessern.

Installationsoptionen

- Sie können AWS Systems Manager es verwenden, um die PV-Treiber automatisch zu aktualisieren. Weitere Informationen finden Sie unter Automatische Aktualisierung von PV-Treibern in Windows EC2-Instances (Konsole) im AWS Systems Manager -Benutzerhandbuch.
- Sie können das Treiberpaket herunterladen und das Installationsprogramm manuell ausführen. Achten Sie darauf, die `readme.txt`-Datei auf Systemanforderungen zu überprüfen. Informationen zum Herunterladen und Installieren der AWS PV-Treiber oder zum Aktualisieren eines Domain-Controllers finden Sie unter Führen Sie ein manuelles Upgrade von Windows Server-Instanzen (AWS PV-Upgrade) durch.

AWS Verlauf des PV-Treiberpakets

Die folgende Tabelle zeigt die Änderungen an den AWS PV-Treibern für jede Treiberversion.

Paketversion	Details	Datum der Veröffentlichung
8.4.3	Behebung von Fehlern im Paketinstallationsprogramm zur Verbesserung der Upgrade-Erfahrung.	24. Januar 2023
8.4.2	Stabilitätsbehebungen für Race-Bedingung.	13. April 2022
8.4.1	Verbessertes Paketinstallationsprogramm.	07. Januar 2022
8.4.0	• Stabilitätskorrekturen zur Behebung seltener Fälle von hängengebliebenen Festplatten-I/O.	2. März 2021

Paketversion	Details	Datum der Veröffentlichung
	• Stabilitätskorrekturen zur Behebung seltener Fälle von Abstürzen während der EBS-Volumenablösung • Es wurde ein Feature hinzugefügt, um die Last auf mehrere Kerne für Workloads zu verteilen, die mehr als 20 000 IOPS verursachen und einen Leistungsabfall aufgrund von Engpässen erfahren. Informationen zum Aktivieren dieses Features finden Sie unter Workloads, die mehr als 20 000 Festplatten-IOPS nutzen, führen zu einem Leistungsabfall aufgrund von CPU-Engpässen. • AWS Die Installation von PV 8.4 auf Windows Server 2008 R2 schlägt fehl. AWS PV-Version 8.3.5 und frühere Versionen werden unter Windows Server 2008 R2 unterstützt.	
8.3.5	Verbessertes Paketinstallationsprogramm.	07. Januar 2022
8.3.4	Verbesserte Zuverlässigkeit der Netzwerkgeräteanbindung.	4. August 2020
8.3.3	• Aktualisierung auf die Komponente, die XenStore direkt vor der Kamera steht, um die Fehlersuche bei Pfaden zur Fehlerbehandlung zu verhindern. • Aktualisieren Sie die Speicherkomponente, um Abstürze zu vermeiden, wenn ein ungültiger SRB gesendet wird. Um diesen Treiber auf Windows Server 2008 R2-Instances zu aktualisieren, müssen Sie zunächst überprüfen, ob die entsprechenden Patches installiert sind, um der folgende Microsoft-Sicherheitsempfehlung nachzukommen: Microsoft Security Advisory 3033929.	4. Februar 2020
8.3.2	Verbesserte Zuverlässigkeit der Netzwerkkomponenten.	30. Juli 2019

Paketversion	Details	Datum der Veröffentlichung
8.3.1	Verbesserte Performance und Robustheit der Speicherkomponente.	12. Juni 2019
8.2.7	Verbesserte Effizienz bei der Migration auf Instance-Typen der neuesten Generation.	20. Mai 2019
8.2.6	Verbesserte Effizienz beim Absturzabbildpfad.	15. Januar 2019
8.2.5	Zusätzliche Verbesserungen bei der Sicherheit. PowerShell Das Installationsprogramm ist jetzt im Paket verfügbar.	12. Dezember 2018
8.2.4	Verbesserung der Zuverlässigkeit.	2. Oktober 2018
8.2.3	Fehlerbehebungen und Leistungsverbesserungen. EBS-Volume-ID als Datenträger-Seriennummer für EBS-Volumen melden. Dies ermöglicht Cluster-Szenarien wie S2D.	29. Mai 2018
8.2.1	Verbesserung der Netzwerk- und Speicherleistung sowie mehrere Stabilitätskorrekturen. Eine Information dazu, ob diese Version installiert wurde, erhalten Sie über den folgenden Windows-Registrierungswert: `HKLM\Software\Amazon\PVDriver\Version 8.2.1` .	8. März 2018
7.4.6	Stabilitätsverbesserungen, um AWS PV-Treiber widerstandsfähiger zu machen.	26. April 2017

Paketversion	Details	Datum der Veröffentlichung
7.4.3	Unterstützung für Windows Server 2016 hinzugefügt Fehlerbehebungen zur Erhöhung der Stabilität für alle unterstützten Windows-Versionen * Die Signatur der AWS PV-Treiberversion 7.4.3 läuft am 29. März 2019 ab. Wir empfehlen, auf den neuesten AWS PV-Treiber zu aktualisieren.	18. Nov. 2016
7.4.2	Fehlerbehebungen zur Erhöhung der Stabilität für den Instance-Typ X1	2. Aug. 2016
7.4.1	• Leistungsverbesserung des AWS PV-Speichertreibers. • Stabilitätsverbesserungen im AWS PV-Speichertreiber: Es wurde ein Problem behoben, bei dem die Instanzen mit dem Bug-Check-Code 0x0000DEAD zu einem Systemabsturz kamen. • Stabilitätskorrekturen im AWS PV-Netzwerktreiber. • Unterstützung für Windows Server 2008 R2 hinzugefügt	12. Juli 2016
7.3.2	• Verbesserte Protokollierung und Diagnose • Stabilitätskorrektur im AWS PV-Speichertreiber. In manchen Fällen werden Datenträger unter Windows nicht angezeigt, nachdem sie der Instance erneut zugeordnet wurden. • Unterstützung für Windows Server 2012 hinzugefügt	24. Juni 2015
7.3.1	TRIM-Aktualisierung: Fehlerbehebung für TRIM-Anfragen. Dieser Patch erhöht die Stabilität und Leistung von Instances bei der Verwaltung einer großen Anzahl von TRIM-Anfragen.	

Paketversion	Details	Datum der Veröffentlichung
7.3.0	TRIM-Unterstützung: Der AWS PV-Treiber sendet jetzt TRIM-Anfragen an den Hypervisor. Flüchtige Datenträger verarbeiten TRIM-Anfragen korrekt, wenn der zugrundeliegende Speicher TRIM (SSD) unterstützt. Beachten Sie, dass EBS-basierter Speicher TRIM nicht unterstützt (Stand März 2015).	
7.2.5	• Stabilitätskorrektur bei AWS PV-Speichertreibern: In einigen Fällen konnte der AWS PV-Treiber ungültigen Speicher dereferenzieren und einen Systemausfall verursachen. • Stabilitätskorrektur beim Generieren eines Crash-Dumps: In einigen Fällen konnte es vorkommen, dass der AWS PV-Treiber beim Schreiben eines Crash-Dumps in einem Race-Zustand stecken blieb. Vor dieser Version konnte das Problem nur dadurch gelöst werden, dass der Treiber beendet und erneut gestartet wurde, wodurch der Speicherauszug verloren ging.	
7.2.4	Persistenz der Geräte-ID: Dieser Patch maskiert die PCI-Geräte-ID der Plattform und erzwingt die Anzeige derselben Geräte-ID im System, auch wenn die Instance verschoben wird. Allgemeiner formuliert wirkt sich der Patch darauf aus, wie der Hypervisor virtuelle Geräte anzeigt. Der Fix beinhaltet auch Änderungen am Co-Installer für die AWS PV-Treiber, sodass das System weiterhin zugeordnete virtuelle Geräte verwendet.	

Paketversion	Details	Datum der Veröffentlichung
7.2.2	• Laden Sie die AWS PV-Treiber im Modus Directory Services Restore Mode (DSRM): Der Directory Services Restore Mode ist eine Startoption im abgesicherten Modus für Windows Server-Domänencontroller. • Persistenz der Geräte-ID, wenn ein virtueller Netzwerkadapter neu zugewiesen wird: Dieser Patch erzwingt eine Prüfung der Zuordnung von MAC-Adressen im System, sodass die Geräte-ID erhalten bleibt. Durch diesen Patch wird sichergestellt, dass die Adapter ihre statischen Einstellungen beibehalten, wenn Sie neu zugewiesen werden.	
7.2.1	• Ausführung im abgesicherten Modus: Behebung eines Problems, bei dem der Treiber im abgesicherten Modus nicht geladen wird. Bisher konnten die AWS PV-Treiber nur in normal laufenden Systemen instanziiert werden. • Hinzufügen von Datenträgern zu Microsoft Windows-Speicherpools: Vor dieser Version wurden Abfragen für Speicherseite 83 synthetisiert. Der Patch entfernt die Unterstützung für Speicherseite 83. Beachten Sie, dass dies keine Auswirkungen auf Speicherpools hat, die in einer Cluster-Umgebung verwendet werden, da PV-Datenträger keine gültigen Cluster-Datenträger sind.	
7.2.0	Base: Die AWS PV-Basisversion.	

Citrix-PV-Treiber

Die Citrix PV-Treiber werden im Verzeichnis `%ProgramFiles%\Citrix\XenTools` (32-Bit-Instances) oder `%ProgramFiles(x86)%\Citrix\XenTools` (64-Bit-Instances) gespeichert.

Die Citrix PV-Treiberkomponenten werden in der Windows-Registry unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services` aufgelistet. Diese Treiberkomponenten umfassen im Einzelnen: xenevtchn, xeniface, xennet, Xennet6, xensvc, xenvbd und xenvif.

Citrix hat auch eine Treiberkomponente namens XenGuestAgent, die als Windows-Dienst ausgeführt wird. Sie übernimmt Aufgaben wie das Beenden und erneute Starten von Ereignissen über die API. Sie können auf Services zugreifen und diese verwalten, indem Sie `Services.msc` in der Befehlszeile ausführen.

Wenn bei der Verarbeitung bestimmter Workloads Netzwerkfehler auftreten, müssen Sie möglicherweise das TCP-Offloading-Feature für den Citrix PV-Treiber deaktivieren. Weitere Informationen finden Sie unter TCP-Offloading.

RedHat PV-Treiber

RedHat Treiber werden für ältere Instanzen unterstützt, werden jedoch aufgrund von Treiberbeschränkungen nicht für neuere Instanzen mit mehr als 12 GB RAM empfohlen. Instanzen mit mehr als 12 GB RAM, auf denen RedHat Treiber ausgeführt werden, können möglicherweise nicht gestartet werden und es kann nicht mehr darauf zugegriffen werden. Wir empfehlen, die RedHat Treiber auf Citrix PV-Treiber und anschließend die Citrix PV-Treiber auf PV-Treiber zu AWS aktualisieren.

Die Quelldateien für die RedHat Treiber befinden sich im Verzeichnis `%ProgramFiles%\RedHat` (32-Bit-Instanzen) oder `%ProgramFiles(x86)%\RedHat` (64-Bit-Instanzen). Die beiden Treiber sind `rhelnet` der RedHat paravirtualisierte Netzwerktreiber und `rhelscsi` der SCSI-Miniporttreiber. RedHat

Abonnieren von -Benachrichtigungen

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen von EC2-Windows-Treibern veröffentlicht werden. Führen Sie die folgenden Schritte durch, um diese Benachrichtigungen zu abonnieren.

> **Note**
>
> Sie müssen die Region für das SNS-Thema angeben, das Sie abonnieren.

Abonnieren von EC2-Benachrichtigungen über die Konsole

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, weil sich die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region befinden.

3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription Folgendes aus:
   a. Kopieren Sie den folgenden Amazon-Ressourcennamen (ARN) unter TopicARN:

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

   b. Wählen Sie unter Protocol die Option `Email` aus.
   c. Geben Sie unter Endpoint eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.
   d. Wählen Sie Create subscription (Abonnement erstellen) aus.
6. Sie erhalten eine Bestätigungs-E-Mail. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Abonnieren Sie EC2-Benachrichtigungen mit dem AWS CLI

Verwenden Sie den folgenden Befehl AWS CLI, um EC2-Benachrichtigungen mit dem zu abonnieren.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-
windows-drivers --region us-east-1 --protocol email --notification-
endpoint YourUserName@YourDomainName.ext
```

Abonnieren Sie EC2-Benachrichtigungen mit dem AWS Tools for PowerShell

Verwenden Sie den folgenden Befehl, um EC2-Benachrichtigungen mit Tools für Windows PowerShell zu abonnieren.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Region us-east-1 -Protocol email -Endpoint 'YourUserName@YourDomainName.ext'
```

Jedes Mal wenn neue EC2-Treiber für Windows veröffentlicht werden, senden wir ein Benachrichtigung an die Abonnenten. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

Kündigen eines Abonnements der Benachrichtigungen zu Amazon-EC2-Treibern für Windows

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.

2. Wählen Sie im Navigationsbereich Subscriptions aus.
3. Aktivieren Sie das Kontrollkästchen für das Abonnement und wählen Sie dann Actions (Aktionen) und Delete subscriptions (Abonnements löschen) aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Upgraden von PV-Treibern auf Windows-Instances

Wir empfehlen, die aktuellen PV-Treiber zu installieren, um die Stabilität und Leistung Ihrer EC2-Instances unter Windows zu verbessern. Die Anweisungen auf dieser Seite helfen Ihnen, das Treiberpaket herunterzuladen und das Installationsprogramm manuell ausführen.

Überprüfen, welchen Treiber Ihre Windows-Instance verwendet

Öffnen Sie Network Connections (Netzwerkverbindungen) in der Systemsteuerung, und zeigen Sie Local Area Connection (LAN-Verbindung) an. Prüfen Sie, ob einer der folgenden Treiber verwendet wird:

- AWS PV-Netzwerkgerät
- Citrix PV Ethernet Adapter
- RedHat PV-NIC-Treiber

Alternativ können Sie auch die Ausgabe des Befehls `pnputil -e` überprüfen.

Systemanforderungen

Überprüfen Sie unbedingt die `readme.txt`-Datei im Download auf Systemanforderungen.

Inhalt

Aktualisieren Sie Windows Server-Instanzen (AWS PV-Upgrade) mit dem Distributor

Sie können den Distributor, eine Funktion von, verwenden AWS Systems Manager, um das AWS PV-Treiberpaket zu installieren oder zu aktualisieren. Die Installation oder das Upgrade kann einmalig oder nach einem Zeitplan installiert oder aktualisiert werden. Die `In-place update` Option für den Installationstyp wird für dieses Distributor-Paket nicht unterstützt.

> **Important**
>
> Wenn Ihre Instance ein Domain-Controller ist, finden Sie weitere Informationen unter Führen Sie ein Upgrade eines Domänencontrollers durch (AWS PV-Upgrade). Das Upgrade-Verfahren für Domain-Controller-Instances unterscheidet sich von dem für die Standard Editions von Windows.

1. Wir empfehlen Ihnen, eine Sicherungskopie zu erstellen, falls Sie Ihre Änderungen rückgängig machen müssen.

   > **Tip**
   >
   > Anstatt das AMI über die Amazon EC2 EC2-Konsole zu erstellen, können Sie Systems Manager Automation verwenden, um das AMI mithilfe des `AWS-CreateImage` Runbooks zu erstellen. Weitere Informationen finden Sie AWS-CreateImageim Referenz-Benutzerhandbuch zum AWS Systems Manager Automation-Runbook.

   a. Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Stellen Sie vor dem Anhalten einer Instance sicher, dass Sie alle benötigten Daten aus den Instance-Speicher-Volumes in den persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.
   b. Wählen Sie im Navigationsbereich Instances aus.
   c. Wählen Sie die Instance, die ein Treiberupgrade benötigt und wählen Sie Instance state (Instance-Zustand), Stop instance (Instance stoppen) aus.
   d. Nachdem die Instance angehalten wurde, wählen Sie die Instance aus, wählen Sie Actions (Aktionen), Image and Templates (Image und Vorlagen) und dann Create image (Image erstellen) aus.
   e. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

2. Verbindung mit der Instance über Remote Desktop. Weitere Informationen finden Sie unter the section called “Stellen Sie mithilfe eines RDP-Clients eine Connect zu Ihrer Windows-Instanz her”.
3. Wir empfehlen, dass Sie alle Nicht-System-Laufwerke offline nehmen und alle Laufwerksbuchstabenzuordnungen zu den sekundären Laufwerken in der Laufwerksverwaltung notieren, bevor Sie dieses Upgrade durchführen. Dieser Schritt ist nicht erforderlich, wenn Sie eine direkte Aktualisierung der AWS PV-Treiber durchführen. Wir empfehlen außerdem, die Start-Option für alle nicht erforderlichen Services in der Services-Konsole auf Manual zu setzen.
4. Anweisungen zur Installation oder Aktualisierung des AWS PV-Treiberpakets mithilfe des Distributors finden Sie in den Verfahren unter Pakete installieren oder aktualisieren im AWS Systems Manager Benutzerhandbuch.
5. Wählen Sie als Name AWSPVDriver.
6. Wählen Sie als Installationstyp die Option Deinstallieren und neu installieren aus.
7. Konfigurieren Sie die anderen Parameter für das Paket nach Bedarf und führen Sie die Installation oder das Upgrade mit dem unter referenzierten Verfahren ausStep 4.

   Nach der Ausführung des Distributor-Pakets wird die Instanz automatisch neu gestartet und anschließend der Treiber aktualisiert. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar.
8. Nachdem das Upgrade abgeschlossen ist und die Instance beide Zustandsprüfungen in der Amazon EC2 EC2-Konsole bestanden hat, stellen Sie sicher, dass der neue Treiber installiert wurde, indem Sie über Remote Desktop eine Verbindung zur Instance herstellen.
9. Sobald Sie die Verbindung hergestellt haben, führen Sie den folgenden PowerShell Befehl aus:

   ```
   Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
   ```
10. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS Verlauf des PV-Treiberpakets Öffnen der Datenträgerverwaltung, um alle sekundären Volumes, die offline sind, zu überprüfen und sie entsprechend den unter angegebenen Laufwerksbuchstaben online zu schaltenStep 3.

Wenn Sie die TCP-Offloading Verwendung von Netsh für Citrix PV-Treiber zuvor deaktiviert haben, empfehlen wir, diese Funktion nach dem Upgrade auf AWS PV-Treiber wieder zu aktivieren. Probleme beim TCP-Offloading mit Citrix-Treibern treten bei den PV-Treibern nicht auf AWS . Infolgedessen bietet TCP-Offloading eine bessere Leistung bei AWS PV-Treibern.

Wenn Sie zuvor eine statische IP-Adresse oder DNS-Konfiguration auf die Netzwerkschnittstelle angewendet haben, müssen Sie nach dem Upgrade der AWS PV-Treiber möglicherweise die statische IP-Adresse oder DNS-Konfiguration erneut anwenden.

Führen Sie ein manuelles Upgrade von Windows Server-Instanzen (AWS PV-Upgrade) durch

Gehen Sie wie folgt vor, um ein direktes Upgrade von AWS PV-Treibern durchzuführen oder ein Upgrade von Citrix PV-Treibern auf AWS PV-Treiber unter Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 oder Windows Server 2022 durchzuführen. Dieses Upgrade ist nicht für RedHat Treiber oder andere Versionen von Windows Server verfügbar.

Einige ältere Versionen von Windows Server können die neuesten Treiber nicht verwenden. Um zu überprüfen, welche Treiberversion für Ihr Betriebssystem verwendet werden soll, lesen Sie die Tabelle mit den Treiberversionen auf der Seite Paravirtual-Treiber für Windows-Instances an.

> **Important**
>
> Wenn Ihre Instance ein Domain-Controller ist, finden Sie weitere Informationen unter Führen Sie ein Upgrade eines Domänencontrollers durch (AWS PV-Upgrade). Das Upgrade-Verfahren für Domain-Controller-Instances unterscheidet sich von dem für die Standard Editions von Windows.

Um AWS PV-Treiber manuell zu aktualisieren

1. Wir empfehlen Ihnen, ein Backup zu erstellen, falls Sie Ihre Änderungen rückgängig machen müssen.

   > **Tip**
   >
   > Anstatt das AMI über die Amazon EC2 EC2-Konsole zu erstellen, können Sie Systems Manager Automation verwenden, um das AMI mithilfe des `AWS-CreateImage` Runbooks zu erstellen. Weitere Informationen finden Sie AWS-CreateImageim Referenz-Benutzerhandbuch zum AWS Systems Manager Automation-Runbook.

   a. Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Stellen Sie vor dem Anhalten einer Instance sicher, dass Sie alle

benötigten Daten aus den Instance-Speicher-Volumes in den persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.

b. Wählen Sie im Navigationsbereich Instances aus.

c. Wählen Sie die Instance, die ein Treiberupgrade benötigt und wählen Sie Instance state (Instance-Zustand), Stop instance (Instance stoppen) aus.

d. Nachdem die Instance angehalten wurde, wählen Sie die Instance aus, wählen Sie Actions (Aktionen), Image and Templates (Image und Vorlagen) und dann Create image (Image erstellen) aus.

e. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

2. Verbindung mit der Instance über Remote Desktop.

3. Wir empfehlen, dass Sie alle Nicht-System-Laufwerke offline nehmen und alle Laufwerksbuchstabenzuordnungen zu den sekundären Laufwerken in der Laufwerksverwaltung notieren, bevor Sie dieses Upgrade durchführen. Dieser Schritt ist nicht erforderlich, wenn Sie eine direkte Aktualisierung der AWS PV-Treiber durchführen. Wir empfehlen außerdem, die Start-Option für alle nicht erforderlichen Services in der Services-Konsole auf Manual zu setzen.

4. Laden Sie das aktuelle Treiberpaket in die Instance herunter.

   Oder führen Sie den folgenden PowerShell Befehl aus:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/
Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip
Expand-Archive $env:userprofile\pv_driver.zip -DestinationPath
 $env:userprofile\pv_drivers
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

5. Extrahieren Sie den Inhalt des Ordners und führen Sie anschließend die Datei `AWSPVDriverSetup.msi` aus.

Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade des Treibers durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar. Nachdem das Upgrade abgeschlossen ist und die Instance beide Zustandsprüfungen in der Amazon EC2 EC2-Konsole bestanden hat, können Sie überprüfen, ob der neue Treiber installiert wurde, indem Sie über Remote Desktop eine Verbindung mit der Instance herstellen und dann den folgenden PowerShell Befehl ausführen:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS Verlauf des PV-Treiberpakets Open Disk Management, um alle sekundären Volumes, die offline sind, zu überprüfen und sie entsprechend den unter angegebenen Laufwerksbuchstaben online zu schalten. Step 3

Wenn Sie die TCP-Offloading Verwendung von Netsh für Citrix PV-Treiber zuvor deaktiviert haben, empfehlen wir, diese Funktion nach dem Upgrade auf AWS PV-Treiber wieder zu aktivieren. Probleme beim TCP-Offloading mit Citrix-Treibern treten bei den PV-Treibern nicht auf AWS . Infolgedessen bietet TCP-Offloading eine bessere Leistung bei AWS PV-Treibern.

Wenn Sie zuvor eine statische IP-Adresse oder DNS-Konfiguration auf die Netzwerkschnittstelle angewendet haben, müssen Sie nach dem Upgrade der AWS PV-Treiber möglicherweise die statische IP-Adresse oder DNS-Konfiguration erneut anwenden.

Führen Sie ein Upgrade eines Domänencontrollers durch (AWS PV-Upgrade)

Gehen Sie auf einem Domänencontroller wie folgt vor, um entweder ein direktes Upgrade von AWS PV-Treibern oder ein Upgrade von Citrix PV-Treibern auf AWS PV-Treibern durchzuführen.

So führen Sie ein Upgrade für einen Domain-Controller durch

1. Wir empfehlen Ihnen, ein Backup für Ihren Domain-Controller zu erstellen, falls Sie Ihre Änderungen rückgängig machen müssen. Die Verwendung eines AMI als Backup wird nicht unterstützt. Weitere Informationen finden Sie in der Microsoft-Dokumentation unter Überlegungen zum Backup und zur Wiederherstellung für virtualisierte Domain-Controller.
2. Führen Sie den folgenden Befehl aus, um Windows so zu konfigurieren, dass nach einem Neustart in den DSRM-Modus (Directory Services Restore Mode) gebootet wird.

> **Warning**
>
> Stellen Sie sicher, dass Sie das DSRM-Passwort kennen, bevor Sie diesen Befehl ausführen. Sie benötigen diese Informationen, um sich bei Ihrer Instance anmelden zu können, wenn das Upgrade durchgeführt wurde und die Instance automatisch neu gestartet wird.

```
bcdedit /set {default} safeboot dsrepair
```

PowerShell:

```
PS C:\> bcdedit /set "{default}" safeboot dsrepair
```

Das System muss mit DSRM gestartet werden, da das Upgrade-Hilfsprogramm die Citrix PV-Speichertreiber entfernt, damit es AWS PV-Treiber installieren kann. Daher empfehlen wir, in der Datenträgerverwaltung alle Laufwerksbuchstaben und Ordnerzuordnungen auf die sekundären Laufwerke zu beachten. Wenn keine Citrix-PV-Speichertreiber vorhanden sind, werden sekundäre Laufwerke nicht erkannt. Domain-Controller, die NTDS-Ordner auf sekundären Laufwerken verwenden, können nicht gebootet werden, da der sekundäre Datenträger nicht erkannt wird.

> **Warning**
>
> Wenn Sie diesen Befehl ausgeführt haben, führen Sie keinen manuellen Neustart des Systems durch. Das System wird nicht gebootet, da die Citrix PV-Treiber DSRM nicht unterstützen.

3. Führen Sie den folgenden Befehl aus, um der Registrierung den Eintrag **`DisableDCCheck`** hinzuzufügenden:

```
reg add HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck /t
 REG_SZ /d true
```

4. Laden Sie das aktuelle Treiberpaket in die Instance herunter.

5. Extrahieren Sie den Inhalt des Ordners und führen Sie anschließend die Datei `AWSPVDriverSetup.msi` aus.

   Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade des Treibers durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar.

6. Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her. Öffnen Sie die Datenträgerverwaltung, um alle sekundären Offline-Volumes zu überprüfen und online zu bringen, die den zuvor beschriebenen Laufwerksbuchstaben und Ordnerzuordnungen entsprechen.

   Sie müssen eine Verbindung mit der Instance herstellen, indem Sie den Benutzernamen im folgenden Format angeben hostname\administrator. Zum Beispiel TestBox Win2k12\administrator.

7. Führen Sie den folgenden Befehl aus, um die DSRM-Bootkonfiguration zu entfernen:

   ```
   bcdedit /deletevalue safeboot
   ```

8. Starten Sie die Instance neu.

9. Vergewissern Sie sich am Ende des Upgrades-Verfahrens, dass der neue Treiber installiert wurde. Suchen Sie im Geräte-Manager unter Storage Controllers den AWS PV Storage Host Adapter. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS Verlauf des PV-Treiberpakets.

10. Führen Sie den folgenden Befehl aus, um den Eintrag **`DisableDCCheck`** aus der Registrierung zu löschen:

    ```
    reg delete HKLM\SOFTWARE\Wow6432Node\Amazon\AWSPVDriverSetup /v DisableDCCheck
    ```

> **Note**
>
> Wenn Sie die TCP-Offloading Verwendung von Netsh für Citrix PV-Treiber zuvor deaktiviert haben, empfehlen wir, diese Funktion nach dem Upgrade auf PV-Treiber wieder zu aktivieren. AWS Probleme beim TCP-Offloading mit Citrix-Treibern treten bei den PV-

Treibern nicht auf AWS . Infolgedessen bietet TCP-Offloading eine bessere Leistung bei AWS PV-Treibern.

Upgrade für Instances unter Windows Server 2008 und 2008 R2 (Upgrade von RedHat auf Citrix PV)

Bevor Sie mit dem Upgrade Ihrer RedHat Treiber auf Citrix PV-Treiber beginnen, stellen Sie sicher, dass Sie Folgendes tun:

- Installieren Sie die aktuelle Version des EC2Config-Service. Weitere Informationen finden Sie unter Installieren der neuesten Version von EC2Config.
- Stellen Sie sicher, dass Sie Windows PowerShell 3.0 installiert haben. Führen Sie den folgenden Befehl in einem PowerShell Fenster aus, um zu überprüfen, welche Version Sie installiert haben:

  ```
  PS C:\> $PSVersionTable.PSVersion
  ```

  Windows PowerShell 3.0 ist im Installationspaket Version 3.0 von Windows Management Framework (WMF) enthalten. Wenn Sie Windows PowerShell 3.0 installieren müssen, finden Sie weitere Informationen unter Windows Management Framework 3.0 im Microsoft Download Center.
- Erstellen Sie ein Backup Ihrer wichtigen Daten in der Instance oder erstellen Sie ein AMI aus der Instance. Weitere Informationen zum Erstellen eines AMI finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

  > **Tip**
  >
  > Anstatt das AMI über die Amazon EC2 EC2-Konsole zu erstellen, können Sie Systems Manager Automation verwenden, um das AMI mithilfe des `AWS-CreateImage` Runbooks zu erstellen. Weitere Informationen finden Sie AWS-CreateImageim Referenz-Benutzerhandbuch zum AWS Systems Manager Automation-Runbook.

  Wenn Sie ein AMI erstellen, sollten Sie unbedingt wie folgt vorgehen:

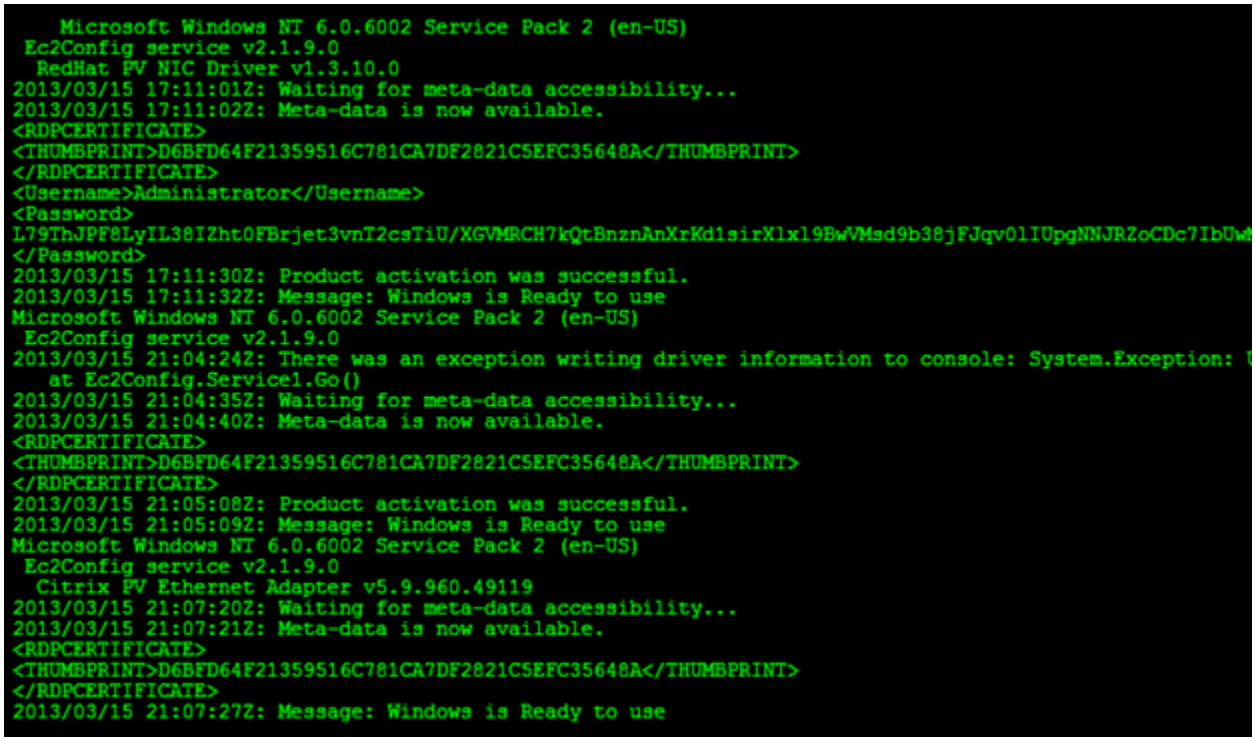
  - Notieren Sie sich Ihr Passwort.
  - Führen Sie das Sysprep-Tool nicht manuell oder mithilfe des EC2Config-Service aus.
  - Stellen Sie Ihren Ethernet-Adapter so ein, dass ihm automatisch eine IP-Adresse über DHCP zugewiesen wird. Weitere Informationen finden Sie unter Konfigurieren von TCP/IP-Einstellungen in der Microsoft-Bibliothek. TechNet

Um Treiber zu aktualisieren RedHat

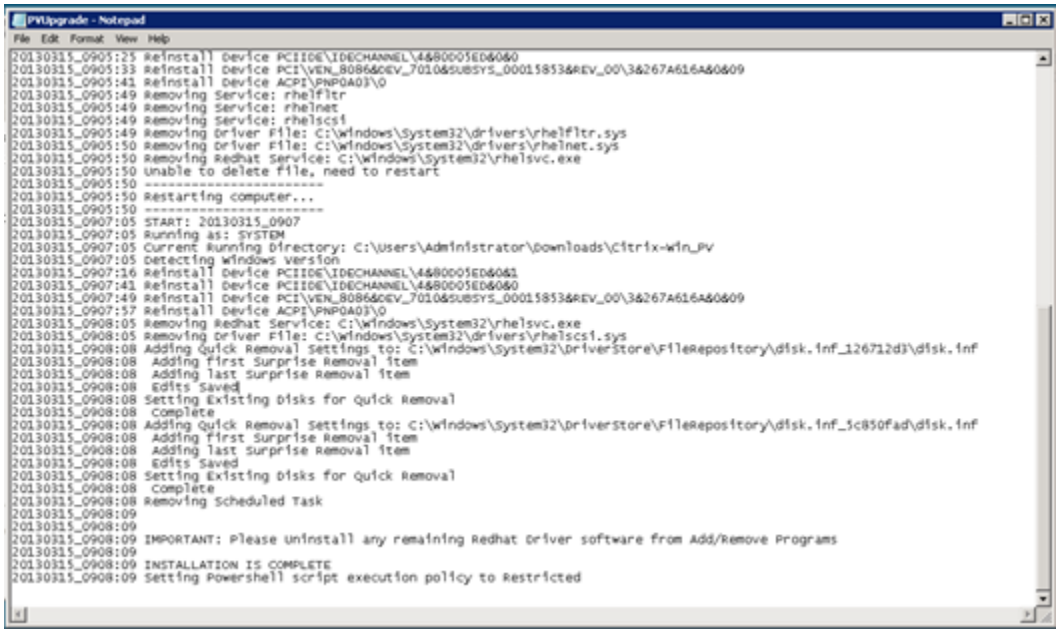
1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung mit Ihrer -Windows-Instance.
2. Laden Sie das Citrix PV-Upgrade-Paket in die Instance herunter.
3. Extrahieren Sie die Inhalte des Upgrade-Pakets an einem Speicherort Ihrer Wahl.
4. Doppelklicken Sie auf die Datei Upgrade.bat. Wenn eine Sicherheitswarnung angezeigt wird, wählen Sie Ausführen.
5. Prüfen Sie die Informationen im Dialogfeld Upgrade Drivers (Treiber upgraden) und klicken Sie auf Yes (Ja), wenn Sie bereit sind, das Upgrade zu starten.
6. Wählen Sie im Deinstallationsdialogfeld für Red Hat Paravirtualized Xen Drivers for Windows die Option Ja, um die Software zu entfernen. RedHat Ihre Instance wird neu gestartet.

> **Note**
>
> Wenn das Dialogfeld für das Deinstallationsprogramm nicht angezeigt wird, klicken Sie in der Windows-Taskleiste auf Red Hat Paravirtualize.

7. Prüfen Sie, ob die Instance neu gestartet wurde und einsatzbereit ist.
   a. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
   b. Wählen Sie auf der Seite Instances die Option Actions (Aktionen), dann Monitor and troubleshoot (Überwachung und Fehlerbehebung) aus und wählen Sie dann Get system log (Systemprotokoll abrufen) aus.
   c. Der Server sollte während des Upgrade-Vorgangs 3 oder 4 mal neu gestartet worden sein. Sie können das in der Protokolldatei daran erkennen, wie oft `Windows is Ready to use` angezeigt wird.



8. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
9. Schließen Sie das Dialogfeld Red Hat Paravirtualized Xen Drivers for Windows uninstaller.
10. Vergewissern Sie sich, dass die Installation abgeschlossen wurde. Navigieren Sie zu dem Ordner `Citrix-WIN_PV`, den Sie extrahiert haben, öffnen Sie die Datei `PVUpgrade.log` und suchen Sie nach dem Text `INSTALLATION IS COMPLETE`.



Upgrade des Citrix-Xen-Guest-Agent-Service

Wenn Sie Citrix PV-Treiber unter Windows-Server verwenden, können Sie ein Upgrade des Citrix Xen Guest Agent-Service durchführen. Dieser Windows-Service übernimmt Aufgaben wie das Beenden und erneute Starten von Ereignissen über die API. Sie können dieses Upgrade-Paket unter jeder Version von Windows Server ausführen, wenn in der Instance die Citrix PV-Treiber ausgeführt werden.

> **Important**
>
> Für Windows Server 2008 R2 und höher empfehlen wir Ihnen, ein Upgrade auf AWS PV-Treiber durchzuführen, die das Guest Agent-Update enthalten.

Erstellen Sie unbedingt ein Backup Ihrer wichtigen Daten in der Instance oder erstellen Sie ein AMI aus der Instance, bevor Sie mit dem Upgrade der Treiber beginnen. Weitere Informationen zum Erstellen eines AMI finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

> **Tip**
>
> Anstatt das AMI über die Amazon EC2 EC2-Konsole zu erstellen, können Sie Systems Manager Automation verwenden, um das AMI mithilfe des `AWS-CreateImage` Runbooks zu erstellen. Weitere Informationen finden Sie AWS-CreateImageim Referenz-Benutzerhandbuch zum AWS Systems Manager Automation-Runbook.

Wenn Sie ein AMI erstellen, sollten Sie unbedingt wie folgt vorgehen:

- Aktivieren Sie das Sysprep-Tool nicht mithilfe des EC2Config-Service.
- Notieren Sie sich Ihr Passwort.
- Stellen Sie Ihren Ethernet-Adapter auf DHCP ein.

So erstellen Sie ein Upgrade des Citrix Xen Guest Agent-Service

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an. Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung mit Ihrer -Windows-Instance.
2. Laden Sie das Citrix-Upgrade-Paket in die Instance herunter.

3. Extrahieren Sie die Inhalte des Upgrade-Pakets an einem Speicherort Ihrer Wahl.
4. Doppelklicken Sie auf die Datei Upgrade.bat. Wenn eine Sicherheitswarnung angezeigt wird, wählen Sie Ausführen.
5. Prüfen Sie die Informationen im Dialogfeld Upgrade Drivers (Treiber upgraden) und klicken Sie auf Yes (Ja), wenn Sie bereit sind, das Upgrade zu starten.
6. Wenn das Upgrade abgeschlossen ist, wird die Datei `PVUpgrade.log` geöffnet; diese enthält den Text `UPGRADE IS COMPLETE`.
7. Starten Sie Ihre Instance neu.

Problembehandlung bei PV-Treibern auf Windows-Instanzen

Nachstehend sind Lösungen für Probleme aufgeführt, auf die Sie möglicherweise mit älteren Amazon EC2-Images und PV-Treibern stoßen.

Inhalt

Windows Server 2012 R2 verliert die Netzwerkverbindung und Speicheranbindung nach einem Neustart der Instance

> **Important**
>
> Dieses Problem tritt nur bei AMIs auf, die vor September 2014 zur Verfügung gestellt wurden.

Amazon Machine Images (AMIs) für Windows Server 2012 R2, die vor dem 10. September 2014 verfügbar gemacht wurden, können die Netzwerkverbindung und Speicheranbindung nach einem Neustart der Instance verlieren. Der Fehler im AWS Management Console Systemprotokoll besagt: „Schwierigkeiten beim Erkennen von PV-Treiberdetails für die Konsolenausgabe“. Der Verlust der Verbindung wird durch das Feature "Plug & Play Cleanup" verursacht. Dieses Feature sucht

alle 30 Tage nach inaktiven Systemgeräten und deaktiviert sie. Das Feature identifiziert das EC2-Netzwerkgerät irrtümlicherweise als inaktiv und entfernt es aus dem System. Wenn dies geschieht, verliert die Instance die Netzwerkverbindung nach einem Neustart.

Wenn Sie den Verdacht haben, dass ein System von diesem Problem betroffen ist, können Sie ein direktes Treiber-Upgrade herunterladen und ausführen. Wenn Sie das direkte Treiber-Upgrade nicht durchführen können, können Sie ein Hilfsskript ausführen. Das Skript ermittelt, ob Ihre Instance betroffen ist. Wenn das zutrifft und das Amazon EC2-Netzwerkgerät noch nicht entfernt wurde, wird die "Plug & Play Cleanup"-Suche durch das Skript deaktiviert. Wenn das Netzwerkgerät entfernt wurde, wird das Gerät von dem Skript repariert und die "Plug & Play Cleanup"-Suche deaktiviert. Anschließend kann Ihre Instance neu gestartet werden und die Netzwerkverbindung bleibt erhalten.

Inhalt

Auswahl der Probleme, die behoben werden sollen

Es gibt zwei Methoden zum Wiederherstellen der Netzwerkverbindung und Speicheranbindung für eine Instance, die von diesem Problem betroffen ist. Wählen Sie eine der folgenden Methoden:

Art	Voraussetzungen	Übersicht über das Verfahren
Methode 1 – Enhanced Networking	Enhanced Networking ist nur in einer Virtual Private Cloud (VPC) verfügbar und setzt den Instance-Typ C3 voraus. Wenn der Server aktuell nicht C3 als Instance-Typ verwendet, müssen Sie diesen temporär ändern.	Sie ändern den Instance-Typ des Servers in eine C3-Instance. Danach können Sie mit Enhanced Networking eine Verbindung mit der betroffenen Instance herstellen und das Problem beheben. Wenn Sie das Problem behoben haben, ändern Sie den Instance-Typ wieder in den ursprünglichen Wert. Diese Methode ist in der Regel schneller als Methode 2

Art	Voraussetzungen	Übersicht über das Verfahren
		und es treten wahrscheinlich weniger Benutzerfehler auf. Solange die C3-Instance ausgeführt wird, werden Ihnen zusätzlich Kosten berechnet.
Methode 2 – Konfiguration der Registrierung	Möglichkeit, einen zweiten Server zu erstellen bzw. auf einen zuzugreifen. Möglichkeit, Registrierungseinstellungen zu ändern.	Sie trennen das Root-Volume von der betroffenen Instance, ordnen es einer anderen Instance zu, stellen eine Verbindung her und nehmen Änderungen an der Registrierung vor. Solange der zusätzliche Server ausgeführt wird, werden Ihnen zusätzlich Kosten berechnet. Diese Methode ist langsamer als Methode 1, funktioniert aber auch in Situationen, in denen Methode 1 das Problem nicht lösen konnte.

Methode 1 – Enhanced Networking

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Starten Sie die betroffene Instance. Wählen Sie die Instance und wählen Sie Instance state (Instance-Status) und dann Stop instance (Instance anhalten).

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wenn die Instance angehalten wurde, erstellen Sie ein Backup. Wählen Sie die Instance und wählen Sie Actions (Aktionen), dann Image und Templates (Image und Vorlagen) und dann Create image (Image erstellen).
5. Ändern Sie den Instance-Typ in eine C3-Instance.
6. Starten Sie die Instance.
7. Stellen Sie über Remote Desktop Connect mit der Instanz her und laden Sie dann das AWS PV Drivers Upgrade-Paket auf die Instanz herunter.
8. Extrahieren Sie den Inhalt des Ordners und führen Sie die Datei `AWSPVDriverSetup.msi` aus.

   Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade der Treiber durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar.
9. Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her und prüfen Sie, ob die neuen Treiber installiert wurden. Suchen Sie im Geräte-Manager unter Storage Controllers den AWS PV Storage Host Adapter. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS Verlauf des PV-Treiberpakets.
10. Halten Sie die Instance an und ändern Sie den Instance-Typ wieder in den ursprünglichen Wert.
11. Starten Sie die Instance und fahren Sie mit der normalen Verwendung fort.

Methode 2 – Konfiguration der Registrierung

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Starten Sie die betroffene Instance. Wählen Sie die Instance, wählen Sie Instance state (Instance-Status) und dann Stop instance (Instance anhalten).

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wählen Sie die Option Launch instances (Instances starten) und erstellen Sie eine temporäre Windows-Server-2008- oder Windows-Server-2012-Instance in derselben Availability Zone wie die betroffene Instance. Erstellen Sie keine Windows Server 2012 R2-Instance.

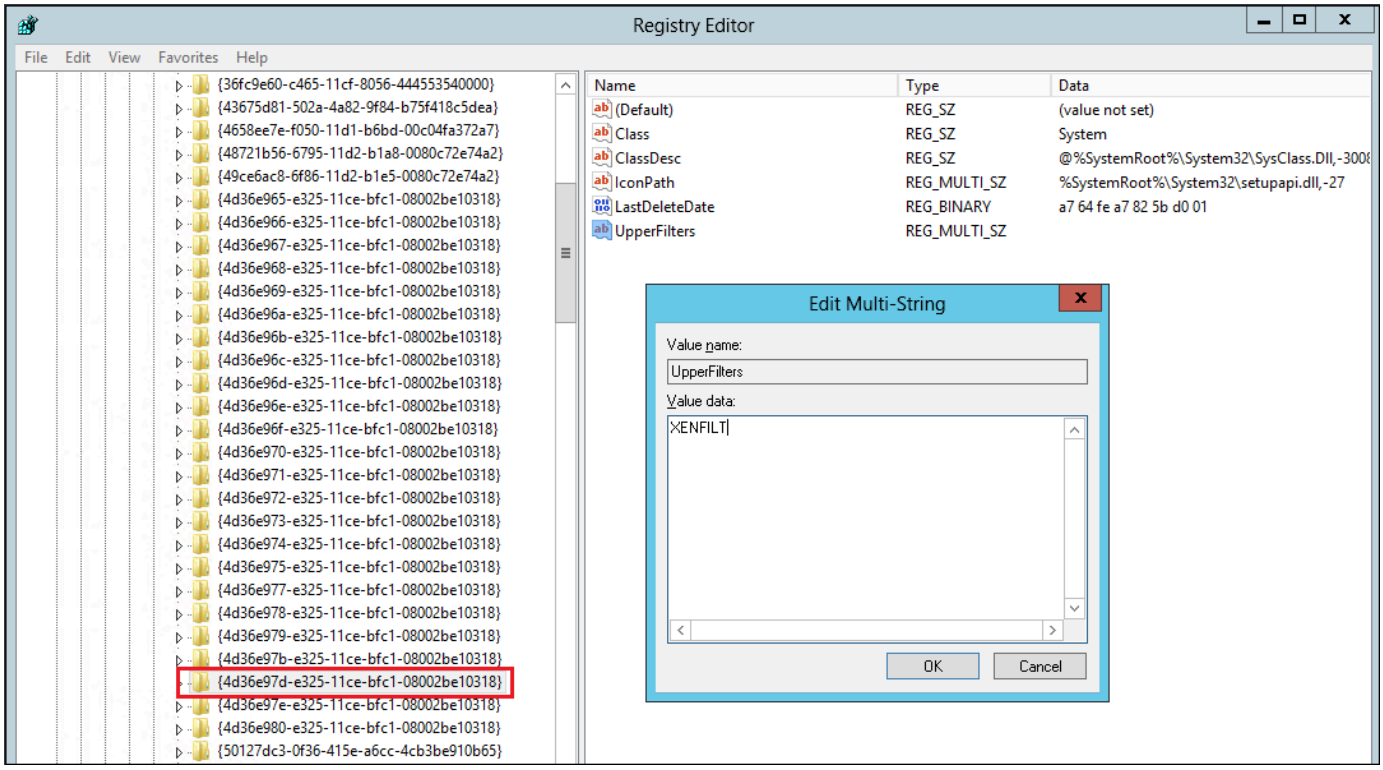
   > **Important**
   >
   > Wenn Sie die Instance nicht in der gleichen Availability Zone wie die betroffene Instance erstellen, können Sie das Stamm-Volume der betroffenen Instance nicht der neuen Instance anfügen.

5. Wählen Sie im Navigationsbereich Volumes aus.
6. Lokalisieren Sie das Stamm-Volume der betroffenen Instance. Trennen Sie das Volume und fügen Sie das Volume anschließend der temporären Instance an, die Sie zuvor erstellt haben. Fügen Sie es dem standardmäßigen Gerätenamen (xvdf) an.
7. Stellen Sie über Remote Desktop eine Verbindung mit der temporären Instance her und verwenden Sie anschließend das Dienstprogramm für die Datenträgerverwaltung, um das Volume verfügbar zu machen und es zu verwenden.
8. Öffnen Sie in der temporären Instance das Dialogfeld Ausführen, geben Sie **`regedit`** ein und drücken Sie die Eingabetaste.
9. Wählen Sie im Navigationsbereich des Registrierungs-Editors die Option HKEY_LOCAL_MACHINE aus und wählen Sie dann im Menü File die Option Load Hive.
10. Navigieren Sie im Dialogfeld Load Hive zu Betroffenes Volume\Windows\System32\config \System" und geben Sie im Dialogfeld Key Name einen temporären Namen ein. Geben Sie z. B. ei OldSys.
11. Suchen Sie im Navigationsbereich des Registrierungs-Editors die folgenden Schlüssel:

    HKEY_LOCAL_MACHINE\ ***`your_temporary_key_name\ 001\ Control\ Class\ 4d36e97d-e325-11ce-bfc1-08002be10318`*** ControlSet

    HKEY_LOCAL_MACHINE\ ***`Name Ihres temporären Schlüssels\ ControlSet 001\ Control\ Class\ 4d36e96a-e325-11ce-bfc1-08002be10318`***

12. Doppelklicken Sie für jeden Schlüssel, geben Sie den Wert UpperFiltersXENFILT ein, und wählen Sie dann OK.



13. Suchen Sie den folgenden Schlüssel:

    HKEY_LOCAL_MACHINE\ Name ***Ihres temporären Schlüssels\ 001\ Services\ XENBUS\ Parameters*** ControlSet

14. Erstellen Sie eine neue Zeichenfolge (REG_SZ) mit dem Namen und dem folgenden Wert: ActiveDevice

    PCI\VEN_5853&DEV_0001&SUBSYS_00015853&REV_01

15. Suchen Sie den folgenden Schlüssel:

    HKEY_LOCAL_MACHINE\ Name Ihres temporären Schlüssels\ 001\ Services\ XENBUS ControlSet

16. Ändern Sie den Wert unter Count von 0 in 1.

17. Suchen Sie die folgenden Schlüssel und löschen Sie sie:

    HKEY_LOCAL_MACHINE\ ***Ihr_temporäre_Schlüsselname***\ ControlSet 001\ Services\ xenvbd\ StartOverride

    HKEY_LOCAL_MACHINE\ ***Ihr_temporäre_Schlüsselname***\ ControlSet 001\ Services\ xenfilt\ StartOverride

18. Wählen Sie im Navigationsbereich "Registry Editor" den temporären Schlüssel aus, den Sie beim ersten Öffnen des Registrierungs-Editors erstellt haben.
19. Wählen Sie im Menü File die Option Unload Hive aus.
20. Wählen Sie im Dienstprogramm für die Datenträgerverwaltung das Laufwerk aus, das Sie zugewiesen haben, öffnen Sie das Kontextmenü (rechte Maustaste) und wählen Sie die Option Offline aus.
21. Trennen Sie in der Amazon EC2-Konsole das betroffene Volume von der temporären Instance und ordnen Sie es wieder Ihrer Windows Server 2012 R2-Instance mit den Gerätenamen „/dev/sda1” zu. Sie müssen diesen Gerätenamen angeben, um das Volume als Stamm-Volume hinzufügen zu können.
22. Starten Sie die Instance.
23. Stellen Sie über Remote Desktop Connect mit der Instanz her und laden Sie dann das AWS PV Drivers Upgrade-Paket auf die Instanz herunter.
24. Extrahieren Sie den Inhalt des Ordners und führen Sie die Datei `AWSPVDriverSetup.msi` aus.

    Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade der Treiber durchgeführt. Die Instance ist für die Dauer von bis zu 15 Minuten nicht verfügbar.
25. Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her und prüfen Sie, ob die neuen Treiber installiert wurden. Suchen Sie im Geräte-Manager unter Storage Controllers den AWS PV Storage Host Adapter. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS Verlauf des PV-Treiberpakets.
26. Löschen Sie die in diesem Vorgang erstellte temporäre Instance bzw. beenden Sie sie.

Ausführen des Korrekturskripts

Wenn Sie kein direktes Upgrade der Treiber durchführen oder nicht in eine aktuelle Instance migrieren können, haben Sie die Möglichkeit, das Korrekturskript auszuführen, um die Probleme zu beheben, die von der „Plug & Play Cleanup”-Task verursacht wurden.

So führen Sie das Korrekturskript aus

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie die Instance aus, für die Sie das Korrekturskript ausführen möchten. Wählen Sie Instance state (Instance-Status) und dann Stop instance (Instance anhalten) aus.

   > **Warning**
   >
   > Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wenn die Instance angehalten wurde, erstellen Sie ein Backup. Wählen Sie die Instance, wählen Sie Actions (Aktionen), dann Image und Templates (Image und Vorlagen) und dann Create image (Image erstellen).
5. Wählen Sie Instance state (Instance-Status) und dann Start instance (Instance starten) aus.
6. Stellen Sie mithilfe von Remote Desktop eine Connect mit der Instanz her und laden Sie dann den RemediateDriverIssue ZIP-Ordner auf die Instanz herunter.
7. Extrahieren Sie die Inhalte der Datei.
8. Führen Sie das Korrekturskript aus; befolgen Sie dazu die Anweisungen in der Datei Readme.txt. Die Datei befindet sich in dem Ordner, in den Sie die ZIP-Datei extrahiert haben RemediateDriverIssue.

TCP-Offloading

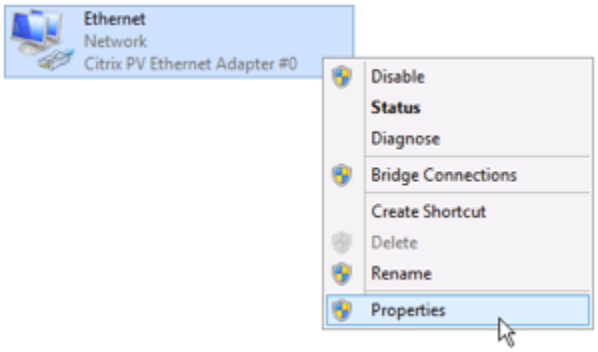
> **Important**
>
> Dieses Problem gilt nicht für Instances, auf denen AWS PV- oder Intel-Netzwerktreiber ausgeführt werden.

TCP-Offloading ist standardmäßig für Citrix PV-Treiber in Windows-AMIs aktiviert. Wenn Fehler auf der Transportebene oder bei der Übertragung von Paketen auftreten, bzw. in der Windows—Leistungsüberwachung angezeigt werden, z. B. wenn Sie bestimmte SQL—Workloads ausführen, dann müssen Sie dieses Feature möglicherweise deaktivieren.

> **Warning**
>
> Durch die Deaktivierung des TCP-Offloading verschlechtert sich möglicherweise die Netzwerkleistung Ihre Instance.

So deaktivieren Sie TCP-Offloading unter Windows Server 2012 und 2008

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Wenn Sie Windows Server 2012 verwenden, drücken Sie Ctrl+Esc, um den Start-Bildschirm aufzurufen, und wählen Sie dann Control Panel (Systemsteuerung). Wenn Sie Windows Server 2008 verwenden, wählen Sie Start und dann die Option Control Panel (Systemsteuerung) aus.
3. Wählen Sie dann Netzwerk und Internet und anschließend Netzwerk- und Freigabecenter aus.
4. Wählen Sie Change adapter settings (Adapter-Einstellungen ändern) aus.
5. Klicken Sie mit der rechten Maustaste auf Citrix PV Ethernet Adapter #0 und wählen Sie die Option Properties.



6. Wählen Sie im Dialogfeld Eigenschaften der LAN-Verbindung die Option Konfigurieren aus, um das Dialogfeld Citrix PV Ethernet Adapter #0 Properties (Eigenschaften für Citrix PV Ethernet Adapter #0) zu öffnen.
7. Deaktivieren Sie auf der Registerkarte Erweitert jede der Eigenschaften, mit Ausnahme von Correct TCP/UDP Checksum Value (TCP/UDP-Prüfsummenwert korrigieren). Um eine Eigenschaft zu deaktivieren, wählen Sie sie unter Eigenschaft aus und wählen Sie unter dem Punkt Wert die Option Deaktiviert aus.
8. Klicken Sie auf OK.
9. Führen Sie die folgenden Befehle in einem Eingabeaufforderungsfenster aus.

```
netsh int ip set global taskoffload=disabled
netsh int tcp set global chimney=disabled
netsh int tcp set global rss=disabled
netsh int tcp set global netdma=disabled
```

10. Starten Sie die Instance neu.

Zeitsynchronisierung

Vor der Veröffentlichung der Windows-AMI 2013.02.13 konnte der Citrix Xen Guest Agent die Systemzeit falsch einstellen. Das kann dazu führen, dass Ihr DHCP-Lease abläuft. Wenn Sie Probleme mit der Verbindung zu Ihrer Instance haben, müssen Sie den Agent möglicherweise aktualisieren.

Sie können ermitteln, ob Sie bereits den aktualisierten Citrix Xen Guest Agent installiert haben, indem Sie prüfen, ob die Datei `C:\Program Files\Citrix\XenGuestAgent.exe` im März 2013 erstellt wurde. Wenn der Zeitstempel dieser Datei ein früheres Datum anzeigt, sollten sie den Citrix Xen Guest Agent-Service aktualisieren. Weitere Informationen finden Sie unter Upgrade des Citrix-Xen-Guest-Agent-Service.

Workloads, die mehr als 20 000 Festplatten-IOPS nutzen, führen zu einem Leistungsabfall aufgrund von CPU-Engpässen

Sie können von diesem Problem betroffen sein, wenn Sie Windows-Instances verwenden, auf denen AWS -PV-Treiber ausgeführt werden, die mehr als 20 000 IOPS nutzen, und es zu Fehlerprüfungscode `0x9E: USER_MODE_HEALTH_MONITOR` kommt.

Festplatten-Lese- und Schreibvorgänge (IOs) in den AWS PV-Treibern erfolgen in zwei Phasen: IO-Vorbereitung und IO-Abschluss. Standardmäßig läuft die Vorbereitungsphase auf einem einzelnen beliebigen Kern ab. Die Abschlussphase läuft auf Kern `0`. Die Menge an Berechnung, die für die Verarbeitung eines I/O erforderlich ist, hängt von der Größe und anderen Eigenschaften ab. Einige iOS verwenden in der Vorbereitungsphase mehr Berechnungen und andere in der Abschlussphase. Wenn eine Instance mehr als 20 000 IOPS steuert, kann die Vorbereitungs- oder Abschlussphase zu einem Engpass führen, bei dem die CPU, auf der sie läuft, eine Kapazität von 100% hat. Ob die Vorbereitungs- oder Abschlussphase zu einem Engpass wird oder nicht, hängt von den Eigenschaften des von der Anwendung verwendeten iOS ab.

Ab den AWS PV-Treibern 8.4.0 kann die Last der Vorbereitungs- und Fertigstellungsphase auf mehrere Kerne verteilt werden, wodurch Engpässe vermieden werden. Jede Anwendung verwendet

verschiedene I/O-Eigenschaften. Daher kann die Anwendung einer der folgenden Konfigurationen die Leistung Ihrer Anwendung erhöhen, verringern oder nicht beeinflussen. Nachdem Sie eine dieser Konfigurationen angewendet haben, überwachen Sie die Anwendung, um sicherzustellen, dass sie Ihre gewünschte Leistung erfüllt.

1. Voraussetzungen

   Bevor Sie mit diesem Fehlerbehebungsverfahren beginnen, sollten Sie die folgenden Voraussetzungen überprüfen:

   - Ihre Instance verwendet AWS PV-Treiber der Version 8.4.0 oder höher. Informationen zum Upgrade finden Sie unter Upgraden von PV-Treibern auf Windows-Instances.
   - Sie haben RDP-Zugriff auf die Instance. Schritte zum Herstellen einer Verbindung mit Ihrer Windows-Instance über RDP finden Sie unter Stellen Sie mithilfe eines RDP-Clients eine Connect zu Ihrer Windows-Instanz her .
   - Sie haben Administratorzugriff auf die Instance.

2. Beobachten Sie die CPU-Auslastung in Ihrer Instance

   Sie können den Windows Task-Manager verwenden, um die Auslastung jeder CPU anzuzeigen, um potenzielle Engpässe bei der Festplatten-I/O zu ermitteln.

   1. Stellen Sie sicher, dass Ihre Anwendung läuft und ähnlich wie Ihr Produktions-Workload Datenverkehr verarbeitet.
   2. Herstellen einer Verbindung mit Ihrer Instance über RDP.
   3. Wähle das Menü Start auf Ihrer Instance.
   4. Geben Sie `Task Manager` im Menü Start ein, um den Task-Manager zu öffnen.
   5. Wenn Task-Manager die Zusammenfassungsansicht anzeigt, wählen Sie More details (Weitere Einzelheiten), um die Detailansicht zu erweitern.
   6. Wählen Sie die Registerkarte Performance (Leistung) aus.
   7. Wählen Sie CPU im linken Bereich.
   8. Klicken Sie mit der rechten Maustaste auf das Diagramm im Hauptbereich und wählen Sie Change graph to (Diagramm ändern zu) > Logical processors (Logische Prozessoren), um jeden einzelnen Kern anzuzeigen.
   9. Je nachdem, wie viele Kerne sich auf Ihrer Instance befinden, sehen Sie möglicherweise Zeilen, die im Laufe der Zeit die CPU-Auslastung anzeigen oder Sie sehen nur eine Zahl.

- Wenn Sie Diagramme sehen, die die Last über die Zeit anzeigen, suchen Sie nach CPUs, bei denen das Kästchen fast vollständig schattiert ist.
- Wenn Sie auf jedem Kern eine Zahl sehen, suchen Sie nach Kernen, die durchweg 95% oder mehr anzeigen.

10 Beachten Sie, ob Kern `0` oder ein anderer Kern stark ausgelastet ist.

3. Wählen Sie, welche Konfiguration angewendet werden soll

Konfigurationsname	Wann diese Konfiguration angewendet werden	Hinweise
Default configuration	Workload verursacht weniger als 20 000 IOPS oder haben andere Konfigurationen die Leistung oder Stabilität nicht verbessert.	Für diese Konfiguration tritt I/O auf einigen Kernen auf, was kleineren Workloads zugute kommen kann, indem die Cache-Lokalität erhöht und der Kontextwechsel reduziert wird.
Allow driver to choose whether to distribute completion	Der Workload nutzt mehr als 20 000 IOPS, und eine moderate oder hohe Last wird im Kern `0` beobachten.	Diese Konfiguration wird für alle Xen-Instances empfohlen, die PV 8.4.0 oder höher verwenden und mehr als 20 000 IOPS nutzen, unabhängig davon, ob Probleme auftreten oder nicht.
Distribute both preparation and completion	Workload verursacht mehr als 20 000 IOPS, und entweder verbesserte die Erlaubnis für den Treiber, die Verteilung zu wählen, die Leistung nicht oder ein anderer Kern als `0` weit eine hohe Auslastung auf.	Diese Konfiguration ermöglicht die Verteilung sowohl der I/O-Vorbereitung als auch des I/O-Abschluss.

> **Note**
>
> Wir empfehlen, dass Sie die I/O-Vorbereitung nicht verteilen, ohne auch die I/O-Abschluss zu verteilen (Einstellung `DpcRedirection` ohne Einstellung `NotifierDistributed`), da die Abschlussphase empfindlich auf Überlastung durch die Vorbereitungsphase reagiert, wenn die Vorbereitungsphase parallel läuft.

Werte für Registrierungsschlüssel

- NotifierDistributed

  Wert `0` oder nicht vorhanden — Die Abschlussphase läuft auf Kern `0` .

  Wert `1` — Der Treiber entscheidet sich für die Durchführung der Abschlussphase oder Kern `0` oder einen zusätzlicher Kern pro angeschlossener Festplatte.

  Wert `2` — Der Treiber führt die Abschlussphase auf einem zusätzlichen Kern pro angeschlossener Festplatte aus.
- DpcRedirection

  Wert `0` oder nicht vorhanden — Die Vorbereitungsphase läuft auf einem einzigen, willkürlichen Kern.

  Wert `1` — Die Vorbereitungsphase ist auf mehrere Kerne verteilt.

Standardkonfiguration

Wenden Sie die Standardkonfiguration bei AWS PV-Treiberversionen vor 8.4.0 an oder wenn nach der Anwendung einer der anderen Konfigurationen in diesem Abschnitt ein Leistungs- oder Stabilitätsverlust beobachtet wird.

1. Herstellen einer Verbindung mit Ihrer Instance über RDP.
2. Öffnen Sie als Administrator eine neue PowerShell Eingabeaufforderung.

3. Führen Sie die folgenden Befehle aus, um `NotifierDistributed` und `DpcRedirection`-Registrierungsschlüssel zu entfernen.

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name NotifierDistributed
```

```
Remove-ItemProperty -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Name DpcRedirection
```

4. Starten Sie Ihre Instance neu.

Treiber können auswählen, ob die Fertigstellung verteilt werden soll

Legen Sie den `NotiferDistributed`-Registrierungsschlüssel fest, damit der PV-Speichertreiber wählen kann, ob der I/O-Abschluss verteilt werden soll oder nicht.

1. Herstellen einer Verbindung mit Ihrer Instance über RDP.
2. Öffnen Sie als Administrator eine neue PowerShell Eingabeaufforderung.
3. Führen Sie den folgenden Befehl aus, um den `NotiferDistributed`-Registrierungsschlüssel festzulegen:

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name NotifierDistributed
```

4. Starten Sie Ihre Instance neu.

Verteilen Sie sowohl Vorbereitung als auch Fertigstellung

Legen Sie `NotifierDistributed` und `DpcRedirection`-Registrierungsschlüssel fest, um immer sowohl die Vorbereitungs- als auch die Abschlussphase zu verteilen.

1. Herstellen einer Verbindung mit Ihrer Instance über RDP.
2. Öffnen Sie als Administrator eine neue PowerShell Eingabeaufforderung.
3. Führen Sie die folgenden Befehle aus, um den `NotifierDistributed`- und `DpcRedirection`- Registrierungsschlüssel festzulegen.

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000002 -Name NotifierDistributed
```

```
Set-ItemProperty -Type DWORD -Path HKLM:\System\CurrentControlSet\Services\xenvbd
\Parameters -Value 0x00000001 -Name DpcRedirection
```

4. Starten Sie Ihre Instance neu.

AWS NVMe-Treiber für Windows-Instanzen

Amazon EBS-Volumes und Instance-Speicher-Volumes werden als NVMe-Blockgeräte auf Instances bereitgestellt, die auf dem AWS Nitro System basieren. Um die Leistung und die Funktionen der Amazon EBS-Funktionen für Volumes, die als NVMe-Blockgeräte bereitgestellt werden, vollständig nutzen zu können, muss auf der Instance der AWS NVMe-Treiber installiert sein. Auf allen AWS Windows-AMIs der aktuellen Generation ist der AWS NVMe-Treiber standardmäßig installiert.

Weitere Informationen zu EBS und NVMe finden Sie unter Amazon EBS und NVMe im Amazon EBS-Benutzerhandbuch. Weitere Informationen über SSD-Instance-Speicher und NVMe finden Sie unter Instance-Speicher-Volumes auf SSD.

Installieren oder aktualisieren Sie NVMe-Treiber mit AWS PowerShell

Wenn Sie nicht die neuesten von Amazon bereitgestellten AWS Windows-AMIs verwenden, verwenden Sie das folgende Verfahren, um den aktuellen AWS NVMe-Treiber zu installieren. Sie sollten diese Aktualisierung zu einem Zeitpunkt durchführen, zu dem Ihre Instance neu gestartet werden kann. Entweder wird das Installationsskript Ihre Instance neu starten oder Sie müssen sie als letzten Schritt neu starten.

Voraussetzungen

PowerShell 3.0 oder höher

Um den neuesten AWS NVMe-Treiber herunterzuladen und zu installieren

1. Wir empfehlen Ihnen, ein AMI wie folgt als Backup zu erstellen, falls Sie Ihre Änderungen rückgängig machen müssen.

   a. Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Stellen Sie vor dem Anhalten einer Instance sicher, dass Sie alle

benötigten Daten aus den Instance-Speicher-Volumes in den persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.

b. Wählen Sie im Navigationsbereich Instances aus.

c. Wählen Sie die Instance, die ein Treiberupgrade benötigt und wählen Sie Instance state (Instance-Zustand), Stop instance (Instance stoppen) aus.

d. Nachdem die Instance angehalten wurde, wählen Sie die Instance aus, wählen Sie Actions (Aktionen), Image and Templates (Image und Vorlagen) und dann Create image (Image erstellen) aus.

e. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten).

2. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.

3. Laden Sie die Treiber mit einer der folgenden Optionen auf Ihre Instance herunter und extrahieren Sie sie:

   - Verwenden eines Browsers:

     a. Laden Sie das aktuelle Treiberpaket in die Instance herunter.

     b. Extrahieren Sie die ZIP-Datei.

   - Verwenden von PowerShell:

```
Invoke-WebRequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/
Latest/AWSNVMe.zip -outfile $env:USERPROFILE\nvme_driver.zip
Expand-Archive $env:userprofile\nvme_driver.zip -DestinationPath
 $env:userprofile\nvme_driver
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder früher verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Installieren Sie den Treiber auf Ihrer Instanz, indem Sie das `install.ps1` PowerShell Skript aus dem `nvme_driver` Verzeichnis (`.\install.ps1`) ausführen. Wenn Sie eine Fehlermeldung erhalten, stellen Sie sicher, dass Sie PowerShell 3.0 oder höher verwenden.

   a. (Optional) Ab der AWS NVMe-Version `1.5.0` werden persistente Reservierungen für Small Computer System Interface (SCSI) für Windows Server 2016 und höher unterstützt. Dieses Feature fügt Unterstützung für Windows Server Failover Clustering mit gemeinsam genutztem Amazon EBS-Speicher hinzu. Dieses Feature ist bei der Installation standardmäßig nicht aktiviert.

      Sie können das Feature aktivieren, wenn Sie das `install.ps1` Skript zur Installation des Treibers ausführen, indem Sie den `EnableSCSIPersistentReservations` Parameter mit dem Wert angeben`$true`.

      ```
      PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $true
      ```

      Sie können das Feature deaktivieren, wenn Sie das `install.ps1` Skript zur Installation des Treibers ausführen, indem Sie den `EnableSCSIPersistentReservations` Parameter mit dem Wert angeben`$false`.

      ```
      PS C:\> .\install.ps1 -EnableSCSIPersistentReservations $false
      ```

   b. Ab AWS NVMe installiert `1.5.0` das `install.ps1` Skript das `ebsnvme-id` Tool immer zusammen mit dem Treiber.

      (Optional) Für die Versionen `1.4.0` `1.4.1` und `1.4.2` können Sie mit dem `install.ps1` Skript angeben, ob das `ebsnvme-id` Tool zusammen mit dem Treiber installiert werden soll.

      i. Um das `ebsnvme-id`-Tool zu installieren, geben Sie `InstallEBSNVMeIdTool 'Yes'` an.

      ii. Wenn Sie das Tool nicht installieren möchten, geben Sie `InstallEBSNVMeIdTool 'No'` an.

      Wenn Sie `InstallEBSNVMeIdTool` nicht angeben, und das Tool bereits bei `C:\ProgramData\Amazon\Tools` vorhanden ist, aktualisiert das Paket das Tool standardmäßig. Wenn das Tool nicht vorhanden ist, aktualisiert `install.ps1` das Tool standardmäßig nicht.

Wenn Sie das Tool nicht als Teil des Pakets, sondern zu einem späteren Zeitpunkt, installieren möchten, finden Sie die neueste Version oder das Tool im Treiberpaket. Alternativ können Sie die Version `1.0.0` von Amazon S3 herunterladen:

Laden Sie das `ebsnvme-id`-Tool herunter.

5. Wenn das Installationsprogramm Ihre Instance nicht neu startet, starten Sie die Instance neu.

Installieren oder aktualisieren Sie AWS NVMe-Treiber mit dem Distributor

Sie können den Verteiler, eine Funktion von AWS Systems Manager, verwenden, um das NVMe-Treiberpaket einmalig oder mit geplanten Updates zu installieren.

1. Anweisungen zum Installieren des NVMe-Treiberpakets mit Distributor finden Sie in den Verfahren unter Installieren oder Aktualisieren von Paketen im Benutzerhandbuch für Amazon EC2 Systems Manager.
2. Wählen Sie unter Name die Option AWSNVMe.
3. Wählen Sie als Installationstyp die Option Deinstallieren und neu installieren aus.
4. (Optional) Passen Sie die Installation an, indem Sie Werte für `AdditionalArguments` angeben.

   a. Ab AWS NVMe `1.5.0` unterstützt der Treiber persistente SCSI-Reservierungen für Windows Server 2016 und höher. Dieses Feature ist bei der Installation standardmäßig nicht aktiviert. Um dieses Feature zu aktivieren, geben Sie `{"SSM_EnableSCSIPersistentReservations": $true}` für `AdditionalArguments` an. Wenn Sie dieses Feature nicht aktivieren möchten, geben Sie `{"SSM_EnableSCSIPersistentReservations": $false}` für `AdditionalArguments` an.

   b. Ab AWS NVMe installiert `1.5.0` das `install.ps1` Skript das Tool immer. `ebsnvme-id`

   (Optional) Für die Versionen`1.4.0`, `1.4.1` und`1.4.2` können Sie mit dem `install.ps1`-Skript angeben, ob das Tool ebsnvme-id mit dem Treiber installiert werden soll.

      i. Um das Tool ebsnvme-id zu installieren, geben Sie `{"SSM_InstallEBSNVMeIdTool": "Yes"}` für `AdditionalArguments` an.

      ii. Wenn Sie das Tool nicht installieren möchten, geben Sie `{"SSM_InstallEBSNVMeIdTool": "No"}` für `AdditionalArguments` an.

Wenn `SSM_InstallEBSNVMeIdTool` nicht für `AdditionalArguments` angegeben und das Tool bereits bei `C:\ProgramData\Amazon\Tools` vorhanden ist, aktualisiert das Paket das Tool standardmäßig. Wenn das Tool nicht vorhanden ist, aktualisiert das Paket das Tool standardmäßig nicht. Zusätzliche Argumente müssen mit einer gültigen JSON-Syntax formatiert werden. Beispiele für die Übergabe zusätzlicher Argumente für das `aws configure`-Paket finden Sie in der Dokumentation zu Amazon EC2 Systems Manager.

Wenn Sie das Tool nicht als Teil des Pakets, sondern zu einem späteren Zeitpunkt, installieren möchten, finden Sie die neueste Version des Tools im Treiberpaket. Alternativ können Sie die Version `1.0.0` von Amazon S3 herunterladen:

Laden Sie das `ebsnvme-id`-Tool herunter.

5. Wenn das Installationsprogramm Ihre Instance nicht neu startet, starten Sie die Instance neu.

Konfigurieren Sie persistente SCSI-Reservierungen

Nachdem die AWS NVMe-Treiberversion `1.5.0` oder höher installiert wurde, können Sie persistente SCSI-Reservierungen mithilfe der Windows-Registrierung für Windows Server 2016 und höher aktivieren oder deaktivieren. Sie müssen die Instance neu starten, damit die Registry-Änderungen übernommen werden.

Sie können persistente SCSI-Reservierungen mit dem folgenden Befehl aktivieren, der den Wert `EnableSCSIPersistentReservations` auf den Wert 1 setzt.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 1
```

Sie können persistente SCSI-Reservierungen mit dem folgenden Befehl deaktivieren, der den Wert `EnableSCSIPersistentReservations` auf den Wert `0` setzt.

```
PS C:\> $registryPath = "HKLM:\SYSTEM\CurrentControlSet\Services\AWSNVMe\Parameters
\Device"
Set-ItemProperty -Path $registryPath -Name EnableSCSIPersistentReservations -Value 0
```

AWS Versionsverlauf des NVMe-Treibers

In der folgenden Tabelle werden die veröffentlichten Versionen des AWS NVMe-Treibers beschrieben.

Paketversion	Treiberversion	Details	Datum der Veröffentlichung
1.5.1	1.5.0	Das Installationsskript wurde korrigiert, um bei Bedarf einen Ordner für das Tool „ebsnvme-id“ zu erstellen.	17. November 2023
1.5.0	1.5.0	Unterstützung für persistente Reservierungen mit Small Computer System Interface (SCSI) für Instances hinzugefügt, auf denen Windows Server 2016 und höher ausgeführt wird. Das Tool ebsnvme-id (`ebsnvme-id.exe`) ist jetzt standardmäßig installiert.	31. August 2023
1.4.2	1.4.2	Es wurde ein Fehler behoben, bei dem Instance-Speicher-Volumes auf D3-Instances AWS-NVMe-Treiber nicht unterstützt wurden.	16. März 2023
1.4.1	1.4.1	Meldet Namespace Preferred Write Granularity (NPGW) für EBS-Volumes, die dieses optionale NVMe-Feature unterstützen. Weitere Informationen finden Sie in Abschnitt 8.25, „Verbesserung der Leistung durch I/O-Größe und Ausrichtungsadhärenz“ in derNVMe Basisspezifikation, Version 1.4.	20. Mai 2022
1.4.0	1.4.0	• Unterstützung für IoCTLs wurde hinzugefügt, mit denen Anwendungen mit NVMe-Geräten interagieren können. Diese Unterstützung ermöglicht es Anwendungen, `IdentifyController` -, `IdentifyNamespace` - und `NameSpace` -Listen vom NVMe-Gerät abzurufen. Weitere Informationen	23. November 2021

Paketversion	Treiberversion	Details	Datum der Veröffentlichung
		finden Sie unter Protokollspezifische Abfragen in der Microsoft-Dokumentation. • AWSNVMe Die Installation von 1.4.0 auf Windows Server 2008 R2 schlägt fehl. AWSNVMe Version 1.3.2 und frühere Versionen werden unter Windows Server 2008 R2 unterstützt. • Die Treiberversion 1.4.0 und das neueste `ebsnvme-id` -Tool (`ebsnvme-id.exe`) sind in einem einzigen Paket vereint. Mit dieser Kombination können Sie sowohl Treiber als auch Tool aus einem einzigen Paket installieren. Weitere Details finden Sie unter Installieren oder aktualisieren Sie NVMe-Treiber mit AWS PowerShell. • Fehlerbehebungen und verbesserte Zuverlässigkeit.	
1.3.2	1.3.2	Behebung eines Problems bei der Modifizierung von EBS-Volumes während einer aktiven I/O-Verarbeitung, das zu beschädigten Daten führen könnte. Kunden, die EBS-Online-Volumes nicht modifizieren (beispielsweise durch Ändern von Größe oder Typ) sind nicht betroffen.	10. September 2019
1.3.1	1.3.1	Verbesserung der Zuverlässigkeit.	21. Mai 2019
1.3.0	1.3.0	Verbesserungen der Geräteoptimierung.	31. August 2018
1.2.0	1.2.0	Leistungs- und Zuverlässigkeitsverbesserungen für AWS NVMe-Geräte auf allen unterstützten Instances, einschließlich Bare-Metal-Instances.	13. Juni 2018

Paketversion	Treiberversion	Details	Datum der Veröffentlichung
1.0.0	1.0.0	AWS NVMe-Treiber für unterstützte Instanztypen, auf denen Windows Server ausgeführt wird.	12. Februar 2018

Abonnieren von -Benachrichtigungen

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen von EC2-Windows-Treibern veröffentlicht werden. Führen Sie die folgenden Schritte durch, um diese Benachrichtigungen zu abonnieren.

So abonnieren Sie EC2-Benachrichtigungen über die Konsole

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, weil sich die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region befinden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription Folgendes aus:
   a. Kopieren Sie den folgenden Amazon-Ressourcennamen (ARN) unter TopicARN:

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers
   b. Wählen Sie unter Protocol die Option `Email` aus.
   c. Geben Sie unter Endpoint eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.
   d. Wählen Sie Create subscription (Abonnement erstellen) aus.
6. Sie erhalten eine Bestätigungs-E-Mail. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Jedes Mal wenn neue EC2-Treiber für Windows veröffentlicht werden, senden wir ein Benachrichtigung an die Abonnenten. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

So kündigen Sie ein Abonnement der Benachrichtigungen zu Amazon EC2-Treibern für Windows

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Subscriptions aus.
3. Aktivieren Sie das Kontrollkästchen für das Abonnement und wählen Sie dann Actions (Aktionen) und Delete subscriptions (Abonnements löschen) aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Um EC2-Benachrichtigungen zu abonnieren, verwenden Sie AWS CLI

Verwenden Sie den folgenden Befehl AWS CLI, um EC2-Benachrichtigungen mit dem zu abonnieren.

```
aws sns subscribe --topic-arn arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers --
protocol email --notification-endpoint YourUserName@YourDomainName.ext
```

Um EC2-Benachrichtigungen zu abonnieren, verwenden Sie AWS Tools for Windows PowerShell

Verwenden Sie den folgenden Befehl AWS Tools for Windows PowerShell, um EC2-Benachrichtigungen mit zu abonnieren.

```
Connect-SNSNotification -TopicArn 'arn:aws:sns:us-east-1:801119661308:ec2-windows-
drivers' -Protocol email -Region us-east-1 -Endpoint 'YourUserName@YourDomainName.ext'
```

Konfigurieren Ihrer Windows-Instance

Nachdem Sie eine Windows-Instanz gestartet haben, können Sie sich als Administrator anmelden, um zusätzliche Konfigurationen für Launch-Agents und Windows-spezifische Funktionen vorzunehmen. Die folgenden Themen konzentrieren sich auf die Konfiguration von Windows-Instanzen.

Inhalt

- Verwenden Sie Amazon Elastic Graphics-Beschleuniger auf Windows-Instances
- Installieren des WSL auf Ihrer Windows-Instance

Starteinstellungen für Amazon EC2 EC2-Windows-Instances konfigurieren

Amazon EC2 EC2-Start-Agenten führen Aufgaben während des Instance-Starts aus und werden ausgeführt, wenn eine Instance gestoppt und später gestartet oder neu gestartet wird. Informationen zu einem bestimmten Agenten finden Sie auf den Detailseiten in der folgenden Liste.

- Konfigurieren einer Windows-Instance mithilfe von EC2Launch v2
- Konfigurieren einer Windows-Instance mithilfe von EC2Launch
- Konfigurieren Sie eine Windows-Instanz mithilfe des EC2Config-Dienstes (Legacy)

Inhalt

Amazon EC2 Launch Agents vergleichen

Die folgende Tabelle zeigt die wichtigsten funktionalen Unterschiede zwischen EC2Config, EC2Launch v1 und EC2Launch v2.

Feature	EC2Config	EC2Launch v1	EC2Launch v2
Run as (Ausführen als)	Windows Service	PowerShell Skripte	Windows Service
Unterstützt	Nur Legacy-Betriebssysteme	Windows 2016 Windows 2019 (LTSC und SAC)	Windows 2016 Windows 2019 (LTSC und SAC) Windows 2022
Konfigurationsdatei	XML	XML	YAML

Feature	EC2Config	EC2Launch v1	EC2Launch v2
Festgelegter Administratorbenutzername	Nein	Nein	Ja
Größe der Benutzerdaten	16 KB	16 KB	60 KB (komprimiert)
Erstellung lokaler Benutzereigen auf AMI	Nein	Nein	Ja, konfigurierbar.
Aufgabenkonfiguration in Benutzerdaten	Nein	Nein	Ja
Konfigurierbares Hintergrundbild	Nein	Nein	Ja
Reihenfolge der Aufgabenausführung anpassen	Nein	Nein	Ja
Konfigurierbare Aufgaben	15	9	20 bei Start
Unterstützt Windows Event Viewer	Ja	Nein	Ja
Anzahl der Event Viewer-Ereignistypen	2	0	30

Note

Die EC2Config-Dokumentation dient nur als historische Referenz. Die Betriebssystemversionen, auf denen es ausgeführt wird, werden von Microsoft nicht mehr unterstützt. Wir empfehlen dringend, auf den neuesten Startdienst zu aktualisieren.

Konfigurieren Sie das DNS-Suffix für Windows-Startagenten

Mit Amazon EC2 Launch Agents können Sie eine Liste von DNS-Suffixen konfigurieren, die Windows-Instances für die Auflösung von Domainnamen verwenden. Die Launch-Agents überschreiben die Windows-Standardeinstellungen im `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` Registrierungsschlüssel, indem sie der DNS-Suffix-Suffix-Suchliste die folgenden Werte hinzufügen:

- Die Domäne der Instanz
- Die Suffixe, die sich aus der Dezentralisierung der Instanzdomäne ergeben
- NV-Domäne
- Die von den einzelnen Netzwerkschnittstellenkarten angegebenen Domänen

Alle Launch-Agents unterstützen die DNS-Suffixkonfiguration. Weitere Informationen finden Sie in Ihrer spezifischen Launch Agent-Version:

- Informationen zur `setDnsSuffix` Aufgabe und zur Konfiguration von DNS-Suffixen in EC2Launch v2 finden Sie unter. setDnsSuffix
- Informationen zur Einrichtung der DNS-Suffixliste und zur Aktivierung oder Deaktivierung der Dezentralisierung für EC2Launch v1 finden Sie unter. Konfigurieren von EC2Launch
- Informationen zur Einrichtung einer DNS-Suffixliste und zur Aktivierung oder Deaktivierung der Dezentralisierung für EC2Config finden Sie unter. EC2Config-Einstellungsdateien

Dezentralisierung von Domainnamen

Die Dezentralisierung von Domänennamen ist ein Active Directory-Verhalten, das es Computern in einer untergeordneten Domäne ermöglicht, auf Ressourcen in der übergeordneten Domäne zuzugreifen, ohne einen vollqualifizierten Domänennamen zu verwenden. Standardmäßig wird die Übertragung von Domänennamen so lange fortgesetzt, bis nur noch zwei Knoten in der Reihenfolge des Domänennamens übrig sind.

Wenn die Instance mit einer Domain verbunden ist, führen die Start-Agents eine Dezentralisierung des Domainnamens durch und fügen die Ergebnisse der DNS-Suffix-Suchliste hinzu, die **`System\CurrentControlSet\Services\Tcpip\Parameters\SearchList`**im Registrierungsschlüssel verwaltet wird. Die Agents verwenden die Einstellungen der folgenden Registrierungsschlüssel, um das Dezentralisierungsverhalten zu bestimmen.

- **`System\CurrentControlSet\Services\Tcpip\Parameters\UseDomainNameDevolution`**
  - Wenn nicht festgelegt, wird die Dezentralisierung deaktiviert
  - Wenn auf gesetzt`1`, wird die Dezentralisierung aktiviert (Standard)
  - Wenn auf gesetzt, wird die `0` Dezentralisierung deaktiviert
- **`System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel`**
  - Wenn nicht gesetzt, verwenden Sie die Stufe von `2` (Standard)
  - Wenn der Wert auf `3` oder höher gesetzt ist, verwenden Sie den Wert, um den Wert festzulegen

Wenn Sie die Dezentralisierung deaktivieren oder Ihre Dezentralisierungseinstellungen auf eine höhere Ebene ändern, enthält der `System\CurrentControlSet\Services\Tcpip\Parameters\SearchList` Registrierungsschlüssel immer noch die Suffixe, die zuvor hinzugefügt wurden. Sie werden nicht automatisch entfernt. Sie können die Liste manuell aktualisieren, oder Sie können die Liste löschen und Ihren Agenten den Vorgang zur Einrichtung der neuen Liste durchführen lassen.

> **Note**
>
> Um die DNS-Suffixliste aus der Registrierung zu löschen, können Sie den folgenden Befehl ausführen.
>
> ```
> PS C:\> Invoke-CimMethod -ClassName Win32_NetworkAdapterConfiguration -
> MethodName "SetDNSSuffixSearchOrder" -Arguments @{ DNSDomainSuffixSearchOrder =
>  $null } | Out-Null
> ```

Beispiele für Dezentralisierung

Die folgenden Beispiele zeigen die Entwicklung von Domainnamen während des Dezentralisierungsprozesses.

`corp.example.com`

- Fortschreitet fort zu `example.com`

`locale.region.corp.example.com`

1. Geht weiter zu `region.corp.example.com`
2. Geht weiter zu `corp.example.com`
3. Geht weiter zu `example.com`

`locale.region.corp.example.com`mit einer Einstellung von `DomainNameDevolutionLevel=3`

1. Geht weiter zu `region.corp.example.com`
2. Geht weiter zu. `corp.example.com` Der Fortschritt hört hier aufgrund der Leveleinstellung auf.

Konfigurieren einer Windows-Instance mithilfe von EC2Launch v2

Alle unterstützten Instances von Amazon EC2, auf denen Windows Server 2022 ausgeführt wird, enthalten standardmäßig den EC2Launch v2 Launch Agent (`EC2Launch.exe`). Darüber hinaus bieten wir AMIs für Windows Server 2016 und 2019 an, bei denen EC2Launch v2 als Standard-Launch-Agent installiert ist. Diese AMIs werden zusätzlich zu den AMIs für Windows Server 2016 und 2019 bereitgestellt, die EC2Launch v1 enthalten. Sie können nach Windows-AMIs suchen, die standardmäßig EC2Launch v2 enthalten, indem Sie in der Suche auf der Seite AMIs in der Amazon-EC2-Konsole das folgende Präfix eingeben: `EC2LaunchV2-Windows_Server-*`.

EC2Launch v2 ist ein Service, der während des Instance-Startups Aufgaben ausführt und ausgeführt wird, wenn eine Instance gestoppt und später gestartet oder neu gestartet wird. Außerdem kann EC2Launch v2 nach Bedarf Aufgaben ausführen. Einige dieser Aufgaben sind automatisch aktiviert, während andere manuell aktiviert werden müssen. Der EC2Launch v2-Service unterstützt alle Features von EC2Config und EC2Launch.

Dieser Service verwendet eine Konfigurationsdatei zur Steuerung seines Betriebs. Sie können die Konfigurationsdatei entweder mit einem grafischen Tool aktualisieren oder direkt als einzelne .yml-Datei (`agent-config.yml`) bearbeiten. Die Binärdateien des Services befinden sich im `%ProgramFiles%\Amazon\EC2Launch`-Verzeichnis.

EC2Launch v2 veröffentlicht Windows-Ereignisprotokolle, um Ihnen bei der Fehlerbehebung und beim Festlegen von Auslösern zu helfen. Weitere Informationen finden Sie unter Windows-Ereignisprotokolle.

Unterstützte Betriebssysteme

- Windows Server 2022
- Windows Server 2019 (Langzeitwartungskanal und halbjährlicher Kanal)
- Windows Server 2016

Inhalt des EC2Launch v2-Abschnitts

- Überblick über EC2Launch v2
- Installieren der neuesten Version von EC2Launch v2
- Migrieren zu EC2Launch v2
- Beenden, Neustarten, Löschen oder Deinstallieren von EC2Launch v2
- Abonnement von EC2Launch v2-Servicebenachrichtigungen
- Einstellungen für EC2Launch v2
- Fehlersuche bei EC2Launch v2
- EC2Launch v2-Versionsverläufe

Überblick über EC2Launch v2

EC2Launch v2 ist ein Service, der während des Instance-Startups Aufgaben ausführt und ausgeführt wird, wenn eine Instance gestoppt und später gestartet oder neu gestartet wird.

Übersichtsthemen

- Konzepte für EC2Launch v2
- EC2Launch v2-Aufgaben
- Telemetrie

Einen Vergleich der Funktionen der Launch Agent-Version finden Sie unterAmazon EC2 Launch Agents vergleichen.

Konzepte für EC2Launch v2

Die folgenden Konzepte sind nützlich für die Verwendung von EC2Launch v2.

Aufgabe

Sie können eine Aufgabe aufrufen, um eine Aktion für eine Instance durchzuführen. Sie können Aufgaben in der `agent-config.yml`-Datei oder über Benutzerdaten konfigurieren. Eine Liste der verfügbaren Aufgaben für EC2Launch v2 finden Sie unter EC2Launch v2-Aufgaben. Schemata und Einzelheiten zur Aufgabenkonfiguration finden Sie unter Aufgabenkonfiguration in EC2Launch v2.

Stufe

Eine Stufe ist eine logische Gruppierung von Aufgaben, die vom EC2Launch-v2-Agenten ausgeführt werden. Einige Aufgaben können nur in einer bestimmten Phase ausgeführt werden. Andere können in mehreren Phasen ausgeführt werden. Bei der Verwendung von `agent-config.yml` müssen Sie eine Liste von Stufen und eine Liste von Aufgaben angeben, die innerhalb jeder Stufe ausgeführt werden sollen.

Der Service führt die Phasen in der folgenden Reihenfolge aus:

Phase 1: Boot

Phase 2: Netzwerk

Stufe 3: PreReady

Windows ist bereit

Nach Abschluss der PreReady Phase sendet der Service die `Windows is ready` Nachricht an die Amazon EC2 EC2-Konsole.

Stufe 4: PostReady

Benutzerdaten werden während der PostReadyPhase ausgeführt. Einige Skriptversionen werden vor der `agent-config.yml` PostReadyDateiphase ausgeführt, andere danach, und zwar wie folgt:

Vor `agent-config.yml`

- YAML-Benutzerdaten-Version 1.1
- XML-Benutzerdaten

Nach `agent-config.yml`

- YAML-Benutzerdatenversion 1.0 (Legacy-Version für Abwärtskompatibilität)

Beispiele für Phasen und Aufgaben finden Sie unter Beispiel: `agent-config.yml`.

Wenn Sie Benutzerdaten verwenden, müssen Sie eine Liste von Aufgaben angeben, die der Startagent ausführen soll. Die Phase ist impliziert. Beispiele für Aufgaben finden Sie unter Beispiel: Benutzerdaten.

EC2Launch v2 führt die Liste der Aufgaben in der Reihenfolge aus, die Sie in `agent-config.yml` und in den Benutzerdaten angeben. Die Phasen werden der Reihe nach ausgeführt. Die nächste Phase beginnt, nachdem die vorherige Phase abgeschlossen ist. Aufgaben werden nacheinander ausgeführt.

Häufigkeit

Die Frequenz der Aufgaben bestimmt, wann Aufgaben ausgeführt werden sollen, abhängig vom Startkontext. Die meisten Aufgaben haben nur eine zulässige Frequenz. Sie können eine Frequenz für `executeScript`-Aufgaben festlegen.

Sie können die folgenden Frequenzen in der Aufgabenkonfiguration in EC2Launch v2 anzeigen.

- Einmal – Die Aufgabe wird einmal ausgeführt, wenn das AMI zum ersten Mal gestartet wurde (Sysprep abgeschlossen).
- Immer – Die Aufgabe wird jedes Mal ausgeführt, wenn der Startagent ausgeführt wird. Der Launch-Agent wird ausgeführt, wenn:
  - eine Instance startet oder neu startet
  - der EC2Launch-Service läuft
  - `EC2Launch.exe run` wird aufgerufen

agent-config

`agent-config` ist eine Datei, die sich im Konfigurationsordner für EC2Launch v2 befindet. Es umfasst die Konfiguration für den Start, das Netzwerk und die PostReady Stufen. PreReady Diese Datei wird verwendet, um die Instance-Konfiguration für Aufgaben festzulegen, die beim ersten oder späteren Start des AMI ausgeführt werden sollen.

Standardmäßig wird bei der EC2Launch v2-Installation eine `agent-config`-Datei installiert, die empfohlene Konfigurationen enthält, die in Standard-Amazon-Windows-AMIs verwendet werden. Sie können die Konfigurationsdatei aktualisieren, um die Standardstartumgebung für Ihr AMI zu ändern, die EC2Launch v2 angibt.

Benutzerdaten

Benutzerdaten sind Daten, die beim Starten einer Instance konfiguriert werden können. Sie können Benutzerdaten aktualisieren, um dynamisch zu ändern, wie benutzerdefinierte AMIs oder Schnellstart-AMIs konfiguriert werden. EC2Launch-v2-unterstützt eine Eingabelänge von 60 KB. Benutzerdaten enthalten nur den UserData Stagingbereich und werden daher nach der `agent-config` Datei ausgeführt. Sie können Benutzerdaten eingeben, wenn Sie eine Instance mit dem Launch Instance Wizard starten oder Sie können Benutzerdaten über die EC2-Konsole ändern. Weitere Informationen zum Arbeiten mit Benutzerdaten finden Sie unter So verarbeitet Amazon EC2 Benutzerdaten für Windows-Instances.

EC2Launch v2-Aufgaben

EC2Launch v2 kann bei jedem Start die folgenden Aufgaben ausführen:

- Einrichten eines neuen und optional angepassten Hintergrundbildes, das Informationen über die Instance wiedergibt.
- Festlegen der Attribute für das Administratorkonto, das auf dem lokalen Computer erstellt wird.
- Hinzufügen von DNS-Suffixen zur Liste der Suffixe. Nur Suffixe, die noch nicht vorhanden sind, werden der Liste hinzugefügt.
- Festlegen von Laufwerkbuchstaben für zusätzliche Volumes und deren Erweiterung, um den verfügbaren Speicherplatz zu nutzen.
- Schreiben Sie Dateien aus der Konfiguration auf die Festplatte.
- Führt die in der EC2Launch v2-Konfigurationsdatei angegebenen Skripts aus oder von. `user-data` Skripten von `user-data` können Klartext oder gezippt sein und im Base64-Format bereitgestellt werden.
- Führen Sie ein Programm mit angegebenen Argumenten aus.
- Erstellen des Computer-Namens.
- Senden von Instance-Informationen an die Amazon EC2-Konsole.
- Senden Sie den Fingerabdruck des RDP-Zertifikats an die Amazon-EC2-Konsole.
- Erweiterung der Betriebssystempartition, um den gesamten nicht partitionierten Speicherplatz mit einzuschließen.
- Führen Sie Benutzerdaten aus. Weitere Informationen zur Angabe von Benutzerdaten finden Sie unter Aufgabenkonfiguration in EC2Launch v2.
- Legen Sie nicht-persistente statische Routen fest, um den Metadatendienst und die AWS KMS - Server zu erreichen.

- Setzen Sie Partitionen, die keine Startpartitionen sind, auf oder. `mbr` `gpt`
- Starten Sie den Systems-Manager-Service nach Sysprep.
- Optimieren der ENA-Einstellungen.
- Aktivieren von OpenSSH für spätere Windows-Versionen.
- Aktivieren von Jumbo-Frames.
- Einstellen von Sysprep so ein, dass es mit EC2Launch v2 ausgeführt wird.
- Veröffentlichen von Windows-Ereignisprotokollen.

Telemetrie

Bei Telemetrie handelt es sich AWS um zusätzliche Informationen, die Ihnen helfen, Ihre Anforderungen besser zu verstehen, Probleme zu diagnostizieren und Funktionen bereitzustellen, mit denen Sie Ihr Benutzererlebnis verbessern können. AWS-Services

EC2Launch v2-Version `2.0.592` und später sammeln Telemetrie, wie Nutzungsmetriken und Fehler. Diese Daten werden von der Amazon-EC2-Instance erfasst, auf der EC2Launch v2 ausgeführt wird. Dies schließt alle Windows-AMIs ein, die Eigentum von AWS.

EC2Launch v2 bietet folgende Telemetrie-Typen:

- Nutzungsinformationen – Agent-Befehle, Installationsmethode und geplante Ausführungsfrequenz.
- Fehler und Diagnoseinformationen — Fehlercodes bei der Agenteninstallation, Ausführungsfehlercodes und Aufruf-Stacks für Fehler.

Beispiele für die gesammelten Daten:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

Die Telemetrie ist standardmäßig aktiviert. Sie können die Telemetriesammlung jederzeit deaktivieren. Wenn Telemetrie aktiviert ist, sendet EC2Launch v2 Telemetriedaten ohne zusätzliche Kundenbenachrichtigungen.

Telemetrie-Sichtbarkeit

Wenn die Telemetrie aktiviert ist, wird sie in der Amazon-EC2-Konsolenausgabe wie folgt angezeigt.

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Deaktivieren der Telemetrie auf einer Instance

Um die Telemetrie für eine einzelne Instance zu deaktivieren, können Sie entweder eine Systemumgebungsvariable festlegen oder die Installation mit dem MSI ändern.

Um Telemetrie durch Festlegen einer Systemumgebungsvariablen zu deaktivieren, führen Sie den folgenden Befehl als Administrator aus.

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Um die Telemetrie mithilfe der MSI zu deaktivieren, führen Sie den folgenden Befehl aus, nachdem Sie die MSI-Datei herunterladen.

```
msiexec /i ".\AmazonEC2Launch.msi" Remove="Telemetry" /q
```

Installieren der neuesten Version von EC2Launch v2

Sie können eine der folgenden Methoden verwenden, um den EC2Launch v2-Agenten auf Ihrer EC2-Instance zu installieren:

- Laden Sie den Agenten von Amazon S3 herunter und installieren Sie ihn mit Windows PowerShell. Download-URLs finden Sie unter EC2Launch v2 kann auf Amazon S3 heruntergeladen werden.
- Installation mit SSM-Distributor.
- Installation von einer EC2-Image-Builder-Komponente.
- Starten Sie Ihre Instance über ein AMI, auf dem EC2Launch v2 vorinstalliert ist.

> **Warning**
>
> AmazonEC2Launch.msi deinstalliert frühere Versionen der EC2-Startservices, z. B. EC2Launch (v1) oder EC2Config.

Wählen Sie für die Installationsschritte die Registerkarte aus, die Ihrer bevorzugten Methode entspricht.

Windows PowerShell

Gehen Sie folgendermaßen vor, um die neueste Version des EC2Launch v2-Agents mit Windows PowerShell zu installieren.

1. Erstellen Sie Ihr lokales Verzeichnis.

```
New-Item -Path "$env:USERPROFILE\Desktop\EC2Launchv2" -ItemType Directory
```

2. Legen Sie die URL für Ihren Download-Speicherort fest. Führen Sie den folgenden Befehl mit der von Ihnen verwendeten Amazon-S3-URL aus. Download-URLs finden Sie unter EC2Launch v2 kann auf Amazon S3 heruntergeladen werden

```
$Url = "Amazon S3 URL/AmazonEC2Launch.msi"
```

3. Verwenden Sie den folgenden zusammengesetzten Befehl, um den Agenten herunterzuladen und die Installation auszuführen

```
$DownloadFile = "$env:USERPROFILE\Desktop\EC2Launchv2\" + $(Split-Path -Path
 $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadFile
msiexec /i "$DownloadFile"
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```

4. Um die Installation zu überprüfen, stellen Sie sicher, dass die MSI-Datei im EC2Launch v2-Verzeichnis auf Ihrer Instance vorhanden ist (`C:\ProgramData\Amazon\EC2Launch`).

AWS Systems Manager Distributor

Informationen zur Konfiguration automatischer Updates für EC2Launch v2 mit AWS Systems Manager Quick Setup finden Sie unter. Automatische Installation und Aktualisierung mit Distributor Quick Setup

Sie können das `AWSEC2Launch-Agent` Paket auch einmalig über den Distributor installieren. AWS Systems Manager Anweisungen zum Installieren eines Pakets vom Systems Manager Distributor finden Sie unter Installieren oder Aktualisieren von Paketen im AWS Systems Manager -Benutzerhandbuch.

EC2 Image Builder component

Sie können die Komponente `ec2launch-v2-windows` installieren, wenn Sie ein benutzerdefiniertes Image mit EC2 Image Builder erstellen. Anweisungen zum Erstellen eines benutzerdefinierten Image mit EC2 Image Builder finden Sie unterErstellen einer Image-Pipeline mithilfe des EC2-Image-Builder-Konsolenassistenten im Benutzerhandbuch für EC2 Image Builder.

AMI

EC2Launch v2 ist standardmäßig auf den folgenden AMIs von Windows Server 2022 und UEFI vorinstalliert:

- Windows_Server-2022-English-Full-Base
- Windows_Server-2022-English-Core-Base
- AMIs mit Windows Server 2022 mit allen anderen Sprachen
- AMIs mit Windows Server 2022 mit installiertem SQL
- Windows_Server-2022-English-Core-EKS_Optimized

EC2Launch v2 ist ebenfalls auf den folgenden Windows-Server-AMIs vorinstalliert. Sie können diese AMIs über die Amazon-EC2-Konsole oder mithilfe des folgenden Suchpräfixes finden: `EC2LaunchV2-` in der AWS CLI.

- EC2LaunchV2-Windows_Server-2019-English-Core-Base
- EC2LaunchV2-Windows_Server-2019-English-Full-Base
- EC2LaunchV2-Windows_Server-2016-English-Core-Base
- EC2LaunchV2-Windows_Server-2016-English-Full-Base
- EC2LaunchV2-Windows_Server-2012_R2_RTM-English-Full-Base

- EC2LaunchV2-Windows_Server-2012_RTM-English-Full-Base

Installieren und aktualisieren Sie EC2Launch v2 automatisch mit AWS Systems Manager Distributor Quick Setup

Mit AWS Systems Manager Distributor Quick Setup können Sie automatische Updates für EC2Launch v2 einrichten. Der folgende Prozess richtet eine Systems Manager Association auf Ihrer Instance ein, die den EC2Launch v2-Agenten automatisch mit einer von Ihnen angegebenen Frequenz aktualisiert. Die Zuordnung, die der Distributor Quick Setup erstellt, kann Instances innerhalb einer AWS-Konto UND-Region oder Instances innerhalb einer AWS Organisation umfassen. Weitere Informationen zum Einrichten einer Organisation finden Sie unter Tutorial: Organisation erstellen und konfigurieren im AWS Organizations Benutzerhandbuch.

Bevor Sie beginnen, stellen Sie sicher, dass Ihre Instanzen alle Voraussetzungen erfüllen.

Voraussetzungen

Um automatische Updates mit Distributor Quick Setup einzurichten, müssen Ihre Instances die folgenden Voraussetzungen erfüllen.

- Sie haben mindestens eine laufende Instance, die EC2Launch v2 unterstützt. Weitere Informationen finden Sie unter Unterstützte Betriebssysteme. EC2Launch v2
- Sie haben die Systems Manager Manager-Setup-Aufgaben auf Ihren Instances ausgeführt. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Systems Manager einrichten.
- EC2Launch v2 muss der einzige Launch-Agent sein, der auf Ihrer Instance installiert ist. Wenn Sie mehr als einen Launch-Agent installiert haben, schlägt die Quick-Setup-Konfiguration Ihres Distributors fehl. Bevor Sie EC2Launch v2 mit einem Distributor Quick Setup konfigurieren, deinstallieren Sie EC2Config- oder EC2Launch v1-Launch-Agents, falls vorhanden.

Konfigurieren Sie das Distributor Quick Setup für EC2Launch v2

Um eine Konfiguration für EC2Launch v2 mit Distributor Quick Setup zu erstellen, verwenden Sie die folgenden Einstellungen, wenn Sie die Schritte für die Bereitstellung des Distributor-Pakets abschließen:

- Softwarepakete: Amazon EC2Launch v2-Agent.
- Aktualisierungshäufigkeit: Wählen Sie eine Frequenz aus der Liste aus.

- Ziele: Wählen Sie aus den verfügbaren Bereitstellungsoptionen.

Um den Status Ihrer Konfiguration zu überprüfen, navigieren Sie zur Registerkarte Systems Manager Quick Setup Configurations in der AWS Management Console.

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Quick Setup aus.
3. Wählen Sie auf der Registerkarte Konfigurationen die Zeile aus, die der von Ihnen erstellten Konfiguration zugeordnet ist. Die Registerkarte Konfigurationen listet Ihre Konfigurationen auf und enthält eine Zusammenfassung der wichtigsten Details wie Region, Bereitstellungsstatus und Zuordnungsstatus.

   > **Note**
   >
   > Der Zuordnungsname für jede EC2Launch v2-Verteilerkonfiguration beginnt mit dem folgenden Präfix:. `AWS-QuickSetup-Distributor-EC2Launch-Agent-`

4. Um Details anzuzeigen, wählen Sie die Konfiguration aus und klicken Sie auf Details anzeigen.

Weitere Informationen und Schritte zur Fehlerbehebung finden Sie im AWS Systems Manager Benutzerhandbuch unter Problembehandlung bei Ergebnissen der Schnellinstallation.

EC2Launch v2 kann auf Amazon S3 heruntergeladen werden

Um die neueste Version von EC2Launch v2 zu installieren, laden Sie das Installationsprogramm von einem der folgenden Speicherorte herunter:

> **Note**
>
> Der 32-Bit-Installationslink wird veraltet sein. Wir empfehlen Ihnen, den 64-Bit-Installationslink für die Installation von EC2Launch v2 zu verwenden. Wenn Sie einen 32-Bit-Launch-Agenten benötigen, verwenden Sie EC2Config.

- 64Bit — https://s3.amazonaws.com/amazon-ec2launch-v2/windows/amd64/latest/AmazonEC2Launch.msi

- 32Bit — https://s3.amazonaws.com/amazon-ec2launch-v2/windows/386/latest/AmazonEC2Launch.msi

Installationsoptionen konfigurieren

Wenn Sie EC2Launch v2 installieren oder aktualisieren, können Sie Installationsoptionen mit dem Installationsdialogfeld von EC2Launch v2 oder mit dem msiexec-Befehl in einer Befehlszeilen-Shell konfigurieren.

Wenn das EC2Launch-v2-Installationsprogramm zum ersten Mal auf einer Instance ausgeführt wird, initialisiert es die Einstellungen des Startagenten auf Ihrer Instance wie folgt:

- Es erstellt den lokalen Pfad und schreibt die Datei des Startagenten dorthin. Dies wird manchmal als Neuinstallation bezeichnet.
- Es erstellt die Umgebungsvariable `EC2LAUNCH_TELEMETRY`, sofern diese noch nicht vorhanden ist, und legt sie basierend auf Ihrer Konfiguration fest.

Wählen Sie für Konfigurationsdetails die Registerkarte aus, die der von Ihnen verwendeten Konfigurationsmethode entspricht.

Amazon EC2Launch Setup dialog

Wenn Sie EC2Launch v2 installieren oder aktualisieren, können Sie die folgenden Installationsoptionen über den EC2Launch-v2-Installationsdialog konfigurieren.

Optionen der Grundlegende Installation

Telemetrie senden

Wenn Sie dieses Feature in den Einrichtungsdialog aufnehmen, legt das Installationsprogramm die Umgebungsvariable `EC2LAUNCH_TELEMETRY` auf einen Wert von 1 fest. Wenn Sie Telemetrie senden deaktivieren, legt das Installationsprogramm die Umgebungsvariable auf den Wert `0` fest.

Wenn der EC2Launch-v2-Agent ausgeführt wird, liest er die Umgebungsvariable `EC2LAUNCH_TELEMETRY`, um festzustellen, ob Telemetriedaten hochgeladen werden sollen. Wenn der Wert gleich 1 ist, werden die Daten hochgeladen. Andernfalls wird der Upload nicht durchgeführt.

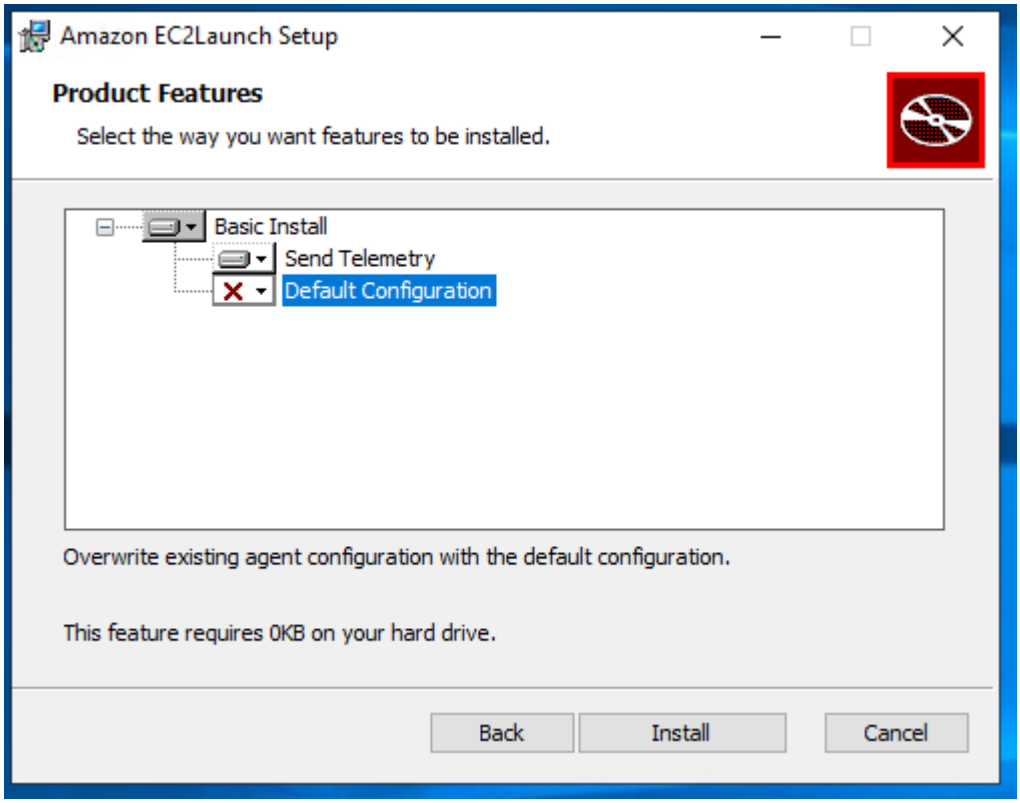
Standardkonfiguration

Die Standardkonfiguration für EC2Launch v2 besteht darin, den lokalen Startagenten zu überschreiben, falls dieser bereits vorhanden ist. Wenn Sie zum ersten Mal eine Installation auf einer Instance ausführen, wird in der Standardkonfiguration eine Neuinstallation durchgeführt. Wenn Sie die Standardkonfiguration bei der Erstinstallation deaktivieren, schlägt die Installation fehl.

Wenn Sie die Installation auf der Instance erneut ausführen, können Sie die Standardkonfiguration deaktivieren, um ein Upgrade durchzuführen, bei dem die `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`-Datei nicht ersetzt wird.

Beispiel: Upgrade von EC2Launch v2 mit Telemetrie

Das folgende Beispiel zeigt das EC2Launch-v2-Einrichtungsdialog, das zum Aktualisieren der aktuellen Installation und zum Aktivieren der Telemetrie konfiguriert ist. Diese Konfiguration führt eine Installation durch, ohne die Agent-Konfigurationsdatei zu ersetzen, und legt die Umgebungsvariable `EC2LAUNCH_TELEMETRY` auf den Wert 1 fest.



Command line

Wenn Sie EC2Launch v2 installieren oder aktualisieren, können Sie die folgenden Installationsoptionen mit dem msiexec-Befehl in einer Befehlszeilen-Shell konfigurieren.

`ADDLOCAL`-Parameterwerte

Grundlegend (erforderlich)

Installieren Sie den Start-Agenten. Wenn dieser Wert im `ADDLOCAL`-Parameter nicht vorhanden ist, wird die Installation beendet.

Bereinigen

Wenn Sie den `Clean`-Wert in den `ADDLOCAL`-Parameter einbeziehen, schreibt das Installationsprogramm die Agent-Konfigurationsdatei an den folgenden Speicherort: `%ProgramData%/Amazon/EC2Launch/config/agent-config.yml`. Wenn die Agent-Konfigurationsdatei bereits vorhanden ist, wird die Datei überschrieben.

Wenn Sie den `Clean`-Wert im `ADDLOCAL`-Parameter weglassen, führt das Installationsprogramm ein Upgrade durch, das die Agent-Konfigurationsdatei nicht ersetzt.

Telemetrie

Wenn Sie den `Telemetry`-Wert in den `ADDLOCAL`-Parameter einbeziehen, legt das Installationsprogramm die Umgebungsvariable `EC2LAUNCH_TELEMETRY` auf den Wert `1` fest.

Wenn Sie den `Telemetry`-Wert in den `ADDLOCAL`-Parameter einbeziehen, legt das Installationsprogramm die Umgebungsvariable auf den Wert `0` fest.

Wenn der EC2Launch-v2-Agent ausgeführt wird, liest er die Umgebungsvariable `EC2LAUNCH_TELEMETRY`, um festzustellen, ob Telemetriedaten hochgeladen werden sollen. Wenn der Wert gleich `1` ist, werden die Daten hochgeladen. Andernfalls wird der Upload nicht durchgeführt.

Beispiel: EC2Launch v2 mit Telemetrie installieren

```
& msiexec /i "C:\Users\Administrator\Desktop\EC2Launchv2\AmazonEC2Launch.msi"
 ADDLOCAL="Basic,Clean,Telemetry" /q
```

Prüfen der Version EC2Launch v2

Überprüfen Sie mithilfe eines der folgenden Verfahren, welche Version von EC2Launch v2 in Ihren Instances installiert ist.

Windows PowerShell

Überprüfen Sie die installierte Version von EC2Launch v2 mit Windows wie PowerShell folgt.

1. Starten Sie eine Instance von Ihrem AMI und stellen Sie eine Verbindung damit her.
2. Führen Sie den folgenden Befehl aus PowerShell , um die installierte Version von EC2Launch v2 zu überprüfen:

```
& "C:\Program Files\Amazon\EC2Launch\EC2Launch.exe" version
```

Windows Control Panel

Überprüfen Sie die installierte Version von EC2Launch v2 in der Windows-Systemsteuerung wie folgt.

1. Starten Sie eine Instance von Ihrem AMI und stellen Sie eine Verbindung damit her.
2. Öffnen Sie die Windows-Systemsteuerung und wählen Sie Programme und Features.
3. Suchen Sie in der Liste mit den installierten Programmen nach `Amazon EC2Launch`. Die Versionsnummer wird in der Spalte Version angegeben.

Die neuesten Updates für die AWS Windows-AMIs finden Sie im Windows AMI-Versionsverlauf in der AWS Windows AMI-Referenz.

Die neueste Version von EC2Launch v2 finden Sie unter EC2Launch v2-Versionsverlauf.

Die neueste Version des EC2Launch-v2-Migrationstools finden Sie unter Versionshistorie des EC2Launch v2-Migrationstools.

Sie können benachrichtigt werden, wenn neue Versionen des EC2Launch v2-Services veröffentlicht werden. Weitere Informationen finden Sie unter Abonnement von EC2Launch v2-Servicebenachrichtigungen.

Migrieren zu EC2Launch v2

Das EC2Launch-Migrationstool aktualisiert den installierten Startagenten (EC2Config und EC2Launch v1), indem es ihn deinstalliert und EC2Launch v2 installiert. Anwendbare Konfigurationen aus früheren Startservices werden automatisch zu dem neuen Service migriert. Das Migrationstool erkennt keine geplanten Aufgaben, die mit EC2Launch-v1-Skripten verknüpft sind. Daher richtet es diese Aufgaben in EC2Launch v2 nicht automatisch ein. Um diese Aufgaben zu konfigurieren, bearbeiten Sie die `agent-config.yml`-Datei oder verwenden Sie das EC2Launch v2-Einstellungsdialogfeld. Wenn eine Instance beispielsweise eine geplante Aufgabe umfasst, die `InitializeDisks.ps1` ausführt, müssen Sie nach dem Ausführen des Migrationstools die Volumes angeben, die Sie im Einstellungsdialogfeld von EC2Launch v2 initialisieren möchten. Siehe Schritt 6 des Verfahrens zu Ändern der Einstellungen mithilfe des Dialogfelds für EC2Launch v2-Einstellungen.

Sie können das Migrationstool herunterladen oder mit einem RunCommand SSM-Dokument installieren.

Sie können das Tool von den folgenden Speicherorten herunterladen:

> **Note**
>
> Der Link zum 32-Bit-Migrationstool wird veraltet sein. Wir empfehlen Ihnen, den 64-Bit-Link für die Migration auf EC2Launch v2 zu verwenden. Wenn Sie einen 32-Bit-Launch-Agenten benötigen, verwenden Sie EC2Config.

- 64 Bit — https://s3.amazonaws.com/amazon-ec2launch-v2-utils/ MigrationTool /windows/amd64/ latest/EC2 Tool.zip LaunchMigration
- 32 Bit — https://s3.amazonaws.com/amazon-ec2launch-v2-utils/ MigrationTool /windows/386/ latest/EC2 Tool.zip LaunchMigration

> **Note**
>
> Sie müssen das Migrationstool EC2Launch v2 als Administrator ausführen. EC2Launch v2 wird nach dem Ausführen des Migrationstools als Dienst installiert. Es läuft nicht sofort. Standardmäßig wird es während des Startups der Instance ausgeführt und wird ausgeführt, wenn eine Instance gestoppt und später gestartet oder neu gestartet wird.

Verwenden Sie das AWSEC2Launch-RunMigration-SSM-Dokument, um mit SSM Run Command zur neuesten EC2Launch-v2-Version zu migrieren. Für das Dokument sind keine Parameter erforderlich. Weitere Informationen zur Verwendung von SSM Run Command finden Sie unter AWS Systems Manager Run Command.

Das Migrationstool wendet die folgenden Konfigurationen von EC2Config auf EC2Launch v2 an.

- Wenn `Ec2DynamicBootVolumeSize` auf `false` eingestellt ist, wird die `boot`-Phase von EC2Launch v2 entfernt
- Wenn `Ec2SetPassword` auf `Enabled` eingestellt ist, wird der Passworttyp von EC2Launch v2 auf `random` festgelegt
- Wenn `Ec2SetPassword` auf `Disabled` eingestellt ist, wird der Passworttyp von EC2Launch v2 auf `donothing` festgelegt
- Wenn `SetDnsSuffixList` auf `false` eingestellt ist, wird die `setDnsSuffix`-Aufgabe von EC2Launch v2 entfernt
- Wenn `EC2SetComputerName` auf „true“ gesetzt ist, wird die `setHostName`-Aufgabe von EC2Launch v2 zur `yaml`-Konfiguration hinzugefügt

Das Migrationstool wendet die folgenden Konfigurationen von EC2Launch v1 auf EC2Launch v2 an.

- Wenn `ExtendBootVolumeSize` auf `false` eingestellt ist, wird die `boot`-Phase von EC2Launch v2 entfernt
- Wenn `AdminPasswordType` auf `Random` eingestellt ist, wird der Passworttyp von EC2Launch v2 auf `random` festgelegt
- Wenn `AdminPasswordType` auf `Specify` eingestellt ist, werden der Passworttyp von EC2Launch v2 auf `static` und die Passwortdaten auf das in `AdminPassword` angegebene Passwort festgelegt
- Wenn `SetWallpaper` auf `false` eingestellt ist, wird die `setWallpaper`-Aufgabe von EC2Launch v2 entfernt
- Wenn `AddDnsSuffixList` auf `false` eingestellt ist, wird die `setDnsSuffix`-Aufgabe von EC2Launch v2 entfernt
- Wenn `SetComputerName` auf `true` eingestellt ist, wird die `setHostName`-Aufgabe von EC2Launch v2 hinzugefügt

Beenden, Neustarten, Löschen oder Deinstallieren von EC2Launch v2

Sie können den EC2Launch v2-Service genauso verwalten wie jeden anderen Windows-Service.

EC2Launch v2 wird beim Booten einmal ausgeführt und führt alle konfigurierten Aufgaben aus. Nach dem Ausführen der Aufgaben wechselt der Service in einen angehaltenen Zustand. Wenn Sie den Service erneut starten, führt der Service alle konfigurierten Aufgaben erneut aus und kehrt in einen angehaltenen Status zurück.

Um aktualisierte Einstellungen auf Ihrer Instance anzuwenden, können Sie den Service beenden und neu starten. Wenn Sie EC2Launch v2 manuell installieren, müssen Sie zuerst den Service beenden.

So halten Sie den EC2Launch v2-Dienst an:

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Wählen Sie im Menü Start die Option Administrative Tools (Verwaltungstools) und öffnen Sie dann Services.
3. Klicken Sie in der Liste der Services mit der rechten Maustaste auf Amazon EC2Launch und wählen Sie Stop (Beenden).

So starten Sie den EC2Launch v2-Dienst erneut:

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Wählen Sie im Menü Start die Option Administrative Tools (Verwaltungstools) und öffnen Sie dann Services.
3. Klicken Sie in der Liste der Services mit der rechten Maustaste auf Amazon EC2Launch und wählen Sie Restart (Neu starten).

Wenn Sie weder die Konfigurationseinstellungen aktualisieren, Ihr eigenes AMI erstellen oder AWS Systems Manager verwenden müssen, können Sie den Service löschen und deinstallieren. Durch das Löschen eines Services wird der Registrierungsunterschlüssel entfernt. Durch die Deinstallation eines Services werden die Dateien, der Registrierungsunterschlüssel und alle Shortcuts zum Service entfernt.

So löschen Sie den EC2Launch v2-Dienst:

1. Öffnen Sie ein Befehlszeilenfenster.
2. Führen Sie den folgenden Befehl aus:

```
sc delete EC2Launch
```

So deinstallieren Sie EC2Launch v2:

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Wählen Sie im Start-Menü die Option Control Panel (Systemsteuerung).
3. Öffnen Sie Programs (Programme) und dann Programs and Features (Programme und Features).
4. Wählen Sie in der Liste der Programme Amazon EC2Launch. Um zu bestätigen, dass Sie v2 wählen, überprüfen Sie die Spalte Version.
5. Wählen Sie Deinstallieren.

Abonnement von EC2Launch v2-Servicebenachrichtigungen

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen des EC2Launch v2-Services veröffentlicht werden. Führen Sie die folgenden Schritte durch, um diese Benachrichtigungen zu abonnieren.

Abonnement von EC2Launch v2-Benachrichtigungen

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die Amazon SNS SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, da die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region erstellt wurden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld „Create subscription (Abonnement erstellen)“ Folgendes aus:
   a. Verwenden Sie für Topic ARN (Themen-ARN) den folgenden Amazon-Ressourcennamen (ARN): arn:aws:sns:us-east- 1:309726204594:amazon-ec2launch-v2.
   b. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
   c. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.

d. Wählen Sie Create subscription.

6. Sie erhalten eine E-Mail-Nachricht, in der Sie aufgefordert werden, Ihr Abonnement zu bestätigen. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Sobald eine neue Version des EC2Launch v2-Services veröffentlicht wird, senden wir den Abonnenten Benachrichtigungen. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

1. Öffnen Sie die Amazon SNS-Konsole.
2. Wählen Sie im Navigationsbereich Subscriptions aus.
3. Wählen Sie das Abonnement und dann Actions (Aktionen), Delete subscriptions (Abonnements löschen) aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Einstellungen für EC2Launch v2

Dieser Abschnitt enthält Informationen zum Konfigurieren von Einstellungen für EC2Launch v2.

Zu den Themen gehören:

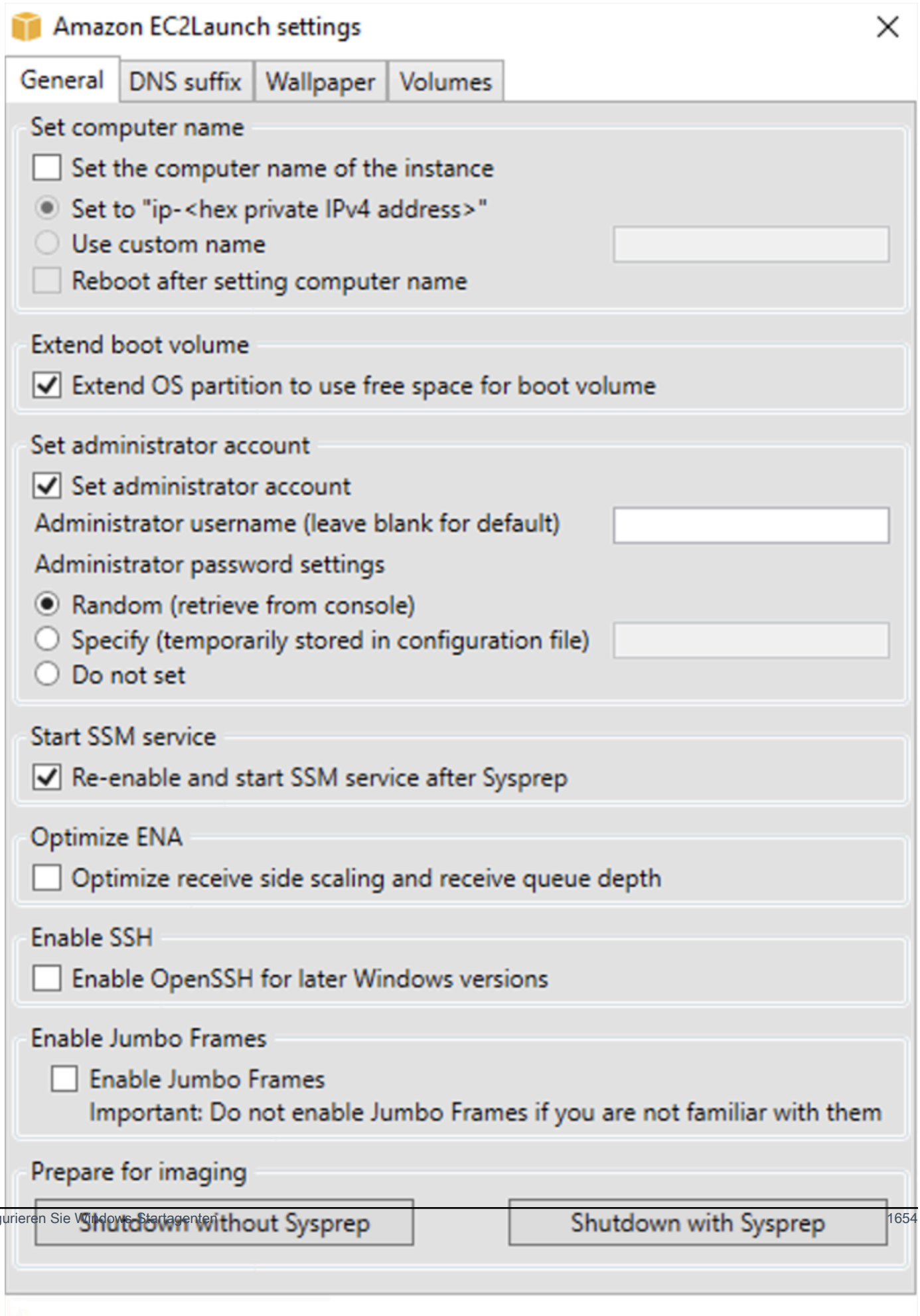
- Ändern der Einstellungen mithilfe des Dialogfelds für EC2Launch v2-Einstellungen
- EC2Launch v2-Verzeichnisstruktur
- Konfigurieren von EC2Launch v2 mit der CLI
- Aufgabenkonfiguration in EC2Launch v2
- Exit-Codes und Neustarts für EC2Launch v2
- EC2Launch v2 und Sysprep

Ändern der Einstellungen mithilfe des Dialogfelds für EC2Launch v2-Einstellungen

Der folgende Vorgang beschreibt, wie die Einstellungen anhand des Dialogfelds für EC2Launch v2-Einstellungen aktiviert bzw. deaktiviert werden.

> **Note**
>
> Wenn Sie benutzerdefinierte Aufgaben in der Datei agent-config.yml falsch konfigurieren und versuchen, das Dialogfeld mit den Amazon-EC2Launch-Einstellungen zu öffnen, erhalten Sie eine Fehlermeldung. Ein Beispielschema finden Sie unter Beispiel: `agent-config.yml`.

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Wählen Sie im Startmenü All Programs (Alle Programme) und navigieren Sie zu den EC2Launch settings (Einstellungen).


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Set computer name
Set the computer name of the instance
Set to "ip-<hex private IPv4 address>"
Use custom name
Reboot after setting computer name
Extend boot volume
Extend OS partition to use free space for boot volume
Set administrator account
Set administrator account
Administrator username (leave blank for default)
Administrator password settings
Random (retrieve from console)
Specify (temporarily stored in configuration file)
Do not set
Start SSM service
Re-enable and start SSM service after Sysprep
Optimize ENA
Optimize receive side scaling and receive queue depth
Enable SSH
Enable OpenSSH for later Windows versions
Enable Jumbo Frames
Enable Jumbo Frames
Important: Do not enable Jumbo Frames if you are not familiar with them
Prepare for imaging
Shutdown without Sysprep
Shutdown with Sysprep

3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte General (Allgemeines) im Dialogfeld EC2Launch Service Properties (EC2Launch-Service-Eigenschaften) die folgenden Einstellungen.

   a. Set Computer Name

      Wenn diese Einstellung aktiviert ist (standardmäßig deaktiviert), wird der aktuelle Hostname bei jedem Start mit dem gewünschten Host-Namen verglichen. Wenn die Host-Namen nicht übereinstimmen, wird der Host-Name zurückgesetzt, und das System wird optional neu gestartet, um den neuen Host-Namen aufzunehmen. Wenn kein benutzerdefinierter Host-Name angegeben wird, wird er mit der hexadezimalformatierten privaten IPv4-Adresse generiert, beispielsweise `ip-AC1F4E6`. Um zu verhindern, dass Ihr bestehender Hostname geändert wird, aktivieren Sie diese Einstellung nicht.

   b. Extend Boot Volume (Erweitern des Start-Volumes)

      Diese Einstellung erweitert Festplatte `Disk 0`/`Volume 0` dynamisch so, dass der gesamte nicht partitionierte Speicherplatz eingeschlossen ist. Dies ist nützlich, wenn die Instance von einem Root-Gerät-Volume gestartet wird, das eine benutzerdefinierte Größe besitzt.

   c. Set Administrator Account (Festlegen des Administratorkontos)

      Wenn diese Option aktiviert ist, können Sie die Attribute „Username (Benutzername)“ und „Password (Passwort)“ für das Administratorkonto festlegen, das auf Ihrem lokalen Computer erstellt wird. Wenn dieses Feature nicht aktiviert ist, wird auf dem System nach Sysprep kein Administratorkonto erstellt. Geben Sie in `adminPassword` nur dann ein Passwort an, wenn `adminPasswordtype` `Specify` ist.

      Die Passworttypen sind wie folgt definiert:

      i. `Random`

         EC2Launch generiert ein Passwort und verschlüsselt es mit dem Schlüssel des Benutzers: Die Einstellung wird vom System nach dem Start der Instance deaktiviert, so dass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.

      ii. `Specify`

         EC2Launch verwendet das Passwort, das Sie unter `adminPassword` angeben. Wenn das Passwort nicht den Systemanforderungen entspricht, erstellt EC2Launch stattdessen ein zufälliges Passwort. Das Passwort wird in `agent-config.yml` im

Klartext gespeichert und gelöscht, wenn Sysprep das Administratorpasswort einstellt. EC2Launch verschlüsselt das Passwort mit dem Schlüssel des Benutzers.

iii. `Do not set`

EC2Launch verwendet das Passwort, das Sie in der Datei unattend.xml angeben. Wenn Sie in der Datei unattend.xml kein Passwort angeben, ist das Administratorkonto deaktiviert.

d. Start SSM Service (Starten des SSM-Services)

Wenn diese Option ausgewählt ist, wird der Systems Manager Dienst aktiviert, um nach Sysprep zu starten. EC2Launch v2 führt alle zuvor beschriebenen Aufgaben aus und SSM Agent verarbeitet Anforderungen für Systems Manager-Funktionen wie Run Command und Statusmanager.

Sie können über Run Command Ihre vorhandenen Instances upgraden, damit diese die aktuelle Version des EC2Launch v2-Service und von SSM Agent verwenden. Weitere Informationen erhalten Sie unter Aktualisieren von SSM Agent mit Run Command im AWS Systems Manager-Benutzerhandbuch.

e. Optimize ENA (Optimieren von ENA)

Wenn diese Option ausgewählt ist, werden die ENA-Einstellungen so konfiguriert, dass die ENA-Einstellungen für AWS Receive Side Scaling und Receive Queue Depth optimiert sind. Weitere Informationen finden Sie unter Konfigurieren von RSS-CPU-Affinität.

f. Enable SSH (Aktivieren von SSH)

Diese Einstellung aktiviert OpenSSH für spätere Windows-Versionen, um die Remote-Systemverwaltung zu ermöglichen.

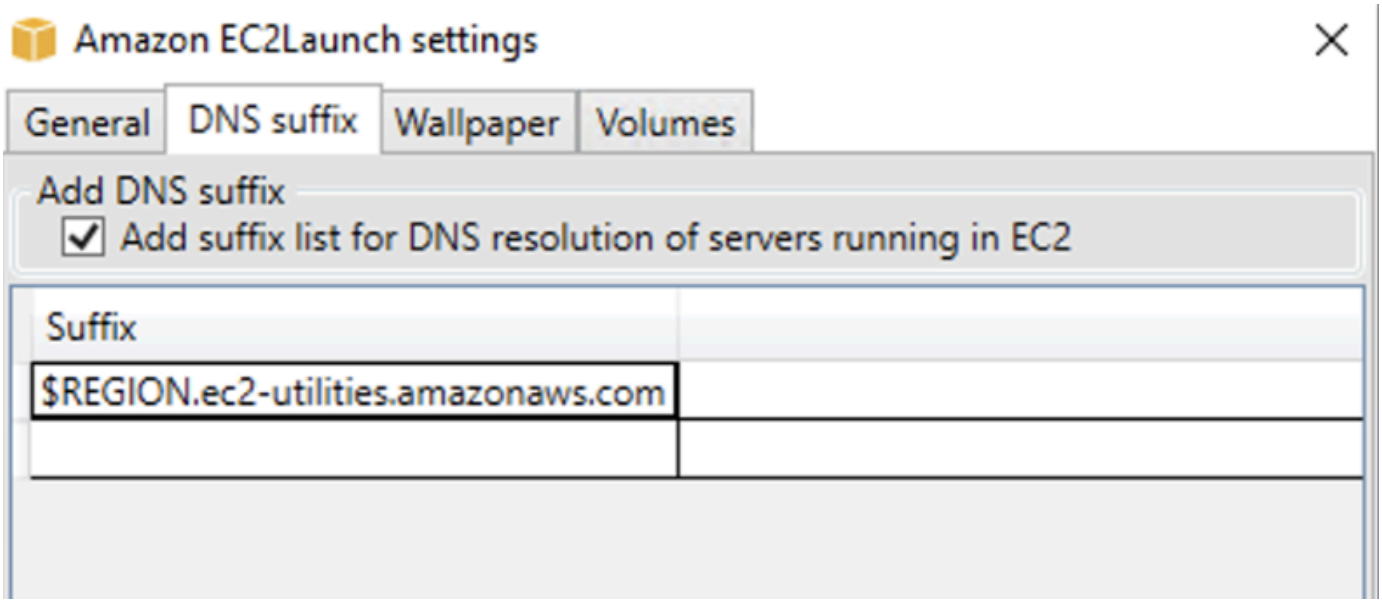
g. Enable Jumbo Frames (Aktivieren von Jumbo Frames)

Wählen Sie diese Option aus, um Jumbo Frames zu aktivieren. Jumbo Frames können unbeabsichtigte Auswirkungen auf Ihre Netzwerkkommunikation haben. Stellen Sie also sicher, dass Sie wissen, wie sich Jumbo Frames auf Ihr System auswirken, bevor Sie diese aktivieren. Weitere Informationen zu Jumbo Frames finden Sie unter Jumbo-Frames (9001 MTU).

h. Prepare for Imaging (Vorbereitung zum Imaging)

Wählen Sie aus, ob Ihre EC2-Instance mit oder ohne Sysprep heruntergefahren werden soll. Wenn Sie Sysprep mit EC2Launch v2 ausführen möchten, wählen Sie Shutdown with Sysprep (Mit Sysprep herunterfahren).

4. Auf der Registerkarte DNS Suffix (DNS-Suffix) können Sie auswählen, ob Sie eine DNS-Suffixliste für die DNS-Auflösung von Servern mit EC2 hinzufügen möchten, ohne den vollqualifizierten Domain-Namen anzugeben. DNS-Suffixe können die Variablen `$REGION` und `$AZ` enthalten. Nur Suffixe, die noch nicht vorhanden sind, werden der Liste hinzugefügt.



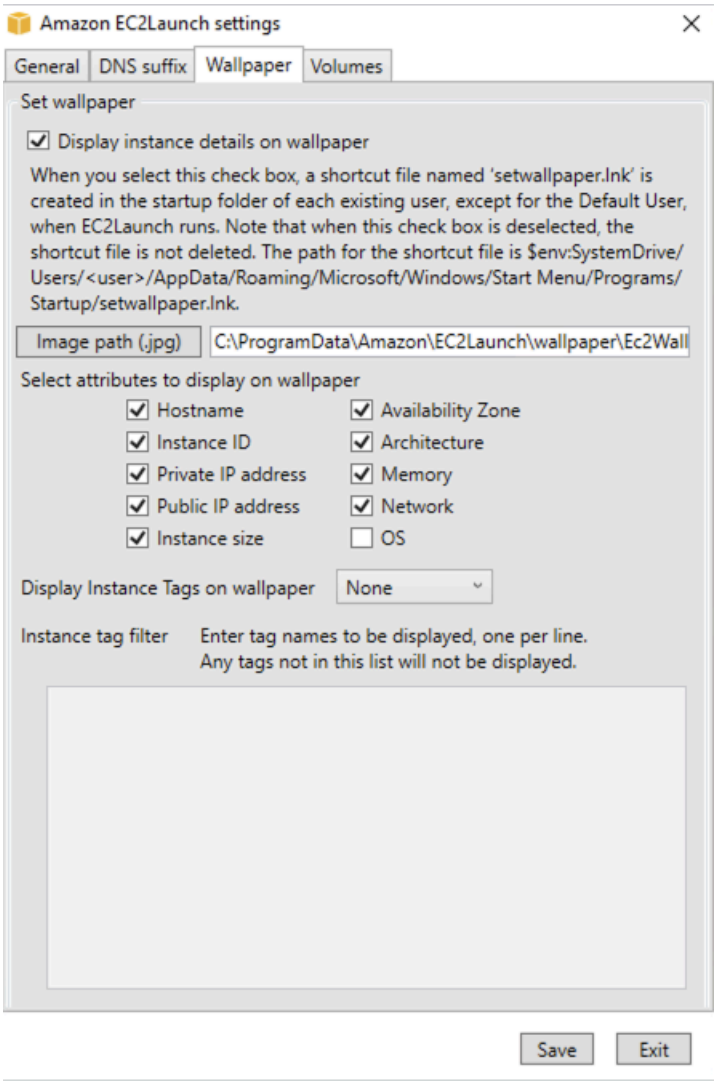
5. Auf der Registerkarte Hintergrundbild können Sie Ihr Instance-Hintergrundbild mit einem Hintergrundbild konfigurieren und Instance-Details für das anzuzeigende Hintergrundbild angeben. Amazon EC2 generiert die Details bei jeder Anmeldung.

   Sie können Ihr Hintergrundbild mit den folgenden Steuerelementen konfigurieren.

   - Instance-Details auf dem Hintergrundbild anzeigen – Dieses Kontrollkästchen aktiviert oder deaktiviert die Anzeige von Instance-Details auf dem Hintergrundbild.
   - Image-Pfad (.jpg) – Geben Sie den Pfad zu dem Image an, das als Hintergrundhintergrund verwendet werden soll.
   - Auf Hintergrund anzuzeigende Attribute auswählen – Aktivieren Sie die Kontrollkästchen für die Instance-Details, die auf dem Hintergrund angezeigt werden sollen. Deaktivieren Sie die Kontrollkästchen für zuvor ausgewählte Instance-Details, die Sie aus dem Hintergrundbild entfernen möchten.
   - Instance-Tags auf Hintergrundbild anzeigen – Wählen Sie eine der folgenden Einstellungen aus, um Instance-Tags auf dem Hintergrundbild anzuzeigen:

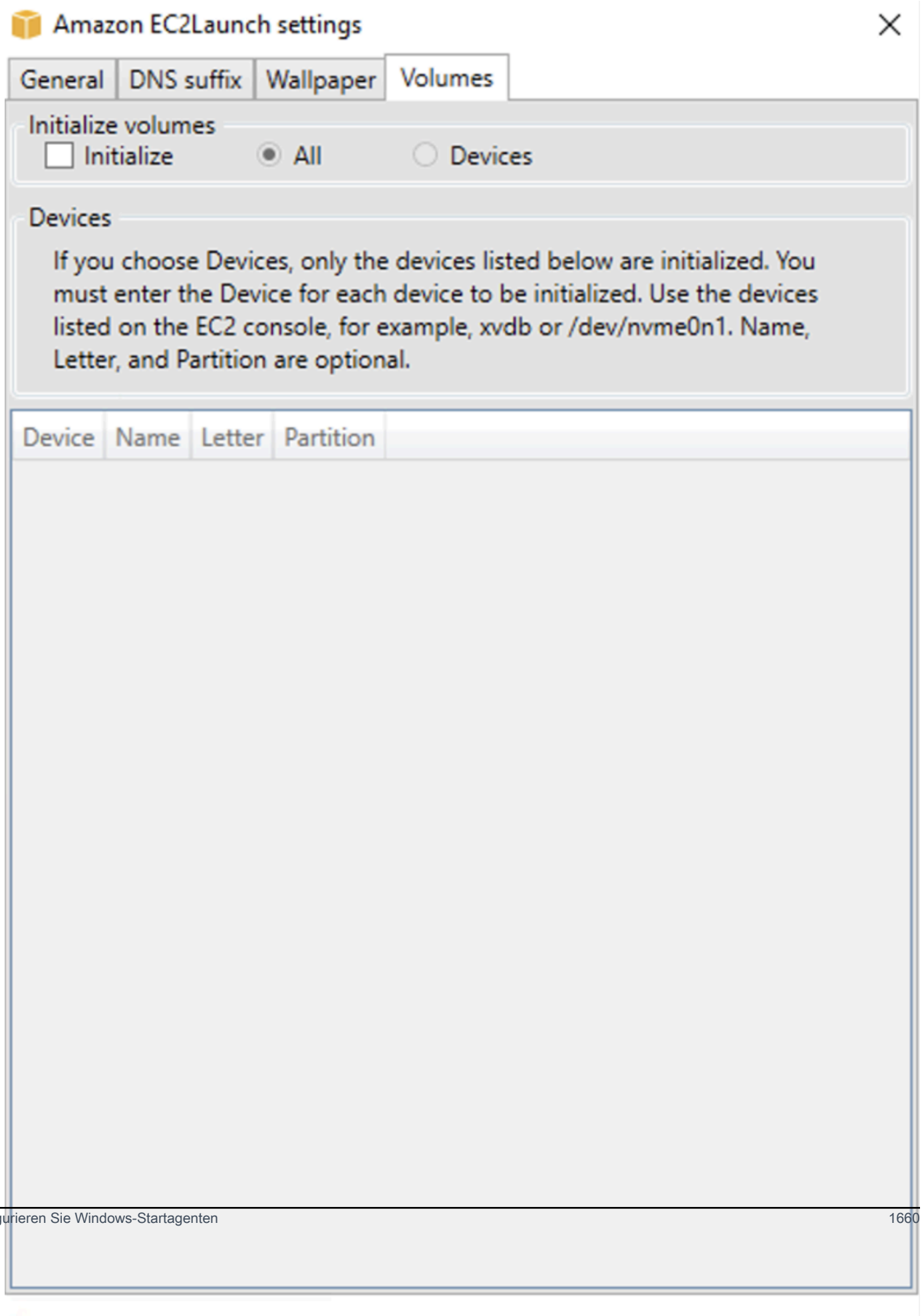
- Keine – Keine Instance-Tags auf dem Hintergrundbild anzeigen.
- Alles anzeigen – Alle Instance-Tags auf dem Hintergrund anzeigen.
- Gefiltert anzeigen – Angegebene Instance-Tags auf dem Hintergrundbild anzeigen. Wenn Sie diese Einstellung wählen, können Sie die Instance-Tags, die Sie auf Ihrem Hintergrundbild anzeigen möchten, zum Feld Instance-Tag-Filter hinzufügem.

> **Note**
>
> Sie müssen Tags in Metadaten aktivieren, um Tags auf dem Hintergrundbild anzuzeigen. Weitere Informationen zu Instance-Tags und Metadaten finden Sie unter Arbeiten mit Instance-Tags in Instance-Metadaten.



6. Wählen Sie auf der Registerkarte Volumes aus, ob Sie die Volumes initialisieren möchten, die der Instance angefügt sind. Durch die Aktivierung werden Laufwerkbuchstaben für zusätzliche Volumes festgelegt und diese erweitert, um verfügbaren Speicherplatz zu nutzen. Wenn Sie All (Alle) auswählen, werden alle Speicher-Volumes initialisiert. Wenn Sie Devices (Geräte) auswählen, werden nur Geräte initialisiert, die in der Liste angegeben sind. Sie müssen jedes zu initialisierende Gerät eingeben. Verwenden Sie beispielsweise die Geräte, die auf der EC2-Konsole aufgeführt sind, `xvdb` oder `/dev/nvme0n1`. In der Dropdown-Liste werden die Speicher-Volumes angezeigt, die der Instance zugeordnet sind. Um ein Gerät einzugeben, das nicht an die Instance angefügt ist, geben Sie es in das Textfeld ein.

   Name, Letter (Buchstabe) und Partition sind optionale Felder. Wenn kein Wert für Partition angegeben ist, werden Speichervolumes, die größer als 2 TB sind, mit dem `gpt` Partitionstyp initialisiert, und Speichervolumes, die kleiner als 2 TB sind, werden mit dem `mbr` Partitionstyp initialisiert. Wenn Geräte konfiguriert sind und ein Nicht-NTFS-Gerät entweder eine Partitionstabelle enthält oder die ersten 4 KB des Datenträgers Daten enthalten, wird der Datenträger übersprungen und die Aktion protokolliert.


Amazon EC2Launch settings
General
DNS suffix
Wallpaper
Volumes
Initialize volumes
Initialize
All
Devices
Devices
If you choose Devices, only the devices listed below are initialized. You must enter the Device for each device to be initialized. Use the devices listed on the EC2 console, for example, xvdb or /dev/nvme0n1. Name, Letter, and Partition are optional.
Device
Name
Letter
Partition

Nachfolgend finden Sie ein Beispiel für eine YAML-Konfigurationsdatei, die aus den Einstellungen erstellt wurde, die im EC2Launch-Dialog eingegeben wurden.

```
version: 1.0
config:
  - stage: boot
 tasks:
      - task: extendRootPartition
  - stage: preReady
    tasks:
      - task: activateWindows
        inputs:
          activation:
            type: amazon
      - task: setDnsSuffix
        inputs:
          suffixes:
            - $REGION.ec2-utilities.amazonaws.com
      - task: setAdminAccount
        inputs:
          password:
            type: random
      - task: setWallpaper
        inputs:
          path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
          attributes:
            - hostName
            - instanceId
            - privateIpAddress
            - publicIpAddress
            - instanceSize
            - availabilityZone
            - architecture
            - memory
            - network
  - stage: postReady
    tasks:
      - task: startSsm
```

EC2Launch v2-Verzeichnisstruktur

EC2Launch v2 sollte in den folgenden Verzeichnissen installiert werden:

- Service-Binärdateien: `%ProgramFiles%\Amazon\EC2Launch`
- Servicedaten (Einstellungen, Protokolldateien und Statusdateien): `%ProgramData%\Amazon\EC2Launch`

> **Note**
>
> Windows blendet Dateien und Ordner unter `C:\ProgramData` standardmäßig aus. Um die EC2Launch v2-Verzeichnisse und -Dateien anzuzeigen, müssen Sie entweder den Pfad im Windows Explorer eingeben oder die Ordnereigenschaften so ändern, dass ausgeblendete Dateien und Ordner angezeigt werden.

Das `%ProgramFiles%\Amazon\EC2Launch`-Verzeichnis enthält Binärdateien und unterstützende Bibliotheken. Es enthält die folgenden Unterverzeichnisse:

- `settings`
  - `EC2LaunchSettingsUI.exe` — Benutzeroberfläche zum Ändern der `agent-config.yml`-Datei
  - `YamlDotNet.dll` — DLL zur Unterstützung einiger Operationen der Benutzeroberfläche
- `tools`
  - `ebsnvme-id.exe` — Werkzeug zum Überprüfen der Metadaten der EBS-Volumes auf der Instance
  - `AWSAcpiSpcrReader.exe` — Werkzeug zur Bestimmung des korrekten zu verwendenden COM-Ports
  - `EC2LaunchEventMessage.dll` — DLL zur Unterstützung der Windows-Ereignisprotokollierung für EC2Launch.
- `service`
  - `EC2LaunchService.exe` — Ausführbare Windows-Dienstdatei, die gestartet wird, wenn der Launch-Agent als Dienst ausgeführt wird.
- `EC2Launch.exe` — zentrale ausführbare EC2Launch-Datei
- `EC2LaunchAgentAttribution.txt` — Zuweisung für Code, der innerhalb von EC2 Launch verwendet wird

Das Verzeichnis `%ProgramData%\Amazon\EC2Launch` enthält die folgenden Unterverzeichnisse. Alle von dem Service erzeugten Daten, einschließlich Protokolle, Konfiguration und Status, werden in diesem Verzeichnis gespeichert.

- `config` — Konfiguration

  Die Servicekonfigurationsdatei wird in diesem Verzeichnis als `agent-config.yml` gespeichert. Diese Datei kann aktualisiert werden, um Standardaufgaben zu ändern, hinzuzufügen oder zu entfernen, die von dem Service ausgeführt werden. Die Berechtigung zum Erstellen von Dateien in diesem Verzeichnis ist auf das Administratorkonto beschränkt, um die Eskalation von Berechtigungen zu verhindern.
- `log` — Instance-Protokolle

  Protokolle für den Service (`agent.log`), die Konsole (`console.log`), die Leistung (`bench.log`) und Fehler (`error.log`) werden in diesem Verzeichnis gespeichert. Protokolldateien werden bei nachfolgenden Ausführungen des Services angehängt.
- `state` — Servicestatusdaten

  Hier wird der Status gespeichert, mit dem der Service ermittelt wird, welche Aufgaben ausgeführt werden sollen. Es gibt eine `.run-once`-Datei, die angibt, ob der Service bereits nach Sysprep ausgeführt wurde (so dass Aufgaben mit der Häufigkeit "einmal" bei der nächsten Ausführung übersprungen werden). Dieses Unterverzeichnis enthält ein `state.json` und `previous-state.json`, um den Status jeder Aufgabe zu verfolgen.
- `sysprep` — Sysprep

  Dieses Verzeichnis enthält Dateien, die verwendet werden, um zu bestimmen, welche Operationen von Sysprep ausgeführt werden sollen, wenn ein angepasstes Windows-AMI erstellt wird, das wiederverwendet werden kann.

Konfigurieren von EC2Launch v2 mit der CLI

Sie können die Befehlszeilenschnittstelle (CLI) verwenden, um Ihre EC2Launch-Einstellungen zu konfigurieren und den Service zu verwalten. Der folgende Abschnitt enthält Beschreibungen und Verwendungsinformationen für die CLI-Befehle, die Sie zum Verwalten von EC2Launch v2 verwenden können.

Befehle

- collect-logs

- get-agent-config
- list-Volumes
- reset
- run
- Status
- sysprep
- validieren
- version
- Hintergrundbild

collect-logs

Erfasst Protokolldateien für EC2Launch, komprimiert die Dateien und speichert sie in einem angegebenen Verzeichnis.

Beispiel

```
ec2launch collect-logs -o C:\Mylogs.zip
```

Usage

`ec2launch collect-logs [flags]`

Flags

`-h, --help`

Hilfe für `collect-logs`

`-o, --output string`

Pfad zu komprimierten Ausgabe-Protokolldateien

get-agent-config

Druckt `agent-config.yml` im angegebenen Format (JSON oder YAML). Wenn kein Format angegeben ist, wird `agent-config.yml` in dem zuvor angegebenen Format gedruckt.

Beispiel

```
ec2launch get-agent-config -f json
```

Beispiel 2

Die folgenden PowerShell Befehle zeigen, wie die `agent-config` Datei im JSON-Format bearbeitet und gespeichert wird.

```
$config = & "$env:ProgramFiles/Amazon/EC2Launch/EC2Launch.exe" --format json |
 ConvertFrom-Json
$jumboFrame =@"
{
   "task": "enableJumboFrames"
}
"@
$config.config | %{if($_.stage -eq 'postReady'){$_.tasks += (ConvertFrom-Json -
InputObject $jumboFrame)}}
$config | ConvertTo-Json -Depth 6 | Out-File -encoding UTF8
$env:ProgramData/Amazon/EC2Launch/config/agent-config.yml
```

Usage

`ec2launch get-agent-config [flags]`

Flags

`-h`, `--help`

Hilfe für `get-agent-config`

`-f`, `--format string`

Ausgabeformat der `agent-config`-Datei: `json`, `yaml`

list-Volumes

Listet alle Speicher-Volumes auf, die der Instance zugeordnet sind, einschließlich flüchtiger und EBS-Volumes.

Beispiel

```
ec2launch list-volumes
```

Usage

`ec2launch list-volumes`

Flags

`-h, --help`

Hilfe für `list-volumes`

reset

Das Hauptziel dieser Aufgabe besteht darin, den Agenten für die nächste Ausführung zurückzusetzen. Dazu löscht der reset-Befehl alle Statusdaten des Agenten für EC2Launch v2 aus dem lokalen `EC2Launch`-Verzeichnis (weitere Informationen unter EC2Launch v2-Verzeichnisstruktur). Beim Zurücksetzen werden optional die Service- und Sysprep-Protokolle gelöscht.

Das Verhalten des Skripts hängt davon ab, in welchem Modus der Agent die Skripte ausführt – inline oder getrennt.

Inline (Standard)

Der EC2Launch-v2-Agent führt die Skripte nacheinander aus (`detach: false`). Dies ist die Standardeinstellung.

> **Note**
>
> Wenn Ihr Inline-Skript einen reset- oder sysprep-Befehl ausgibt, wird es sofort ausgeführt und setzt den Agenten zurück. Die aktuelle Aufgabe wird beendet, dann wird der Agent heruntergefahren, ohne weitere Aufgaben auszuführen.
> Wenn beispielsweise auf die Aufgabe, die den Befehl ausgibt, eine `startSsm`-Aufgabe folgen würde (die standardmäßig nach der Ausführung der Benutzerdaten enthalten ist), wird die Aufgabe nicht ausgeführt und der Systems-Manager-Service nicht gestartet.

Detached (Getrennt)

Der EC2Launch-v2-Agent führt Skripte gleichzeitig mit anderen Aufgaben aus (`detach: true`).

> **Note**
>
> Wenn Ihr abgetrenntes Skript einen reset- oder sysprep-Befehl ausgibt, warten diese Befehle, bis der Agent fertig ist, bevor sie ausgeführt werden. Aufgaben nach dem executeScript werden weiterhin ausgeführt.

Beispiel

```
ec2launch reset -c
```

Usage

`ec2launch reset [flags]`

Flags

`-c`, `--clean`

bereinigt Instance-Protokolle vor `reset`

`-h`, `--help`

Hilfe für `reset`

run

Führt EC2Launch v2 aus.

Beispiel

```
ec2launch run
```

Usage

`ec2launch run [flags]`

Flags

`-h`, `--help`

Hilfe für `run`

Status

Ruft den Status eines EC2Launch-v2-Agents ab. Blockiert optional den Prozess, bis der Agent beendet ist. Der Prozess-Beendigungscode bestimmt den Agentenstatus:

- `0` – der Agent wurde ausgeführt und war erfolgreich.
- `1` – der Agent wurde ausgeführt und ist fehlgeschlagen.
- `2` – der Agent wird noch ausgeführt.
- `3` – der Agent befindet sich in einem unbekannten Status. Der Agentenstatus wird nicht ausgeführt oder ist beendet.
- `4` – beim Versuch, den Agentenstatus abzurufen, ist ein Fehler aufgetreten.
- `5` – der Agent wird nicht ausgeführt und der Status der letzten bekannten Ausführung ist unbekannt. Dies könnte eines der folgenden bedeuten:
  - Sowohl `state.json` und `previous-state.json` werden gelöscht.
  - `previous-state.json` ist beschädigt.

  Dies ist der Agentenstatus nach dem Ausführen des `reset`-Befehls.

Beispiel:

```
ec2launch status -b
```

Usage

`ec2launch status [flags]`

Flags

`-b,--block`

blockiert den Prozess, bis die Ausführung des Agenten beendet ist

`-h,--help`

Hilfe für `status`

sysprep

Das Hauptziel dieser Aufgabe besteht darin, den Agenten für die nächste Ausführung zurückzusetzen. Dazu setzt der sysprep-Befehl den Agentenstatus zurück, aktualisiert die `unattend.xml`-Datei, deaktiviert RDP und führt Sysprep aus.

Das Verhalten des Skripts hängt davon ab, in welchem Modus der Agent die Skripte ausführt – inline oder getrennt.

Inline (Standard)

Der EC2Launch-v2-Agent führt die Skripte nacheinander aus (`detach: false`). Dies ist die Standardeinstellung.

> **Note**
>
> Wenn Ihr Inline-Skript einen reset- oder sysprep-Befehl ausgibt, wird es sofort ausgeführt und setzt den Agenten zurück. Die aktuelle Aufgabe wird beendet, dann wird der Agent heruntergefahren, ohne weitere Aufgaben auszuführen.
> Wenn beispielsweise auf die Aufgabe, die den Befehl ausgibt, eine `startSsm`-Aufgabe folgen würde (die standardmäßig nach der Ausführung der Benutzerdaten enthalten ist), wird die Aufgabe nicht ausgeführt und der Systems-Manager-Service nicht gestartet.

Detached (Getrennt)

Der EC2Launch-v2-Agent führt Skripte gleichzeitig mit anderen Aufgaben aus (`detach: true`).

> **Note**
>
> Wenn Ihr abgetrenntes Skript einen reset- oder sysprep-Befehl ausgibt, warten diese Befehle, bis der Agent fertig ist, bevor sie ausgeführt werden. Aufgaben nach dem executeScript werden weiterhin ausgeführt.

Beispiel:

```
ec2launch sysprep
```

Usage

```
ec2launch sysprep [flags]
```

Flags

`-c,--clean`

bereinigt Instance-Protokolle vor `sysprep`

`-h,--help`

Hilfe für Sysprep

`-s,--shutdown`

fährt die Instance nach `sysprep` herunter

validieren

Validiert die `agent-config`-Datei `C:\ProgramData\Amazon\EC2Launch\config\agent-config.yml`.

Beispiel

```
ec2launch validate
```

Usage

```
ec2launch validate [flags]
```

Flags

`-h , --help`

Hilfe für `validate`

version

Ruft die ausführbare Version ab.

Beispiel

```
ec2launch version
```

Usage

`ec2launch version [flags]`

Flags

`-h`, `--help`

Hilfe für `version`

Hintergrundbild

Legt das bereitgestellte Hintergrundbild für den Hintergrundbildpfad fest (JPG-Datei) und zeigt die ausgewählten Instance-Details an.

Syntax

```
ec2launch wallpaper ^
--path="C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg" ^
--all-tags ^
--
attributes=hostName,instanceId,privateIpAddress,publicIpAddress,instanceSize,availabilityZone,a
```

Eingaben

Parameter

--allowed-tags [***`tag-name-1`***, ***`tag-name-n`***]

(Optional) Base64-codiertes JSON-Array von Instance-Tag-Namen zur Anzeige auf dem Hintergrundbild. Sie können dieses Tag oder das `--all-tags` verwenden, aber nicht beides.

--attributes ***`attribute-string-1`***, ***`attribute-string-n`***

(Optional) Eine durch Kommas getrennte Liste von `wallpaper`-Attributzeichenfolgen zum Anwenden von Einstellungen auf das Hintergrundbild.

[--path | -p] ***`path-string`***

(Erforderlich) Gibt den `wallpaper`-Dateipfad für das Hintergrundbild an.

Flags

--all-tags

(Optional) Zeigt alle Instance-Tags auf dem Hintergrund an. Sie können dieses Tag oder das `--allowed-tags` verwenden, aber nicht beides.

[--help | -h]

Zeigt Hilfe für den wallpaper-Befehl an.

Aufgabenkonfiguration in EC2Launch v2

Dieser Abschnitt enthält das Konfigurationsschema, Aufgaben, Details und Beispiele für `agent-config.yml` und Benutzerdaten.

Aufgaben und Beispiele

- Schema: agent-config.yml
- Schema: Benutzerdaten
- Aufgabendefinitionen

Schema: **`agent-config.yml`**

Die Struktur der `agent-config.yml`-Datei wird unten gezeigt. Beachten Sie, dass eine Aufgabe nicht in derselben Phase wiederholt werden kann. Informationen zu den Aufgabeneigenschaften finden Sie in den folgenden Aufgabenbeschreibungen.

Dokumentstruktur: agent-config.yml

JSON

```
{
 "version": "1.0",
 "config": [
  {
   "stage": "string",
   "tasks": [
    {
     "task": "string",
     "inputs": {
```

```
      ...
     }
    },
    ...
   ]
  },
  ...
 ]
}
```

YAML

```
version: 1.0
config:
- stage: string
  tasks:
  - task: string
 inputs:
   ...
  ...
...
```

Beispiel: **`agent-config.yml`**

Das folgende Beispiel zeigt die Einstellungen für die `agent-config.yml`-Konfigurationsdatei.

```
version: 1.0
config:
- stage: boot
  tasks:
  - task: extendRootPartition
- stage: preReady
  tasks:
  - task: activateWindows
    inputs:
      activation:
        type: amazon
  - task: setDnsSuffix
    inputs:
      suffixes:
      - $REGION.ec2-utilities.amazonaws.com
  - task: setAdminAccount
    inputs:
```

```
      password:
        type: random
  - task: setWallpaper
    inputs:
      path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
      attributes:
      - hostName
      - instanceId
      - privateIpAddress
      - publicIpAddress
      - instanceSize
      - availabilityZone
      - architecture
      - memory
      - network
- stage: postReady
  tasks:
  - task: startSsm
```

Schema: Benutzerdaten

Die folgenden JSON- und YAML-Beispiele zeigen die Dokumentstruktur für Benutzerdaten. Amazon EC2 analysiert jede Aufgabe, die im `tasks`-Array genannt wird, das Sie im Dokument angeben. Jede Aufgabe hat ihre eigenen Eigenschaften und Anforderungen. Einzelheiten finden Sie im Aufgabendefinitionen.

> **Note**
>
> Eine Aufgabe darf nur einmal im Array mit Benutzerdatenaufgaben vorkommen.

Dokumentenstruktur: Benutzerdaten

JSON

```
{
 "version": "1.1",
 "tasks": [
  {
   "task": "string",
   "inputs": {
    ...
```

```
   },
  },
  ...
 ]
}
```

YAML

```
version: 1.1
tasks:
- task: string
  inputs:
    ...
...
```

Beispiel: Benutzerdaten

Weitere Informationen zu Benutzerrollen finden Sie unter So verarbeitet Amazon EC2 Benutzerdaten für Windows-Instances.

Das folgende Beispiel für ein YAML-Dokument zeigt ein PowerShell Skript, das EC2Launch v2 als Benutzerdaten ausführt, um eine Datei zu erstellen.

```
version: 1.1
tasks:
- task: executeScript
  inputs:
  - frequency: always
    type: powershell
    runAs: localSystem
    content: |-
      New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
```

Sie können ein XML-Format für die Benutzerdaten verwenden, das mit früheren Versionen des Startagenten kompatibel ist. EC2Launch v2 führt das Skript als `executeScript`-Aufgabe in der `UserData`-Stufe aus. Um dem EC2Launch-v1- und EC2Config-Verhalten zu entsprechen, wird das Benutzerdatenskript standardmäßig als angefügter/Inline-Prozess ausgeführt.

Sie können optionale Tags hinzufügen, um die Ausführung Ihres Skripts anzupassen. Um beispielsweise das Benutzerdatenskript beim Neustart der Instance zusätzlich zum einmaligen Starten der Instance auszuführen, können Sie das folgende Tag verwenden:

`<persist>true</persist>`

Beispiel:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<persist>true</persist>
```

Sie können ein oder mehrere PowerShell Argumente mit dem Tag angeben. `<powershellArguments>` Wenn keine Argumente übergeben werden, fügt EC2Launch v2 standardmäßig das folgende Argument hinzu:. `-ExecutionPolicy Unrestricted`

Beispiel:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<powershellArguments>-ExecutionPolicy Unrestricted -NoProfile -NonInteractive</
powershellArguments>
```

Um ein XML-Benutzerdatenskript als getrennten Prozess auszuführen, fügen Sie Ihren Benutzerdaten das folgende Tag hinzu.

`<detach>true</detach>`

Beispiel:

```
<powershell>
  $file = $env:SystemRoot + "\Temp" + (Get-Date).ToString("MM-dd-yy-hh-mm")
  New-Item $file -ItemType file
</powershell>
<detach>true</detach>
```

> **Note**
>
> Das Abtrennungs-Tag wird auf früheren Startagenten nicht unterstützt.

Änderungsprotokoll: Benutzerdaten

In der folgenden Tabelle sind die Änderungen für Benutzerdaten aufgeführt und sie werden mit der jeweiligen Version des EC2Launch-v2-Agents verglichen.

Benutzerdatenversion	Details	Eingeführt in
1.1	• Benutzerdatenaufgaben werden vor der `PostReady` -Phase in der Agentenkonfigurationsdatei ausgeführt. • Führt Benutzerdaten aus, bevor der Systems Manager Agent gestartet wird (gleiches Verhalten wie EC2Launch v1 und EC2Config).*	EC2Launch -v2-Version 2.0.1245
1,0	• Wird veraltet sein. • Benutzerdatenaufgaben werden nach der `PostReady` -Phase in der Agentenkonfigurationsdatei ausgeführt. Dies ist nicht abwärtskompatibel mit EC2Launch-v1. • Wirkt sich auf eine Race-Bedingung zwischen dem Start des Systems Manager Agents und den Benutzerdatenaufgaben aus.	EC2Launch -v2-Version 2.0.0

* Bei Verwendung mit der `agent-config.yml`-Standarddatei.

Aufgabendefinitionen

Jede Aufgabe hat ihre eigenen Eigenschaften und Anforderungen. Einzelheiten finden Sie unter den einzelnen Aufgaben, die in Ihr Dokument aufgenommen werden sollen.

Aufgaben

- activateWindows
- enableJumboFrames
- enableOpenSsh

- executeProgram
- executeScript
- extendRootPartition
- initializeVolume
- optimizeEna
- einstellen AdminAccount
- setDnsSuffix
- setHostName
- setWallpaper
- startSsm
- sysprep
- writeFile

activateWindows

Aktiviert Windows für eine Reihe von Servern. AWS KMS Die Aktivierung wird übersprungen, wenn die Instance als Bring-Your-Own-License (BYOL) erkannt wird.

Häufigkeit - einmal

AllowedStages — `[PreReady]`

Eingaben —

`activation`: (Zuordnung)

`type`: (Zeichenfolge) Aktivierungstyp, der verwendet werden soll, auf `amazon` gesetzt

Beispiel

```
task: activateWindows
inputs:
  activation:
    type: amazon
```

enableJumboFrames

Aktiviert Jumbo Frames, die die Maximum Transmission Unit (MTU) des Netzwerkadapters erhöhen. Weitere Informationen finden Sie unter Jumbo-Frames (9001 MTU).

Häufigkeit — immer

AllowedStages — `[PostReady, UserData]`

Eingaben — keine

Beispiel

```
task: enableJumboFrames
```

enableOpenSsh

Aktiviert Windows OpenSSH und fügt den öffentlichen Schlüssel für die Instance dem Ordner für autorisierte Schlüssel hinzu.

Häufigkeit - einmal

AllowedStages — `[PreReady, UserData]`

Eingaben — keine

Beispiel

Im folgenden Beispiel wird gezeigt, wie OpenSSH für eine Instance aktiviert und der öffentliche Schlüssel für die Instance dem Ordner für autorisierte Schlüssel hinzugefügt wird. Diese Konfiguration funktioniert nur auf Instances, auf denen Windows Server 2019 ausgeführt wird.

```
task: enableOpenSsh
```

executeProgram

Führt ein Programm mit optionalen Argumenten und einer angegebenen Häufigkeit aus.

Phasen: Sie können die Aufgabe `executeProgram` während der Phasen `PreReady`, `PostReady` und `UserData` ausführen.

Frequenz: konfigurierbar, siehe Eingänge.

Eingaben

Sie können Laufzeitparameter wie folgt konfigurieren:

Frequenz (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `once`
- `always`

Pfad (Zeichenfolge)

(Erforderlich) Der Dateipfad für die auszuführende Datei.

Argumente (Liste von Zeichenfolgen)

(Optional) Eine durch Kommas getrennte Liste von Argumenten, die dem Programm als Eingabe zur Verfügung gestellt werden sollen.

runAs (Zeichenfolge)

(Erforderlich) Muss auf `localSystem` gesetzt sein

Output

Alle Aufgaben schreiben Logfile-Einträge in die `agent.log`-Datei. Zusätzliche Ausgaben der Aufgabe `executeProgram` werden wie folgt separat in einem dynamisch benannten Ordner gespeichert:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.tmp`*

Der genaue Pfad zu den Ausgabedateien ist in der `agent.log`-Datei enthalten, zum Beispiel:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\ExecuteProgramInputs.tmp
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Ausgabedateien für die Aufgabe **`executeProgram`**

`ExecuteProgramInputs.tmp`

Enthält den Pfad für die ausführbare Datei und alle Eingabeparameter, die die Aufgabe `executeProgram` bei der Ausführung an sie übergibt.

`Output.tmp`

Enthält die Laufzeitausgabe des Programms, das die Aufgabe `executeProgram` ausführt.

`Err.tmp`

Enthält die Laufzeit-Fehlermeldungen des Programms, das die Aufgabe `executeProgram` ausführt.

Beispiele

Die folgenden Beispiele zeigen, wie eine ausführbare Datei aus einem lokalen Verzeichnis auf einer Instance mit der Aufgabe `executeProgram` ausgeführt wird.

Beispiel 1: Setup Executable mit einem Argument

Dieses Beispiel zeigt eine `executeProgram`-Aufgabe, die eine Setup Executable im Modus „Quiet“ ausführt.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\Users\Administrator\Desktop\setup.exe
  arguments: ['-quiet']
```

Beispiel 2: VLC-Executable mit zwei Argumenten

Dieses Beispiel zeigt eine `executeProgram`-Aufgabe, die eine VLC-Executable-Datei mit zwei als Eingabeparameter übergebenen Argumenten ausführt.

```
task: executeProgram
inputs:
- frequency: always
  path: C:\vlc-3.0.11-win64.exe
```

```
  arguments: ['/L=1033','/S']
  runAs: localSystem
```

executeScript

Führt ein Skript mit optionalen Argumenten und einer angegebenen Häufigkeit aus. Das Verhalten des Skripts hängt davon ab, in welchem Modus der Agent die Skripte ausführt – inline oder getrennt.

Inline (Standard)

Der EC2Launch-v2-Agent führt die Skripte nacheinander aus (`detach: false`). Dies ist die Standardeinstellung.

> **Note**
>
> Wenn Ihr Inline-Skript einen reset- oder sysprep-Befehl ausgibt, wird es sofort ausgeführt und setzt den Agenten zurück. Die aktuelle Aufgabe wird beendet, dann wird der Agent heruntergefahren, ohne weitere Aufgaben auszuführen.
> Wenn beispielsweise auf die Aufgabe, die den Befehl ausgibt, eine `startSsm`-Aufgabe folgen würde (die standardmäßig nach der Ausführung der Benutzerdaten enthalten ist), wird die Aufgabe nicht ausgeführt und der Systems-Manager-Service nicht gestartet.

Detached (Getrennt)

Der EC2Launch-v2-Agent führt Skripte gleichzeitig mit anderen Aufgaben aus (`detach: true`).

> **Note**
>
> Wenn Ihr abgetrenntes Skript einen reset- oder sysprep-Befehl ausgibt, warten diese Befehle, bis der Agent fertig ist, bevor sie ausgeführt werden. Aufgaben nach dem executeScript werden weiterhin ausgeführt.

Phasen: Sie können die Aufgabe `executeScript` während der Phasen `PreReady`, `PostReady` und `UserData` ausführen.

Frequenz: konfigurierbar, siehe Eingänge.

Eingaben

Sie können Laufzeitparameter wie folgt konfigurieren:

Frequenz (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `once`
- `always`

Typ (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `batch`
- `powershell`

Argumente (Liste von Zeichenfolgen)

(Optional) Eine Liste von Zeichenfolgenargumenten, die an die Shell übergeben werden sollen. Dieser Parameter wird nicht für `type: batch` unterstützt. Wenn keine Argumente übergeben werden, fügt EC2Launch v2 standardmäßig das folgende Argument hinzu:. `-ExecutionPolicy Unrestricted`

Inhalt (Zeichenfolge)

(Erforderlich) Skriptinhalt.

runAs (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `admin`
- `localSystem`

trennen (Boolean)

(Optional) Der EC2Launch v2-Agent führt standardmäßig Skripts einzeln aus (`detach: false`). Um das Skript gleichzeitig mit anderen Aufgaben auszuführen, setzen Sie den Wert auf `true` (`detach: true`).

> **Note**
>
> Skript-Exitcodes (einschließlich `3010`) haben keine Wirkung, wenn `detach` auf `true` festgelegt wird.

Output

Alle Aufgaben schreiben Logfile-Einträge in die `agent.log`-Datei. Zusätzliche Ausgaben von Skripten, die die Aufgabe `executeScript` ausführt, werden wie folgt separat in einem dynamisch benannten Ordner gespeichert:

`%LocalAppData%\Temp\`*`EC2Launch#########\outputfilename.ext`*

Der genaue Pfad zu den Ausgabedateien ist in der `agent.log`-Datei enthalten, zum Beispiel:

```
Program file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\UserScript.ps1
Output file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Output.tmp
Error file is created at: C:\Windows\system32\config\systemprofile\AppData\Local
\Temp\EC2Launch123456789\Err.tmp
```

Ausgabedateien für die Aufgabe **`executeScript`**

`UserScript.`*`ext`*

Enthält das Skript, das die Aufgabe `executeScript` ausgeführt hat. Die Dateierweiterung hängt wie folgt von der Art des Skripts ab, das Sie im `type`-Parameter für die `executeScript`-Aufgabe angegeben haben:

- Wenn der Typ `batch` ist, dann ist die Dateierweiterung `.bat`.
- Wenn der Typ `powershell` ist, dann ist die Dateierweiterung `.ps1`.

`Output.tmp`

Enthält die Laufzeitausgabe des Skripts, das die Aufgabe `executeScript` ausführt.

`Err.tmp`

Enthält die Laufzeit-Fehlermeldungen des Skripts, das die Aufgabe `executeScript` ausführt.

Beispiele

Die folgenden Beispiele zeigen, wie Sie ein Inline-Skript mit der Aufgabe `executeScript` ausführen.

Beispiel 1: Hello World Ausgabetextdatei

Dieses Beispiel zeigt eine `executeScript` Aufgabe, die ein PowerShell Skript ausführt, um eine „Hello World“ -Textdatei auf dem `C:` Laufwerk zu erstellen.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: admin
  content: |-
    New-Item -Path 'C:\PowerShellTest.txt' -ItemType File
    Set-Content 'C:\PowerShellTest.txt' "Hello world"
```

Beispiel 2: Zwei Skripts ausführen

Dieses Beispiel zeigt, dass die Aufgabe `executeScript` mehr als ein Skript ausführen kann und der Skripttyp nicht unbedingt übereinstimmen muss.

Das erste Skript (`type: powershell`) schreibt eine Zusammenfassung der Prozesse, die derzeit auf der Instance ausgeführt werden, in eine Textdatei auf dem `C:`-Laufwerk.

Das zweite Skript (`batch`) schreibt die Systeminformationen in die `Output.tmp`-Datei.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  content: |
    Get-Process | Out-File -FilePath C:\Process.txt
  runAs: localSystem
- frequency: always
  type: batch
  content: |
    systeminfo
```

Beispiel 3: Idempotenz-Systemkonfiguration mit Neustarts

Dieses Beispiel zeigt eine Aufgabe `executeScript`, die ein idempotentes Skript ausführt, um die folgende Systemkonfiguration mit einem Neustart zwischen den einzelnen Schritten durchzuführen:

- Den Computer umbenennen.

- Den Computer mit der Domain verbinden.
- Aktivieren von Telnet.

Das Skript stellt sicher, dass jede Operation nur einmal ausgeführt wird. Dies verhindert eine Neustartschleife und macht das Skript idempotent.

```
task: executeScript
inputs:
- frequency: always
  type: powershell
  runAs: localSystem
  content: |-
    $name = $env:ComputerName
     if ($name -ne $desiredName) {
       Rename-Computer -NewName $desiredName
       exit 3010
     }
     $domain = Get-ADDomain
     if ($domain -ne $desiredDomain)
     {
       Add-Computer -DomainName $desiredDomain
       exit 3010
     }
    $telnet = Get-WindowsFeature -Name Telnet-Client
    if (-not $telnet.Installed)
    {
      Install-WindowsFeature -Name "Telnet-Client"
      exit 3010
    }
```

extendRootPartition

Erweitert das Stammvolume, um den gesamten verfügbaren Speicherplatz auf der Festplatte zu nutzen.

Häufigkeit - einmal

AllowedStages — `[Boot]`

Eingaben — keine

Beispiel

```
task: extendRootPartition
```

initializeVolume

Initialisiert leere Volumes, die an die Instance angefügt sind, sodass diese aktiviert und partitioniert werden. Der Startagent überspringt die Initialisierung, wenn er erkennt, dass das Volume nicht leer ist. Ein Volume gilt als leer, wenn die ersten 4 KiB des Volumes leer sind oder wenn das Volume kein von Windows erkennbares Laufwerkslayout aufweist.

Der Eingabeparameter wird `letter` immer angewendet, wenn diese Aufgabe ausgeführt wird, unabhängig davon, ob das Laufwerk bereits initialisiert ist.

Das `initializeVolume` führt die folgenden Aktionen aus.

- Setzen Sie die Festplattenattribute `offline` und `readonly` auf false.
- Erstellen Sie eine Partition. Wenn im Eingabeparameter `partition` kein Partitionstyp angegeben ist, gelten die folgenden Standardwerte:
  - Wenn die Festplattengröße kleiner als 2 TB ist, legen Sie den Partitionstyp auf `mbr` fest.
  - Wenn die Festplattengröße 2 TB oder größer ist, legen Sie den Partitionstyp auf `gpt` fest.
- Formatieren Sie das Volume als NTFS.
- Legen Sie die Volume-Bezeichnung wie folgt fest:
  - Verwenden Sie den Wert des Eingabeparameters `name`, falls angegeben.
  - Wenn es sich um ein kurzlebiges Volume handelt und kein Name angegeben wurde, legen Sie die Volume-Bezeichnung auf `Temporary Storage Z` fest.
- Wenn das Volume kurzlebig ist (SSD oder HDD – nicht Amazon EBS), erstellen Sie im Stammverzeichnis des Volumes eine `Important.txt`-Datei mit dem folgenden Inhalt:

  ```
  This is an 'Instance Store' disk and is provided at no additional charge.

  *This disk offers increased performance since it is local to the host
  *The number of Instance Store disks available to an instance vary by instance type
  *DATA ON THIS DRIVE WILL BE LOST IN CASES OF IMPAIRMENT OR STOPPING THE INSTANCE.
   PLEASE ENSURE THAT ANY IMPORTANT DATA IS BACKED UP FREQUENTLY

  For more information, please refer to: Amazon EC2-Instance-Speicher.
  ```

- Legen Sie den Laufwerkbuchstaben auf den im Eingabeparameter `letter` angegebenen Wert fest.

Phasen: Sie können die Aufgabe `initializeVolume` während der Phasen `PostReady` und `UserData` ausführen.

Häufigkeit: immer.

Eingaben

Sie können Laufzeitparameter wie folgt konfigurieren:

Geräte (Liste der Zuordnungen)

(Bedingt) Konfiguration für jedes Gerät, das vom Startagenten initialisiert wird. Dies ist erforderlich, wenn der Eingabeparameter `initialize` auf `devices` festgelegt ist.

- Gerät (Zeichenfolge, erforderlich) – Identifiziert das Gerät während der Instance-Erstellung. Beispiel: `xvdb`, `xvdf` oder `\dev\nvme0n1`.
- Buchstabe (Zeichenfolge, optional) – Ein Zeichen. Der Laufwerkbuchstabe, der zugewiesen werden soll.
- Name (Zeichenfolge, optional) – Der zuzuweisende Volume-Name.
- Partition (Zeichenfolge, optional) – Geben Sie einen der folgenden Werte für den Typ der zu erstellenden Partition an oder lassen Sie den Startagenten basierend auf der Volume-Größe als Standard festlegen:
  - mbr
  - gpt

initialisieren (Zeichenfolge)

(Erforderlich) Geben Sie genau einen der folgenden Werte an:

- `all`
- `devices`

Beispiele

Die folgenden Beispiele zeigen Beispiele für Eingabekonfigurationen für die `initializeVolume`-Aufgabe.

Beispiel 1: Initialisieren von zwei Volumes auf einer Instance

Dieses Beispiel zeigt eine `initializeVolume`-Aufgabe, die zwei sekundäre Volumes auf einer Instance initialisiert. Das Gerät mit dem Namen `DataVolume2` im Beispiel ist kurzlebig.

```
task: initializeVolume
inputs:
  initialize: devices
  devices:
  - device: xvdb
    name: DataVolume1
    letter: D
    partition: mbr
  - device: /dev/nvme0n1
    name: DataVolume2
    letter: E
    partition: gpt
```

Beispiel 2: Initialisieren von EBS-Volumes, die an eine Instance angefügt sind

Dieses Beispiel zeigt eine `initializeVolume`-Aufgabe, die alle leeren EBS-Volumes initialisiert, die an die Instance angefügt sind.

```
task: initializeVolume
inputs:
  initialize: all
```

optimizeEna

Optimiert ENA-Einstellungen basierend auf dem aktuellen Instance-Typ. Möglicherweise wird die Instance neu gestartet.

Häufigkeit — immer

AllowedStages — `[PostReady, UserData]`

Eingaben — keine

Beispiel

```
task: optimizeEna
```

einstellen AdminAccount

Legt Attribute für das Standardadministratorkonto fest, das auf dem lokalen Computer erstellt wird.

Häufigkeit - einmal

AllowedStages — `[PreReady]`

Eingaben —

`name`: (Zeichenfolge) Name des Administratorkontos

`password`: (Zuordnung)

`type`: (Zeichenfolge) Strategie zum Setzen des Passworts, entweder als `static`, `random` oder `doNothing`

`data`: (Zeichenfolge) speichert Daten, wenn das Feld `type` statisch ist

Beispiel

```
task: setAdminAccount
inputs:
  name: Administrator
  password:
    type: random
```

setDnsSuffix

Fügt DNS-Suffixe zur Liste der Suchsuffixe hinzu. Nur Suffixe, die noch nicht vorhanden sind, werden der Liste hinzugefügt. Weitere Hinweise dazu, wie Launch-Agents DNS-Suffixe festlegen, finden Sie unter. Konfigurieren Sie das DNS-Suffix für Windows-Startagenten

Häufigkeit — immer

AllowedStages — `[PreReady]`

Eingaben —

`suffixes`: (Liste von Zeichenfolgen) Liste mit einem oder mehreren gültigen DNS-Suffixen; gültige Substitutionsvariablen sind `$REGION` und `$AZ`

Beispiel

```
task: setDnsSuffix
inputs:
```

```
  suffixes:
  - $REGION.ec2-utilities.amazonaws.com
```

setHostName

Setzt den Host-Namen des Computers auf eine benutzerdefinierte Zeichenfolge oder, falls `hostName`, die private IPv4-Adresse, nicht angegeben ist.

Häufigkeit — immer

AllowedStages — `[PostReady, UserData]`

Eingaben —

`hostName`: (Zeichenfolge) optionaler Host-Name, der wie folgt formatiert werden muss.

- Muss 15 Zeichen oder weniger haben
- Muss nur alphanumerische (a-z, A-Z, 0-9) und Bindestriche (-) enthalten.
- Darf nicht ausschließlich aus numerischen Zeichen bestehen.

`reboot`: (boolescher Wert) gibt an, ob ein Neustart zulässig ist, wenn der Hostname geändert wird

Beispiel

```
task: setHostName
inputs:
  reboot: true
```

setWallpaper

Erstellt die Verknüpfungsdatei `setwallpaper.lnk` im Startup-Ordner jedes vorhandenen Benutzers, mit Ausnahme von `Default User`. Diese Verknüpfungsdatei wird ausgeführt, wenn sich der Benutzer nach dem Start der Instance zum ersten Mal anmeldet. Hiermit wird die Instance mit einem benutzerdefinierten Hintergrundbild eingerichtet, auf dem die Instance-Attribute zu sehen sind.

Der Pfad der Verknüpfungsdatei lautet:

```
$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/
Startup/setwallpaper.lnk
```

> **Note**
>
> Wenn Sie die `setWallpaper`-Aufgabe entfernen, wird diese Verknüpfungsdatei nicht gelöscht. Weitere Informationen finden Sie unter Die Aufgabe `setWallpaper` ist nicht aktiviert, aber das Hintergrundbild wird beim Neustart zurückgesetzt.

Phasen: Sie können das Hintergrundbild während der Phasen `PreReady` und `UserData` konfigurieren.

Häufigkeit: `always`

Konfiguration des Hintergrundbilds

Sie können Ihr Hintergrundbild mit den folgenden Steuerelementen konfigurieren.

Eingaben

Von Ihnen bereitgestellte Eingabeparameter und Attribute, die Sie zum Konfigurieren Ihres Hintergrundbilds festlegen können:

Attribute (Liste von Zeichenfolgen)

(Optional) Sie können Ihrem Hintergrundbild eines oder mehrere der folgenden Attribute hinzufügen:

- `architecture`
- `availabilityZone`
- `hostName`
- `instanceId`
- `instanceSize`
- `memory`
- `network`
- `privateIpAddress`
- `publicIpAddress`

instanceTags

(Optional) Sie können genau eine der folgenden Optionen für diese Einstellung verwenden.

- AllTags(string) — Fügen Sie Ihrem Hintergrundbild alle Instanz-Tags hinzu.

```
instanceTags: AllTags
```

- instanceTags (Liste von Zeichenfolgen) – Geben Sie eine Liste mit Instance-Tag-Namen an, die Ihrem Hintergrundbild hinzugefügt werden sollen. Beispielsweise:

```
instanceTags:
  - Tag 1
  - Tag 2
```

Pfad (Zeichenfolge)

(Erforderlich) Der Dateinamenspfad der lokalen Bilddatei im .jpg-Format, die für Ihr Hintergrundbild verwendet werden soll.

Beispiel

Das folgende Beispiel zeigt Hintergrundkonfigurationseingaben, die den Dateipfad für das Hintergrundbild festlegen, zusammen mit Instance-Tags mit den Namen `Tag 1` und `Tag 2` und Attributen, die den Hostnamen, die Instance-ID und die privaten und öffentlichen IP-Adressen für die Instance enthalten.

```
task: setWallpaper
inputs:
  path: C:\ProgramData\Amazon\EC2Launch\wallpaper\Ec2Wallpaper.jpg
  attributes:
  - hostName
  - instanceId
  - privateIpAddress
  - publicIpAddress
  instanceTags:
  - Tag 1
  - Tag 2
```

> **Note**
>
> Sie müssen Tags in Metadaten aktivieren, um Tags auf dem Hintergrundbild anzuzeigen. Weitere Informationen zu Instance-Tags und Metadaten finden Sie unter Arbeiten mit Instance-Tags in Instance-Metadaten.

startSsm

Starten des Systems Manager-Services (SSM) nach Sysprep.

Häufigkeit — immer

AllowedStages — `[PostReady, UserData]`

Eingaben — keine

Beispiel

```
task: startSsm
```

sysprep

Setzt den Servicestatus zurück, aktualisiert `unattend.xml`, deaktiviert RDP und führt Sysprep aus. Diese Aufgabe wird erst ausgeführt, wenn alle anderen Aufgaben abgeschlossen sind.

Häufigkeit - einmal

AllowedStages — `[UserData]`

Eingaben —

`clean`: (boolescher Wert) bereinigt Instance-Protokolle vor dem Ausführen von Sysprep

`shutdown`: (boolescher Wert) fährt die Instance nach dem Ausführen von Sysprep herunter

Beispiel

```
task: sysprep
inputs:
  clean: true
  shutdown: true
```

writeFile

Schreibt eine Datei in ein Ziel.

Häufigkeit — siehe Eingaben

AllowedStages — `[PostReady, UserData]`

Eingaben —

`frequency`: (Zeichenfolge) `once` oder `always`

`destination`: (Zeichenfolge) Pfad, in den der Inhalt geschrieben werden soll

`content`: (Zeichenfolge) Text, der an das Ziel geschrieben werden soll

Beispiel

```
task: writeFile
inputs:
- frequency: once
  destination: C:\Users\Administrator\Desktop\booted.txt
  content: Windows Has Booted
```

Exit-Codes und Neustarts für EC2Launch v2

Sie können EC2Launch v2 verwenden, um zu definieren, wie Beendigungscodes in Ihren Skripts gehandhabt werden. Standardmäßig wird der Beendigungscode des letzten in einem Skript ausgeführten Befehls als Beendigungscode für das gesamte Skript gemeldet. Wenn ein Skript beispielsweise drei Befehle enthält und der erste Befehl fehlschlägt, aber die folgenden erfolgreich sind, wird der Ausführungsstatus als `success` gemeldet, da der endgültige Befehl erfolgreich war.

Wenn Sie möchten, dass ein Skript eine Instance neu startet, müssen Sie `exit 3010` in Ihrem Skript angeben, auch wenn der Neustart der letzte Schritt in Ihrem Skript ist. `exit 3010` weist EC2Launch v2 an, die Instance neu zu starten und das Skript erneut aufzurufen, bis ein Beendigungscode zurückgegeben wird, der nicht `3010` ist oder bis die maximale Neustartanzahl erreicht ist. EC2Launch v2 erlaubt maximal 5 Neustarts pro Aufgabe. Wenn Sie versuchen, eine Instance aus einem Skript mit einem anderen Mechanismus wie `Restart-Computer` neu zu starten, ist der Skriptausführungsstatus inkonsistent. Er kann beispielsweise in einer Neustartschleife stecken bleiben oder den Neustart nicht durchführen.

Wenn Sie ein XML-Benutzerdatenformat verwenden, das mit älteren Agenten kompatibel ist, werden die Benutzerdaten möglicherweise öfter ausgeführt, als Sie beabsichtigen. Weitere Informationen finden Sie im Abschnitt zur Fehlerbehebung unter Der Service führt Benutzerdaten mehr als einmal aus.

EC2Launch v2 und Sysprep

Der EC2Launch v2-Service führt Sysprep aus, ein Microsoft-Tool, mit dem Sie ein benutzerdefiniertes Windows-AMI erstellen können, das wiederverwendet werden kann. Wenn EC2Launch v2 Sysprep aufruft, verwendet es die Dateien in `%ProgramData%\Amazon\EC2Launch`, um zu bestimmen, welche Operationen ausgeführt werden sollen. Sie können diese Dateien indirekt über das EC2Launch settings (Einstellungen)-Dialogfeld oder direkt über einen YAML-Editor oder einen Texteditor bearbeiten. Es gibt jedoch einige erweiterte Einstellungen, die nicht im Dialogfeld EC2Launch settings (Einstellungen) verfügbar sind. Diese Einträge müssen Sie direkt bearbeiten.

Wenn Sie ein AMI aus einer Instance erstellen, nachdem Sie deren Einstellungen aktualisiert haben, werden die neuen Einstellungen auf alle Instances angewandt, die von diesem AMI gestartet werden. Weitere Informationen über die Erstellung eines AMI finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

Fehlersuche bei EC2Launch v2

In diesem Abschnitt werden allgemeine Problembehandlungsszenarien für EC2Launch v2, Informationen zum Anzeigen von Windows-Ereignisprotokollen sowie die Konsolenprotokollausgabe und -meldungen aufgeführt.

Themen zur Fehlerbehebung

- Allgemeine Problembehandlungsszenarien
- Windows-Ereignisprotokolle
- EC2Launch v2-Konsolenprotokollausgabe

Allgemeine Problembehandlungsszenarien

In diesem Abschnitt werden allgemeine Problembehandlungsszenarien und Lösungsschritte aufgeführt.

Szenarien

- Der Service kann das Hintergrundbild nicht festlegen
- Service kann Benutzerdaten nicht ausführen
- Der Service führt eine Aufgabe nur einmal aus
- Service kann eine Aufgabe nicht ausführen
- Der Service führt Benutzerdaten mehr als einmal aus

- Geplante Aufgaben von EC2Launch-v1 werden nach der Migration zu EC2Launch v2 nicht ausgeführt
- Der Service initialisiert ein EBS-Volume, das nicht leer ist
- Die Aufgabe setWallpaper ist nicht aktiviert, aber das Hintergrundbild wird beim Neustart zurückgesetzt
- Der Dienst hängt im laufenden Status fest
- Ungültige agent-config.yml verhindert das Öffnen des Dialogfelds für EC2Launch-v2-Einstellungen
- task:executeScript should be unique and only invoked once

Der Service kann das Hintergrundbild nicht festlegen

Auflösung

1. Überprüfen Sie, ob `%AppData%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\setwallpaper.lnk` vorhanden ist.
2. Überprüfen Sie `%ProgramData%\Amazon\EC2Launch\log\agent.log` darauf, ob Fehler aufgetreten sind.

Service kann Benutzerdaten nicht ausführen

Mögliche Ursache: Der Service ist möglicherweise fehlgeschlagen, bevor Benutzerdaten ausgeführt werden konnten.

Auflösung

1. Überprüfen Sie `%ProgramData%\Amazon\EC2Launch\state\previous-state.json`.
2. Sehen Sie nach, ob `boot`, `network`, `preReady` und `postReadyLocalData` wurden alle als erfolgreich markiert wurden.
3. Wenn eine der Phasen fehlgeschlagen ist, überprüfen Sie `%ProgramData%\Amazon\EC2Launch\log\agent.log` auf bestimmte Fehler.

Der Service führt eine Aufgabe nur einmal aus

Auflösung

1. Überprüfen Sie die Häufigkeit der Aufgabe.

2. Wenn der Service bereits nach Sysprep ausgeführt wurde und die Aufgabenhäufigkeit auf `once` festgelegt ist, wird die Aufgabe nicht erneut ausgeführt.
3. Legen Sie die Häufigkeit der Aufgabe auf `always` fest, wenn die Aufgabe bei jeder Ausführung von EC2Launch v2 ausgeführt werden soll.

Service kann eine Aufgabe nicht ausführen

Auflösung

1. Überprüfen Sie die neuesten Einträge in `%ProgramData%\Amazon\EC2Launch\log\agent.log`.
2. Wenn keine Fehler aufgetreten sind, versuchen Sie, den Service manuell von `"%ProgramFiles%\Amazon\EC2Launch\EC2Launch.exe" run` auszuführen, um festzustellen, ob die Aufgaben ausgeführt werden.

Der Service führt Benutzerdaten mehr als einmal aus

Auflösung

Benutzerdaten werden von EC2Launch v1 und EC2Launch v2 unterschiedlich behandelt. EC2Launch v1 führt Benutzerdaten als geplante Aufgabe auf der Instance aus, wenn `persist` auf `true` gesetzt ist. Wenn `persist` auf `false` festgelegt ist, wird die Aufgabe nicht geplant, selbst wenn sie mit einem Neustart beendet wird oder während der Ausführung unterbrochen wird.

EC2Launch v2 führt Benutzerdaten als Agentenaufgabe aus und verfolgt deren Ausführungsstatus. Wenn Benutzerdaten einen Neustart des Computers ausstellen oder Benutzerdaten während der Ausführung unterbrochen wurden, bleibt der Ausführungsstatus als `pending` bestehen und die Benutzerdaten werden beim nächsten Instance-Start erneut ausgeführt. Wenn Sie verhindern möchten, dass das Benutzerdatenskript mehr als einmal ausgeführt wird, machen Sie das Skript idempotent.

Das folgende Beispiel für ein idempotentes Skript legt den Computer-Namen fest und schließt sich einer Domain an.

```
<powershell>
  $name = $env:computername
  if ($name -ne $desiredName) {
 Rename-Computer -NewName $desiredName
```

```
  }
  $domain = Get-ADDomain
  if ($domain -ne $desiredDomain)
  {
 Add-Computer -DomainName $desiredDomain
  }
  $telnet = Get-WindowsFeature -Name Telnet-Client
  if (-not $telnet.Installed)
  {
 Install-WindowsFeature -Name "Telnet-Client"
  }
</powershell>
<persist>false</persist>
```

Geplante Aufgaben von EC2Launch-v1 werden nach der Migration zu EC2Launch v2 nicht ausgeführt

Auflösung

Das Migrationstool erkennt keine geplanten Aufgaben, die mit EC2Launch-v1-Skripten verknüpft sind. Daher richtet es diese Aufgaben in EC2Launch v2 nicht automatisch ein. Um diese Aufgaben zu konfigurieren, bearbeiten Sie die `agent-config.yml`-Datei oder verwenden Sie das EC2Launch v2-Einstellungsdialogfeld. Wenn eine Instance beispielsweise eine geplante Aufgabe umfasst, die `InitializeDisks.ps1` ausführt, müssen Sie nach dem Ausführen des Migrationstools die Volumes angeben, die Sie im Einstellungsdialogfeld von EC2Launch v2 initialisieren möchten. Siehe Schritt 6 des Verfahrens zu Ändern der Einstellungen mithilfe des Dialogfelds für EC2Launch v2-Einstellungen.

Der Service initialisiert ein EBS-Volume, das nicht leer ist

Auflösung

Bevor ein Volume initialisiert wird, versucht EC2Launch v2 zu erkennen, ob es leer ist. Wenn ein Volume nicht leer ist, überspringt es die Initialisierung. Alle Volumes, die als nicht leer erkannt werden, werden nicht initialisiert. Ein Volume gilt als leer, wenn die ersten 4 KiB eines Volumes leer sind oder wenn ein Volume kein Windows-erkennbares Laufwerkslayout hat. Ein Volume, das auf einem Linux-System initialisiert und formatiert wurde, hat kein Windows-erkennbares Laufwerkslayout, zum Beispiel MBR oder GPT. Daher wird es als leer und initialisiert betrachtet. Wenn Sie diese Daten beibehalten möchten, verlassen Sie sich nicht auf die Erkennung leerer Laufwerke durch EC2Launch v2. Geben Sie stattdessen Volumes an, die Sie im EC2Launch v2-Einstellungsdialogfeld (siehe Schritt 6) oder in `agent-config.yml` initialisieren möchten.

Die Aufgabe **`setWallpaper`** ist nicht aktiviert, aber das Hintergrundbild wird beim Neustart zurückgesetzt

Die Aufgabe `setWallpaper` erstellt die Verknüpfungsdatei `setwallpaper.lnk` im Startup-Ordner jedes vorhandenen Benutzers, mit Ausnahme von `Default User`. Diese Verknüpfungsdatei wird ausgeführt, wenn sich der Benutzer nach dem Start der Instance zum ersten Mal anmeldet. Hiermit wird die Instance mit einem benutzerdefinierten Hintergrundbild eingerichtet, auf dem die Instance-Attribute zu sehen sind. Durch das Entfernen der Aufgabe `setWallpaper` wird diese Verknüpfungsdatei nicht gelöscht. Sie müssen die Datei manuell oder mithilfe eines Skripts löschen.

Der Verknüpfungspfad lautet:

`$env:SystemDrive/Users/<user>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/setwallpaper.lnk`

Auflösung

Löschen Sie die Datei manuell oder mithilfe eines Skripts.

PowerShell Beispielskript zum Löschen der Shortcut-Datei

```
foreach ($userDir in (Get-ChildItem "C:\Users" -Force -Directory).FullName)
{
 $startupPath = Join-Path $userDir -ChildPath "AppData\Roaming\Microsoft\Windows\Start
 Menu\Programs\Startup"
 if (Test-Path $startupPath)
 {
  $wallpaperSetupPath = Join-Path $startupPath -ChildPath "setwallpaper.lnk"
  if (Test-Path $wallpaperSetupPath)
  {
   Remove-Item $wallpaperSetupPath -Force -Confirm:$false
  }
 }
}
```

Der Dienst hängt im laufenden Status fest

Beschreibung

EC2Launch v2 ist blockiert, mit Protokollmeldungen (`agent.log`) ähnlich der folgenden:

```
2022-02-24 08:08:58 Info:
 ********************************************************************************
```

```
2022-02-24 08:08:58 Info: EC2Launch Service starting
2022-02-24 08:08:58 Info: Windows event custom log exists: Amazon EC2Launch
2022-02-24 08:08:58 Info: ACPI SPCR table not supported. Bailing Out
2022-02-24 08:08:58 Info: Serial port is in use. Waiting for Serial Port...
2022-02-24 08:09:00 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:02 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:04 Info: ACPI SPCR table not supported. Use default console port.
2022-02-24 08:09:06 Info: ACPI SPCR table not supported. Use default console port.
```

Mögliche Ursache

SAC ist aktiviert und verwendet die serielle Schnittstelle. Weitere Informationen finden Sie unter SAC zur Fehlerbehhebung von Windows-Instances verwenden.

Auflösung

Versuchen Sie, das Problem wie folgt zu beheben:

- Deaktivieren Sie den Dienst, der den seriellen Port verwendet.
- Wenn Sie möchten, dass der Dienst weiterhin den seriellen Port verwendet, schreiben Sie benutzerdefinierte Skripte, um Launch-Agent-Aufgaben auszuführen, und rufen Sie diese als geplante Aufgaben auf.

Ungültige **`agent-config.yml`** verhindert das Öffnen des Dialogfelds für EC2Launch-v2-Einstellungen

Beschreibung

Die Einstellungen für EC2Launch v2 versuchen, dieselbe `agent-config.yml`-Datei zu analysieren, bevor sie das Dialogfeld öffnen. Wenn die YAML-Konfigurationsdatei nicht dem unterstützten Schema folgt, zeigt das Dialogfeld den folgenden Fehler an:

```
Unable to parse configuration file agent-config.yml. Review configuration
file. Exiting application.
```

Auflösung

1. Stellen Sie sicher, dass die Konfigurationsdatei dem unterstützten Schema entspricht.
2. Wenn Sie von vorne anfangen möchten, kopieren Sie die Standardkonfigurationsdatei in `agent-config.yml`. Sie können das Beispiel`agent-config.yml` im Abschnitt „Aufgabenkonfiguration“ verwenden.

3. Sie können auch von vorne beginnen, indem Sie `agent-config.yml` löschen. Die Einstellungen für EC2Launch v2 generieren eine leere Konfigurationsdatei.

`task:executeScript should be unique and only invoked once`

Beschreibung

Eine Aufgabe nicht in derselben Phase wiederholt werden kann.

Auflösung

Einige Aufgaben müssen als Array eingegeben werden, z. B. executeScript und executeProgram. Ein Beispiel für das Schreiben des Skripts als Array finden Sie unter executeScript.

Windows-Ereignisprotokolle

EC2Launch v2 veröffentlicht Windows-Ereignisprotokolle für wichtige Ereignisse, z. B. Servicestart, Windows ist bereit und Erfolg und Misserfolg von Aufgaben. Ereignis-IDs identifizieren eindeutig ein bestimmtes Ereignis. Jedes Ereignis enthält Informationen zu Phase, Aufgabe und Ebene sowie eine Beschreibung. Sie können mithilfe der Ereignis-ID Auslöser für bestimmte Ereignisse festlegen.

Event-IDs liefern Informationen über ein Ereignis und identifizieren einige Ereignisse eindeutig. Die am wenigsten signifikante Ziffer einer Ereignis-ID gibt den Schweregrad eines Ereignisses an.

Veranstaltung	Am wenigsten bedeutende Ziffer
`Success`	`. . .0`
`Informational`	`. . .1`
`Warning`	`. . .2`
`Error`	`. . .3`

Dienstbezogene Ereignisse, die beim Start oder Ende des Dienstes generiert werden, enthalten eine einstellige Ereigniskennung.

Veranstaltung	Einstellige ID
`Success`	`0`

Veranstaltung	Einstellige ID
`Informational`	1
`Warning`	2
`Error`	3

Die Ereignisnachrichten für `EC2LaunchService.exe`-Ereignisse beginnen mit `Service:`. Die Ereignisnachrichten für `EC2Launch.exe`-Ereignisse beginnen nicht mit `Service:`.

Vierstellige Ereignis-IDs enthalten Informationen über die Phase, Aufgabe und den Schweregrad eines Ereignisses.

Themen

- Format der Ereignis-ID
- Beispiele für Ereignis-IDs
- Windows-Ereignisprotokollschema

Format der Ereignis-ID

Die folgende Tabelle zeigt das Format einer EC2Launch v2-Ereignis-ID.

3	2 1	0
S	T	L

Die Buchstaben und Zahlen in der Tabelle stehen für die folgenden Ereignistypen und Definitionen.

Ereignistyp	Definition
S (Stage)	0 - Nachricht auf Service-Ebene 1 - Boot 2 - Netzwerk

Ereignistyp	Definition
	3 - PreReady 5 - Windows ist bereit 6 - PostReady 7 - Benutzerdaten
T (Aufgabe)	Die Aufgaben, die durch die entsprechenden beiden Werte dargestellt werden, sind für jede Phase unterschiedlich. Informationen zur vollständigen Liste der Ereignisse finden Sie unter Windows-Ereignisprotokollschema.
L (Ebene des Ereignisses)	0 - Erfolg 1 - Informativ 2 - Warnung 3 - Fehler

Beispiele für Ereignis-IDs

Nachfolgend finden Sie Beispiele für Ereignis-IDs.

- `5000` - Windows ist einsatzbereit
- `3010`- Die Windows-Aufgabe in der PreReady Phase aktivieren war erfolgreich
- `6013`- Bei der Aufgabe „Hintergrundbild festlegen“ ist in der Phase „ PostReady Lokale Daten“ ein Fehler aufgetreten

Windows-Ereignisprotokollschema

MessageId/Ereignis-ID	Ereignismeldung
. . .0	Success
. . .1	Informational
. . .2	Warning
. . .3	Error
x	EC2Launch service-level logs
0	EC2Launch service exited successfully
1	EC2Launch service informational logs
2	EC2Launch service warning logs
3	EC2Launch service error logs
10	Replace state.json with previous-state.json
100	Serial Port
200	Sysprep
300	PrimaryNic
400	Metadata
x000	Stage (1 digit), Task (2 digits), Status (1 digit)
1000	Boot
1010	Boot - extend_root_partition

MessageId/Ereignis-ID	Ereignismeldung
2000	Network
2010	Network - add_routes
3000	PreReady
3010	PreReady - activate_windows
3020	PreReady - install_egpu_manager
3030	PreReady - set_monitor_on
3040	PreReady - set_hibernation
3050	PreReady - set_admin_account
3060	PreReady - set_dns_suffix
3070	PreReady - set_wallpaper
3080	PreReady - set_update_schedule
3090	PreReady - output_log
3100	PreReady - enable_open_ssh
5000	Windows is Ready to use
6000	PostReadyLocalData
7000	PostReadyUserData
6010/7010	PostReadyLocal/UserData - set_wallpaper
6020/7020	PostReadyLocal/UserData - set_update_schedule

MessageId/Ereignis-ID	Ereignismeldung
6030/7030	PostReadyLocal/UserData - set_hostname
6040/7040	PostReadyLocal/UserData - execute_program
6050/7050	PostReadyLocal/UserData - execute_script
6060/7060	PostReadyLocal/UserData - manage_package
6070/7070	PostReadyLocal/UserData - initialize_volume
6080/7080	PostReadyLocal/UserData - write_file
6090/7090	PostReadyLocal/UserData - start_ssm
7100	PostReadyUserData - enable_open_ssh
6110/7110	PostReadyLocal/UserData - enable_jumbo_frames

EC2Launch v2-Konsolenprotokollausgabe

Dieser Abschnitt enthält eine Beispielausgabe des Konsolenprotokolls für EC2Launch v2 und führt alle Fehlermeldungen des EC2Launch v2-Konsolenprotokolls auf, mit denen Sie Probleme beheben können. Weitere Informationen zur Ausgabe der Instanzkonsole und wie Sie darauf zugreifen können, finden Sie unterthe section called “Instance-Konsolenausgabe”.

Outputs

- EC2Launch v2-Konsolenprotokollausgabe

- EC2Launch v2-Konsolenprotokollmeldungen

EC2Launch v2-Konsolenprotokollausgabe

Im Folgenden finden Sie eine Beispiel-Konsolenprotokollausgabe für EC2Launch v2.

```
2023/11/30 20:18:53Z: Windows sysprep configuration complete.
2023/11/30 20:18:57Z: Message: Waiting for access to metadata...
2023/11/30 20:18:57Z: Message: Meta-data is now available.
2023/11/30 20:18:57Z: AMI Origin Version: 2023.11.15
2023/11/30 20:18:57Z: AMI Origin Name: Windows_Server-2022-English-Full-Base
2023/11/30 20:18:58Z: OS: Microsoft Windows NT 10.0.20348
2023/11/30 20:18:58Z: OsVersion: 10.0
2023/11/30 20:18:58Z: OsProductName: Windows Server 2022 Datacenter
2023/11/30 20:18:58Z: OsBuildLabEx: 20348.1.amd64fre.fe_release.210507-1500
2023/11/30 20:18:58Z: OsCurrentBuild: 20348
2023/11/30 20:18:58Z: OsReleaseId: 2009
2023/11/30 20:18:58Z: Language: en-US
2023/11/30 20:18:58Z: TimeZone: UTC
2023/11/30 20:18:58Z: Offset: UTC +0000
2023/11/30 20:18:58Z: Launch: EC2 Launch v2.0.1643
2023/11/30 20:18:58Z: AMI-ID: ami-1234567890abcdef1
2023/11/30 20:18:58Z: Instance-ID: i-1234567890abcdef0
2023/11/30 20:18:58Z: Instance Type: c5.large
2023/11/30 20:19:00Z: Driver: AWS NVMe Driver v1.5.0.33
2023/11/30 20:19:00Z: SubComponent: AWS NVMe Driver v1.5.0.33;
 EnableSCSIPersistentReservations: 0
2023/11/30 20:19:00Z: Driver: AWS PV Driver Package v8.4.3
2023/11/30 20:19:01Z: Driver: Amazon Elastic Network Adapter v2.6.0.0
2023/11/30 20:19:01Z: RDPCERTIFICATE-SUBJECTNAME: EC2AMAZ-SO1T009
2023/11/30 20:19:01Z: RDPCERTIFICATE-THUMBPRINT:
 1234567890ABCDEF1234567890ABCDEF1234567890
2023/11/30 20:19:09Z: SSM: Amazon SSM Agent v3.2.1705.0
2023/11/30 20:19:13Z: Username: Administrator
2023/11/30 20:19:13Z: Password: <Password>
1234567890abcdef1EXAMPLEPASSWORD
</Password>
2023/11/30 20:19:14Z: User data format: no_user_data
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsTelemetryEnabled=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentOsArch=windows_amd64
2023/11/30 20:19:14Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2023/11/30 20:19:14Z: EC2LaunchTelemetry: AgentCommandErrorCode=0
```

```
2023/11/30 20:19:14Z: Message: Windows is Ready to use
```

EC2Launch v2-Konsolenprotokollmeldungen

Im Folgenden finden Sie eine Liste aller EC2Launch v2-Konsolenprotokollmeldungen.

```
Message: Error EC2Launch service is stopping. {error message}
 Error setting up EC2Launch agent folders
 See instance logs for detail
 Error stopping service
 Error initializing service
Message: Windows sysprep configuration complete
Message: Invalid administrator username: {invalid username}
Message: Invalid administrator password
Username: {username}
Password: <Password>{encrypted password}</Password>
AMI Origin Version: {amiVersion}
AMI Origin Name: {amiName}
Microsoft Windows NT {currentVersion}.{currentBuildNumber}
OsVersion: {currentVersion}
OsProductName: {productName}
OsBuildLabEx: {buildLabEx}
OsCurrentBuild: {currentBuild}
OsReleaseId: {releaseId}
Language: {language}
TimeZone: {timeZone}
Offset: UTC {offset}
Launch agent: EC2Launch {BuildVersion}
AMI-ID: {amiId}
Instance-ID: {instanceId}
Instance Type: {instanceType}
RDPCERTIFICATE-SUBJECTNAME: {certificate subject name}
RDPCERTIFICATE-THUMBPRINT: {thumbprint hash}
SqlServerBilling: {sql billing}
SqlServerInstall: {sql patch leve, edition type}
Driver: AWS NVMe Driver {version}
Driver: Inbox NVMe Driver {version}
Driver: AWS PV Driver Package {version}
Microsoft-Hyper-V is installed.
Unable to get service status for vmms
Microsoft-Hyper-V is {status}
SSM: Amazon SSM Agent {version}
AWS VSS Version: {version}
Message: Windows sysprep configuration complete
```

```
Message: Windows is being configured. SysprepState is {state}
Windows is still being configured. SysprepState is {state}
Message: Windows is Ready to use
Message: Waiting for meta-data accessibility...
Message: Meta-data is now available.
Message: Still waiting for meta-data accessibility...
Message: Failed to find primary network interface...retrying...
User data format: {format}
```

EC2Launch v2-Versionsverläufe

Versionsverläufe

- EC2Launch v2-Versionsverlauf
- Versionshistorie des EC2Launch v2-Migrationstools

EC2Launch v2-Versionsverlauf

Die folgende Tabelle beschreibt die von EC2Launch v2 veröffentlichten Versionen.

Version	Details	Datum der Veröffentlichung
2.0.1924	• Die Benutzeroberfläche mit den EC2Launch-Einstellungen wurde aktualisiert. • Der CLI-Befehl für das Hintergrundbild wurde aktualisiert. • Das EC2Launch-Installationsprogramm wurde aktualisiert.	10. Juni 2024
2.0.1914	• Fügen Sie Routen mit nicht spezifizierten Gateway-Adressen hinzu (`0.0.0.0`für IPv4 oder `::` für IPv6). • Fügen Sie immer sowohl IPv4- als auch IPv6-Routen hinzu. • Es wurde ein Problem behoben, bei dem der `Administrator` Benutzername zur `agent-config.yml` Datei hinzugefügt wurde, obwohl er nicht angegeben wurde.	5. Juni 2024

Version	Details	Datum der Veröffentlichung
	• Geänderte EC2Launch v2-Berechtigungen.	
2.0.1881	• Der Aufgabe wurde eine Option für ein verschlüsseltes Passwort hinzugefügt`setAdminAccount` . • CLI-Befehl zum Verschlüsseln des statischen Passworts in agent-config.yml hinzugefügt. • Es wurde ein Problem behoben, bei dem XML-Benutzerdaten keine PowerShell Argumente hinzufügen, wenn sie mit Administratorrechten ausgeführt wurden. Weitere Details finden Sie unter So verarbeitet Amazon EC2 Benutzerdaten für Windows-Instances. • Die PowerShell Argumente für die `executeScript` Aufgaben- und Benutzerdatenskripts wurden angepasst, wenn sie mit `LocalSystem` Berechtigungen ausgeführt wurden. Wenn Argumente leer sind, verwendet der Agent den folgenden Standardwert:`-ExecutionPolicy Unrestricted` . • Das Drucken doppelter Treiberversionen in das Konsolenprotokoll wurde verhindert.	8. Mai 2024

Version	Details	Datum der Veröffentlichung
2.0.1815	• Die Fehlerbehandlung wurde so angepasst, dass sie bei kritischen Einrichtungsproblemen vor Sysprep fehlschlägt. • Es wurde ein Problem behoben, bei dem Hintergrundbild- und Hostnamen-Tasks auf Instanzen, denen mehrere IP-Adressen der primären Netzwerkschnittstelle zugewiesen waren, eine falsche IP-Adresse verwenden konnten. • Die Aufgaben für Hintergrundbild und Hostname wurden dahingehend geändert, dass sie zuerst private IP-Adressen von IMDS abrufen und dann wieder zu WMI zurückkehren, wenn IMDS deaktiviert ist. • Es wurde ein Problem mit der `initializeVolume` Aufgabe behoben, bei dem `sc1` Volumes aufgrund eines vorüberge henden Fehlers nicht initialisiert werden konnten.	6. März 2024
2.0.1739	• Es wurde ein Problem behoben, das verhinderte, dass Exit-Codes von `executeScript` Aufgaben erfasst wurden, die als Windows-Administratorbenutzer ausgeführt wurden.	17. Januar 2024

Version	Details	Datum der Veröffentlichung
2.0.1702	• Eingeschränkte `Telemetry.log` Berechtigungen `read-execute` nur für Standardbenutzer. • Der EC2Launch-Windows-Dienst wurde so konfiguriert, dass er bei einem Startfehler neu gestartet wird. • `add-routes` Fehler wurden durch Protokollierung der Ausgabe umsetzbar gemacht. `route.exe stderr` • Es wurde ein Problem behoben, das auftritt, wenn Routenmetriken außerhalb des Bereichs [1, 9999] liegen. • Mehrere neue Instance-Typen unterstützen jetzt Bildschirmhintergründe. • Es wurde ein Problem behoben, das durch Skripte für Benutzerdaten verursacht wurde, die als Windows-Administrator ausgeführt werden und Ausgaben an `stderr`senden.	04. Januar 2024

Version	Details	Datum der Veröffentlichung
2.0.1643	• Das `ebsnvme-id.exe` -Tool wurde auf Version 1.1.0.7 aktualisiert. • Es wurde ein Problem mit den Einstellungen für die empfangsseitige Skalierung (RSS, Receive Side Scaling) und Receive Queue Depth bei Metal-Instance-Typen behoben, die mit 'metal-*' beginnen, wie z. B. metal-48x1. • Das Telemetrieereignis, das über XML-Benutzerdatenbefehle berichtet, die den Agenten blockieren, wurde entfernt. • Die `setDnsSuffix` -Aufgabe wurde aktualisiert, um die Übertragung von Domainnamen auf der Grundlage eines Registrierungseintrags einzuschränken: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Es wurden eine öffentliche Aufgabe und eine CLI hinzugefügt, die Netzwerkrouten hinzufügt. • Hinweis – Dies ist die letzte Version, die offiziell Windows Server 2012 unterstützt. • Hinweis – Dies ist die letzte Version, die offiziell 32-Bit-Betriebssysteme unterstützt.	04. Oktober 2023

Version	Details	Datum der Veröffentlichung
2.0.1580	• Die Art und Weise, wie der Launch-Agent Fehler behandelt, wenn Sie die Berechtigungen für Protokolldateien ändern, wurde geändert. • Es wurde ein Timeout für die Verbindung zur seriellen Schnittstelle hinzugefügt. Das Timeout ermöglicht es dem Launch-Agent, weiter zu laufen, wenn die serielle Schnittstelle verwendet wird.	5. September 2023

Version	Details	Datum der Veröffentlichung

2.0.1521	• Die –`block`-Markierung der `EC2Launch.exe` reset- und sysprep-Befehle ist veraltet.
	• `EC2Launch.exe` wurde aktualisiert, um die reset- und sysprep-Befehle zu erkennen und zu verarbeiten, die in Inline-`executeScript` -Aufgaben verwendet werden. Diese Befehle führen dazu, dass der Agent nicht mehr ausgeführt wird, nachdem die `executeScript` -Aufgabe diese ausgeführt hat.
	• Aktualisierte XML-Benutzerdatenskripte, sodass sie standardmäßig inline ausgeführt werden.
	• Ermöglichen Sie die getrennte Ausführung von XML-Benutzerdatenskripten mit dem neuen `detach`-Tag. Weitere Details finden Sie unter Benutzerdatenskripts.
	• Die folgenden Änderungen wurden am Agentenprotokoll vorgenommen.
	  • Aktualisierte Agentenprotokollmeldungen.
	  • `executeScript` -Inhalt und Ausgabe aus dem Agentenprotokoll entfernt.
	  • `executeProgram` -Argumente und Ausgabe aus dem Agentenprotokoll entfernt.
	• Die folgenden Änderungen wurden am Konsolenprotokoll vorgenommen.
	  • Der `EnableSCSIPersistentReservations` -Wert wurde dem Konsolenprotokoll hinzugefügt.
		03. Juli 2023

Version	Details	Datum der Veröffentlichung
2.0.1303	• Zusätzliche Fehlerbehandlung und Protokollzeilen beim Hinzufügen von Netzwerkrouten wurden hinzugefügt. • Erlaubt `executeScript` und `executeProgram` Aufgaben in der PreReady Phase. • Die Aufgabe `executeProgram` wurde aktualisiert, um Ausgabedateien zu generieren, die der Ausgabe der ExecuteScript-Aufgabe ähneln. Weitere Informationen finden Sie unter executeProgram. • Telemetrie wurde hinzugefügt, um die Verwendung von blockierenden Agentenbefehlen in XML-Benutzerdaten zu überwachen.	3. Mai 2023
2.0.1245	• Verbesserte Transparenz bei Abstürzen durch die Protokollierung von Crash-Call-Stacks im Klartext. • Der EventLog Service wurde als Startabhängigkeit hinzugefügt, um einen Absturz zu beheben, wenn der Amazon EC2Launch-Service schneller startet als der EventLog Service. • XML-Benutzerdaten wurden vor der PostReady Phase aus der Agentenkonfigurationsdatei ausgeführt (wie EC2Launch v1 und EC2Config). • YAML-Benutzerdaten Version 1.1 wurden hinzugefügt, damit Benutzerdaten vor der PostReady Phase aus der Agenten-Konfigurationsdatei ausgeführt werden (YAML-Benutzerdaten Version 1.0 werden nach der PostReady Phase aus der Agenten-Konfigurationsdatei ausgeführt).	08. März 2023

Version	Details	Datum der Veröffentlichung
2.0.1173	• Fügt ein optionales Feature zur Anzeige von Instance-Tags auf dem Hintergrundbild hinzu. Weitere Informationen finden Sie unter setWallpaper . • Fügt eine Fehlerbehandlung hinzu, wenn die Sicherheitsgruppe für Elastic Graphics nicht richtig eingerichtet ist. • Behebt eine Zeitüberschreitung, wenn der Instance-Metadaten-Service nicht aktiviert ist.	06. Februar 2023
2.0.1121	• Behebt ein Problem, bei dem ein 404-Fehler auf das Hintergrundbild gedruckt wurde, wenn keine öffentliche IPv4-Adresse zugewiesen wurde. • Behebt ein Problem, bei dem das Dateisystem des Volumes als `RAW` anstelle von `NTFS` formatiert wird, wenn der Laufwerksbuchstabe des Geräts auf `D` eingestellt ist. • Behebt ein Problem, bei dem NVMe-SSD-Volumes fälschlicherweise als EBS-Volumes identifiziert werden. • Behebt einen Fehler beim Aktivieren von Windows, wenn IMDS deaktiviert ist.	4. Januar 2023

Version	Details	Datum der Veröffentlichung
2.0.1082	• Behebt ein Problem, bei dem das `setWallpaper : privateIpAddress` -Feld leer ist, wenn IMDS deaktiviert ist. • Behebt ein Problem beim Festlegen des Hostnamen auf die private IPv4-Adresse, wenn IMDS deaktiviert ist. • Behebt ein Problem mit der Initialisierung von Volumes auf Windows Server 2012. • Behebt ein Problem mit der Einstellung von Jumbo-Frames. • Behebt einen Fehler, wenn beim Start der Instance kein SSH-Schlüssel angegeben wurde. • Behebt einen Fehler auf Windows Server 2012, wenn Windows keinen Registrierungsschlüssel 'ReleaseId' hat.	7. Dezember 2022
2.0.1011	• Korrigiert die Logik für die Suche nach einem Netzwerkadapter, wenn PnPDeviceID leer ist.	11. November 2022
2.0.1009	• Verwendet PCI-Segmentinformationen, um den Konsolenport auszuwählen.	8. November 2022

Version	Details	Datum der Veröffentlichung
2.0.982	• Fügt eine Wiederholungslogik zum Abrufen von RDP-Informationen hinzu. • Behebt Fehler bei der Volume-Initialisierung auf `d2.8xlarge` -Instances. • Behebt ein Problem, bei dem nach einem Neustart ein falscher Netzwerkadapter ausgewählt werden kann. • Entfernt eine Fehlalarm-Fehlermeldung, wenn ACPI SPCR nicht verfügbar ist.	31. Oktober 2022
2.0.863	• Aktualisiert die IMDS-Wartelogik, um nur noch IMDSv2-Anforderung zu stellen. • Fügt Logik hinzu, um Laufwerksbuchstaben Volumes zuzuweisen, die bereits initialisiert, aber nicht gemountet sind. • Druckt eine genauere Fehlermeldung, wenn der Schlüsselpaartyp nicht unterstützt wird. • Behebt einen 3010-Neustartcode-Fehler. • Fügt eine Überprüfung auf ungültige base64-verschlüsselte Benutzerdaten hinzu.	6. Juli 2022
2.0.698	• Rechtschreibfehler in der Protokollausgabe beim Ausführen von Skripten behoben.	30. Januar 2022

Version	Details	Datum der Veröffentlichung
2.0.674	• Die Telemetrie lädt die aktivierte/deaktivierte Datenschutzkontrolle hoch. • Behebt den Fehler `index out of bounds`. • Entfernt Hintergrundverknüpfungen während `sysprep`.	15. November 2021
2.0.651	• Fügt Logik zum Deinstallieren von Legacy-Agents während der Installation von EC2Launch v2 hinzu. • Behebt ein Problem mit dem CLI-Befehl `list-volume` , wenn das Root-Volume nicht als Volume 0 aufgeführt ist.	7. Oktober 2021
2.0.592	• Behebt Fehler, um den Status der Phase korrekt zu melden. • Entfernt Fehlalarmfehlermeldungen, wenn Protokolldateien geschlossen werden. • Fügt Telemetrie hinzu.	31. August 2021
2.0.548	• Fügt führende Nullen für Hex-IP-Hostnamen hinzu. • Behebt Dateiberechtigungen für `enableOpenSsh` -Aufgabe. • Behebt den Absturz des Sysprep-Befehls.	4. August 2021

Version	Details	Datum der Veröffentlichung
2.0.470	• Behebt einen Fehler in der Netzwerkphase, um zu warten, bis DHCP der Instance eine IP zuweist. • Behebt einen Fehler mit `setDnsSuffix` , wenn `SearchList` -Registrierungsschlüssel nicht vorhanden ist. • Behebt Fehler in DNS-Devolutionslogik in `setDnsSuffix` . • Fügt Netzwerkrouten nach Zwischenneustarts hinzu. • Erlaubt `initializeVolume` , um vorhandene Volumes neu zu schreiben. • Entfernt zusätzliche Informationen aus dem Unterbefehl Version.	20. Juli 2021
2.0.285	• Fügt die Option hinzu, Benutzerskripte in einem separaten Prozess auszuführen. • Legacy-Benutzerdaten (XML-Benutzerdaten) werden jetzt in einem losgelösten Prozess ausgeführt, der dem früheren Start-Agenten ähnlich ist. • Fügt `sysprep` und `reset`-Befehlen die CLI-Flag hinzu, die es ihnen ermöglichen, zu blockieren, bis der Dienst beendet ist. • Schränkt die Berechtigungen für den Konfigurationsordner ein.	8. März 2021

Version	Details	Datum der Veröffentlichung
2.0.207	• Fügt der `setHostName` -Aufgabe ein optionales `hostName`-Feld hinzu. • Behebt den Neustartfehler. Die Neustartaufgaben `executeScript` und `executeProgram` werden als „in Ausführung“ markiert. • Fügt dem Status-Befehl weitere Rückgabekodes hinzu. • Fügt einen Ladeprogramm-Dienst hinzu, um das Startup-Problem bei der Ausführung auf `t2.nano`-Instance-Typ zu beheben • Behebt den Bereinigungsinstallationsmodus, um Dateien zu entfernen, die vom Installationsprogramm nicht verfolgt werden	2. Februar 2021
2.0.160	• Behebt den `validate`-Befehl, um einen ungültigen Phasennamen zu erkennen. • Fügt den `w32tm resync`-Befehl in die `addroutes` -Aufgabe hinzu. • Behebt das Problem mit der Änderung der DNS-Suffixsuchreihenfolge. • Fügt Prüfbedingungen hinzu, um ungültige Benutzerdaten besser zu melden.	4. Dezember 2020
2.0.153	Fügt Sysprep-Funktionalität hinzu. UserData	3. November 2020

Version	Details	Datum der Veröffentlichung
2.0.146	• Behebt ein Problem mit AMIs, die nicht RootExtend auf Englisch sind. • Erteilt Benutzergruppen Schreibberechtigung für Protokolldateien. • Erstellt MS-Reserved-Partition für GPT-Volumes. • Fügt in den Amazon-EC2Launch-Einstellungen den Befehl „list-volumes“ und ein Volume Dropdown hinzu. • Fügt einen get-agent-config Befehl zum Drucken der Datei agent-config.yml im Yaml- oder JSON-Format hinzu. • Löscht das statische Passwort, wenn kein öffentlicher Schlüssel erkannt wurde.	6. Oktober 2020
2.0.124	• Fügt eine Option hinzu, um die OS-Version auf dem Bildschirmhintergrund anzuzeigen. • Initialisiert verschlüsselte EBS-Volumes. • Fügt Routen für VPCs ohne lokalen DNS-Namen hinzu.	10. September 2020
2.0.104	• Erstellt die DNS-Suffix-Suchliste, wenn keine vorhanden ist. • Überspringt den Ruhezustand, wenn nicht angefordert.	12. August 2020
2.0.0	Erstversion.	30. Juni 2020

Versionshistorie des EC2Launch v2-Migrationstools

Die folgende Tabelle beschreibt die veröffentlichten Versionen des EC2Launch v2-Migrationstools.

Version	Details	Datum der Veröffentlichung
1.0.396	• Aktualisieren Sie das Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1924.	11. Juni 2024
1.0.394	• Aktualisieren Sie das Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1914.	6. Juni 2024
1.0.384	• Aktualisieren Sie das Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1881.	8. Mai 2024
1.0.358	• Aktualisieren Sie das Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1815.	8. März 2024
1.0.345	• Aktualisieren Sie das Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1739.	18. Januar 2024
1.0.342	• Aktualisieren Sie das Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1702.	5. Januar 2024
1.0.331	• Das Migrationstool wurde mit der neuesten Version des EC2Launch-v2-Agents aktualisiert: 2.0.1643 • Ein Fehler beim Ausführen von `.Install.ps1 -DryRun` wurde behoben. • Ein Problem wurde behoben, bei dem die Passwortkonfiguration bei der Migration von EC2Config fälschlicherweise auf `random` festgelegt wurde.	3. November 2023

Version	Details	Datum der Veröffentlichung
	• Ein Fehler wurde behoben, der auftrat, wenn `setWallpaper` während der Migration von EC2Launch auf `False` festgelegt ist.	
1.0.303	Aktualisierung des Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1580.	14. September 2023
1.0.286	Aktualisierung des Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1521.	14. Juli 2023
1.0.272	Aktualisierung des Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1303.	3. Mai 2023
1.0.262	Aktualisierung des Migrationstool mit der neuesten Version des EC2Launch v2-Agenten: 2.0.1245.	09. März 2023
1.0.241	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.1011.	7. Dezember 2022
1.0.218	• Validiert den aus den Metadaten der Instance abgerufenen Regionswert. • Behebt einen Fehler bei der Migration in Sprachpaketen. • Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.863.	3. September 2022
1.0.162	• Verschiebt die Logik, um Legacy-Agents auf EC2Launch v2 MSI zu entfernen. • Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.698.	18. März 2022
1.0.136	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.651.	13. Oktober 2021

Version	Details	Datum der Veröffentlichung
1.0.130	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.548.	05. August 2021
1.0.113	Verwendet IMDSv2 anstelle von IMDSv1.	4. Juni 2021
1.0.101	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.285.	12. März 2021
1.0.86	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.207.	3. Februar 2021
1.0.76	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.160.	4. Dezember 2020
1.0.69	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.153.	5. November 2020
1.0.65	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.146.	9. Oktober 2020
1.0.60	Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.124.	10. September 2020
1.0.54	• Installiert EC2Launch v2, wenn keine Agents installiert sind. • Erhöht die Versionsnummer des EC2Launch v2-Agenten auf 2.0.104. • Entkoppelt SSM Agent.	12. August 2020
1.0.50	Entfernt die NuGet Abhängigkeit.	10. August 2020
1.0.0	Erstversion.	30. Juni 2020

Konfigurieren einer Windows-Instance mithilfe von EC2Launch

EC2Launch ist eine Reihe von PowerShell Windows-Skripts, die den EC2Config-Dienst auf Windows Server 2016- und 2019-AMIs ersetzt haben. Viele dieser AMIs sind noch verfügbar. EC2Launch v2 ist der neueste Launch-Agent für alle unterstützten Windows-Versionen, der sowohl EC2Config als auch EC2Launch ersetzt. Weitere Informationen finden Sie unter Konfigurieren einer Windows-Instance mithilfe von EC2Launch v2.

> **Note**
>
> Zur Verwendung von EC2Launch mit IMDSv2 muss die Version 1.3.2002730 oder höher vorhanden sein.

Inhalt

EC2Launch-Aufgaben

EC2Launch führt beim ersten Starten einer Instance standardmäßig die folgenden Aufgaben aus:

- Richtet einen neuen Bildschirmhintergrund ein, der Informationen über die Instance gibt.
- Legt den Computernamen auf die private IPv4-Adresse der Instance fest.
- Sendet Instance-Informationen an die Amazon EC2-Konsole.
- Sendet den RDP-Zertifikat-Thumbprint an die EC2-Konsole.
- Richtet ein zufälliges Passwort für das Administratorkonto ein.
- Fügt DNS-Suffixe hinzu.
- Erweitert die Betriebssystempartition dynamisch mit nicht partitioniertem Speicherplatz.

- Führt Benutzerdaten aus (falls angegeben). Weitere Informationen zur Angabe von Benutzerdaten finden Sie unter Arbeiten mit Instance-Benutzerdaten.
- Legt persistente statische Routen fest, um den Metadatendienst und die AWS KMS Server zu erreichen.

> **Important**
>
> Wenn aus dieser Instance ein benutzerdefiniertes AMI erstellt wird, werden diese Routen als Teil der OS-Konfiguration erfasst. Alle neuen Instances, die über dieses AMI gestartet werden, übernehmen ungeachtet der Subnetz-Platzierung dieselben Routen. Informationen zum Aktualisieren dieser Routen finden Sie unter Aktualisieren von Metadaten/KMS-Routen für Server 2016 und höher beim Starten eines benutzerdefinierten AMI.

Die folgenden Aufgaben tragen dazu bei, die Abwärtskompatibilität mit dem EC2Config-Service zu erhalten. Sie können EC2Launch auch zur Ausführung dieser Aufgaben beim Startup konfigurieren:

- Initialisieren von sekundären EBS-Volumes.
- Senden von Windows-Ereignisprotokollen an die EC2-Konsolenprotokolle.
- Senden der Windows ist einsatzbereit-Meldung an die EC2-Konsole.

Weitere Informationen zu Windows Server 2019 finden Sie unter Vergleich der Features der Windows Server-Versionen auf Microsoft.com.

Telemetrie

Bei Telemetrie handelt es sich AWS um zusätzliche Informationen, die Ihnen helfen, Ihre Anforderungen besser zu verstehen, Probleme zu diagnostizieren und Funktionen bereitzustellen, mit denen Sie Ihre Erfahrung mit AWS Diensten verbessern können.

EC2Launch-Version `1.3.2003498` und später erfassen Telemetriedaten wie Nutzungsmetriken und Fehler. Diese Daten werden von der Amazon-EC2-Instance erfasst, auf der EC2Launch ausgeführt wird. Dies schließt alle Windows-AMIs ein, die Eigentum von AWS.

EC2Launch erfasst folgende Telemetrie-Typen:

- Nutzungsinformationen – Agent-Befehle, Installationsmethode und geplante Ausführungsfrequenz.
- Fehler und Diagnoseinformationen – Agent-Installation und Ausführen von Fehlercodes.

Beispiele für die gesammelten Daten:

```
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsAgentScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: IsUserDataScheduledPerBoot=true
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandCode=1
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentCommandErrorCode=5
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallCode=2
2021/07/15 21:44:12Z: EC2LaunchTelemetry: AgentInstallErrorCode=0
```

Die Telemetrie ist standardmäßig aktiviert. Sie können die Telemetriesammlung jederzeit deaktivieren. Wenn Telemetrie aktiviert ist, sendet EC2Launch Telemetriedaten ohne zusätzliche Kundenbenachrichtigungen.

Ihre Entscheidung, Telemetrie zu aktivieren oder zu deaktivieren, wird erfasst.

Sie können die Telemetriesammlung aktivieren oder deaktivieren. Ihre Auswahl zur Aktivierung bzw. Deaktivierung von Telemetrie wird erfasst, um sicherzustellen, dass wir die festgelegte Option einhalten.

Telemetrie-Sichtbarkeit

Wenn Telemetrie aktiviert ist, wird sie in der Ausgabe der Amazon-EC2-Konsole wie folgt angezeigt:

```
2021/07/15 21:44:12Z: Telemetry: <Data>
```

Deaktivieren der Telemetrie auf einer Instance

Um Telemetrie durch Festlegen einer Systemumgebungsvariablen zu deaktivieren, führen Sie den folgenden Befehl als Administrator aus:

```
setx /M EC2LAUNCH_TELEMETRY 0
```

Um die Telemetrie während der Installation zu deaktivieren, führen Sie `install.ps1` wie folgt aus:

```
. .\install.ps1 -EnableTelemetry:$false
```

Installieren der neuesten Version von EC2Launch

Mit dem folgenden Verfahren können Sie die neueste Version von EC2Launch herunterladen und auf Ihren Instances installieren.

So laden Sie die neueste Version von EC2Launch herunter und installieren sie

1. Wenn Sie EC2Launch bereits auf einer Instance installiert und konfiguriert haben, erstellen Sie ein Backup der EC2Launch-Konfigurationsdatei. Beim Installationsprozess werden Änderungen an dieser Datei nicht übernommen. Standardmäßig befindet sich die Datei im Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Laden Sie die Datei EC2-Windows-Launch.zip in ein Verzeichnis auf der Instance herunter.
3. Laden Sie die Datei install.ps1 in dasselbe Verzeichnis herunter, in das Sie `EC2-Windows-Launch.zip` heruntergeladen haben.
4. Führen Sie Folgendes aus:`install.ps1`
5. Wenn Sie ein Backup der EC2Launch-Konfigurationsdatei erstellt haben, kopieren Sie sie in das Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Um die neueste Version von EC2Launch herunterzuladen und zu installieren PowerShell

Wenn Sie EC2Launch bereits auf einer Instance installiert und konfiguriert haben, erstellen Sie ein Backup der EC2Launch-Konfigurationsdatei. Beim Installationsprozess werden Änderungen an dieser Datei nicht übernommen. Standardmäßig befindet sich die Datei im Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Um die neueste Version von EC2Launch mit zu installieren PowerShell, führen Sie die folgenden Befehle in einem Fenster aus PowerShell

```
mkdir $env:USERPROFILE\Desktop\EC2Launch
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/EC2-Windows-Launch.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Launch/latest/install.ps1"
$DownloadZipFile = "$env:USERPROFILE\Desktop\EC2Launch\" + $(Split-Path -Path $Url -Leaf)
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
& $env:USERPROFILE\Desktop\EC2Launch\install.ps1
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert

werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Prüfen Sie zur Verifizierung der Installation, ob `C:\ProgramData\Amazon\EC2-Windows\Launch` angelegt wurde.

Prüfen der EC2Launch-Version

Verwenden Sie den folgenden PowerShell Windows-Befehl, um die installierte Version von EC2Launch zu überprüfen.

```
PS C:\> Test-ModuleManifest -Path "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1" | Select Version
```

EC2Launch-Verzeichnisstruktur

EC2Launch wird bei AMIs mit Windows Server 2016 und höher standardmäßig im Stammverzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch` installiert.

> **Note**
>
> Windows blendet Dateien und Ordner unter `C:\ProgramData` standardmäßig aus. Um die EC2Launch-Verzeichnisse und -Dateien anzuzeigen, müssen Sie entweder den Pfad im Windows Explorer eingeben oder die Ordnereigenschaften so ändern, dass ausgeblendete Dateien und Ordner angezeigt werden.

Das Verzeichnis `Launch` enthält die folgenden Unterverzeichnisse.

- `Scripts`— Enthält die PowerShell Skripten, aus denen EC2Launch besteht.
- `Module` — Enthält das Modul zum Aufbau von Amazon EC2-Scripts.
- `Config` — Enthält Script-Konfigurationsdateien, die Sie anpassen können.
- `Sysprep` — Enthält Sysprep-Ressourcen.
- `Settings` — Enthält eine Anwendung für die grafische Benutzeroberfläche von Sysprep.

- `Library`: Enthält freigegebene Bibliotheken für EC2-Startagenten.
- `Logs` — Enthält von Scripts generierte Protokolldateien.

EC2Launch-Version und höher **`1.3.2004592`**

Benutzer der `Administrators` Gruppe haben `Full control` Berechtigungen für alle EC2Launch-Verzeichnisse. Benutzer, die nicht zur Administratorgruppe gehören, haben `Read & execute` Berechtigungen für alle EC2Launch-Verzeichnisse außer. `C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Config` Das `Config` Verzeichnis ist auf Benutzer beschränkt, die Mitglieder der `Administrators` Gruppe sind.

EC2Launch-Version **`1.3.2004491`** und früher

Alle EC2Launch-Verzeichnisse erben ihre Berechtigungen von, außer `C:\ProgramData` `C:\ProgramData\Amazon\EC2-Windows\Launch\Module\Scripts` Dieser Ordner erbt alle ursprünglichen Berechtigungen aus dem `C:\ProgramData` Zeitpunkt seiner Erstellung, entzieht normalen Benutzern jedoch den Zugriff auf das Verzeichnis. `CreateFiles`

Konfigurieren von EC2Launch

Wenn Ihre Instance zum ersten Mal initialisiert wurde, können Sie EC2Launch so konfigurieren, dass das Programm erneut ausgeführt wird und beim Startup verschiedene Aufgaben ausführt.

Aufgaben

- Konfigurieren von Initialisierungsaufgaben
- Planen von EC2Launch für die Ausführung bei jedem Start
- Initialisieren von Laufwerken und Zuordnen von Laufwerksbuchstaben
- Senden von Windows-Ereignisprotokollen an die EC2-Konsole
- Senden einer „Windows ist einsatzbereit“-Meldung nach erfolgreichem Start

Konfigurieren von Initialisierungsaufgaben

Geben Sie die Einstellungen in der Datei `LaunchConfig.json` an, um die folgenden Initialisierungsaufgaben zu aktivieren oder zu deaktivieren:

- Setzen Sie den Computernamen auf die private IPv4-Adresse der Instance.
- Stellen Sie den Monitor so ein, dass er immer eingeschaltet bleibt.

- Erstellen eines neuen Bildschirmhintergrunds.
- Hinzufügen einer DNS-Suffixliste.

> **Note**
>
> Dadurch wird eine DNS-Suffix-Suffixsuche für die folgende Domäne hinzugefügt und andere Standardsuffixe konfiguriert. Weitere Informationen darüber, wie Launch-Agents DNS-Suffixe festlegen, finden Sie unter. Konfigurieren Sie das DNS-Suffix für Windows-Startagenten
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- Erweitern der Größe des Boot-Volumes.
- Legen Sie das Administrator-Passwort fest.

So konfigurieren Sie die Initialisierungseinstellungen

1. Öffnen Sie in der Instance, die Sie konfigurieren möchten, die folgende Datei in einem Texteditor: `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\LaunchConfig.json`.
2. Aktualisieren Sie nach Bedarf die folgenden Einstellungen, und speichern Sie Ihre Änderungen. Geben Sie in `adminPassword` nur dann ein Passwort an, wenn `adminPasswordtype` `Specify` ist.

```
{
 "setComputerName": false,
 "setMonitorAlwaysOn": true,
 "setWallpaper": true,
 "addDnsSuffixList": true,
 "extendBootVolumeSize": true,
 "handleUserData": true,
 "adminPasswordType": "Random | Specify | DoNothing",
 "adminPassword": "password that adheres to your security policy (optional)"
}
```

Die Passworttypen sind wie folgt definiert:

`Random`

EC2Launch generiert ein Passwort und verschlüsselt es mit dem Schlüssel des Benutzers: Die Einstellung wird vom System nach dem Start der Instance deaktiviert, so dass das Passwort weiterhin gilt, wenn die Instance neu gestartet bzw. angehalten und gestartet wird.

`Specify`

EC2Launch verwendet das Passwort, das Sie unter angebe `adminPassword`. Wenn das Passwort nicht den Systemanforderungen entspricht, erstellt EC2Launch stattdessen ein zufälliges Passwort. Das Passwort wird in `LaunchConfig.json` im Klartext gespeichert und gelöscht, wenn Sysprep das Administratorpasswort einstellt. EC2Launch verschlüsselt das Passwort mit dem Schlüssel des Benutzers.

`DoNothing`

EC2Launch verwendet das Passwort, das Sie in der Datei `unattend.xml`-Datei angeben. Wenn Sie in der Datei `unattend.xml` kein Passwort angeben, ist das Administratorkonto deaktiviert.

3. Führen Sie in Windows den folgenden Befehl aus PowerShell, um die Ausführung des Skripts als geplante Windows-Aufgabe zu planen. Das Script wird beim nächsten Starten einmal ausgeführt und deaktiviert dann die erneute Ausführung dieser Aufgaben.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
Schedule
```

Planen von EC2Launch für die Ausführung bei jedem Start

Sie können EC2Launch so planen, dass es bei jedem Start läuft und nicht nur beim ersten Start.

So aktivieren Sie die Ausführung von EC2Launch bei jedem Start

1. Öffnen Sie Windows PowerShell und führen Sie den folgenden Befehl aus:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -
SchedulePerBoot
```

2. Alternativ können Sie die ausführbare Datei mit dem folgenden Befehl ausführen:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe
```

Wählen Sie dann `Run EC2Launch on every boot` aus. Sie können für Ihre EC2-Instance `Shutdown without Sysprep` oder `Shutdown with Sysprep` festlegen.

> **Note**
>
> Wenn Sie EC2Launch bei jedem Start aktivieren, passiert folgendes, wenn EC2Launch das nächste Mal ausgeführt wird:
>
> - Wenn `AdminPasswordType` immer noch auf `Random` gesetzt ist, generiert EC2Launch beim nächsten Booten ein neues Passwort. Nach diesem Bootvorgang wird `AdminPasswordType` automatisch auf `DoNothing` gesetzt, um zu verhindern, dass EC2Launch bei nachfolgenden Bootvorgängen neue Kennwörter generiert. Um zu verhindern, dass EC2Launch beim ersten Booten ein neues Passwort generiert, setzen Sie `AdminPasswordType` vor dem Neustart manuell auf `DoNothing`.
> - `HandleUserData` wird auf `false` zurückgesetzt, es sei denn, für die Benutzerdaten ist `persist` für die Einstellung `true` angegeben. Weitere Informationen finden Sie unter the section called “Benutzerdatenskripts”.

Initialisieren von Laufwerken und Zuordnen von Laufwerksbuchstaben

Geben Sie die Einstellungen in der Datei `DriveLetterMappingConfig.json` an, um den Volumes auf Ihrer EC2-Instance Laufwerksbuchstaben zuzuordnen. Das Skript initialisiert Laufwerke, die noch nicht initialisiert und partitioniert sind. Weitere Informationen zum Abrufen von Volume-Details in Windows finden Sie unter Get-Volume in der Microsoft-Dokumentation.

So ordnen Sie Volumes Laufwerkbuchstaben zu

1. Öffnen Sie die Datei `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` in einem Text-Editor.
2. Geben Sie die folgenden Volume-Einstellungen an, und speichern Sie Ihre Änderungen:

```
{
 "driveLetterMapping": [
  {
```

```
    "volumeName": "sample volume",
    "driveLetter": "H"
   }
  ]
}
```

3. Öffnen Sie Windows PowerShell und führen Sie mit dem folgenden Befehl das EC2Launch-Skript aus, das die Festplatten initialisiert:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Fügen Sie die Flag `-Schedule` wie folgt hinzu, um die Datenträger bei jedem Start der Instance zu initialisieren:

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

Senden von Windows-Ereignisprotokollen an die EC2-Konsole

Geben Sie die Einstellungen in der Datei `EventLogConfig.json` an, damit Windows-Ereignisprotokolle an EC2-Konsolenprotokolle gesendet werden.

So konfigurieren Sie die Einstellungen zum Senden von Windows-Ereignisprotokollen

1. Öffnen Sie in der Instance die Datei `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\EventLogConfig.json` in einem Text-Editor.
2. Konfigurieren Sie die folgenden Protokoll-Einstellungen an, und speichern Sie Ihre Änderungen:

```
{
 "events": [
  {
   "logName": "System",
   "source": "An event source (optional)",
   "level": "Error | Warning | Information",
   "numEntries": 3
  }
 ]
}
```

3. Führen Sie in Windows den folgenden Befehl aus PowerShell, sodass das System das Skript so plant, dass es bei jedem Start der Instance als geplante Windows-Aufgabe ausgeführt wird.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendEventLogs.ps1 -
Schedule
```

   Es kann drei Minuten oder länger dauern, bis die Protokolle in den EC2-Konsolenprotokollen angezeigt werden.

Senden einer „Windows ist einsatzbereit“-Meldung nach erfolgreichem Start

Der EC2Config-Service sendete nach jedem Starten die Meldung „Windows ist einsatzbereit“ an die EC2-Konsole. EC2Launch sendet diese Meldung nur nach dem ersten Starten. Um die Abwärtskompatibilität mit dem EC2Config-Service zu gewährleisten, können Sie EC2Launch so konfigurieren, dass diese Meldung nach jedem Startvorgang gesendet wird. Öffnen Sie auf der Instance Windows PowerShell und führen Sie den folgenden Befehl aus. Das System führt das Skript als geplante Windows-Task aus.

```
PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\SendWindowsIsReady.ps1 -
Schedule
```

EC2Launch-Versionsverlauf

Windows AMIs ab Windows Server 2016 enthalten eine Reihe von Windows Powershell-Scripts mit der Bezeichnung EC2Launch. EC2Launch führt während des ersten Starts der Instance einige Aktionen durch. Informationen zu den in Windows-AMIs enthaltenen EC2Launch-Versionen finden Sie im AWS AWS Windows AMI-Versionsverlauf.

Informationen zum Herunterladen der neuesten Version von EC2Launch finden Sie unter Installieren der neuesten Version von EC2Launch.

Die folgende Tabelle beschreibt die von EC2Launch veröffentlichten Versionen. Beachten Sie, dass sich das Versionsformat nach Version 1.3.610 geändert hat.

Version	Details	Datum der Veröffentlichung
1.3.2004891	•	31. Mai 2024

Version	Details	Datum der Veröffentlichung
	Es wurde ein Problem behoben, bei dem nicht wie erwartet auf eingestellt `HandleUserData` war. `false` • Es wurde eine `Encrypted` Passwortoption zu hinzugefügt`LaunchConfig.json` . • Das `Settings UI` Verhalten wurde geändert, sodass das vom Benutzer angegebene Passwort standardmäßig verschlüsselt wird. • Es wurde hinzugefügt`SetAdminPasswordConfig.ps1` , um die `Specify` Kennwortoption in die `Encrypted` Kennwortoption in der Agenten-Konfigurationsdatei zu konvertieren.	
1.3.2004617	• Ein Fehler beim Einstellen des Hintergrundbilds wurde behoben.	15. Januar 2024

Version	Details	Datum der Veröffentlichung
1.3.2004592	• Die von install.ps1 festgelegten Zugriffsrechte für `%ProgramData%\Amazon\EC2-Windows\Launch` wurden aktualisiert. • Eingeschränkter EC2Launch-Ordner-/Dateizugriff auf Lese- und Ausführungsrechte nur für Standardbenutzerkonten. • Der Agent wartet nun nicht mehr auf die Initialisierung des Instance Metadata Service (IMDS), wenn IMDS für die Instance nicht aktiviert ist. • Beim Warten auf die Initialisierung des IMDS wurde ein Zeitlimit von fünf Minuten hinzugefügt. • Der Agent schreibt nun die Telemetriedaten vor der `Windows is Ready`-Meldung in das Konsolenprotokoll der Instance, anstatt danach. • Mehrere neue Instance-Typen unterstützen jetzt Bildschirmhintergründe. Weitere Informationen zu Zugriffsberechtigungen und Benutzerkontenberechtigungen für EC2Launch-Verzeichnisse finden Sie unter. the section called “EC2Launch-Verzeichnisstruktur”	2. Januar 2024
1.3.2004491	• Telemetrie wurde hinzugefügt, um die Verwendung der Option Administratorpasswort angeben zu überwachen.	9. November 2023
1.3.2004462	• Es wurde ein Leerungsvorgang nach jedem Schreibvorgang in die serielle Konsole hinzugefügt.	18. Oktober 2023

Version	Details	Datum der Veröffentlichung
1.3.2004438	• Einschränkung der Übertragung von Domainnamen auf der Grundlage eines Registrierungseintrags: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • `UserdataExecution.log` -Berechtigungen nur auf `Administrators` beschränkt. • Dem Windows-Ereignisprotokoll wurden Fehlermeldungen hinzugefügt, wenn die Protokollinitialisierung fehlschlägt.	04. Oktober 2023
1.3.2004256	• `EnableSCSIPersistentReservations` -Wert dem Konsolenprotokoll hinzugefügt. • Wiederholungsfunktion für Get-ConsolePort hinzugefügt.	07. Juli 2023
1.3.2004052	• Fehler behoben, wenn beim Start der Instance kein SSH-Schlüssel angegeben wurde. • Aktualisiert, um den Start des AmazonSSMAgent Windows-Dienstes bei Fehlern zu wiederholen. • Es wurde aktualisiert, sodass die Datei SysprepInstance .ps1 fehlschlägt, falls BeforeSysprep .cmd mit einem Exit-Code ungleich Null fehlschlägt.	08. März 2023
1.3.2003975	• Problem behoben, das sich auf Packer-AMI-Builds auswirkte, bei dem `SysprepInstance.ps1` einen `$LastErrorCode` von 1 zurückgegeben hat.	24. Dezember 2022

Version	Details	Datum der Veröffentlichung
1.3.2003961	• Problem behoben, bei dem explizit angegebene Administratorkennwörter auf schnell gestarteten Instances mit einem zufälligen Passwort überschrieben wurden. • Problem behoben, bei dem der SSM-Agent auf kleineren Instance-Typen nicht gestartet werden konnte. • Problem behoben, bei dem das Instance-Konsolenprotokoll `RDPCERTIFICATE-THUMBPRINT: 0000000000000000000000000000000000000000` anstelle eines gültigen RDP-Zertifikats einen Fingerabdruckwert enthielt.	6. Dezember 2022
1.3.2003923	• Korrigiert die Logik für die Suche nach einem Netzwerkadapter, wenn PnPDeviceID leer ist.	9. November 2022
1.3.2003919	• Die PCI-Segmentinformationen ConsolePort zur Verwendung wurden aktualisiert. • Problem behoben, bei dem nach einem Neustart ein falscher Netzwerkadapter ausgewählt werden konnte. • Die Timeout-Logik für den Start-SSM-Agent wurde korrigiert. • Die Abwärtskompatibilität für den Alias der AdminCredentials Send-Funktion wurde behoben.	8. November 2022
1.3.2003857	• Priorisiert Adapter mit einem Standard-Gateway, wenn der primäre Netzwerkadapter ausgewählt ist. • Speicherinterne Passwortverschlüsselung erweitert.	3. Oktober 2022

Version	Details	Datum der Veröffentlichung
1.3.2003824	• Fehler bei `setComputerName` behoben. • Logik hinzugefügt, um die Windows-Aktivierung bei Erkennung eines BYOL-Abrechnungscodes zu überspringen. • Speicherinterne Passwortverschlüsselung hinzugefügt. • Fehler bei der Volume-Initialisierung auf `m6id.4xlarge` behoben.	30. August 2022
1.3.2003691	• Die IMDS-Wartelogik wurde aktualisiert, um nur IMDSv2-Anforderungen zu stellen. • Fehler behoben, der die eGPU-Installation beeinträchtigte.	21. Juni 2022
1.3.2003639	• Die Wartelogik des Netzwerkadapters wurde hinzugefügt, um die Verwendung vor der Initialisierung zu verhindern. • Kleinere Probleme wurden behoben.	10. Mai 2022
1.3.2003498	• Telemetrie hinzugefügt. • Verknüpfung zur Einstellungen-Benutzeroberfläche hinzugefügt. • Formatierte Skripte. PowerShell • Das Problem, dass das System heruntergefahren wurde, bevor BeforeSysprep .cmd abgeschlossen wurde, wurde behoben.	31. Januar 2022
1.3.2003411	Logik zur Passworterstellung geändert, um Passwörter mit geringer Komplexität auszuschließen.	04. August 2021
1.3.2003364	Aktualisierte Installation — EgpuManager mit IMDSv2-Unterstützung.	7. Juni 2021

Version	Details	Datum der Veröffentlichung
1.3.2003312	• Protokollzeilen vor und nach `setMonitorAlwaysOn` -Einstellung hinzugefügt. • Die AWS Nitro Enclaves-Paketversion wurde zum Konsolenprotokoll hinzugefügt.	04. Mai 2021
1.3.2003284	Das Berechtigungsmodell wurde verbessert, indem der Speicherort von Benutzerdaten zu `LocalAppData` aktualisiert wurde.	23. März 2021
1.3.2003236	• Aktualisierte Methode zum Festlegen des Benutzerpassworts in `Set-AdminAccount` und `Randomize-LocalAdminPassword` . • Behoben`InitializeDisks` , um zu überprüfen, ob die Festplatte nur auf Lesen eingestellt ist, bevor sie auf beschreibbar gesetzt wird.	11. Februar 2021
1.3.2003210	Lokalisierungsupdate für `install.ps1` .	7. Januar 2021
1.3.2003205	Sicherheitsupdate für `install.ps1` zum Aktualisieren von Berechtigungen für das `%ProgramData%AmazonEC2-WindowsLaunchModuleScripts` -Verzeichnis.	28. Dezember 2020
1.3.2003189	`w32tm resync` hinzugefügt, nachdem Routen hinzugefügt wurden.	4. Dezember 2020
1.3.2003155	Informationen zum Instance-Typ wurden aktualisiert.	25. August 2020
1.3.2003150	`OsCurrentBuild` und `OsReleaseId` zur Konsolenausgabe hinzugefügt.	22. April 2020
1.3.2003040	IMDS Version 1 Fallback-Logik wurde korrigiert.	7. April 2020

Version	Details	Datum der Veröffentlichung
1.3.2002730	Unterstützung für IMDS V2 hinzugefügt.	3. März 2020
1.3.2002240	Kleinere Probleme wurden behoben.	31. Oktober 2019
1.3.2001660	Automatisches Anmeldeproblem für Benutzer ohne Passwort nach der ersten Ausführung von Sysprep behoben.	2. Juli 2019
1.3.2001360	Kleinere Probleme wurden behoben.	27. März 2019
1.3.2001220	Alle PowerShell Skripte sind signiert.	28. Februar 2019
1.3.2001200	Es wurde ein Problem mit InitializeDisks .ps1 behoben, bei dem durch die Ausführung des Skripts auf einem Knoten in einem Windows Server-Failovercluster Laufwerke auf Remotekno ten formatiert wurden, deren Laufwerksbuchstabe dem lokalen Laufwerksbuchstaben entsprach.	27. Februar 2019
1.3.2001160	Das fehlende Hintergrundbild in Windows 2019 wurde hinzugefü gt.	22. Februar 2019
1.3.2001040	• Es wurde ein Plug-In hinzugefügt, mit dem sich einstellen lässt, dass der Monitor nie ausgeschaltet wird, um ACPI-Prob leme zu beheben. • SQL Server-Edition und -Version werden in die Konsole geschrieben.	21. Januar 2019
1.3.2000930	Ein Fehler beim Hinzufügen von Routen zu Metadaten auf ENIs mit IPv6-Unterstützung wurde behoben.	2. Januar 2019

Version	Details	Datum der Veröffentlichung
1.3.2000760	• Standardkonfiguration für RSS- und Empfangswarteschlangen-Einstellungen für ENA-Geräte hinzugefügt. • Ruhezustand während Sysprep deaktiviert.	5. Dezember 2018
1.3.2000630	• Route 169.254.169.253/32 für DNS-Server hinzugefügt. • Filter der Einstellung des Admin-Benutzers hinzugefügt. • Verbesserungen beim Instance-Ruhezustand. • Option hinzugefügt, um EC2Launch so zu planen, dass es bei jedem Start ausgeführt wird.	9. November 2018
1.3.2000430.0	• Route 169.254.169.123/32 zum AMZN-Zeitservice hinzugefügt. • Route 169.254.169.249/32 zum GRID-Lizenzdienst hinzugefügt. • Beim Versuch, Systems Manager zu starten, wurde ein Timeout von 25 Sekunden hinzugefügt.	19. September 2018
1.3.200039.0	• Fehlerhafte Laufwerksbeschriftung für EBS NVME-Volumes behoben. • Zusätzliche Protokollierung für NVME-Treiberversionen hinzugefügt.	15. August 2018
1.3.2000080	Kleinere Probleme wurden behoben.	
1.3.610	Behebung eines Fehlers mit der Umleitung von Ausgabe und Fehlern von Benutzerdaten zu Dateien.	
1.3.590	• Hinzufügung fehlender Instance-Types im Hintergrundbild. • Behebung eines Fehlers mit Laufwerkbuchstabenzuordnung und Festplatteninstallation.	

Version	Details	Datum der Veröffentlichung
1.3.580	• Behebung von `Get-Metadata` zur Verwendung der Standard-Systemproxyeinstellungen für Webanfragen. • Hinzufügung eines besonderen Falls für NVMe bei der Festplatteninitialisierung. • Kleinere Probleme wurden behoben.	
1.3.550	Hinzufügung einer `-NoShutdown` -Option zur Aktivierung von Sysprep ohne Herunterfahren.	
1.3.540	Kleinere Probleme wurden behoben.	
1.3.530	Kleinere Probleme wurden behoben.	
1.3.521	Kleinere Probleme wurden behoben.	
1.3.0	• Ein Problem mit einer hexadezimalen Länge für eine Computer-Namen-Änderung wurde behoben. • Ein Problem mit einer möglichen Neustartschleife für eine Computer-Namen-Änderung wurde behoben. • Ein Problem mit der Einrichtung eines Bildschirmhintergrunds wurde behoben.	
1.2.0	• Aktualisierung zum Anzeigen von Informationen über das installierte Betriebssystem (OS) im EC2-Systemprotokoll. • Aktualisierung zum Anzeigen der Version von EC2Launch und SSM Agent im EC2-Systemprotokoll. • Kleinere Probleme wurden behoben.	

Version	Details	Datum der Veröffentlichung
1.1.2	• Aktualisierung zum Anzeigen von ENA-Treiberinformationen im EC2-Systemprotokoll. • Aktualisierung zum Ausschließen von Hyper-V von primärer NIC-Filterlogik. • AWS KMS Server und Port wurden dem Registrierungsschlüssel für die KMS-Aktivierung hinzugefügt. • Die Einrichtung des Bildschirmhintergrunds wurde für mehrere Benutzer verbessert. • Aktualisierung zum Löschen von Routen aus dem persistenten Speicher. • Aktualisierung zum Entfernen des z von Availability Zone in der DNS-Suffixliste. • Update zur Behebung eines Problems mit dem <run AsLocal System>-Tag in den Benutzerdaten.	
1.1.1	Erstversion.	

Konfigurieren Sie eine Windows-Instanz mithilfe des EC2Config-Dienstes (Legacy)

> **Note**
>
> Die EC2Config-Dokumentation dient nur als historische Referenz. Die Betriebssystemversionen, auf denen es ausgeführt wird, werden von Microsoft nicht mehr unterstützt. Wir empfehlen dringend, auf den neuesten Startdienst zu aktualisieren.
> Der neueste Startservice für Windows Server 2022 ist EC2Launch v2, der sowohl EC2Config als auch EC2Launch ersetzt.

Windows-AMIs für Windows Server-Versionen vor Windows Server 2016 beinhalten einen optionalen Dienst, den EC2Config-Dienst ()`EC2Config.exe`. EC2Config startet, wenn die Instance hochgefahren wird. Darüber hinaus führt der Service beim ersten Startup sowie bei jedem Stoppen und Starten der Instance Aufgaben aus. Zudem kann EC2Config nach Bedarf Aufgaben ausführen. Einige dieser Aufgaben sind automatisch aktiviert, während andere manuell aktiviert werden müssen. Obwohl dieser Service optional ist, liefert er Zugriff auf erweiterte Features, die anderweitig nicht verfügbar sind. Dieser Dienst wird im Konto ausgeführt. LocalSystem

> **Note**
>
> EC2Launch ersetzt den EC2Config-Service auf Windows-AMIs für Windows Server 2016 und 2019. Weitere Informationen finden Sie unter Konfigurieren einer Windows-Instance mithilfe von EC2Launch. Der neueste Startservice für alle unterstützten Windows Server-Versionen ist EC2Launch v2, der sowohl EC2Config als auch EC2Launch ersetzt.

EC2Config verwendet Einstellungsdateien, um den eigenen Betrieb zu kontrollieren. Sie können diese Einstellungsdateien aktualisieren, indem Sie entweder ein grafisches Tool verwenden oder die XML-Dateien direkt bearbeiten. Die Binärdateien des Service sowie zusätzliche Dateien befinden sich im Verzeichnis `%ProgramFiles%\Amazon\EC2ConfigService`.

Inhalt

EC2Config-Aufgaben

EC2Config führt die Startaufgaben beim ersten Startup der Instance aus und deaktiviert sie anschließend. Um diese Aufgaben erneut ausführen zu können, müssen Sie sie vor dem Herunterfahren der Instance ausdrücklich aktivieren oder Sysprep manuell ausführen. Es handelt sich dabei um die folgenden Aufgaben:

- Einrichtung eines zufälligen, verschlüsselten Passworts für das Administratorkonto.
- Generation und Installation des Hostzertifikats zur Verwendung für die Remote Desktop Connection.
- Erweiterung der Betriebssystempartition, um den gesamten nicht partitionierten Speicherplatz mit einzuschließen.
- Ausführung der angegebenen Benutzerdaten (sowie von Cloud-Init, sofern installiert). Weitere Informationen zur Angabe von Benutzerdaten finden Sie unter Arbeiten mit Instance-Benutzerdaten.

EC2Config führt beim ersten Start einer Instance die folgenden Aufgaben aus:

- Änderung des Hostnamens, sodass er mit der privaten IP-Adresse in Hexa-Schreibweise übereinstimmt. (Diese Aufgabe ist standardmäßig deaktiviert und muss zunächst aktiviert werden, um beim Start der Instance ausgeführt werden zu können.)
- Konfiguration des Schlüsselverwaltungsservers (Key Management Server,AWS KMS), Überprüfung des Aktivierungsstatus von Windows und gegebenenfalls die Aktivierung von Windows.
- Mounten aller Amazon EBS-Volumes und Instance-Speicher-Volumes sowie Zuweisung der Volumenamen zu den Laufwerkbuchstaben.
- Schreiben der Ereignisprotokolleinträge in die Konsole, um die Fehlerbehebung zu unterstützen. (Diese Aufgabe ist standardmäßig deaktiviert und muss zunächst aktiviert werden, um beim Start der Instance ausgeführt werden zu können.)
- Mitteilung an die Konsole schreiben, dass Windows einsatzbereit ist.
- Hinzufügung einer benutzerdefinierten Route zum primären Netzwerkadapter, um die folgenden IP-Adressen zu aktivieren, wenn eine einzelne NIC oder mehrere NICs zugeordnet sind: `169.254.169.250`, `169.254.169.251` und `169.254.169.254`. Diese Adressen werden von der Windows-Aktivierung und beim Zugriff auf Instance-Metadaten verwendet.

> **Note**
>
> Wenn das Windows-Betriebssystem für die Verwendung von IPv4 konfiguriert ist, können diese Link-local-IPv4-Adressen verwendet werden. Wenn das Windows-Betriebssystem den IPv4-Netzwerkprotokollstack deaktiviert hat und stattdessen IPv6 verwendet, fügen Sie `[fd00:ec2::240]` anstelle von `169.254.169.250` und `169.254.169.251` hinzu. Dann fügen Sie `[fd00:ec2::254]` anstelle von `169.254.169.254` hinzu.

EC2Config führt bei jedem Anmelden eines Benutzers die folgenden Aufgaben aus:

- Anzeigen der Informationen zum Bildschirmhintergrund auf dem Desktop-Hintergrund.

Während die Instance ausgeführt wird, können Sie beantragen, dass EC2Config die folgenden Aufgaben nach Bedarf ausführt:

- Ausführung von Sysprep und Herunterfahren der Instance, damit Sie daraus ein AMI erstellen können. Weitere Informationen finden Sie unter Erstellen Sie ein AMI mit Windows Sysprep.

Installieren der neuesten Version von EC2Config

Der EC2Config-Service ist standardmäßig in AMIs für Windows Server-Versionen vor Windows Server 2016 enthalten. Wenn der EC2Config-Dienst aktualisiert wird, AWS enthalten neue Windows-AMIs von die neueste Version des Dienstes. Sie müssen jedoch Ihre eigenen Windows AMIs und Instances mit der aktuellen Version von EC2Config aktualisieren.

> **Note**
>
> EC2Launch ersetzt den EC2Config-Service auf Windows Server 2016 und 2019. Weitere Informationen finden Sie unter Konfigurieren einer Windows-Instance mithilfe von EC2Launch. Der neueste Startservice für alle unterstützten Windows Server-Versionen ist EC2Launch v2, der sowohl EC2Config als auch EC2Launch ersetzt.

Weitere Informationen darüber, wie Sie Benachrichtigungen über EC2Config-Updates erhalten, finden Sie unter Abonnieren von EC2Config-Service-Benachrichtigungen. Informationen über Änderungen in den einzelnen Versionen finden Sie unter EC2Config-Versionshistorie.

Bevor Sie beginnen

- Vergewissern Sie sich, dass Sie über das .NET-Framework 3.5 SP1 oder höher verfügen.
- Standardmäßig ersetzt Setup Ihre Einstellungsdateien während der Installation mit Standardeinstellungsdateien und startet den EC2Config-Service nach Abschluss der Installation neu. Wenn Sie die EC2Config-Serviceeinstellungen geändert haben, kopieren Sie die Datei `config.xml` aus dem Verzeichnis `%Program Files%\Amazon\Ec2ConfigService\Settings`. Nachdem Sie den EC2Config-Service aktualisiert haben, können Sie die Datei wiederherstellen, um Ihre Konfigurationsänderungen zu erhalten.
- Wenn eine ältere Version von EC2Config vorliegt als Version 2.1.19, können Sie Version 2.2.12 oder höher direkt installieren, müssen Sie zuerst Version 2.1.19 installieren. Um die Version 2.1.19 zu installieren, laden Sie EC2Install_2.1.19.zip herunter, entpacken Sie die Datei und führen Sie `EC2Install.exe` aus.

> **Note**
>
> Wenn eine ältere Version von EC2Config vorliegt als Version 2.1.19, können Sie Version 2.3.313 oder höher direkt installieren, ohne zuerst Version 2.1.19 installieren zu müssen.

Überprüfen der EC2Config-Version

Gehen Sie wie folgt vor, um zu überprüfen, welche Version von EC2Config in Ihren Instances installiert ist.

So überprüfen Sie die installierte EC2Config-Version

1. Starten Sie eine Instance von Ihrem AMI und stellen Sie eine Verbindung damit her.
2. Wählen Sie in der Systemsteuerung Programs and Features aus.
3. Suchen Sie in der Liste mit den installierten Programmen nach `Ec2ConfigService`. Die Versionsnummer wird in der Spalte Version angegeben.

Aktualisieren von EC2Config

Gehen Sie wie folgt vor, um die neueste Version von EC2Config herunterzuladen und in Ihren Instances zu installieren.

So laden Sie die neueste Version von EC2Config herunter und installieren sie

1. Laden Sie das EC2Config-Installationsprogramm herunter und entzippen Sie es.
2. Führen Sie `EC2Install.exe`. Eine vollständige Liste der verfügbaren Optionen erhalten Sie, wenn Sie `EC2Install` mit der Option `/?` ausführen. Standardmäßig werden Eingabeaufforderungen angezeigt. Um den Befehl ohne Eingabeaufforderungen auszuführen, verwenden Sie die Option `/quiet`.

   > **Important**
   >
   > Um die benutzerdefinierten Einstellungen aus der von Ihnen gespeicherten Datei `config.xml` beizubehalten, führen Sie `EC2Install` mit der Option `/norestart` aus, stellen Sie Ihre Einstellungen wieder her und starten Sie den EC2Config-Service manuell neu.

3. Wenn Sie EC2Config Version 4.0 oder höher ausführen, müssen Sie SSM Agent vom Microsoft Service Snap-in aus auf der Instance neu starten.

   > **Note**
   >
   > Die aktualisierten Informationen zur EC2Config-Version werden im Instance-Systemprotokoll oder in der Trusted Advisor-Überprüfung nicht angezeigt, bis Sie Ihre Instance neu starten bzw. beenden und starten.

Um die neueste Version von EC2Config herunterzuladen und zu installieren, verwenden Sie PowerShell

Um die neueste Version von EC2Config herunterzuladen, zu entpacken und zu installieren PowerShell, führen Sie die folgenden Befehle in einem Fenster aus: PowerShell

```
$Url = "https://s3.amazonaws.com/ec2-downloads-windows/EC2Config/EC2Install.zip"
$DownloadZipFile = "$env:USERPROFILE\Desktop\" + $(Split-Path -Path $Url -Leaf)
$ExtractPath = "$env:USERPROFILE\Desktop\"
Invoke-WebRequest -Uri $Url -OutFile $DownloadZipFile
$ExtractShell = New-Object -ComObject Shell.Application
$ExtractFiles = $ExtractShell.Namespace($DownloadZipFile).Items()
$ExtractShell.NameSpace($ExtractPath).CopyHere($ExtractFiles)
Start-Process $ExtractPath
```

```
Start-Process `
    -FilePath $env:USERPROFILE\Desktop\EC2Install.exe `
    -ArgumentList "/S"
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr Terminal aktiviert werden. PowerShell Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
> ```

Prüfen Sie zur Verifizierung der Installation, ob unter `C:\Program Files\Amazon\` das Verzeichnis `Ec2ConfigService` angelegt wurde.

Beenden, Neustarten, Löschen oder Deinstallieren von EC2Config

Sie können den EC2Config-Service wie jeden anderen Service verwalten.

Um aktualisierte Einstellungen auf Ihrer Instance anzuwenden, können Sie den Service beenden und neu starten. Wenn Sie EC2Config manuell installieren möchten, müssen Sie den Service zunächst anhalten.

So beenden Sie den EC2Config-Service

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Zeigen Sie im Menü Start auf Administrative Tools (Verwaltungstools) und klicken Sie anschließend auf Services.
3. Klicken Sie mit der rechten Maustaste in der Liste der Services auf EC2Config und wählen Sie Stop aus.

So starten Sie den EC2Config Service neu

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Zeigen Sie im Menü Start auf Administrative Tools (Verwaltungstools) und klicken Sie anschließend auf Services.

3. Klicken Sie mit der rechten Maustaste auf EC2Config und wählen Sie Restart aus.

Wenn Sie weder die Konfigurationseinstellungen aktualisieren, Ihr eigenes AMI erstellen oder AWS Systems Manager verwenden müssen, können Sie den Service löschen und deinstallieren. Durch das Löschen eines Services wird der Registrierungsunterschlüssel entfernt. Durch die Deinstallation eines Services werden die Dateien, der Registrierungsunterschlüssel und alle Shortcuts zum Service entfernt.

So löschen Sie den EC2Config-Service

1. Öffnen Sie ein Befehlszeilenfenster.
2. Führen Sie den folgenden Befehl aus:

```
sc delete ec2config
```

So deinstallieren Sie EC2Config

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Klicken Sie im Start menü auf Control Panel.
3. Doppelklicken Sie auf Programs and Features.
4. Wählen Sie in der Liste der Programme EC2 ConfigService aus und klicken Sie auf Deinstallieren.

EC2Config und AWS Systems Manager

Der EC2Config-Service verarbeitet Systems Manager-Anfragen auf Instances, die aus AMIs für Windows Server-Versionen vor Windows Server 2016 erstellt und vor November 2016 veröffentlicht wurden.

Instances, die aus AMIs für Windows Server-Versionen vor Windows Server 2016 erstellt und nach November 2016 veröffentlicht wurden, enthalten den EC2Config-Service und SSM Agent. EC2Config führt alle zuvor beschriebenen Aufgaben aus und SSM Agent verarbeitet Anfragen für Systems Manager-Funktionen wie Run Command und State Manager.

Sie können über den Run Command Ihre vorhandenen Instances upgraden, damit diese die aktuelle Version des EC2Config-Service und von SSM Agent verwenden. Weitere Informationen

erhalten Sie unter Aktualisieren von SSM Agent mit Run Command im AWS Systems Manager - Benutzerhandbuch.

EC2Config und Sysprep

Der EC2Config-Service führt Sysprep aus, ein Microsoft-Tool, mit dem Sie ein benutzerdefiniertes Windows-AMI erstellen können, das wiederverwendet werden kann. Wenn EC2Config Sysprep aufruft, verwendet es die Dateien in `%ProgramFiles%\Amazon\EC2ConfigService\Settings`, um zu bestimmen, welche Operationen ausgeführt werden sollen. Sie können diese Dateien indirekt über das Dialogfeld EC2 Service Properties (EC2-Serviceeigenschaften) oder direkt in einem XML-Editor oder einem Texteditor bearbeiten. Es gibt jedoch einige erweiterte Einstellungen, die nicht im Dialogfeld Ec2 Service Properties verfügbar sind. Diese Einträge müssen Sie direkt bearbeiten.

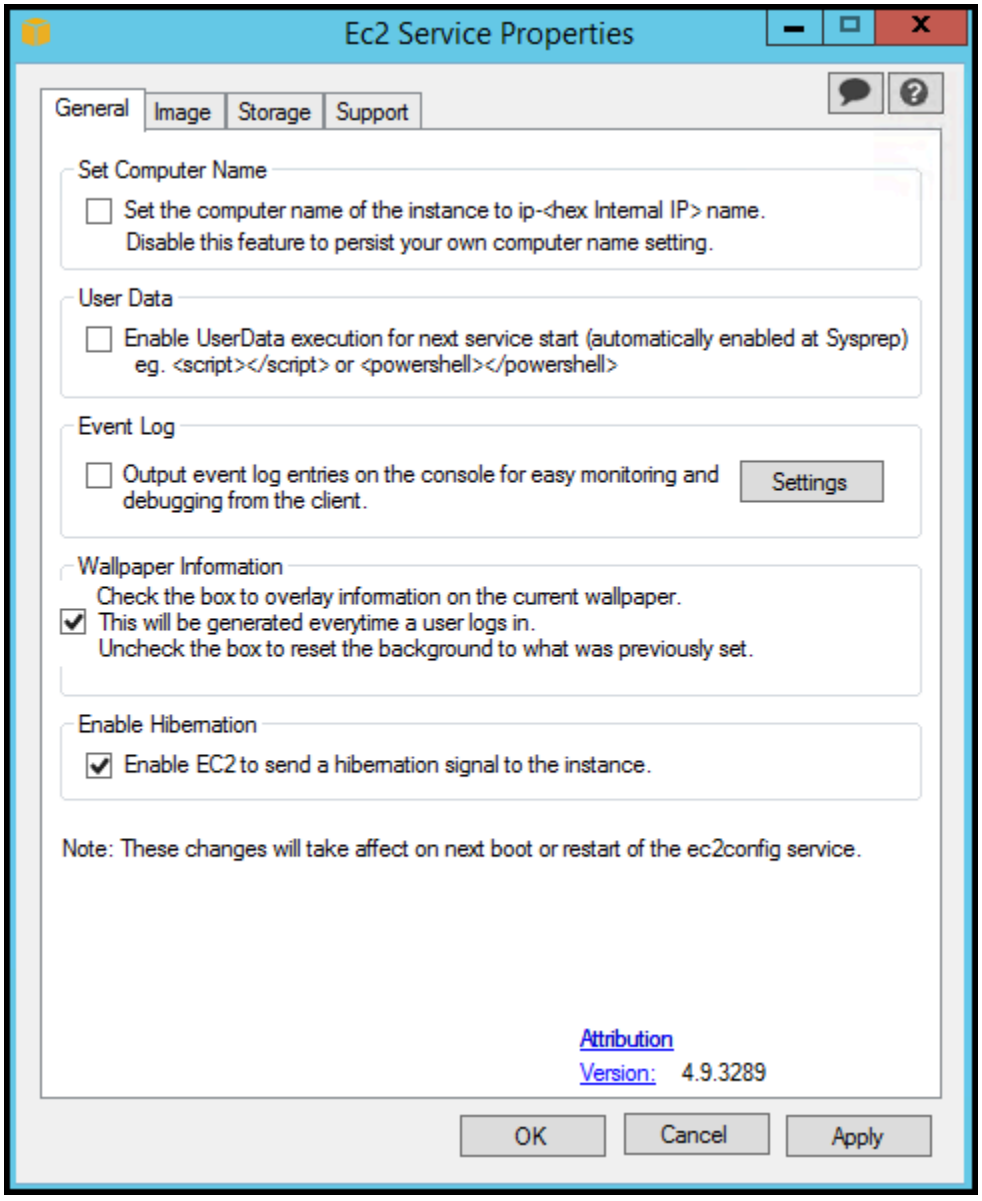
Wenn Sie ein AMI aus einer Instance erstellen, nachdem Sie deren Einstellungen aktualisiert haben, werden die neuen Einstellungen auf alle Instances angewandt, die von diesem AMI gestartet werden. Weitere Informationen über die Erstellung eines AMI finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

EC2-Service-Eigenschaften

Der folgende Vorgang beschreibt, wie die Einstellungen anhand des Dialogfelds Ec2 Service Properties aktiviert bzw. deaktiviert werden.

So ändern Sie die Einstellungen mithilfe des Dialogfelds Ec2 Service Properties

1. Starten Sie die Windows-Instance und stellen Sie eine Verbindung zu ihr her.
2. Klicken Sie im Startmenü auf Alle Programme und dann auf ConfigServiceEC2-Einstellungen.



3. Aktivieren bzw. deaktivieren Sie auf der Registerkarte General (Allgemein) im Dialogfeld EC2 Service Properties (EC2-Serviceeigenschaften) die folgenden Einstellungen.

   Set Computer Name

   Wenn diese Einstellung aktiviert ist (standardmäßig ist sie deaktiviert), wird der Hostname bei jedem Start mit der aktuellen internen IP-Adresse verglichen. Stimmen der Hostname und die interne IP-Adresse nicht überein, wird der Hostname zurückgesetzt, sodass er die interne IP-Adresse enthält und das System wird anschließend neu gestartet, um den neuen Hostnamen zu übernehmen. Aktivieren Sie diese Einstellung nicht, wenn Sie Ihren eigenen Hostnamen einrichten oder verhindern möchten, dass Ihr vorhandener Hostname geändert wird.

User Data

Die Ausführung der Benutzerdaten ermöglicht es Ihnen, in den Instance-Metadaten Skripts anzugeben. Standardmäßig werden diese Skripts beim ersten Start ausgeführt. Sie können sie auch so konfigurieren, dass sie beim nächsten Neustart oder Start der Instance oder bei jedem Neustart oder Start der Instance ausgeführt werden.

Wenn Sie ein großes Skript verwenden, empfehlen wir Ihnen, das Skript mithilfe der Benutzerdaten herunterzuladen und es anschließend auszuführen.

Weitere Informationen finden Sie unter Ausführung von Benutzerdaten.

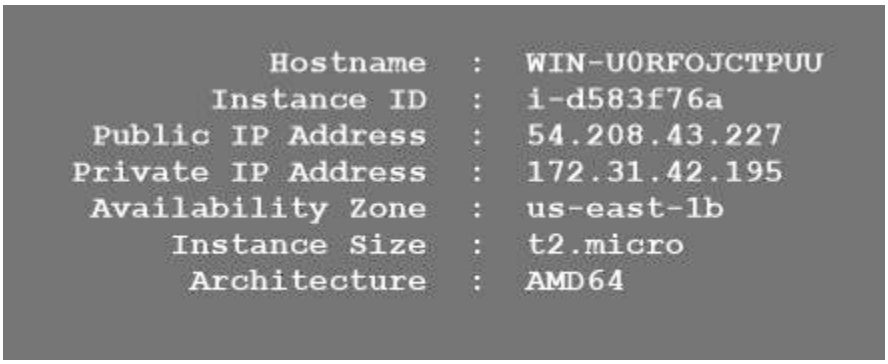
Ereignisprotokoll

Verwenden Sie diese Einstellung, um Ereignisprotokolleinträge während des Starts auf der Konsole anzuzeigen. Dadurch wird die Überwachung und das Debugging vereinfacht.

Klicken Sie auf Settings, um die Filter für die Protokolleinträge festzulegen, die an die Konsole gesendet werden sollen. Der Standardfilter sendet die drei neuesten Fehlereinträge vom Systemereignisprotokoll an die Konsole.

Wallpaper Information

Verwenden Sie diese Einstellung, um die Systeminformationen auf dem Desktop-Hintergrund anzuzeigen. Das folgende Beispiel zeigt die Informationen, die auf dem Desktop-Hintergrund angezeigt werden.

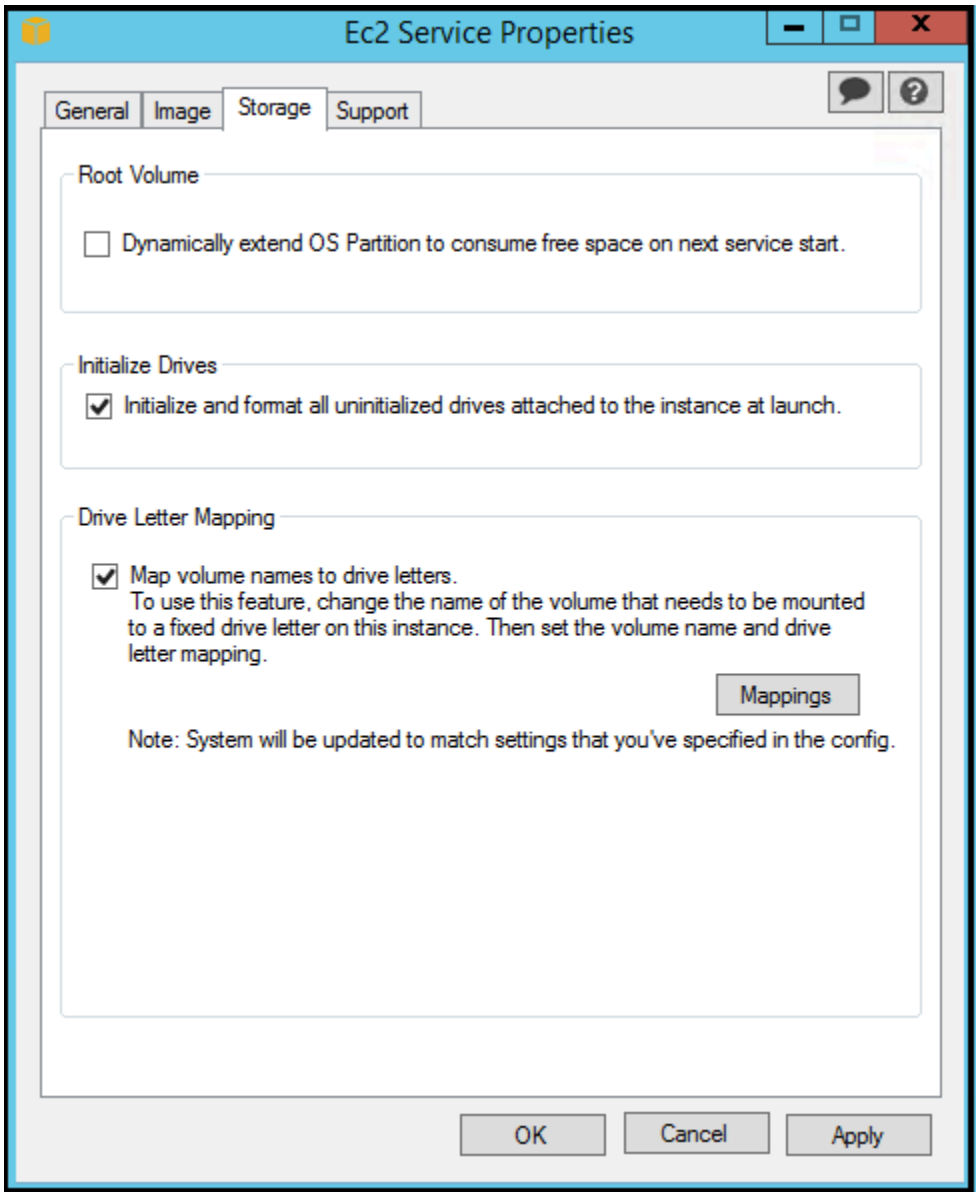


Die auf dem Desktop-Hintergrund angezeigten Informationen werden von der Einstellungsdatei `EC2ConfigService\Settings\WallpaperSettings.xml` gesteuert.

Enable Hibernation (Ruhezustand aktivieren)

Verwenden Sie diese Einstellung, um zuzulassen, dass EC2 dem Betriebssystem signalisiert, die Instance in den Ruhezustand zu versetzen.

4. Klicken Sie auf die Registerkarte Storage. Sie können die folgenden Einstellungen aktivieren oder deaktivieren.



Root Volume

Diese Einstellung erweitert Festplatte 0/Volume 0 dynamisch, sodass der gesamte nicht partitionierte Speicherplatz eingeschlossen ist. Dies ist nützlich, wenn die Instance von einem Root-Gerät-Volume gestartet wird, das eine benutzerdefinierte Größe besitzt.

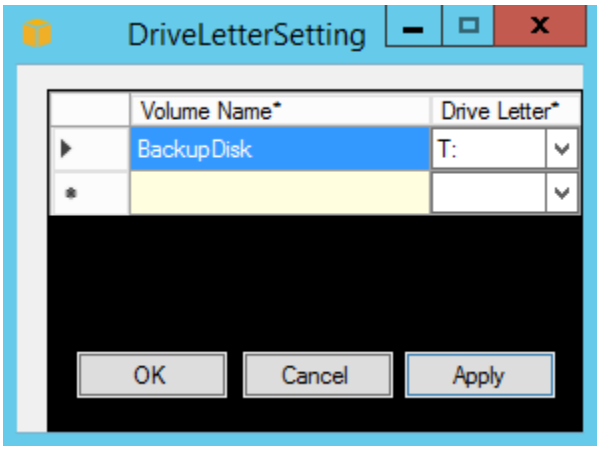
Initialize Drives

Diese Einstellung formatiert und installiert alle Volumes, die der Instance beim Start angefügt sind.

Drive Letter Mapping

Das System ordnet die Volumes, die einer Instance angefügt sind, einem Laufwerkbuchstaben zu. Standardmäßig werden die Amazon EBS-Volumes den Laufwerkbuchstaben von D: nach Z: zugeordnet. Zum Beispiel Speichervolumes, die Standardeinstellung hängt vom Treiber ab. AWS PV-Treiber und Citrix PV-Treiber weisen Instance-Speicher-Volumes Laufwerksbuchstaben von Z: bis A: zu. Red Hat-Treiber ordnen die Instance-Speicher-Volumes den Laufwerkbuchstaben von D: nach Z: zu.

Klicken Sie auf Mappings, um die Laufwerkbuchstaben für die Volumes auszuwählen. Geben Sie im Dialogfeld DriveLetterEinstellungen die Werte für den Volumennamen und den Laufwerksbuchstaben für jedes Volume an, klicken Sie auf Anwenden und dann auf OK. Wir empfehlen Ihnen, Laufwerkbuchstaben zu verwenden, die keine Konflikte mit bereits verwendeten Laufwerkbuchstaben hervorrufen, beispielsweise Laufwerkbuchstaben aus der Mitte des Alphabets.



Nachdem Sie eine Laufwerkzuweisung festgelegt und ein Volume mit der gleichen Kennung wie einer der angegebenen Volumenamen angefügt haben, weist EC2Config den angegebenen Laufwerksbuchstaben automatisch diesem Volume zu. Wird der Laufwerkbuchstabe jedoch bereits verwendet, schlägt die Zuweisung des Laufwerkbuchstaben fehl. Beachten Sie, dass EC2Config die Laufwerkbuchstaben der Volumes, die vor der Zuweisung des Laufwerkbuchstabens bereits gemountet waren, nicht ändert.

5. Um die Einstellungen zu speichern und mit der Arbeit daran an einem späteren Zeitpunkt fortzufahren, klicken Sie auf OK, um das Dialogfeld EC2 Service Properties (EC2-Serviceeigenschaften) zu schließen. Wenn die Anpassung der Instance abgeschlossen ist und Sie ein AMI aus der Instance erstellen möchten, finden Sie weitere Information unter Erstellen Sie ein AMI mit Windows Sysprep.

EC2Config-Einstellungsdateien

Die Einstellungsdateien steuern den Betrieb des EC2Config-Services. Diese Dateien befinden sich im Verzeichnis `C:\Program Files\Amazon\Ec2ConfigService\Settings`:

- `ActivationSettings.xml`: Steuert die Produktaktivierung mithilfe eines Schlüsselverwaltungsservers (AWS KMS).
- `AWS.EC2.Windows.CloudWatch.json`— Steuert, an welche Leistungsindikatoren CloudWatch und welche Protokolle an Logs gesendet werden sollen. CloudWatch
- `BundleConfig.xml` — Steuert, wie EC2Config eine Instance, die von einem Instance-Speicher gestützt wird, auf die AMI-Erstellung vorbereitet.
- `Config.xml` — Steuert die primären Einstellungen.
- `DriveLetterConfig.xml` — Steuert die Zuweisung der Laufwerkbuchstaben.
- `EventLogConfig.xml` — Steuert die Ereignisprotokollinformationen, die während des Starts der Instance auf der Konsole angezeigt werden.
- `WallpaperSettings.xml` — Steuert die Informationen, die auf dem Desktop-Hintergrund angezeigt werden.

ActivationSettings.xml

Diese Datei enthält Einstellungen, die die Produktaktivierung steuern. Beim Start von Windows, überprüft der EC2Config-Service, ob Windows bereits aktiviert ist. Wenn Windows nicht bereits aktiviert ist, versucht der Service, Windows durch die Suche nach dem angegebenen AWS KMS zu aktivieren.

- `SetAutodiscover`: Gibt an, ob ein AWS KMS automatisch erkannt werden soll.
- `TargetKMSServer`— Speichert die private IP-Adresse eines. AWS KMS Das AWS KMS muss sich in derselben Region wie Ihre Instance befinden.
- `DiscoverFromZone`— Erkennt den AWS KMS Server aus der angegebenen DNS-Zone.

- `ReadFromUserData`— Ruft den AWS KMS Server von ab. UserData
- `LegacySearchZones`— Erkennt den AWS KMS Server aus der angegebenen DNS-Zone.
- `DoActivate` — Versucht die Aktivierung anhand der angegebenen Einstellungen im Abschnitt einzuleiten. Dabei kann es sich um den Wert `true` oder `false` handeln.
- `LogResultToConsole` — Zeigt die Ergebnisse auf der Konsole an.

BundleConfig.xml

Diese Datei enthält Einstellungen, die die Vorbereitung einer Instance auf die Erstellung eines AMI durch EC2Config steuern.

- `AutoSysprep` — Gibt an, ob Sysprep automatisch verwendet werden soll. Ändern Sie den Wert auf `Yes`, um Sysprep zu verwenden.
- `SetRDPCertificate` — Legt ein selbstsigniertes Zertifikat für den Remote Desktop-Server fest. Auf diese Weise kann die Übermittlung an die Instances mithilfe von RDP sicher erfolgen. Ändern Sie den Wert zu `Yes`, wenn die neuen Instances über das Zertifikat verfügen sollen.

  Diese Einstellung wird nicht für Instanzen mit Betriebssystemversionen vor Windows Server 2016 verwendet, da sie ihre eigenen Zertifikate generieren können.
- `SetPasswordAfterSysprep` — Legt ein zufälliges Passwort für eine neu gestartete Instance fest, verschlüsselt sie mit dem Benutzer-Startschlüssel und gibt das verschlüsselte Passwort an die Konsole aus. Ändern Sie den Wert dieser Einstellung zu `No`, wenn für die neuen Instances nicht ein zufällig verschlüsseltes Passwort festgelegt werden soll.

Config.xml

Plug-ins

- `Ec2SetPassword` — Generiert bei jedem Start einer Instance ein zufälliges, verschlüsseltes Passwort. Dieses Feature wird standardmäßig nach dem ersten Start deaktiviert, sodass das vom Benutzer festgelegte Passwort auch durch Neustarts dieser Instance nicht geändert wird. Ändern Sie diese Einstellung auf `Enabled`, um weiterhin bei jedem Start einer Instance Passwörter zu generieren.

  Diese Einstellung ist wichtig, wenn Sie planen, aus Ihrer Instance ein AMI zu erstellen.
- `Ec2SetComputerName` — Gibt den Hostnamen einer Instance basierend auf der IP-Adresse der Instance als eindeutigen Namen an und startet die Instance neu. Deaktivieren Sie diese

Einstellung, um Ihren eigenen Hostnamen anzugeben oder den bestehenden Namen vor einer Änderung zu schützen.

- `Ec2InitializeDrives` — Initialisiert und formatiert alle Volumes während des Startups. Dieses Feature ist standardmäßig aktiviert.
- `Ec2EventLog` — Zeigt Protokolleinträge in der Konsole an. Standardmäßig werden die drei neuesten Fehlereinträge vom Systemereignisprotokoll angezeigt. Um festzulegen, welche Ereignisprotokolleinträge angezeigt werden, bearbeiten Sie die Datei `EventLogConfig.xml` im Verzeichnis `EC2ConfigService\Settings`. Weitere Informationen über die Einstellungen in dieser Datei finden Sie unter Eventlog Key in der MSDN Library.
- `Ec2ConfigureRDP` — Richtet eine selbstsignierte Zertifikat auf der Instance ein, sodass Benutzer mithilfe von Remote Desktop sicher auf die Instance zugreifen können. Diese Einstellung wird nicht für Instanzen mit Betriebssystemversionen vor Windows Server 2016 verwendet, da sie ihre eigenen Zertifikate generieren können.
- `Ec2OutputRDPCert` — Zeigt die Informationen zum Remote Desktop-Zertifikat auf der Konsole an, damit der Benutzer die Informationen mit dem Thumbprint vergleichen kann.
- `Ec2SetDriveLetter` — Legt die Laufwerkbuchstaben der bereitgestellten Volumes aufgrund der benutzerdefinierten Einstellungen fest. Wenn ein Amazon EBS-Volume einer Instance angefügt ist, kann es unter Verwendung des Laufwerkbuchstaben auf der Instance angezeigt werden. Um die Zuweisung der Laufwerkbuchstaben festzulegen, bearbeiten Sie die Datei `DriveLetterConfig.xml` im Verzeichnis `EC2ConfigService\Settings`.
- `Ec2WindowsActivate` — Das Plug-in führt die Windows-Aktivierung aus. Es überprüft, ob Windows aktiviert ist. Wenn nicht, werden die AWS KMS Client-Einstellungen aktualisiert und anschließend Windows aktiviert.

  Um die AWS KMS Einstellungen zu ändern, bearbeiten Sie die `ActivationSettings.xml` Datei im `EC2ConfigService\Settings` Verzeichnis.
- `Ec2DynamicBootVolumeSize` — Erweitert Festplatte 0/Volume 0, sodass der gesamte nicht partitionierte Speicherplatz eingeschlossen ist.
- `Ec2HandleUserData` — Erstellt vom Benutzer angefertigte Skripte und führt diese beim ersten Starten einer Instance aus, nachdem Sysprep ausgeführt wurde. In Skript-Tags eingeschlossene Befehle werden in einer Batchdatei gespeichert, und Befehle, die in PowerShell Tags eingeschlossen sind, werden in einer PS1-Datei gespeichert (entspricht dem Kontrollkästchen Benutzerdaten im Dialogfeld Ec2 Service Properties).
- `Ec2ElasticGpuSetup` — Installiert das Elastic GPU-Softwarepaket, wenn die Instance mit einer elastischen GPU verknüpft ist.

- `Ec2FeatureLogging` — Sendet die Installation der Windows-Features und den zugehörigen Service-Status an die Konsole. Wird nur für das Microsoft Hyper-V-Feature und den zugehörigen VMMS-Service unterstützt.

Globale Einstellungen

- `ManageShutdown` — Stellt sicher, dass Instances, die von AMIs gestartet werden, welche wiederum von Instance-Speichern gestützt sind, während der Ausführung von Sysprep nicht beendet werden.
- `SetDnsSuffixList` — Legt das DNS-Suffix des Netzwerkadapters für Amazon EC2 fest. Hierdurch ist die DNS-Auflösung der Server, die in Amazon EC2 ausgeführt werden, ohne Bereitstellung des vollständig qualifizierten Domain-Namens möglich.

> **Note**
>
> Dadurch wird eine DNS-Suffix-Suffixsuche für die folgende Domäne hinzugefügt und andere Standardsuffixe konfiguriert. Weitere Informationen darüber, wie Launch-Agents DNS-Suffixe festlegen, finden Sie unter. Konfigurieren Sie das DNS-Suffix für Windows-Startagenten
>
> ```
> region.ec2-utilities.amazonaws.com
> ```

- `WaitForMetaDataAvailable` — Stellt sicher, dass der EC2Config-Service darauf wartet, dass die Metadaten zugänglich sind und das Netzwerk verfügbar ist, bevor der Start fortgesetzt wird. Durch diese Überprüfung wird sichergestellt, dass EC2Config Informationen aus den Metadaten abrufen kann, die für die Aktivierung und andere Plug-ins hilfreich sind.
- `ShouldAddRoutes` — Hinzufügung einer benutzerdefinierten Route zum primären Netzwerkadapter, um die folgenden IP-Adressen zu aktivieren, wenn mehrere NICs zugeordnet sind: 169.254.169.250, 169.254.169.251 und 169.254.169.254. Diese Adressen werden von der Windows-Aktivierung und beim Zugriff auf Instance-Metadaten verwendet.
- `RemoveCredentialsfromSyspreponStartup` — Entfernt das Administratorpasswort aus `Sysprep.xml`, sobald der Server das nächste Mal gestartet wird. Bearbeiten Sie diese Einstellung, um sicherzustellen, dass das Passwort erhalten bleibt.

DriveLetterConfig.xml

Diese Datei enthält Einstellungen, die die Zuweisung der Laufwerkbuchstaben steuern. Standardmäßig kann ein Volume jedem beliebigen Laufwerkbuchstaben zugeordnet werden. Sie können ein Volume einem bestimmten Laufwerkbuchstaben folgendermaßen bereitstellen.

```
<?xml version="1.0" standalone="yes"?>
<DriveLetterMapping>
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
  . . .
  <Mapping>
    <VolumeName></VolumeName>
    <DriveLetter></DriveLetter>
  </Mapping>
</DriveLetterMapping>
```

- `VolumeName` — Die Bezeichnung des Volumes. z. B. *`My Volume`*. Um die Zuweisung für ein Instance-Speicher-Volume festzulegen, verwenden Sie die Bezeichnung `Temporary Storage X`, wobei `X` eine Zahl zwischen 0 bis 25 ist.
- `DriveLetter` — Der Laufwerkbuchstabe. z. B. *`M:`*. Wird der Laufwerkbuchstabe bereits verwendet, schlägt die Zuweisung fehl.

EventLogConfig.xml

Diese Datei enthält Einstellungen, die die Ereignisprotokollinformationen steuern, die beim Start der Instance auf der Konsole angezeigt werden. Standardmäßig werden die drei neuesten Fehlereinträge aus dem Systemereignisprotokoll angezeigt.

- `Category` — Der zu überwachende Ereignisprotokollschlüssel.
- `ErrorType` — Der Ereignistyp (beispielsweise `Error`, `Warning`, `Information`).
- `NumEntries` — Die Anzahl der gespeicherten Ereignisse in dieser Kategorie.
- `LastMessageTime` — Um zu verhindern, dass die gleiche Nachricht wiederholt mithilfe von Push übertragen wird, aktualisiert der Service diesen Wert jedes Mal, wenn eine Nachricht übertragen wird.
- `AppName` — Die Ereignisquelle oder die Anwendung, die das Ereignis protokolliert hat.

WallpaperSettings.xml

Diese Datei enthält Einstellungen, die die auf dem Desktop-Hintergrund angezeigten Informationen steuern. Standardmäßig werden die folgenden Informationen angezeigt.

- `Hostname` — Zeigt den Computer-Namen an.
- `Instance ID` — Zeigt die Instance-ID an.
- `Public IP Address` — Zeigt die öffentliche IP-Adresse der Instance an.
- `Private IP Address` — Zeigt die private IP-Adresse der Instance an.
- `Availability Zone` — Zeigt die Availability Zone an, in der die Instance ausgeführt wird.
- `Instance Size` — Zeigt den Instance-Typ an.
- `Architecture` — Zeigt die Einstellungen der Umgebungsvariablen `PROCESSOR_ARCHITECTURE` an.

Sie können alle standardmäßig angezeigten Informationen entfernen, indem Sie deren Eintrag löschen. Um zusätzliche Instance-Metadaten anzuzeigen, gehen Sie folgendermaßen vor.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>metadata</source>
  <identifier>meta-data/path</identifier>
</WallpaperInformation>
```

Um zusätzliche Systemumgebungsvariablen anzuzeigen, gehen Sie folgendermaßen vor.

```
<WallpaperInformation>
  <name>display_name</name>
  <source>EnvironmentVariable</source>
  <identifier>variable-name</identifier>
</WallpaperInformation>
```

InitializeDrivesSettings.xml

Diese Datei enthält Einstellungen, die die Initialisierung von Laufwerken durch EC2Config steuern.

EC2Config initialisiert standardmäßig Laufwerke, die nicht mit dem Betriebssystem online geschaltet wurden. Sie können das Plug-in folgendermaßen anpassen.

```
<InitializeDrivesSettings>
    <SettingsGroup>setting</SettingsGroup>
</InitializeDrivesSettings>
```

Verwenden Sie eine Einstellungsgruppe, um festzulegen, wie die Laufwerke initialisiert werden sollen:

FormatWithTRIMMEN

Aktiviert den TRIM-Befehl für die Formatierung der Laufwerke. Nachdem das Laufwerk formatiert und initialisiert wurde, stellt das System die TRIM-Konfiguration wieder her.

Ab EC2Config Version 3.18 ist der TRIM-Befehl standardmäßig während der Formatierungsoperation der Festplatte deaktiviert. Dadurch wird die Formatierungszeit verbessert. Verwenden Sie diese Einstellung, um TRIM während der Festplattenformatierung für EC2Config Version 3.18 und höher zu aktivieren.

FormatWithoutTRIMMEN

Deaktiviert den TRIM-Befehl während der Formatierung der Laufwerke und verbessert die Formatierungszeiten in Windows. Nachdem das Laufwerk formatiert und initialisiert wurde, stellt das System die TRIM-Konfiguration wieder her.

DisableInitializeAntriebe

Deaktiviert die Formatierung neuer Laufwerke. Verwenden Sie diese Einstellung, um Laufwerke manuell zu initialisieren.

Konfigurieren der Proxy-Einstellungen für den EC2Config-Service

Sie können den EC2Config-Dienst so konfigurieren, dass er über einen Proxy kommuniziert, indem Sie eine der folgenden Methoden verwenden: das AWS SDK for .NET, das `system.net` Element oder Microsoft Group Policy und Internet Explorer. Die Verwendung des AWS SDK for .NET ist die bevorzugte Methode, da Sie Anmeldeinformationen angeben können.

Methoden

- Konfigurieren Sie die Proxyeinstellungen mithilfe von AWS SDK for .NET (Bevorzugt)
- Konfigurieren der Proxy-Einstellungen mithilfe des system.net-Elements
- Konfigurieren der Proxy-Einstellungen mithilfe der Microsoft-Gruppenrichtlinien und Microsoft Internet Explorer

Konfigurieren Sie die Proxyeinstellungen mithilfe von AWS SDK for .NET (Bevorzugt)

Sie können die Proxy-Einstellungen für den EC2Config-Service anhand des Elements `proxy` in der Datei `Ec2Config.exe.config` konfigurieren. Weitere Informationen finden Sie unter Referenz zu Konfigurationsdateien für AWS SDK for .NET.

So legen Sie das Proxy-Element in Ec2Config.exe.config fest

1. Bearbeiten Sie die Datei `Ec2Config.exe.config` auf allen Instances, auf denen der EC2Config-Service über einen Proxy kommunizieren soll. Standardmäßig befindet sich die Datei im folgenden Verzeichnis: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Fügen Sie das folgende Element `aws` den `configSections` hinzu. Fügen Sie dies keiner vorhandenen `sectionGroups` hinzu.

   Für EC2Config Versionen 3.17 und niedriger

   ```
   <configSections>
      <section name="aws" type="Amazon.AWSSection, AWSSDK"/>
   </configSections>
   ```

   Für EC2Config Versionen 3.18 und höher

   ```
   <configSections>
        <section name="aws" type="Amazon.AWSSection, AWSSDK.Core"/>
   </configSections>
   ```

3. Fügen Sie das folgende `aws`-Element der Datei `Ec2Config.exe.config` hinzu.

   ```
   <aws>
      <proxy
        host="string value"
        port="string value"
        username="string value"
        password="string value" />
   </aws>
   ```

4. Speichern Sie Ihre Änderungen.

Konfigurieren der Proxy-Einstellungen mithilfe des system.net-Elements

Sie können die Proxy-Einstellungen im `system.net`-Element in der Datei `Ec2Config.exe.config` festlegen. Weitere Informationen finden Sie unter defaultProxy Element (Network Settings) auf MSDN.

So legen Sie das system.net-Element in Ec2Config.exe.config fest

1. Bearbeiten Sie die Datei `Ec2Config.exe.config` auf allen Instances, auf denen der EC2Config-Service über einen Proxy kommunizieren soll. Standardmäßig befindet sich die Datei im folgenden Verzeichnis: `%ProgramFiles%\Amazon\Ec2ConfigService`.
2. Fügen Sie einen `defaultProxy`-Eintrag `system.net` hinzu. Weitere Informationen finden Sie unter defaultProxy Element (Network Settings) auf MSDN.

   In der folgenden Konfiguration verwendet der gesamte Datenverkehr beispielsweise den derzeit für Internet Explorer konfigurierten Proxy. Dabei stellen die Metadaten und der lizensierte Datenverkehr eine Ausnahme dar, da sie den Proxy umgehen.

   ```
   <defaultProxy>
       <proxy usesystemdefault="true" />
       <bypasslist>
           <add address="169.254.169.250" />
           <add address="169.254.169.251" />
           <add address="169.254.169.254" />
           <add address="[fd00:ec2::250]" />
           <add address="[fd00:ec2::254]" />
       </bypasslist>
   </defaultProxy>
   ```
3. Speichern Sie Ihre Änderungen.

Konfigurieren der Proxy-Einstellungen mithilfe der Microsoft-Gruppenrichtlinien und Microsoft Internet Explorer

Der EC2Config-Service wird unter dem lokalen Systembenutzerkonto ausgeführt. Nachdem Sie die Gruppenrichtlinieneinstellungen auf der Instance geändert haben, können Sie für dieses Konto instanceweite Proxy-Einstellungen festlegen.

So konfigurieren Sie Proxy-Einstellungen mithilfe der Gruppenrichtlinie und Internet Explorer

1. Öffnen Sie auf einer Instance, auf der der EC2Config-Service über einen Proxy kommunizieren soll, die Eingabeaufforderung als Administrator, geben Sie **`gpedit.msc`** ein und drücken Sie auf die Eingabetaste.
2. Wählen Sie im lokalen Gruppenrichtlinien-Editor unter Local Computer Policy die Optionen Computer Configuration, Administrative Templates, Windows Components, Internet Explorer aus.
3. Wählen Sie im rechten Bereich Make proxy settings per-machine (rather than per-user) und anschließend Edit policy setting aus.
4. Wählen Sie Enabled und anschließend Apply aus.
5. Öffnen Sie Internet Explorer und wählen Sie die Schaltfläche Tools aus.
6. Wählen Sie Internet Option und anschließend die Registerkarte Connections aus.
7. Wählen Sie LAN settings aus.
8. Wählen Sie unter Proxy server die Option Use a proxy server for your LAN aus.
9. Geben Sie die Adresse und die Port-Informationen ein und wählen Sie anschließend OK aus.

EC2Config-Versionshistorie

Windows AMIs vor Windows Server 2016 schließen den optionalen EC2Config-Service (`EC2Config.exe`) ein. EC2Config startet, wenn die Instance hochgefahren wird. Darüber hinaus führt der Service beim ersten Startup sowie bei jedem Stoppen und Starten der Instance Aufgaben aus.

Sie können benachrichtigt werden, wenn neue Versionen des EC2Config-Services veröffentlicht werden. Weitere Informationen finden Sie unter Abonnieren von EC2Config-Service-Benachrichtigungen.

Die folgende Tabelle beschreibt die veröffentlichten Versionen von EC2Config. Weitere Informationen zu den Aktualisierungen von SSM Agent finden Sie in den Versionshinweisen für Systems Manager-SSM-Agent.

Version	Details	Datum der Veröffentlichung
4.9.5554	• Einschränkung der Übertragung von Domainnamen auf der Grundlage eines Registrierungseintrags: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Dnscache\Parameters\DomainNameDevolutionLevel` . • Neue Version von SSM Agent `3.2.1630.0` .	04. Oktober 2023
4,9,5467	• Wiederholungsfunktion zum Erkennen des Konsolenports hinzugefügt. • Neue Version von SSM Agent `3.1.2282.0` .	01. August 2023
4,9,5288	• AWS Core SDK wurde auf Version `3.7.103.23` aktualisiert. • Es wurde ein Problem behoben, bei dem das `AWS-UpdateEC2Config` -SSM-Dokument `EC2Config` auf Instances, die nur mit IMDSv2 aktiviert sind, nicht aktualisiert. • Neue Version von SSM Agent `3.1.2144.0` .	08. März 2023
4,9,5231	• Neue Version des SSM-Agenten 3.1.1927.0.	14. Februar 2023
4,9,5103	• Problem behoben, bei dem ephemere Volumes in den Instance-Familien R5D und i4i falsch identifiziert wurden. • Neue Version von SSM Agent 3.1.1856.0.	5. Dezember 2022
4,9,5064	• Aktualisiert, um PCI-Segmentinformationen zur Auswahl des Konsolenports zu verwenden. •	16. November 2022

Version	Details	Datum der Veröffentlichung
	Signierte PowerShell Skripte und Copyright-Header hinzugefügt. • Die Auswahllogik für den primären Netzwerkadapter wurde korrigiert. • Neue Version von SSM Agent 3.1.1732.0.	
4.9.4588	• Die IMDS-Wartelogik wurde aktualisiert, um nur IMDSv2-Anforderungen zu stellen. • Die Shared Library libec2launch.dll launch-agent wurde hinzugefügt. • Neue Version von SSM Agent 3.1.1188.0.	31. Mai 2022
4,9,4556	• Wartelogik wurde hinzugefügt, um vollständige Initialisierung des NIC vor der Verwendung sicherzustellen. • Neue Version von Log4Net 2.0.14.0 nimmt Sicherheitspatch auf. • Neue Version von SSM Agent 3.1.1045.0 nimmt Sicherheitspatch auf.	1. März 2022
4,9,4536	• Es wurde ein Problem behoben, bei dem userdata abstürzt, wenn der Temp-Ordner fehlt. • Neue Version von SSM Agent 3.1.804.0.	31. Januar 2022
4,9,4508	• Es wurde ein Problem mit der Berechnung des DiskPart-Skriptpfads behoben. • Neue Version von SSM Agent 3.1.338.0.	6. Oktober 2021

Version	Details	Datum der Veröffentlichung
4,9,4500	• Aktualisiert `Install-EgpuManagerConfig` mit IMDS-v2-Unterstützung. • Weblinks wurden aktualisiert, um https zu verwenden. • Neue Version von SSM Agent 3.1.282.0	7. September 2021
4,9,4419	• IMDS Version 1 Fallback-Logik wurde korrigiert • Aktualisiert die gesamte Verwendung des temporären Windows Verzeichnisses in das temporäre Verzeichnis EC2Config • Neue Version von SSM Agent 3.0.1124.0	2. Juni 2021
4.9.4381	• Unterstützung für das SSM-Dokumentschema Version 2.2 in EC2 wurde hinzugefügt ConfigUpdater • Die AWS Nitro Enclaves-Paketversion wurde zum Konsolenprotokoll hinzugefügt • Neue Version von SSM Agent 3.0.529.0	04. Mai 2021
4.9.4326	• Alle Links in der Einstellungen Benutzeroberfläche entfernt • Dies ist die letzte EC2Config-Version, die Windows Server 2008 unterstützt.	3. März 2021

Version	Details	Datum der Veröffentlichung
4.9.4279	• Sicherheitsproblem im Zusammenhang mit der geplanten Aufgabe `Ec2ConfigMonitor` behoben • Problem mit der Zuordnung von Laufwerksbuchstaben und falscher Anzahl flüchtiger Datenträger behoben • `OsCurrentBuild` und `OsReleaseId` zur Konsolenausgabe hinzugefügt • Neue Version von SSM Agent 2.3.871.0	11. Dezember 2020
4.9.4222	• IMDS Version 1 Fallback-Logik wurde korrigiert • Neue Version von SSM Agent (2.3.842.0)	7. April 2020
4.9.4122	• Unterstützung für IMDS v2 hinzugefügt • Neue Version von SSM Agent (2.3.814.0)	4. März 2020
4.9.3865	• Problem mit dem Erkennen des COM-Anschlusses für Windows Server 2008 R2 auf Metal-Instances behoben • Neue Version von SSM Agent (2.3.722.0)	31. Oktober 2019
4.9.3519	• Neue Version von SSM Agent (2.3.634.0)	18. Juni 2019
4.9.3429	• Neue Version von SSM Agent (2.3.542.0)	25. April 2019
4.9.3289	• Neue Version von SSM Agent 2.3.444.0	11. Februar 2019
4.9.3270	• Plug-In hinzugefügt, mit dem sich einstellen lässt, dass der Monitor nie ausgeschaltet wird, um ACPI-Probleme zu beheben • SQL Server-Edition und -Version in die Konsole geschrieben • Neue Version von SSM Agent 2.3.415.0	22. Januar 2019

Version	Details	Datum der Veröffentlichung
4.9.3230	• Zuweisung des Laufwerkbuchstabens für eine bessere Abstimmung mit der Funktionalität aktualisiert • Neue Version von SSM Agent 2.3.372.0	10. Januar 2019
4.9.3160	• Erhöhte Wartezeit für die primäre NIC • Standardkonfiguration für RSS- und Empfangswarteschlangen-Einstellungen für ENA-Geräte hinzugefügt • Ruhezustand während Sysprep deaktiviert • Neue Version von SSM Agent 2.3.344.0 • SDK auf 3.3.29.13 aktualisiert AWS	15. Dezember 2018
4.9.3067	• Verbesserungen beim Instance-Ruhezustand • Neue Version von SSM Agent 2.3.235.0	8. November 2018
4.9.3034	• Route 169.254.169.253/32 für DNS-Server hinzugefügt • Neue Version von SSM Agent 2.3.193.0	24. Oktober 2018
4.9.2986	• Signatur für alle EC2Config-bezogenen Binärdateien hinzugefügt • Neue Version von SSM Agent 2.3.136.0	11. Oktober 2018
4.9.2953	Neue Version von SSM Agent (2.3.117.0)	2. Oktober 2018
4.9.2926	Neue Version von SSM Agent (2.3.68.0)	18. September 2018

Version	Details	Datum der Veröffentlichung
4.9.2905	• Neue Version von SSM Agent (2.3.50.0) • Route 169.254.169.123/32 zum AMZN-Zeitservice hinzugefügt • Route 169.254.169.249/32 zum GRID-Lizenzdienst hinzugefügt • Behebung eines Fehlers, der dazu geführt hat, dass EBS-NVMe-Volumes flüchtig ausgeführt werden.	17. September 2018
4.9.2854	Neue Version von SSM Agent (2.3.13.0)	17. August 2018
4.9.2831	Neue Version von SSM Agent (2.2.916.0)	7. August 2018
4.9.2818	Neue Version von SSM Agent (2.2.902.0)	31. Juli 2018
4.9.2756	Neue Version von SSM Agent (2.2.800.0)	27. Juni 2018
4.9.2688	Neue Version von SSM Agent (2.2.607.0)	25. Mai 2018
4.9.2660	Neue Version von SSM Agent (2.2.546.0)	11. Mai 2018
4.9.2644	Neue Version von SSM Agent (2.2.493.0)	26. April 2018
4.9.2586	Neue Version von SSM Agent (2.2.392.0)	28. März 2018
4.9.2565	• Neue Version von SSM Agent (2.2.355.0) • Behebung eines Problems auf M5- und C5-Instances (PV-Treiber konnten nicht gefunden werden) • Hinzufügen der Konsolenprotokollierung für den Instance-Typ, neueste PV-Treiber und NVMe-Treiber	13. März 2018
4.9.2549	Neue Version von SSM Agent (2.2.325.0)	8. März 2018

Version	Details	Datum der Veröffentlichung
4.9.2461	Neue Version von SSM Agent (2.2.257.0)	15. Februar 2018
4.9.2439	Neue Version von SSM Agent (2.2.191.0)	6. Februar 2018
4.9.2400	Neue Version von SSM Agent (2.2.160.0)	16. Januar 2018
4.9.2327	• Neue Version von SSM Agent (2.2.120.0) • COM-Port-Discovery auf Amazon EC2-Bare-Metal-Instances hinzugefügt • Hyper-V-Statusprotokollierung auf Amazon EC2-Bare-Metal-Instances hinzugefügt	2. Januar 2018
4.9.2294	Neue Version von SSM Agent (2.2.103.0)	4. Dezember 2017
4.9.2262	Neue Version von SSM Agent (2.2.93.0)	15. November 2017
4.9.2246	Neue Version von SSM Agent (2.2.82.0)	11. November 2017
4.9.2218	Neue Version von SSM Agent (2.2.64.0)	29. Oktober 2017
4.9.2212	Neue Version von SSM Agent (2.2.58.0)	23. Oktober 2017
4.9.2203	Neue Version von SSM Agent (2.2.45.0)	19. Oktober 2017

Version	Details	Datum der Veröffentlichung
4.9.2188	Neue Version von SSM Agent (2.2.30.0)	10. Oktober 2017
4.9.2180	• Neue Version von SSM Agent (2.2.24.0) • Das Elastic GPU-Plug-in für GPU-Instances hinzugefügt.	5. Oktober 2017
4.9.2143	Neue Version von SSM Agent (2.2.16.0)	1. Oktober 2017
4.9.2140	Neue Version von SSM Agent (2.1.10.0)	
4.9.2130	Neue Version von SSM Agent (2.1.4.0)	
4.9.2106	Neue Version von SSM Agent (2.0.952.0)	
4.9.2061	Neue Version von SSM Agent (2.0.922.0)	
4.9.2047	Neue Version von SSM Agent (2.0.913.0)	
4.9.2031	Neue Version von SSM Agent (2.0.902.0)	
4.9.2016	• Neue Version von SSM Agent (2.0.879.0) • Der CloudWatch Protokollverzeichnispfad für Windows Server 2003 wurde korrigiert	
4.9.1981	• Neue Version von SSM Agent (2.0.847.0) • Problem mit der Generierung von `important.txt` in den EBS-Volumes behoben.	
4.9.1964	Neue Version von SSM Agent (2.0.842.0)	

Version	Details	Datum der Veröffentlichung
4.9.1951	• Neue Version von SSM Agent (2.0.834.0) • Problem bei der Zuweisung des Laufwerkbuchstaben für flüchtige Laufwerke von Z: aus behoben.	
4.9.1925	• Neue Version von SSM Agent (2.0.822.0) • [Fehler] Diese Version ist kein gültiges Aktualisierungsziel von SSM Agent v4.9.1775.	
4.9.1900	Neue Version von SSM Agent (2.0.805.0)	
4.9.1876	• Neue Version von SSM Agent (2.0.796.0) • Problem mit der Ausgabe-/Fehlerweiterleitung bei der Ausführung der Administrator-Benutzerdaten behoben.	
4.9.1863	• Neue Version von SSM Agent (2.0.790.0) • Probleme beim Anfügen mehrerer EBS-Volumes an eine Amazon EC2-Instance behoben. • Es wurde CloudWatch ein Konfigurationspfad hinzugefügt, wobei die Abwärtskompatibilität beibehalten wurde.	
4.9.1791	Neue Version von SSM Agent (2.0.767.0)	
4.9.1775	Neue Version von SSM Agent (2.0.761.0)	
4.9.1752	Neue Version von SSM Agent (2.0.755.0)	
4.9.1711	Neue Version von SSM Agent (2.0.730.0)	

Version	Details	Datum der Veröffentlichung
4.8.1676	Neue Version von SSM Agent (2.0.716.0)	
4.7.1631	Neue Version von SSM Agent (2.0.682.0)	
4.6.1579	• Neue Version von SSM Agent (2.0.672.0) • Problem bei der Agenten-Aktualisierung in v4.3, v4.4 und v4.5 behoben.	
4.5.1534	Neue Version von SSM Agent (2.0.645.1)	
4.4.1503	Neue Version von SSM Agent (2.0.633.0)	
4.3.1472	Neue Version von SSM Agent (2.0.617.1)	
4.2.1442	Neue Version von SSM Agent (2.0.599.0)	
4.1.1378	Neue Version von SSM Agent (2.0.558.0)	

Version	Details	Datum der Veröffentlichung
4.0.1343	• Run Command, State Manager, der CloudWatch Agent und die Unterstützung für Domänenbeitritte wurden in einen anderen Agenten namens SSM Agent verschoben. SSM Agent wird als Teil des EC2Config-Upgrades installiert. Weitere Informationen finden Sie unter EC2Config und AWS Systems Manager. • Wenn Sie in EC2Config einen Proxy eingerichtet haben, müssen Sie Ihre Proxy-Einstellungen für SSM Agent aktualisieren, bevor Sie den Upgrade vornehmen können. Wenn Sie die Proxy-Einstellungen nicht aktualisieren, können Sie den Run Command nicht für die Verwaltung Ihrer Instances verwenden. Um dies zu vermeiden, beachten Sie die folgenden Informationen, bevor Sie das Update auf die neuere Version ausführen: Installation und Konfiguration von SSM Agent auf Windows-Instances im AWS Systems Manager - Benutzerhandbuch. • Wenn Sie zuvor die CloudWatch Integration auf Ihren Instances mithilfe einer lokalen Konfigurationsdatei (`AWS.EC2.Windows.CloudWatch.json`) aktiviert haben, müssen Sie die Datei so konfigurieren, dass sie mit SSM Agent funktioniert.	

Version	Details	Datum der Veröffentlichung
3.19.1153	• Das Aktivierungs-Plugin für Instanzen mit alter AWS KMS Konfiguration wurde erneut aktiviert. Überspringen Sie die Aktivierung für BYOL-Benutzer. • Ändern Sie das standardmäßige TRIM-Verhalten so, dass es während der Festplattenformatierung deaktiviert ist, und fügen Sie FormatWith TRIM hinzu, um InitializeDisks das Plugin mit Benutzerdaten zu überschreiben.	
3.18.1118	• Korrektur, um dem primären Netzwerkadapter jetzt zuverlässig Routen hinzufügen zu können. • Updates zur Verbesserung der Unterstützung von Diensten. AWS	
3.17.1032	• Korrektur der duplizierten Systemprotokolle, wenn die Filter auf die gleiche Kategorie gesetzt sind. • Korrektur des "Hängenbleibens" während der Festplatteninitialisierung.	
3.16.930	Zusätzlicher Support beim Start für die Protokollierung des Ereignisses "Windows ist einsatzbereit" im Windows-Ereignisprotokoll.	
3.15.880	Korrektur, um das Hochladen der Systems Manager Run Command-Ausgabe in S3-Bucket-Namen mit dem Zeichen ‘.’ zu erlauben.	

Version	Details	Datum der Veröffentlichung
3.14.786	Unterstützung zum Überschreiben der InitializeDisks Plugin-Einstellungen hinzugefügt. Beispiel: Um die Initialisierung der SSD-Festplatte zu beschleunigen, können Sie TRIM vorübergehend deaktivieren, indem Sie dies in den Benutzerdaten festlegen: < InitializeDrives Einstellungen>< > TRIM</ SettingsGroup ></ FormatWithout Einstellungen SettingsGroup InitializeDrives	
3.13.727	Systems Manager Run Command – Korrektur, um Befehle nach dem Windows-Neustart zuverlässig zu verarbeiten.	
3.12.649	• Korrektur, um den Neustart bei der Ausführung von Befehlen/Skripten zuverlässig auszuführen. • Korrektur, um Ausführungsbefehle zuverlässig abzubrechen. • Unterstützung für das (optionale) Hochladen der MSI-Protokolle nach S3 hinzugefügt, wenn Anwendungen über Systems Manager Run Command installiert werden.	
3.11.521	• Korrektur der Generierung von RDP-Thumbprints für Windows Server 2003 • Korrektur, durch die die Zeitzonen und der UTC-Offset in die EC2Config-Protokollzeilen eingeschlossen werden. • Systems Manager-Unterstützung, um Run Command-Befehle im Parallelmodus auszuführen. • Zurücksetzen der vorangegangenen Änderung, um partitionierte Festplatten online zu stellen.	

Version	Details	Datum der Veröffentlichung
3.10.442	• Behebden der Systems Manager-Konfigurationsfehler bei der Installation von MSI-Anwendungen. • Korrektur, um die Speicherlaufwerke zuverlässig online zu stellen. • Updates zur Verbesserung der Unterstützung von Diensten AWS .	
3.9.359	• Korrektur der Bereitstellung des Sysprep-Skripts, um die Konfiguration des Windows-Updates im Standardstatus zu belassen. • Korrektur des Plug-ins für die Passwortgenerierung, um die Einhaltung der Einstellungen für die GPO-Passwortrichtlinien zu verbessern. • Beschränkung der EC2Config-/SSM-Protokollordnerberechtigungen auf die lokale Administratorgruppe. • Updates zur Verbesserung der Unterstützung von AWS Diensten.	

Version	Details	Datum der Veröffentlichung
3.8.294	• Es wurde ein Problem behoben CloudWatch , das das Hochladen von Protokollen verhinderte, wenn sie sich nicht auf dem primären Laufwerk befanden. • Verbesserung der Festplatteninitialisierung durch das Hinzufügen von Logik für Wiederholversuche. • Es wurde eine verbesserte Fehlerbehandlung hinzugefügt, wenn das SetPassword Plugin bei der AMI-Erstellung gelegentlich ausfiel. • Updates zur Verbesserung der Unterstützung von AWS Diensten.	
3.7.308	• Verbesserungen am Dienstprogramm "ec2config-cli" beim "config"-Testen und bei der Fehlerbehebung innerhalb der Instance. • Vermeiden Sie das Hinzufügen statischer Routen für AWS KMS und Metadatendienste auf einem OpenVPN-Adapter. • Korrektur eines Problems, bei dem bei der Ausführung der Benutzerdaten das "persist"-Tags (Markierungen) nicht berücksichtigt wurde. • Verbesserung der Fehlerbehandlung, wenn die Anmeldung bei der EC2-Konsole nicht möglich war. • Updates zur Verbesserung der Unterstützung von Diensten. AWS	

Version	Details	Datum der Veröffentlichung
3.6.269	• Korrektur der Aktivierungszuverlässigkeit von Windows durch die Verwendung der lokalen Adresse 169.254.0.250/251 für die Aktivierung von Windows über AWS KMS. • Verbesserte Proxy-Handhabung in Systems Manager-, Windows-Aktivierungs- und Domain-Verbindungsszenarien • Korrektur eines Problems, bei dem der Sysprep-Antwortdatei duplizierte Benutzerkontenzeilen hinzugefügt wurden.	
3.5.228	• Es wurde ein Szenario behoben, bei dem das CloudWatch Plugin beim Lesen von Windows-Ereignisprotokollen möglicherweise übermäßig viel CPU und Arbeitsspeicher beansprucht • Es wurde ein Link zur CloudWatch Konfigurationsdokumentation in der Benutzeroberfläche der EC2Config-Einstellungen hinzugefügt	
3.4.212	• Korrektur von EC2Config bei der Verwendung mit VM Import. • Korrektur eines Problems bei der Namensgebung im WiX-Installer.	

Version	Details	Datum der Veröffentlichung
3.3.174	• Verbesserung bei der Ausnahmebehandlung von Fehlschlägen in Systems Manager und bei der Verbindung von Domains. • Änderung zur Unterstützung des Systems Manager-Schema-Versioning. • Fehlerbehebung bei der Formatierung flüchtiger Festplatten unter Win2K3. • Änderung, um die Konfiguration von Festplattengrößen über 2 TB zu unterschützen. • Geringerer Verbrauch des virtuellen Speichers durch die Einrichtung des GC-Modus als Standard. • Unterstützung für Herunterladen von Artefakten aus dem UNC-Pfad im `aws:psModule` - und `aws:application` - Plug-in. • Verbesserung der Protokollierung für das Windows Aktivierungs-Plug-in.	

Version	Details	Datum der Veröffentlichung
3.2.97	• Leistungsverbesserungen durch verzögertes Laden der Systems Manager-SSM-Komponenten. • Verbesserte Ausnahmebehandlung für falsch formatierte sysprep2008.xml. • Befehlszeilenunterstützung für die Systems Manager „Apply“-Konfiguration. • Änderung, um die Verbindung von Domains zu unterstützen, wenn eine Umbenennung des Computers ansteht. • Unterstützung optionaler Parameter im `aws:applications` -Plug-in. • Unterstützung des Befehls-Arrays im `aws:psModule` -Plug-in.	
3.0.54	• Unterstützung für Systems Manager aktiviert. • Automatische Domain-Verbindung von EC2-Windows-Instances mit einem AWS -Verzeichnis über Systems Manager. • Konfigurieren und laden Sie CloudWatch Logs/Metriken über Systems Manager hoch. • Installieren Sie PowerShell Module über Systems Manager. • Installation der MSI-Anwendungen über Systems Manager.	

Version	Details	Datum der Veröffentlichung
2.4.233	• Hinzufügen einer geplanten Aufgabe, um EC2Config nach fehlerhaften Service-Startups wiederherzustellen. • Verbesserungen an den Benachrichtigungen über die Protokollfehler für die Konsole. • Updates zur Verbesserung der Unterstützung von AWS Diensten.	
2.3.313	• Es wurde ein Problem behoben, das in einigen Fällen zu einem hohen Speicherverbrauch führte, wenn die CloudWatch Protokollfunktion aktiviert war. • Upgradefehler behoben, sodass EC2Config-Versionen niedriger als 2.1.19 auf die neueste Version aktualisiert werden können. • Ausnahmebehandlung für die COM-Port-Öffnung aktualisiert, sodass sie benutzerfreundlicher und zweckdienlicher ist. • Die configServiceSettings Ec2-Benutzeroberfläche hat die Größenänderung deaktiviert und die Platzierung der Zuordnung und der Versionsanzeige in der Benutzero berfläche korrigiert.	
2.2.12	• Wird NullPointerException bei der Abfrage eines Registrie rungsschlüssels zur Bestimmung des Windows Sysprep-S tatus verarbeitet, der gelegentlich Null zurückgab. • Freisetzung unverwalteter Ressourcen im finally-Block.	

Version	Details	Datum der Veröffentlichung
2.2.11	Ein Problem im CloudWatch Plugin zur Behandlung leerer Protokollzeilen wurde behoben.	
2.2.10	• Die Konfiguration der CloudWatch Log-Einstellungen über die Benutzeroberfläche wurde entfernt. • Ermöglichen Sie es Benutzern, CloudWatch Protokoll einstellungen in einer `%ProgramFiles%\Amazon\Ec2ConfigService\Settings\AWS.EC2.Windows.CloudWatch.json` Datei zu definieren, um future Verbesserungen zu ermöglichen.	
2.2.9	Problem mit unbehandelten Ausnahmen behoben sowie Protokollierung hinzugefügt.	
2.2.8	• Problem bei der Überprüfung der Windows-Betriebssystemversion im EC2Config-Installer behoben, um Windows Server 2003 SP1 und höher zu unterstützen. • Problem bei der Behandlung des Nullwerts beim Lesen der Registrierungsschlüssel behoben, die für die Aktualisierung der Sysprep-Config-Dateien benötigt werden.	
2.2.7	• Support für EC2Config hinzugefügt, um bei der Ausführung von Sysprep für Windows 2008 und höher ausgeführt zu werden. • Verbesserung der Ausnahmebehandlung und Protokollierung zur Optimierung der Diagnosen.	

Version	Details	Datum der Veröffentlichung
2.2.6	• Die Belastung der Instanz und der CloudWatch Protokolle beim Hochladen von Protokollereignissen wurde reduziert. • Es wurde ein Upgrade-Problem behoben, bei dem das CloudWatch Logs-Plug-In nicht immer aktiviert blieb	
2.2.5	• Unterstützung für das Hochladen von Protokollen in den CloudWatch Log Service hinzugefügt. • Problem mit der Bedingung im EC2OutputRDPCert-Plug-in behoben. • Die Wiederherstellungsoption für den EC2Config-Dienst wurde in „Aus Aktion neu starten“ geändert TakeNo • Weitere Ausnahmeinformationen hinzugefügt, für den Fall, das EC2Config fehlschlägt.	
2.2.4	• Ein Tippfehler in .cmd wurde behoben PostSysprep • Problem beim Anpinnen von EC2Config im Startmenü von OS2012+ behoben.	

Version	Details	Datum der Veröffentlichung
2.2.3	• Option hinzugefügt, sodass EC2Config sofort nach dem Installieren startet, auch ohne Service. Führen Sie dazu "Ec2Install.exe start=false"' von der Befehlszeile aus. • Parameter im Bildschirmhintergrund-Plug-in hinzugefügt, über den das Hinzufügen/Entfernen des Bildschirmhintergrunds gesteuert werden kann. Führen Sie zur Verwendung „Ec2 WallpaperInfo .exe set“ oder „WallpaperInfoEc2 .exe revert“ von der Befehlszeile aus • Suche nach Schlüssel hinzugefügt, falsche Einstellungen des RealTimeIsUniversal Registrierungsschlüssels werden in der Konsole ausgegeben RealTimeIsUniveral • EC2Config-Abhängigkeit vom Windows Temp-Ordner entfernt. • Die UserData Ausführungsabhängigkeit von.Net 3.5 wurde entfernt	
2.2.2	• Zusätzliche Überprüfung des Verhaltens bei der Servicebeendigung, damit sichergestellt wird, dass Ressourcen freigegeben werden. • Problem mit langen Ausführungszeiten bei der Verbindung zur Domain behoben	

Version	Details	Datum der Veröffentlichung
2.2.1	• Installer aktualisiert, damit Upgrades von älteren Versionen möglich sind. • Der WallpaperInfo Ec2-Fehler wurde in einer Nur-.Net4.5-Umgebung behoben • Fehler bei der zeitweiligen Treiberermittlung behoben. • Option zur Installation im Hintergrund hinzugefügt. Führen Sie Ec2Install.exe mit der "q"-Option aus, z. B. "Ec2Install.exe -q"	
2.2.0	• Support für .Net4- und .Net4.5-Umgebungen hinzugefügt. • Installer aktualisiert	
2.1.19	• Unterstützung für die Kennzeichnung flüchtiger Datenspeicher bei Verwendung des Intel-Netzwerktreibers (z. B. C3-Instance-Typ) hinzugefügt. Weitere Informationen finden Sie unter Verbessertes Networking auf Amazon EC2. • Support für AMI Origin Version und AMI Origin Name zur Konsolenausgabe hinzugefügt. • Änderungen an der Konsolenausgabe vorgenommen, um konsistente Formatierung/Analyse zu gewährleisten • Hilfedatei aktualisiert	

Version	Details	Datum der Veröffentlichung
2.1.18	• EC2Config WMI-Objekt für Abschlussbenachrichtigung hinzugefügt (-Namespace root\ Amazon -Class EC2_) ConfigService • Performance der Startup-WMI-Abfrage mit großen Ereignisprotokollen verbessert, kann möglicherweise während der ersten Ausführung zu einer hohen CPU führen	
2.1.17	• Das UserData Ausführungsproblem bei der Pufferfüllung von Standardausgabe und Standardfehler wurde behoben • Anzeige eines falschen RDP-Thumbprints in der Konsolenausgabe für >= w2k8 OS behoben. • Die Konsolenausgabe enthält jetzt 'RDPCERTIFICATE-SubjectName: 'für Windows 2008+, das den Computernamen enthält • Dem Dropdownmenü für die Zuweisung des Laufwerkbuchstaben wurde "D:\" hinzugefügt. • Schaltfläche "Hilfe" wurde nach oben rechts verschoben sowie das Erscheinungsbild verändert • Link zur Feedback-Umfrage hinzugefügt	

Version	Details	Datum der Veröffentlichung
2.1.16	• Registerkarte "General" umfasst einen Link zur EC2Config-Download-Seite für neue Versionen • Das Desktophintergrund-Overlay wird jetzt im lokalen Appdata-Ordner des Benutzers statt im Ordner Eigene Dateien gespeichert, um die Umleitung zu unterstützen MyDoc • MSSQL-Servername wurde mit dem System im Post-Sysprep-Skript (2008+) synchronisiert. • Der Anwendungsordner wurde neu organisiert (Dateien wurden in das Plug-in-Verzeichnis verschoben und doppelte Dateien entfernt). • Ausgabe des Systemprotokolls wurde geändert (Konsole): • * Wechsel zu einem Datums-, Namens-, Wertformat zur Vereinfachung der Analyse. (Beginnen Sie, die Abhängigkeiten in das neue Format zu migrieren.) • *Der Status des Plug-ins „Ec2“ wurde hinzugefügt SetPassword • * Sysprep wurden Start- und Endzeiten hinzugefügt • Problem bei der Kennzeichnung der flüchtigen Festplatten als "Temporary Storage" für Betriebssysteme behoben, die nicht in Englisch ausgeführt werden • Problem beim Deinstallieren von EC2Config nach der Ausführung von Sysprep behoben	

Version	Details	Datum der Veröffentlichung
2.1.15	• Anfragen an den Metadaten-Service optimiert • Metadaten umgehen jetzt die Proxy-Einstellungen • Flüchtige Festplatten werden als "Temporary Storage" gekennzeichnet und Impotant.txt wird, falls gefunden, auf das Volume platziert (nur Citrix PV-Treiber). Weitere Informationen finden Sie unter Upgraden von PV-Treibern auf Windows-Instances. • Flüchtigen Festplatten werden Laufwerkbuchstaben von Z nach A zugeordnet (nur Citrix PV-Treiber) – die Zuweisung kann mithilfe des Plug-ins für die Zuweisung des Laufwerkbuchstaben durch die Volume-Kennzeichnung "Temporary Storage X" überschrieben werden, wobei es sich bei "X" um eine Zahl zwischen 0 und 25 handelt • UserData läuft jetzt unmittelbar nach 'Windows is Ready'	
2.1.14	Korrekturen für den Desktop-Hintergrund	
2.1.13	• Desktop-Hintergrund zeigt den Hostnamen standardmäßig an • Abhängigkeit vom Windows-Zeitdienst wurde entfernt • In Fällen, bei denen einer einzelnen Schnittstelle mehrere IPs zugeordnet wurden, wurde eine Route hinzugefügt	

Version	Details	Datum der Veröffentlichung
2.1.11	• Änderungen am Ec2Activation-Plug-in vorgenommen • - Aktivierungsstatus wird alle 30 Tagse überprüft • - Verbleiben bei der Übergangsfrist 90 Tage (von 180), wird die Aktivierung erneut versucht	
2.1.10	• Überlagerung des Desktop-Hintergrunds bleibt mit Sysprep oder beim Herunterfahren ohne Sysprep nicht länger erhalten • Benutzerdatenoption wird bei jedem Service-Start mit <persist>true</persist> ausgeführt • Ort und Name von DisableWin /Update.cmd wurden in / Scripts/ .cmd geändert PostSysprep • Das Administratorkennwort ist in /Scripts/ .cmd standardmäßig so eingestellt, dass es nicht abläuft PostSysprep • Durch die Deinstallation wird das EC2Config-Skript aus c:\windows\setup\script\ .cmd PostSysprep entfernt CommandComplete • "Add Route" unterstützt benutzerdefinierte Schnittstellenmetriken	
2.1.9	UserData Die Ausführung ist nicht mehr auf 3851 Zeichen beschränkt	

Version	Details	Datum der Veröffentlichung
2.1.7	• Betriebssystemversion und Sprachen-ID werden in die Konsole geschrieben • EC2Config-Version wird in die Konsole geschrieben • PV-Treiber-Version wird in die Konsole geschrieben • Erkennung der Fehlerprüfung und Ausgabe werden beim nächsten Start an die Konsole übermittelt • config.xml wurde eine Option hinzugefügt, um Sysprep-Anmeldeinformationen zu erhalten • Logik zur Routenwiederholung hinzugefügt, falls ENI beim Start nicht verfügbar ist • PID für die Benutzerdaten-Ausführung in die Konsole geschrieben • Mindestlänge für das generierte Passwort vom GPO abgerufen • Legen Sie den Service-Start auf 3 Versuche fest. • Die Beispiele S3_ DownloadFile .ps1 und S3_Upload file.ps1 wurden dem Ordner /Scripts hinzugefügt	

Version	Details	Datum der Veröffentlichung
2.1.6	• Versionsinformationen zur Registerkarte "General" hinzugefügt • Registerkarte "Bundle" zu "Image" umbenannt • Festlegung der Passwörter vereinfacht und passwortbezogene Benutzeroberflächenelemente von der Registerkarte "General" auf die Registerkarte "Image" verschoben • Registerkarte "Disk Settings" zu "Storage" umbenannt • Registerkarte "Support" mit häufig verwendeten Tools zur Fehlerbehebung hinzugefügt • Die Datei `sysprep.ini` unter Windows Server 2003 so eingestellt, dass die Betriebssystempartition standardmäßig erweitert wird. • Private IP-Adresse dem Bildschirmhintergrund hinzugefügt • Private IP-Adresse wird auf dem Bildschirmhintergrund angezeigt • Logik für Wiederholversuche der Konsolenausgabe hinzugefügt • Problem bei der Com-Port-Ausnahme für die Verfügbarkeit der Metadaten behoben – bewirkte, dass EC2Config vor dem Anzeigen der Konsolenausgabe beendet wurde • Überprüfung des Aktivierungsstatus bei jedem Start – Aktivierung nach Bedarf •	

Version	Details	Datum der Veröffentlichung
	Problem bei den relativen Pfaden behoben – hervorgerufen durch die manuelle Ausführung einer Bildschirmhintergrund-Verknüpfung aus dem Startup-Ordner heraus; auf "Administrator/logs" verweisend • Problem mit der Hintergrundfarbe für Benutzer von Windows Server 2003 behoben (abgesehen vom Administrator).	

Version	Details	Datum der Veröffentlichung
2.1.2	• Konsolenzeitstempel auf UTC (Zulu) gesetzt • Anzeige eines Hyperlinks auf der Registerkarte Sysprep entfernt • Feature-Ergänzung zur dynamischen Erweiterung des Stamm-Volumes beim ersten Start von Windows 2008+ • Wenn "Set-Password" aktiviert ist, kann EC2Config automatisch das Passwort festlegen • EC2Config überprüft den Aktivierungsstatus vor dem Ausführen von Sysprep (zeigt Warnung an, falls nicht aktiviert) • Die Datei `Sysprep.xml` für Windows Server 2003 ist jetzt standardmäßig auf die Zeitzone UTC und nicht mehr auf Pacific eingestellt. • Zufällige Aktivierungsserver • Registerkarte "Drive Mapping" zu "Disk Settings" umbenannt • Benutzeroberflächenelemente "Initialize Drives" von der Registerkarte "General" auf die Registerkarte "Disk Settings" verschoben • Schaltfläche "Hilfe" verweist jetzt auf die HTML-Hilfedatei • HTML-Hilfedatei wurde mit den Änderungen aktualisiert • Hinweistext für die Zuweisungen von Laufwerkbuchstaben aktualisiert •	

Version	Details	Datum der Veröffentlichung
	InstallUpdates.ps1 wurde zum Ordner /Scripts hinzugefügt, um Patches und Säuberungen vor Sysprep zu automatisieren	
2.1.0	• Desktop-Hintergrund zeigt beim ersten Anmelden (nicht beim Trennen/Wiederherstellen der Verbindung) standardmäßig Instance-Informationen an • PowerShell kann von den Benutzerdaten aus ausgeführt werden, indem der Code mit umgeben wird<powershell></powershell>	

Abonnieren von EC2Config-Service-Benachrichtigungen

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen des EC2Config-Services veröffentlicht werden. Führen Sie die folgenden Schritte durch, um diese Benachrichtigungen zu abonnieren.

So abonnieren Sie EC2Config-Benachrichtigungen

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, da die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region erstellt wurden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.
5. Führen Sie im Dialogfeld Create subscription Folgendes aus:
   a. Verwenden Sie für Topic ARN den folgenden Amazon-Ressourcennamen (ARN):

      ```
      arn:aws:sns:us-east-1:801119661308:ec2-windows-ec2config
      ```

   b. Wählen Sie unter Protocol die Option `Email` aus.

c. Geben Sie unter Endpoint eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.

d. Wählen Sie Create subscription.

6. Sie erhalten eine E-Mail, in der Sie aufgefordert werden, Ihr Abonnement zu bestätigen. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Sobald eine neue Version des EC2Config-Services veröffentlicht wird, senden wir den Abonnenten Benachrichtigungen. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

So melden Sie sich von den EC2Config-Benachrichtigungen ab

1. Öffnen Sie die Amazon SNS-Konsole.
2. Wählen Sie im Navigationsbereich Subscriptions aus.
3. Wählen Sie das Abonnement aus und wählen Sie anschließend Actions und Delete Subscriptions. Klicken Sie zum Bestätigen auf Delete.

Problembehandlung beim EC2Config-Service

Die folgenden Informationen können Ihnen helfen, Probleme mit Ihrem EC2Config-Service zu beheben.

Aktualisieren von EC2Config auf einer unerreichbaren Instance

Verwenden Sie das folgende Verfahren, um den EC2Config-Service auf einer unerreichbaren Windows Server-Instance mithilfe des Remote Desktop zu aktualisieren.

So aktualisieren Sie EC2Config auf einer von Amazon EBS gestützten Windows-Instance, zu der Sie keine Verbindung herstellen können

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Starten Sie die betroffene Instance. Wählen Sie die Instance und wählen Sie Instance state (Instance-Status) und dann Stop instance (Instance anhalten).

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

4. Wählen Sie Launch Instance (Instance starten) aus und erstellen Sie eine temporäre `t2.micro`-Instance in derselben Availability Zone wie die betroffene Instance. Verwenden Sie ein anderes AMI als das, mit dem die betroffene Instance gestartet wurde.

   > **Important**
   >
   > Wenn Sie die Instance nicht in der gleichen Availability Zone wie die betroffene Instance erstellen, können Sie das Stamm-Volume der betroffenen Instance nicht der neuen Instance anfügen.

5. Wählen Sie in der EC2-Konsole Volumes aus.
6. Lokalisieren Sie das Stamm-Volume der betroffenen Instance. Trennen Sie das Volume und fügen Sie das Volume anschließend der temporären Instance an, die Sie zuvor erstellt haben. Fügen Sie es dem standardmäßigen Gerätenamen (xvdf) an.
7. Stellen Sie über Remote Desktop eine Verbindung mit der temporären Instance her und verwenden Sie anschließend das Dienstprogramm für die Datenträgerverwaltung, um das Volume verfügbar zu machen und es zu verwenden.
8. Laden Sie die aktuelle Version des EC2Config-Service herunter. Extrahieren Sie die Dateien aus der `.zip`-Datei in das `Temp`-Verzeichnis auf dem von Ihnen angefügten Laufwerk.
9. Öffnen Sie in der temporären Instance das Dialogfeld "Ausführen", geben Sie **`regedit`** ein und drücken Sie die Eingabetaste.
10. Wählen Sie `HKEY_LOCAL_MACHINE`. Wählen Sie im Menü File die Option Load Hive aus. Wählen Sie das Laufwerk aus und navigieren Sie zur folgenden Datei und öffnen Sie sie: `Windows\System32\config\SOFTWARE`. Geben Sie nach Aufforderung einen Schlüsselnamen ein.
11. Wählen Sie den gerade geladenen Schlüssel aus und navigieren Sie zu `Microsoft\Windows\CurrentVersion`. Wählen Sie den `RunOnce`-Schlüssel aus. Wenn dieser Schlüssel nicht vorhanden ist, wählen Sie im Kontextmenü (rechte Maustaste) `CurrentVersion`, New und anschließend Key aus. Benennen Sie den Schlüssel `RunOnce`.

12. Wählen Sie im Kontextmenü (rechte Maustaste) den `RunOnce`-Schlüssel, New und anschließend String Value aus. Geben Sie `Ec2Install` als den Namen und `C:\Temp\Ec2Install.exe /quiet` als die Daten ein.
13. Wählen Sie den `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`-Schlüssel aus. Wählen Sie im Kontextmenü (rechte Maustaste) die Option New und anschließend String Value aus. Geben Sie **`AutoAdminLogon`** als den Namen und **`1`** als die Daten ein.
14. Wählen Sie den `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon>`-Schlüssel aus. Wählen Sie im Kontextmenü (rechte Maustaste) die Option New und anschließend String Value aus. Geben Sie **`DefaultUserName`** als den Namen und **`Administrator`** als die Daten ein.
15. Wählen Sie den `HKEY_LOCAL_MACHINE\`*`specified key name`*`\Microsoft\Windows NT\CurrentVersion\Winlogon`-Schlüssel aus. Wählen Sie im Kontextmenü (rechte Maustaste) die Option New und anschließend String Value aus. Geben Sie **`DefaultPassword`** als Namen an und geben Sie ein Passwort in den Wertedaten ein.
16. Wählen Sie im Navigationsbereich „Registry Editor“ den temporären Schlüssel aus, den Sie beim ersten Öffnen des Registrierungs-Editors erstellt haben.
17. Wählen Sie im Menü File die Option Unload Hive aus.
18. Wählen Sie im Dienstprogramm für die Datenträgerverwaltung das Laufwerk aus, das Sie zugewiesen haben, öffnen Sie das Kontextmenü (Rechtsklick) und wählen Sie die Option Offline aus.
19. Trennen Sie in der Amazon EC2-Konsole das betroffene Volume von der temporären Instance und ordnen Sie es wieder der ursprünglichen Instance mit dem Gerätenamen z `/dev/sda1`. Sie müssen diesen Gerätenamen angeben, um das Volume als Stamm-Volume hinzufügen zu können.
20. Führen Sie das Beenden und starten Sie Amazon EC2 EC2-Instances der Instance aus.
21. Überprüfen Sie nach dem Start der Instance das Systemprotokoll und vergewissern Sie sich, dass die Meldung Windows ist einsatzbereit angezeigt wird.
22. Öffnen Sie den Registrierungs-Editor und wählen Sie au `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`. Löschen Sie die zuvor erstellten String-Value-Schlüssel: AutoAdminLogon, DefaultUserName und. DefaultPassword
23. Löschen Sie die in diesem Vorgang erstellte temporäre Instance bzw. beenden Sie sie.

Verwenden Sie EC2 Fast Launch für Ihre Windows-Instances

Jede Windows-Instance von Amazon EC2 muss die Standardstartschritte des Windows-Betriebssystems (OS) durchlaufen, die mehrere Neustarts beinhalten und oft 15 Minuten oder länger dauern. Amazon EC2 Windows Server-AMIs, bei denen die EC2-Schnellstartfunktion aktiviert ist, führen einige dieser Schritte durch und starten im Voraus neu, um die Zeit zu reduzieren, die zum Starten einer Instance benötigt wird.

Wenn Sie ein Windows Server-AMI für EC2 Fast Launch konfigurieren, erstellt Amazon EC2 eine Reihe von vorab bereitgestellten Snapshots, die für einen schnelleren Start wie folgt verwendet werden.

1. Amazon EC2 startet entsprechend Ihren Einstellungen eine Reihe temporärer t3-Instances.
2. Sobald die einzelnen temporären Instances die standardmäßigen Startschritte abschließen, erstellt Amazon EC2 jeweils einen vorab bereitgestellten Snapshot der Instance. Der Snapshot wird in Ihrem Amazon-S3-Bucket gespeichert.
3. Wenn der Snapshot fertig ist, beendet Amazon EC2 die zugehörige t3-Instance, um die Ressourcenkosten so gering wie möglich zu halten.
4. Wenn Amazon EC2 das nächste Mal eine Instance über das EC2 Fast Launch-fähige AMI startet, verwendet es einen der Snapshots, um die Startzeit erheblich zu reduzieren.

Amazon EC2 füllt die Snapshots, die Sie zur Hand haben, automatisch auf, wenn es sie verwendet, um Instances aus dem EC2 Fast Launch-fähigen AMI zu starten.

Jedes Konto, das Zugriff auf ein AMI mit aktiviertem EC2 Fast Launch hat, kann von kürzeren Startzeiten profitieren. Wenn der AMI-Besitzer Ihnen Zugriff zum Starten von Instances gewährt, stammen die vorab bereitgestellten Snapshots aus dem Konto des AMI-Besitzers.

Wenn ein AMI, das EC2 Fast Launch unterstützt, mit Ihnen geteilt wird, können Sie Faster Launching auf dem gemeinsam genutzten AMI selbst aktivieren oder deaktivieren. Wenn Sie ein gemeinsam genutztes AMI für EC2 Fast Launch aktivieren, erstellt Amazon EC2 die vorab bereitgestellten Snapshots direkt in Ihrem Konto. Wenn die in Ihrem Konto verfügbaren Snapshots aufgebraucht sind, können Sie weiterhin Snapshots aus dem Konto des AMI-Besitzers verwenden.

> **Note**
>
> EC2 Fast Launch löscht vorab bereitgestellte Snapshots, sobald sie bei einem Start verbraucht werden, um die Speicherkosten zu minimieren und eine Wiederverwendung

zu verhindern. Wenn die gelöschten Snapshots jedoch einer Aufbewahrungsregel entsprechen, werden sie automatisch im Papierkorb aufbewahrt. Wir empfehlen Ihnen, den Geltungsbereich Ihrer Aufbewahrungsregeln für den Papierkorb zu überprüfen, damit dies nicht passiert. Weitere Informationen finden Sie unter Überlegungen.
Dieses Feature ist nicht identisch mit der schnellen EBS-Snapshot-Wiederherstellung. Die schnelle EBS-Snapshot-Wiederherstellung müssen Sie explizit für jeden einzelnen Snapshot aktivieren, was mit entsprechenden Kosten verbunden ist.

Das folgende Video zeigt, wie Sie Ihr Windows-AMI für einen schnelleren Start konfigurieren können, und bietet einen kurzen Überblick über die zugehörigen Schlüsselbegriffe und ihre Definitionen: EC2-Windows-Instances bis zu 65% schneller starten AWS.

Kosten für die Ressourcen

Für die Konfiguration von Windows-AMIs für EC2 Fast Launch fallen keine Servicegebühren an. Für alle zugrunde liegenden AWS Ressourcen, die Amazon EC2 verwendet, gelten jedoch Standardpreise. Weitere Informationen zu den damit verbundenen Ressourcenkosten und deren Verwaltung finden Sie unter Verwalten Sie die Ressourcenkosten mit EC2 Fast Launch.

Inhalt

Wichtige Begriffe

Die EC2 Fast Launch-Funktion verwendet die folgenden Schlüsselbegriffe:

Vorab bereitgestellter Snapshot

Ein Snapshot einer Instance, die von einem Windows-AMI mit aktiviertem EC2 Fast Launch gestartet wurde und die die folgenden Windows-Startschritte abgeschlossen hat und bei Bedarf neu gestartet wurde.

- Sysprep spezialisieren
- Windows Out of Box Experience (OOBE)

Wenn diese Schritte abgeschlossen sind, stoppt EC2 Fast Launch die Instance und erstellt einen Snapshot, der später basierend auf Ihrer Konfiguration für einen schnelleren Start aus dem AMI verwendet wird.

Starthäufigkeit

Legt die Anzahl der vorab bereitgestellten Snapshots fest, die Amazon EC2 innerhalb des angegebenen Zeitrahmens starten kann. Wenn Sie EC2 Fast Launch für Ihr AMI aktivieren, erstellt Amazon EC2 den ersten Satz von vorab bereitgestellten Snapshots im Hintergrund. Wenn die Startfrequenz beispielsweise auf fünf Starts pro Stunde festgelegt ist, was die Standardeinstellung ist, erstellt EC2 Fast Launch einen ersten Satz von fünf vorab bereitgestellten Snapshots.

Wenn Amazon EC2 eine Instance von einem AMI mit aktiviertem EC2 Fast Launch startet, verwendet es einen der vorab bereitgestellten Snapshots, um die Startzeit zu reduzieren. Wenn Snapshots verwendet werden, werden sie automatisch auf die mit der Startfrequenz angegebenen Anzahl aufgefüllt.

Wenn Sie eine Zunahme der Instances erwarten, die über Ihr AMI gestartet werden – zum Beispiel während eines besonderen Ereignisses – können Sie die Starthäufigkeit im Voraus erhöhen, um die zusätzlich benötigten Instances abzudecken. Wenn Ihr Startvolumen wieder normal ist, können Sie die Häufigkeit wieder nach unten anpassen.

Wenn die Zahl der Starts höher ist als erwartet, verbrauchen Sie unter Umständen alle verfügbaren vorab bereitgestellten Snapshots. Das führt nicht dazu, dass Starts fehlschlagen. Es kann jedoch dazu führen, dass einige Instances den Standardstartprozess durchlaufen, bis Snapshots wieder aufgefüllt werden können.

Anzahl der Zielressourcen

Die Anzahl der vorab bereitgestellten Snapshots, die für ein Amazon EC2 Windows Server-AMI mit aktiviertem EC2 Fast Launch bereitgehalten werden müssen.

Max. Anzahl paralleler Starts

Steuert, wie viele Instances Amazon EC2 gleichzeitig starten kann, um die vorab bereitgestellten Snapshots für EC2 Fast Launch zu erstellen. Wenn die Anzahl der Zielressourcen höher ist als die konfigurierte maximale Anzahl an parallelen Starts, startet Amazon EC2 zunächst die Anzahl an Instances, die durch die Einstellung Max. Anzahl paralleler Starts für die Erstellung der Snapshots festgelegt wurde. Wenn diese Instances den Vorgang abgeschlossen haben, erstellt Amazon EC2 den Snapshot und stoppt die Instance. Anschließend werden weitere Instances gestartet, bis die Gesamtzahl der verfügbaren Snapshots die Anzahl der Zielressourcen erreicht hat. Der Wert für Max. Anzahl paralleler Starts muss 6 oder höher sein.

Voraussetzungen für EC2 Fast Launch

Bevor Sie EC2 Fast Launch einrichten, stellen Sie sicher, dass Sie die folgenden Voraussetzungen erfüllen, die erforderlich sind, um Snapshots für die AMIs in Ihrem zu erstellen: AWS-Konto

- Wenn Sie keine Startvorlage zur Konfiguration Ihrer Einstellungen verwenden, stellen Sie sicher, dass eine Standard-VPC für die Region konfiguriert ist, in der Sie EC2 Fast Launch verwenden.

> **Note**
>
> Wenn Sie versehentlich Ihre Standard-VPC in der Region löschen, in der Sie EC2 Fast Launch konfigurieren möchten, können Sie in dieser Region eine neue Standard-VPC erstellen. Weitere Informationen finden Sie unter Erstellen einer Standard-VPC im Benutzerhandbuch zu Amazon VPC.

- Um eine nicht standardmäßige VPC anzugeben, müssen Sie eine Startvorlage verwenden, wenn Sie Windows Fast Launch konfigurieren. Weitere Informationen finden Sie unter Verwenden Sie eine Startvorlage, wenn Sie EC2 Fast Launch einrichten.
- Wenn Ihr Konto eine Richtlinie enthält, die IMDSv2 für Amazon-EC2-Instances erzwingt, müssen Sie eine Startvorlage erstellen, in der die Metadatenkonfiguration zur Erzwingung von IMDSv2 angegeben ist.
- Private EC2 Fast Launch-AMIs müssen die Ausführung von Benutzerdatenskripten unterstützen.
- Um EC2 Fast Launch für ein AMI zu konfigurieren, müssen Sie das AMI Sysprep mit der Shutdown-Option erstellen. Die EC2 Fast Launch-Funktion unterstützt derzeit keine AMIs, die aus einer laufenden Instance erstellt wurden.

Informationen zum Erstllen eines AMI mit Sysprep finden Sie unter Erstellen Sie ein AMI mit Windows Sysprep.

- Das Standardkontingent für Max. Anzahl paralleler Starts für alle AMIs in einem AWS-Konto beträgt 40 pro Region. Auf folgende Weise können Sie eine Erhöhung der Service Quotas für Ihr Konto anfordern.

  1. Melden Sie sich bei der Service Quotas Quotas-Konsole an AWS Management Console und öffnen Sie sie unter https://console.aws.amazon.com/servicequotas/.
  2. Wählen Sie im Navigationsbereich AWS-Services aus.
  3. Geben Sie in der Suchleiste `EC2 Fast Launch` ein und wählen Sie das Ergebnis aus.
  4. Wählen Sie den Link für `Parallel instance launches` aus. Dadurch gelangen Sie zur Service-Quotas-Detailseite Parallele Instance-Starts.
  5. Wählen Sie Kontingenterhöhung anfordern.

  Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Konfigurieren Sie die EC2 Fast Launch-Einstellungen für Ihr Amazon EC2 Windows Server-AMI

Sie können EC2 Fast Launch für Windows-AMIs konfigurieren, die Sie besitzen, oder für AMIs, die über die API AWS Management Console, SDKs CloudFormation, oder AWS Command Line Interface () für Sie freigegeben wurden.AWS CLI Bevor Sie EC2 Fast Launch konfigurieren, stellen Sie sicher, dass Ihr AMI alle Voraussetzungen erfüllt, die für die Erstellung der vorab bereitgestellten Snapshots erforderlich sind. Weitere Informationen finden Sie unter Voraussetzungen für EC2 Fast Launch.

In den folgenden Abschnitten werden die Konfigurationsschritte für die Amazon EC2 EC2-Konsole und AWS CLI behandelt.

Aktivieren Sie EC2 Fast Launch

Um EC2 Fast Launch zu aktivieren, wählen Sie die Registerkarte, die Ihrer Umgebung entspricht, und folgen Sie den Schritten.

> **Note**
>
> Um diese Einstellungen zu ändern, stellen Sie sicher, dass Ihr AMI und die Region, in der Sie ausführen, alle Voraussetzungen für EC2 Fast Launch erfüllen.

Console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Images die Option AMIs aus.
3. Wählen Sie das zu aktualisierende AMI aus, indem Sie das Kontrollkästchen neben dem Namen aktivieren.
4. Wählen Sie im Menü Aktionen über der Liste der AMIs den Befehl Schnellstart konfigurieren. Dadurch wird die Seite Schnellstart konfigurieren geöffnet, auf der Sie die Einstellungen für EC2 Fast Launch konfigurieren.
5. Um mit vorab bereitgestellten Snapshots Instances schneller über Ihr Windows-AMI zu starten, aktivieren Sie das Kontrollkästchen Schnellstarts für Windows aktivieren.
6. Wählen Sie in der Dropdownliste Set anticipated launch frequency (Voraussichtliche Starthäufigkeit festlegen) einen Wert aus, um die Anzahl der Snapshots festzulegen, die erstellt und beibehalten werden, um das erwartete Startvolumen Ihrer Instance abzudecken.
7. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save changes (Änderungen speichern).

> **Note**
>
> Wenn Sie eine Startvorlage verwenden müssen, um eine nicht standardmäßige VPC anzugeben oder um Metadateneinstellungen für IMDSv2 zu konfigurieren, siehe Verwenden Sie eine Startvorlage, wenn Sie EC2 Fast Launch einrichten.

AWS CLI

Der enable-fast-launch Befehl ruft den Amazon EC2 EnableFastLaunch API-Vorgang auf.

Syntax:

```
aws ec2 enable-fast-launch \
```

```
  --image-id <value> \
  --resource-type <value> \ (optional)
  --snapshot-configuration <value> \ (optional)
  --launch-template <value> \ (optional)
  --max-parallel-launches <value> \ (optional)
  --dry-run | --no-dry-run \  (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Beispiel:

Das folgende Enable-Fast-Launch-Beispiel aktiviert EC2 Fast Launch für das angegebene AMI und startet sechs parallel Instances für die Vorbereitstellung. Der `ResourceType` wird auf `snapshot` gesetzt, was der Standardwert ist.

```
aws ec2 enable-fast-launch \
         --image-id ami-01234567890abcedf  \
         --max-parallel-launches 6 \
         --resource-type snapshot
```

Ausgabe:

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {
         "TargetResourceCount": 10
     },
     "LaunchTemplate": {},
     "MaxParallelLaunches": 6,
     "OwnerId": "0123456789123",
     "State": "enabling",
     "StateTransitionReason": "Client.UserInitiated",
     "StateTransitionTime": "2022-01-27T22:16:03.199000+00:00"
 }
```

Tools for PowerShell

Das Enable-EC2FastLaunch Cmdlet ruft den Amazon EC2 EnableFastLaunch API-Vorgang auf, um EC2 Fast Launch auf Ihrem Windows-AMI zu aktivieren.

Syntax:

```
Enable-EC2FastLaunch
      -ImageId <String>
      -LaunchTemplate_LaunchTemplateId <String>
      -LaunchTemplate_LaunchTemplateName <String>
      -MaxParallelLaunch <Int32>
      -ResourceType <String>
      -SnapshotConfiguration_TargetResourceCount <Int32>
      -LaunchTemplate_Version <String>
      -Select <String>
      -PassThru <SwitchParameter>
      -Force <SwitchParameter>
```

Beispiel:

Das folgende Enable-EC2FastLaunchBeispiel aktiviert EC2 Fast Launch für das angegebene AMI und startet sechs parallel Instances für die Vorbereitstellung. Der `ResourceType` wird auf `snapshot` gesetzt, was der Standardwert ist.

```
Enable-EC2FastLaunch `
 -ImageId ami-01234567890abcedf `
 -MaxParallelLaunch 6 `
 -Region us-west-2 `
 -ResourceType snapshot
```

Ausgabe:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration : Amazon.EC2.Model.FastLaunchSnapshotConfigurationResponse
State                 : enabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:24:11 PM
```

Deaktivieren Sie EC2 Fast Launch

Um EC2 Fast Launch zu deaktivieren, wählen Sie die Registerkarte, die Ihrer Umgebung entspricht, und folgen Sie den Schritten.

> **Note**
>
> Um diese Einstellungen zu ändern, stellen Sie sicher, dass Ihr AMI und die Region, in der Sie ausführen, alle Voraussetzungen für EC2 Fast Launch erfüllen.

Console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Images die Option AMIs aus.
3. Wählen Sie das zu aktualisierende AMI aus, indem Sie das Kontrollkästchen neben dem Namen aktivieren.
4. Wählen Sie im Menü Aktionen über der Liste der AMIs den Befehl Schnellstart konfigurieren. Dadurch wird die Seite Schnellstart konfigurieren geöffnet, auf der Sie die Einstellungen für EC2 Fast Launch konfigurieren.
5. Deaktivieren Sie das Kontrollkästchen Schnellstart für Windows aktivieren, um EC2 Fast Launch zu deaktivieren und vorab bereitgestellte Snapshots zu entfernen. Dies führt dazu, dass das AMI in Zukunft den Standardstartprozess für jede Instance verwendet.

   > **Note**
   >
   > Wenn Sie die Windows-Image-Optimierung deaktivieren, werden alle vorhandenen vorab bereitgestellten Snapshots automatisch gelöscht. Dieser Schritt muss abgeschlossen sein, bevor Sie das Feature erneut verwenden können.

6. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save changes (Änderungen speichern).

AWS CLI

Der disable-fast-launch Befehl ruft den Amazon EC2 DisableFastLaunch API-Vorgang auf.

Syntax:

```
aws ec2 disable-fast-launch \
  --image-id <value> \
  --force | --no-force \ (optional)
```

```
  --dry-run | --no-dry-run \ (optional)
  --cli-input-json <value> \ (optional)
  --generate-cli-skeleton <value> \ (optional)
```

Beispiel:

Das folgende Beispiel für disable-fast-launch deaktiviert EC2 Fast Launch auf dem angegebenen AMI und bereinigt vorhandene vorab bereitgestellte Snapshots.

```
aws ec2 disable-fast-launch \
        --image-id ami-01234567890abcedf
```

Ausgabe:

```
{
     "ImageId": "ami-01234567890abcedf",
     "ResourceType": "snapshot",
     "SnapshotConfiguration": {},
     "LaunchTemplate": {
         "LaunchTemplateId": "lt-01234567890abcedf",
         "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
         "Version": "1"
     },
     "MaxParallelLaunches": 6,
     "OwnerId": "0123456789123",
     "State": "disabling",
     "StateTransitionReason": "Client.UserInitiated",
     "StateTransitionTime": "2022-01-27T22:47:29.265000+00:00"
 }
```

Tools for PowerShell

Das Disable-EC2FastLaunch Cmdlet ruft den Amazon EC2 DisableFastLaunch API-Vorgang auf.

Syntax:

```
Disable-EC2FastLaunch
      -ImageId <String>
      -ForceStop <Boolean>
      -Select <String>
```

```
    -PassThru <SwitchParameter>
    -Force <SwitchParameter>
```

Beispiel:

Im folgenden Disable-EC2FastLaunchBeispiel wird EC2 Fast Launch auf dem angegebenen AMI deaktiviert und vorhandene vorab bereitgestellte Snapshots bereinigt.

```
Disable-EC2FastLaunch -ImageId ami-01234567890abcedf
```

Ausgabe:

```
ImageId               : ami-01234567890abcedf
LaunchTemplate        :
Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : disabling
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 1:10:08 PM
```

Verwenden Sie eine Startvorlage, wenn Sie EC2 Fast Launch einrichten

Mit einer Startvorlage können Sie eine Reihe von Startparametern konfigurieren, die Amazon EC2 bei jedem Start einer Instance aus dieser Vorlage verwendet. Sie können Dinge wie ein AMI angeben, das für Ihr Basis-Image, Instance-Typen, Speicher, Netzwerkeinstellungen und mehr verwendet werden soll.

Startvorlagen sind optional, mit Ausnahme der folgenden Sonderfälle, in denen Sie eine Startvorlage für Ihr Windows-AMI verwenden müssen, wenn Sie einen schnelleren Start konfigurieren:

- Sie müssen eine Startvorlage verwenden, um eine nicht standardmäßige VPC für Ihr Windows-AMI anzugeben.
- Wenn Ihr Konto eine Richtlinie enthält, die IMDSv2 für Amazon-EC2-Instances erzwingt, müssen Sie eine Startvorlage erstellen, in der die Metadatenkonfiguration zur Erzwingung von IMDSv2 angegeben ist.

Verwenden Sie die Startvorlage, die Ihre Metadatenkonfiguration enthält, von der EC2-Konsole aus, oder wenn Sie den Befehl enable-fast-launch in der ausführen oder die LaunchAWS CLI API-Aktion aufrufen. EnableFast

Amazon EC2 EC2 Fast Launch unterstützt die folgende Konfiguration nicht, wenn Sie eine Startvorlage verwenden. Wenn Sie eine Startvorlage für EC2 Fast Launch verwenden, dürfen Sie keine der folgenden Angaben machen:

- Benutzerdatenskripts
- Termination protection
- Deaktivierte Metadaten
- Spot-Option
- Verhalten beim Herunterfahren, das die Instance beendet
- Ressourcen-Tags für Netzwerkschnittstellen-, Elastic Graphic- oder Spot-Instance-Anfragen

Angeben einer nicht standardmäßigen VPC

Schritt 1: Eine Startvorlage erstellen

Erstellen Sie eine Startvorlage, die die folgenden Details für Ihre Windows-Instances angibt:

- Das VPC-Subnetz.
- Einen Instance-Typ von `t3.xlarge`.

Weitere Informationen finden Sie unter Erstellen einer Startvorlage.

Schritt 2: Geben Sie die Startvorlage für Ihr EC2 Fast Launch AMI an

Wählen Sie die Registerkarte, die zu Ihrem Vorgang passt:

Console

Gehen Sie wie folgt vor, um die Startvorlage für EC2 Fast Launch vom AWS Management Console anzugeben:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich unter Images die Option AMIs aus.
3. Wählen Sie das zu aktualisierende AMI aus, indem Sie das Kontrollkästchen neben dem Namen aktivieren.
4. Wählen Sie im Menü Aktionen über der Liste der AMIs den Befehl Schnellstart konfigurieren. Dadurch wird die Seite Schnellstart konfigurieren geöffnet, auf der Sie die Einstellungen für EC2 Fast Launch konfigurieren.
5. Die Launch template (Startvorlage) führt eine gefilterte Suche durch, bei der Startvorlagen in Ihrem Konto in der aktuellen Region gefunden werden, die mit dem von Ihnen eingegebenen Text übereinstimmen. Geben Sie den Namen oder die ID der Startvorlage ganz oder teilweise in das Feld ein, um eine Liste mit übereinstimmenden Startvorlagen anzuzeigen. Wenn Sie beispielsweise `fast` in der Box eingeben, findet Amazon EC2 alle Startvorlagen in Ihrem Konto in der aktuellen Region, die „schnell“ im Namen haben.

   Um eine neue Startvorlage zu erstellen, können Sie Create launch template (Startvorlage erstellen) wählen.
6. Wenn Sie eine Startvorlage auswählen, zeigt Amazon EC2 die Standardversion für diese Vorlage im Feld Source template version (Quellvorlagenversion) an. Um eine andere Version anzugeben, markieren Sie die Standardversion, um sie zu ersetzen, und geben Sie die gewünschte Versionsnummer in das Feld ein.
7. Wenn Sie die gewünschten Änderungen vorgenommen haben, wählen Sie Save changes (Änderungen speichern).

AWS CLI, API

Um die Startvorlage für EC2 Fast Launch aus dem anzugeben AWS CLI, geben Sie den Namen oder die ID der Startvorlage im `--launch-template` Parameter an, wenn Sie den Befehl enable-fast-launch in der ausführen. AWS CLI

Um die Startvorlage für EC2 Fast Launch in einer API-Anfrage anzugeben, geben Sie den Namen oder die ID der Startvorlage im `LaunchTemplate` Parameter an, wenn Sie die Aktion „API starten“ aufrufen. EnableFast

Weitere Informationen über EC2-Startvorlagen finden Sie unter Starten einer Instance über eine Startvorlage.

Erstellen Sie ein benutzerdefiniertes Image mit aktiviertem EC2 Fast Launch

Amazon EC2 EC2 Fast Launch ist in EC2 Image Builder integriert, sodass Sie benutzerdefinierte Images mit aktiviertem EC2 Fast Launch erstellen können. Weitere Informationen finden Sie unter Erstellen von Verteilungseinstellungen für ein Windows-AMI mit aktiviertem EC2-Schnellstart (AWS CLI) im Benutzerhandbuch von EC2 Image Builder.

AMIs mit aktiviertem EC2 Fast Launch anzeigen

Sie können den Befehl describe-fast-launch-images im oder die Get-EC2FastLaunchImageTools for PowerShell Cmdlet verwenden, um Details zu AMIs abzurufen AWS CLI, für die EC2 Fast Launch aktiviert ist.

Amazon EC2 bietet die folgenden Details für jedes Windows-AMI in den Ergebnissen:

- Die Image-ID für ein AMI mit aktiviertem EC2 Fast Launch.
- Der Ressourcentyp, der für die Vorabbereitstellung des zugeordneten Windows-AMI verwendet wird. Unterstützter Wert: `snapshot`.
- Die Snapshot-Konfiguration, also eine Gruppe von Parametern, die die Vorabbereitstellung für das zugehörige Windows-AMI mit Snapshots konfigurieren.
- Startvorlageninformationen, einschließlich der ID, des Namens und der Version der Startvorlage, die das zugeordnete AMI verwendet, wenn es Window-Instances aus vorab bereitgestellten Snapshots startet.
- Die maximale Anzahl an Instances, die, zum Erstellen von Ressourcen, gleichzeitig gestartet werden können.
- Das ist die Besitzer-ID für das zugeordnete AMI. Für AMIs, die für Sie freigegeben wurden, wurde dieses Feld nicht ausgefüllt.
- Der aktuelle Status von EC2 Fast Launch für das zugehörige AMI. Zu den unterstützten Werten gehören: `enabling | enabling-failed | enabled | enabled-failed | disabling | disabling-failed`.

> **Note**
>
> Sie können den aktuellen Status auch auf der Seite Manage image optimization (Image-Optimierung verwalten) in der EC2-Konsole als Image optimization state (Image-Optimierungsstatus) anzeigen.

- Der Grund, warum EC2 Fast Launch für das zugehörige AMI auf den aktuellen Status geändert wurde.
- Der Zeitpunkt, zu dem EC2 Fast Launch für das zugehörige AMI auf den aktuellen Status geändert wurde.

Wählen Sie die Registerkarte aus, die Ihrer Befehlszeilenumgebung entspricht:

AWS CLI

Der describe-fast-launch-images Befehl ruft den Amazon EC2 DescribeFastLaunchImagesEC2-API-Vorgang auf.

Syntax:

```
aws ec2 describe-fast-launch-images \
 --image-ids <value> \ (optional)
 --filters <value> \ (optional)
 --dry-run | --no-dry-run \ (optional)
 --cli-input-json <value> \ (optional)
 --starting-token <value> \ (optional)
 --page-size <value> \ (optional)
 --max-items <value> \ (optional)
 --generate-cli-skeleton <value> \ (optional)
```

Beispiel:

Das folgende Beispiel für describe-fast-launch-images beschreibt die Details für die einzelnen AMIs im Konto, die für EC2 Fast Launch konfiguriert sind. In diesem Beispiel ist nur ein AMI im Konto für EC2 Fast Launch konfiguriert.

```
aws ec2 describe-fast-launch-images
```

Ausgabe:

```
{
    "FastLaunchImages": [
        {
            "ImageId": "ami-01234567890abcedf",
            "ResourceType": "snapshot",
            "SnapshotConfiguration": {},
```

```
            "LaunchTemplate": {
                "LaunchTemplateId": "lt-01234567890abcedf",
                "LaunchTemplateName": "EC2FastLaunchDefaultResourceCreation-
a8c6215d-94e6-441b-9272-dbd1f87b07e2",
                "Version": "1"
            },
            "MaxParallelLaunches": 6,
            "OwnerId": "0123456789123",
            "State": "enabled",
            "StateTransitionReason": "Client.UserInitiated",
            "StateTransitionTime": "2022-01-27T22:20:06.552000+00:00"
        }
    ]
}
```

Tools for PowerShell

Das Get-EC2FastLaunchImage Cmdlet ruft den Amazon EC2 DescribeFastLaunchImagesEC2-API-Vorgang auf.

Syntax:

```
Get-EC2FastLaunchImage
-Filter <Filter[]>
-ImageId <String[]>
-MaxResult <Int32>
-NextToken <String>
-Select <String>
-NoAutoIteration <SwitchParameter>
```

Beispiel:

Im folgenden Get-EC2FastLaunchImageBeispiel werden die Details für die einzelnen AMIs im Konto beschrieben, die für EC2 Fast Launch konfiguriert sind. In diesem Beispiel ist nur ein AMI im Konto für EC2 Fast Launch konfiguriert.

```
Get-EC2FastLaunchImage -ImageId ami-01234567890abcedf
```

Ausgabe:

```
ImageId               : ami-01234567890abcedf
```

```
LaunchTemplate        :
 Amazon.EC2.Model.FastLaunchLaunchTemplateSpecificationResponse
MaxParallelLaunches   : 6
OwnerId               : 0123456789123
ResourceType          : snapshot
SnapshotConfiguration :
State                 : enabled
StateTransitionReason : Client.UserInitiated
StateTransitionTime   : 2/25/2022 12:54:43 PM
```

Verwalten Sie die Ressourcenkosten mit EC2 Fast Launch

Für die Konfiguration von Windows-AMIs für EC2 Fast Launch fallen keine Servicegebühren an. Wenn Sie jedoch EC2 Fast Launch für ein Amazon EC2 Windows AMI aktivieren, gelten die Standardpreise für die zugrunde liegenden AWS Ressourcen, die Amazon EC2 zur Vorbereitung und Speicherung der vorab bereitgestellten Snapshots verwendet. Sie können Tags zur Kostenzuweisung konfigurieren, um die Kosten im Zusammenhang mit EC2 Fast Launch-Ressourcen nachzuverfolgen und zu verwalten. Weitere Informationen zum Konfigurieren von Kostenzuweisungs-Tags finden Sie unter Verfolgen Sie die Kosten für EC2 Fast Launch auf Ihrer Rechnung.

Das folgende Beispiel zeigt, wie die mit den Kosten für EC2 Fast Launch-Snapshots verbundenen Kosten aufgeteilt werden können.

Beispielszenario: Das AtoZ-Beispielunternehmen hat ein Windows-AMI mit einem 50-GiB-EBS-Root-Volume. Sie aktivieren EC2 Fast Launch für ihr AMI und legen die Anzahl der Zielressourcen auf fünf fest. Im Laufe eines Monats kostet sie die Nutzung von EC2 Fast Launch für ihr AMI etwa 5,00$, und die Kosten teilen sich wie folgt auf:

1. Wenn AtoZ Example EC2 Fast Launch aktiviert, startet Amazon EC2 fünf kleine Instances. Jede Instance läuft durch die Startschritte von Sysprep und OOBE Windows und wird bei Bedarf neu gestartet. Dies dauert für jede Instance mehrere Minuten (die Zeit kann variieren, je nachdem, wie ausgelastet diese Region oder Availability Zone (AZ) ist, und wie groß das AMI ist).

   Kosten

   - Instance-Laufzeitkosten (oder ggf. minimale Laufzeit): fünf Instances
   - Volumenkosten: fünf EBS Root-Volumes
2. Wenn der Vorab-Bereitstellungsprozess abgeschlossen ist, erstellt Amazon EC2 einen Snapshot der Instance und speichert diesen in Amazon S3. Snapshots werden in der Regel 4-8 Stunden

lang gespeichert, bevor sie bei einem Start verbraucht werden. In diesem Fall betragen die Kosten etwa 0,02 bis 0,05 USD pro Snapshot.

Kosten

- Snapshot-Speicher (Amazon S3): Fünf Snapshots

3. Nachdem Amazon EC2 den Snapshot erstellt hat, stoppt es die Instance. Zu diesem Zeitpunkt fallen für die Instance keine Kosten mehr an. Die EBS-Volumenkosten fallen jedoch weiterhin an.

   Kosten

   - EBS-Volumes: Die Kosten für die zugehörigen EBS Root-Volumes laufen weiter.

> **Note**
>
> Die hier angegebenen Kosten dienen nur zu Demonstrationszwecken. Ihre Kosten variieren je nach AMI-Konfiguration und Preisplan.

Verfolgen Sie die Kosten für EC2 Fast Launch auf Ihrer Rechnung

Mithilfe von Tags zur Kostenzuweisung können Sie Ihre AWS Rechnung so organisieren, dass sie die mit EC2 Fast Launch verbundenen Kosten widerspiegelt. Sie können das folgende Tag verwenden, das Amazon EC2 zu den Ressourcen hinzufügt, die es erstellt, wenn es vorab bereitgestellte Snapshots für EC2 Fast Launch vorbereitet und speichert:

Tag-Schlüssel: `CreatedBy`, Wert: `EC2 Fast Launch`

Nachdem Sie das Tag in der Konsole für Fakturierung und Kostenmanagement aktiviert und Ihren detaillierten Rechnungsbericht eingerichtet haben, erscheint die Spalte `user:CreatedBy` im Bericht. Die Spalte enthält Werte aus allen Services. Wenn Sie jedoch die CSV-Datei herunterladen, können Sie die Daten in eine Tabellenkalkulation importieren und nach `EC2 Fast Launch` im Wert filtern. Diese Informationen werden auch angezeigt, AWS Cost and Usage Report wenn das Tag aktiviert wird.

Schritt 1: Benutzerdefinierte Kostenzuordnungs-Tags aktivieren

Um Ressourcen-Tags in Ihre Kostenberichte aufzunehmen, müssen Sie sie zuerst in der Konsole für Fakturierung und Kostenmanagement aktivieren. Weitere Informationen finden Sie unter

Benutzerdefinierte Kostenzuordnungs-Tags aktivieren im AWS Billing and Cost Management - Benutzerhandbuch.

> **Note**
>
> Die Aktivierung kann bis zu 24 Stunden dauern.

Schritt 2: Kostenbericht einrichten

Wenn Sie bereits einen Kostenbericht eingerichtet haben, wird bei der nächsten Ausführung des Berichts nach Abschluss der Aktivierung eine Spalte für Ihr Tag angezeigt. Um Kostenberichte zum ersten Mal zu erstellen, wählen Sie eine der folgenden Optionen aus.

- Weitere Informationen finden Sie unter Einrichten Ihres monatlichen Kostenzuordnungsberichts im AWS Billing and Cost Management -Benutzerhandbuch.
- Weitere Informationen finden Sie im Benutzerhandbuch zu AWS Cost and Usage Report en unter Erstellen von Kosten- und Nutzungsberichten.

> **Note**
>
> Es kann bis zu 24 Stunden dauern AWS , bis Berichte an Ihren S3-Bucket gesendet werden.

Sie können EC2 Fast Launch für Windows-AMIs konfigurieren, die Sie besitzen, oder AMIs, die über die Amazon EC2 EC2-Konsole, API CloudFormation, SDKs oder ec2 Befehle in der für Sie freigegeben wurden. AWS CLI In den folgenden Abschnitten werden die Konfigurationsschritte für die Amazon EC2 EC2-Konsole und AWS CLI behandelt.

Sie können auch benutzerdefinierte Windows-AMIs erstellen, die für EC2 Fast Launch mit EC2 Image Builder konfiguriert sind. Weitere Informationen finden Sie unter Erstellen von Verteilungseinstellungen für ein Windows-AMI mit aktiviertem EC2-Schnellstart (AWS CLI).

Überwachen Sie EC2 Fast Launch

In diesem Abschnitt wird beschrieben, wie Sie die Amazon EC2 Windows Server-AMIs in Ihrem Konto überwachen, für die EC2 Fast Launch aktiviert ist.

Überwachen Sie die Statusänderungen von EC2 Fast Launch mit EventBridge

Wenn sich der Status für ein Windows-AMI mit aktiviertem EC2 Fast Launch ändert, generiert Amazon EC2 ein `EC2 Fast Launch State-change Notification` Ereignis. Dann sendet Amazon EC2 das Statusänderungsereignis an Amazon EventBridge (früher bekannt als Amazon CloudWatch Events).

Sie können EventBridge Regeln erstellen, die als Reaktion auf das Zustandsänderungsereignis eine oder mehrere Aktionen auslösen. Sie können beispielsweise eine EventBridge Regel erstellen, die erkennt, wann EC2 Fast Launch aktiviert ist, und die folgenden Aktionen ausführt:

- Sendet eine Nachricht an ein Amazon-SNS-Thema, um die Abonnenten zu benachrichtigen.
- Ruft eine Lambda-Funktion auf, die eine Aktion ausführt.
- Sendet die Daten zur Statusänderung zur Analyse an Amazon Data Firehose.

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter Erstellen von EventBridge Amazon-Regeln, die auf Ereignisse reagieren.

Statusänderungsereignisse

Die EC2-Schnellstartfunktion gibt Statusänderungsereignisse im JSON-Format nach bestem Wissen aus. Amazon EC2 sendet die Ereignisse nahezu EventBridge in Echtzeit an. In diesem Abschnitt werden die Ereignisfelder beschrieben und ein Beispiel für das Ereignisformat gezeigt.

`EC2 Fast Launch State-change Notification`

imageId

Identifiziert das AMI mit der EC2 Fast Launch-Statusänderung.

RessourcenTyp

Der Ressourcentyp, der für die Vorabbereitstellung verwendet werden soll. Unterstützter Wert: `snapshot`. Der Standardwert ist `snapshot`.

state

Der aktuelle Status der EC2 Fast Launch-Funktion für das angegebene AMI. Gültige Werte sind unter anderem:

- aktivieren — Sie haben die EC2-Schnellstartfunktion für das AMI aktiviert und Amazon EC2 hat mit der Erstellung von Snapshots für den Prozess vor der Bereitstellung begonnen.

- enabling-failed — Es ist ein Fehler aufgetreten, der dazu führte, dass der Vorbereitstellungsprozess fehlschlug, als Sie den EC2 Fast Launch für ein AMI zum ersten Mal aktivierten. Dies kann jederzeit während des Vorabbereitstellungsprozesses passieren.
- aktiviert — Die EC2 Fast Launch-Funktion ist aktiviert. Der Status wechselt zu, `enabled` sobald Amazon EC2 den ersten vorab bereitgestellten Snapshot für ein neu aktiviertes EC2 Fast Launch AMI erstellt. Wenn das AMI bereits aktiviert war und erneut die Vorabbereitstellung durchläuft, erfolgt die Statusänderung sofort.
- enabled-failed — Dieser Status gilt nur, wenn es nicht das erste Mal ist, dass Ihr EC2 Fast Launch AMI den Vorbereitstellungsprozess durchläuft. Dies kann passieren, wenn die EC2 Fast Launch-Funktion deaktiviert und später wieder aktiviert wird, oder wenn nach Abschluss der Vorbereitstellung zum ersten Mal eine Konfigurationsänderung oder ein anderer Fehler auftritt.
- Deaktivierung — Der AMI-Besitzer hat die EC2-Schnellstartfunktion für das AMI deaktiviert und Amazon EC2 hat den Bereinigungsprozess gestartet.
- deaktiviert — Die EC2 Fast Launch-Funktion ist deaktiviert. Der Status wechselt zu `disabled`, sobald Amazon EC2 den Bereinigungsprozess abgeschlossen hat.
- deaktivieren fehlgeschlagen – Es ist ein Fehler aufgetreten, der dazu geführt hat, dass der Bereinigungsprozess fehlschlug. Das bedeutet, dass einige vorab bereitgestellte Snapshots möglicherweise noch im Konto verbleiben.

Zustand TransitionReason

Der Grund, warum sich der Status für das EC2 Fast Launch AMI geändert hat.

> **Note**
>
> Alle Felder in dieser Ereignisnachricht sind erforderlich.

Das folgende Beispiel zeigt ein neu aktiviertes EC2 Fast Launch AMI, das die erste Instance gestartet hat, um den Pre-Provisioning-Prozess zu starten. Zu diesem Zeitpunkt ist der Status `enabling`. Nachdem Amazon EC2 den ersten vorab bereitgestellten Snapshot erstellt hat, ändert sich der Status zu `enabled`.

```
{
 "version": "0",
 "id": "01234567-0123-0123-0123-012345678901",
 "detail-type": "EC2 Fast Launch State-change Notification",
```

```
 "source": "aws.ec2",
 "account": "123456789012",
 "time": "2022-08-31T20:30:12Z",
 "region": "us-east-1",
 "resources": [
  "arn:aws:ec2:us-east-1:123456789012:image/ami-123456789012"
 ],
 "detail": {
  "imageId": "ami-123456789012",
  "resourceType": "snapshot",
  "state": "enabling",
  "stateTransitionReason": "Client.UserInitiated"
 }
}
```

Überwachen Sie EC2 Fast Launch-Metriken mit CloudWatch

Amazon EC2 EC2-AMIs mit aktiviertem EC2 Fast Launch senden Metriken an Amazon. CloudWatch Sie können die AWS Management Console, oder eine API verwenden AWS CLI, um die Metriken aufzulisten, an die EC2 Fast Launch sendet. CloudWatch Der `AWS/EC2` Namespace umfasst die folgenden EC2 Fast Launch-Metriken:

Metrik	Beschreibung
NumberOfAvailableFastLaunchSnapshots	Die Anzahl der vorab bereitgestellten Snapshots, die pro EC2 Fast Launch-ak tiviertem AMI verfügbar sind.
NumberOfInstancesFastGestartet	Die Anzahl der Instances pro AMI mit EC2 Fast Launch, die aus vorab bereitgestellten Snapshots gestartet wurden.
NumberOfInstancesNotFastLaunched	Die Anzahl der Instances pro EC2 Fast Launch aktiviertem AMI führte aufgrund des Fehlens verfügbarer vorab bereitgestellter Snapshots zum Startzeitpunkt zu einem Kaltstart.
FastLaunchSnapshotUsedToRefillStartTime	Der Zeitstempel, zu dem Amazon EC2 ein neues Image von einem EC2-Schnellstart aus startete, ermöglichte es AMI, einen weiteren

Metrik	Beschreibung
	Snapshot zu erstellen, nachdem ein vorhanden er Snapshot verwendet wurde.
FastLaunchSnapshotCreationZeit	Misst die Zeit, die Amazon EC2 benötigt hat, um eine Instance zu starten und einen Snapshot für ein EC2 Fast Launch-fähiges AMI zu erstellen.

Servicebezogene Rolle für EC2 Fast Launch

Amazon EC2 nutzt serviceverknüpfte Rollen für die Berechtigungen, die für den Aufruf anderer AWS-Services in Ihrem Namen benötigt werden. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit einer verknüpft ist. AWS-Service Dienstbezogene Rollen bieten eine sichere Möglichkeit, Berechtigungen zu delegieren, AWS-Services da nur der verknüpfte Dienst eine dienstbezogene Rolle übernehmen kann. Weitere Informationen zur Verwendung von IAM-Rollen – einschließlich serviceverknüpfter Rollen – durch Amazon EC2 finden Sie unter IAM-Rollen für Amazon EC2.

Amazon EC2 verwendet die serviceverknüpfte Rolle namens `AWSServiceRoleForEC2FastLaunch`, um eine Reihe von vorab bereitgestellten Snapshots zu erstellen und zu verwalten, die die Zeit für den Start von Instances über Ihr Windows-AMI reduzieren.

Sie müssen diese serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie EC2 Fast Launch für Ihr AMI verwenden, erstellt Amazon EC2 die serviceverknüpfte Rolle für Sie, sofern sie noch nicht existiert.

> **Note**
>
> Wenn die dienstverknüpfte Rolle aus Ihrem Konto gelöscht wird, können Sie EC2 Fast Launch für ein anderes Windows-AMI aktivieren, um die Rolle in Ihrem Konto neu zu erstellen. Alternativ können Sie EC2 Fast Launch für Ihr aktuelles AMI deaktivieren und dann wieder aktivieren. Das Deaktivieren des Features führt jedoch dazu, dass das AMI den Standardstartprozess für alle neuen Instances verwendet, während Amazon EC2 alle vorab bereitgestellten Snapshots entfernt. Nachdem alle vorab bereitgestellten Snapshots weg sind, können Sie die Verwendung von EC2 Fast Launch für Ihr AMI wieder aktivieren.

Amazon EC2 verhindert die Bearbeitung der serviceverknüpften Rolle `AWSServiceRoleForEC2FastLaunch`. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter Bearbeiten einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Sie können eine serviceverknüpfte Rolle nur löschen, nachdem Sie alle zugehörigen Ressourcen gelöscht haben. Dadurch werden die Amazon EC2-Ressourcen geschützt, die mit Ihrem Amazon EC2 Windows Server-AMI verknüpft sind, wenn EC2 Fast Launch aktiviert ist, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entziehen können.

Amazon EC2 unterstützt die serviceverknüpfte Rolle EC2 Fast Launch in allen Regionen, in denen der Amazon EC2-Service verfügbar ist. Weitere Informationen finden Sie unter Regionen.

Berechtigungen von**`AWSServiceRoleForEC2FastLaunch`**

Amazon EC2 verwendet die verwaltete Richtlinie `EC2FastLaunchServiceRolePolicy`, um die folgenden Aktionen auszuführen:

- `cloudwatch:PutMetricData`— Veröffentlichen Sie mit EC2 Fast Launch verknüpfte Metrikdaten im Amazon EC2 EC2-Namespace.
- `ec2:CreateLaunchTemplate`— Erstellen Sie eine Startvorlage für Ihr Amazon EC2 Windows Server-AMI mit aktiviertem EC2 Fast Launch.
- `ec2:CreateSnapshot`— Erstellen Sie vorab bereitgestellte Snapshots für Ihr Amazon EC2 Windows Server-AMI mit aktiviertem EC2 Fast Launch.
- `ec2:CreateTags`— Erstellen Sie Tags für Ressourcen, die mit dem Starten und der Vorbereitstellung von Windows-Instances für Ihr Amazon EC2 Windows Server-AMI mit aktiviertem EC2 Fast Launch verknüpft sind.
- `ec2:DeleteSnapshots`— Löschen Sie alle zugehörigen vorab bereitgestellten Snapshots, wenn EC2 Fast Launch für ein zuvor aktiviertes AMI deaktiviert ist.
- `ec2:DescribeImages`: Beschreiben von Images für alle Ressourcen
- `ec2:DescribeInstanceAttribute`: Beschreiben von Instance-Attributen für alle Ressourcen
- `ec2:DescribeInstanceStatus`: Beschreiben von Instance-Status für alle Ressourcen
- `ec2:DescribeInstances`: Beschreiben von Instances für alle Ressourcen
- `ec2:DescribeInstanceTypeOfferings`: Beschreiben von Instance-Typ-Angeboten für alle Ressourcen

- `ec2:DescribeLaunchTemplates`: Beschreiben von Startvorlagen für alle Ressourcen
- `ec2:DescribeLaunchTemplateVersions`: Beschreiben von Startvorlagenversionen für alle Ressourcen
- `ec2:DescribeSnapshots`: Beschreiben von Snapshot-Ressourcen für alle Ressourcen
- `ec2:DescribeSubnets`: Beschreiben von Subnetzen für alle Ressourcen
- `ec2:RunInstances`— Starten Sie Instances von einem Amazon EC2 Windows Server-AMI mit aktiviertem EC2 Fast Launch, um Bereitstellungsschritte durchzuführen.
- `ec2:StopInstances`— Stoppen Sie Instances, die von einem Amazon EC2 Windows Server-AMI mit aktiviertem EC2 Fast Launch gestartet wurden, um vorab bereitgestellte Snapshots zu erstellen.
- `ec2:TerminateInstances`— Beenden Sie eine Instance, die von einem Amazon EC2 Windows Server-AMI mit aktiviertem EC2 Fast Launch gestartet wurde, nachdem Sie den vorab bereitgestellten Snapshot daraus erstellt haben.
- `iam:PassRole`: Ermöglicht der serviceverknüpften Rolle `AWSServiceRoleForEC2FastLaunch` das Starten von Instances in Ihrem Namen unter Verwendung des Instance-Profils aus Ihrer Startvorlage

Weitere Informationen zur Verwendung verwalteter Richtlinien für Amazon EC2 finden Sie unter AWS verwaltete Richtlinien für Amazon EC2.

Gewähren von Zugriff auf von Kunden verwaltete Schlüssel zur Verwendung mit verschlüsselten AMIs und EBS-Snapshots

Voraussetzung

- Damit Amazon EC2 in Ihrem Namen auf ein verschlüsseltes AMI zugreifen kann, müssen Sie über die Berechtigung für die `createGrant`-Aktion im vom Kunden verwalteten Schlüssel verfügen.

Wenn Sie EC2 Fast Launch für ein verschlüsseltes AMI aktivieren, stellt Amazon EC2 sicher, dass der `AWSServiceRoleForEC2FastLaunch` Rolle die Erlaubnis erteilt wird, den vom Kunden verwalteten Schlüssel für den Zugriff auf Ihr AMI zu verwenden. Diese Berechtigung ist erforderlich, um Instances zu starten und in Ihrem Namen vorab bereitgestellte Snapshots zu erstellen.

Verwenden Sie Amazon Elastic Graphics-Beschleuniger auf Windows-Instances

> **Important**
>
> Amazon Elastic Graphics hat am 8. Januar 2024 das Lebensende erreicht. Für Workloads, die Grafikbeschleunigung erfordern, empfehlen wir die Verwendung von Amazon EC2 G4ad-, G4dn- oder G5-Instances.

Amazon Elastic Graphics bietet flexible, kostengünstige und leistungsstarke Grafikbeschleunigung für Ihre Windows-Instances. Elastic Graphics Accelerators sind in verschiedenen Größen erhältlich und stellen eine kostengünstige Alternative zur Verwendung von GPU-Grafik-Instance-Typen (wie G3) dar. Sie haben die Möglichkeit, einen Instance-Typ auszuwählen, der die Anforderungen Ihrer Anwendung an Rechenleistung, Arbeitsspeicher und Speicherplatz erfüllt. Wählen Sie dann den Accelerator für Ihre Instance aus, der den Grafikanforderungen Ihres Workloads entspricht.

Elastic Graphics ist für Anwendungen geeignet, die eine kleine oder wechselnde Menge an zusätzlicher Grafikbeschleunigung benötigen und die die OpenGL-Grafikunterstützung verwenden. Wenn Sie den Zugriff auf vollständige, direkt angefügte GPUs benötigen und die Parallelcomputingframeworks DirectX, CUDA oder Open Computing Language (OpenCL) verwenden, verwenden Sie stattdessen eine Instance des beschleunigten Computing-Typs.

Inhalt

Elastic Graphics-Grundlagen

Um Elastic Graphics zu verwenden, starten Sie eine Windows-Instance und geben Sie beim Start einen Beschleunigertyp für die Instance an. AWS findet verfügbare Elastic Graphics-Kapazität und stellt eine Netzwerkverbindung zwischen Ihrer Instance und dem Elastic Graphics Accelerator her.

> **Note**
>
> Bare Metal-Instances werden nicht unterstützt.

Elastic Graphics-Beschleuniger sind in den folgenden AWS Regionen verfügbar: `us-east-1`us-east-2,`us-west-2`,`ap-northeast-1`,`ap-southeast-1`, `ap-southeast-2`eu-central-1, undeu-west-1.

Die folgenden Instance-Typen unterstützen Elastic Graphics-Accelerators.

- Universeller Zweck: M3, M4, M5, M5d, M5dn, M5n, T2, T3

  > **Note**
  >
  > Nur `t2.medium` und größer, sowie `t3.medium` und größer werden unterstützt.

- Für Rechenleistung optimiert: C3, C4, C5, C5a, C5ad, C5d, C5n
- Arbeitsspeicheroptimiert: R3, R4, R5, R5d, R5dn, R5n, X1, X1e, z1d
- Speicheroptimiert: D2, D3, D3en, H1, I3, I3en
- Beschleunigte Datenverarbeitung: P2, P3, P3dn

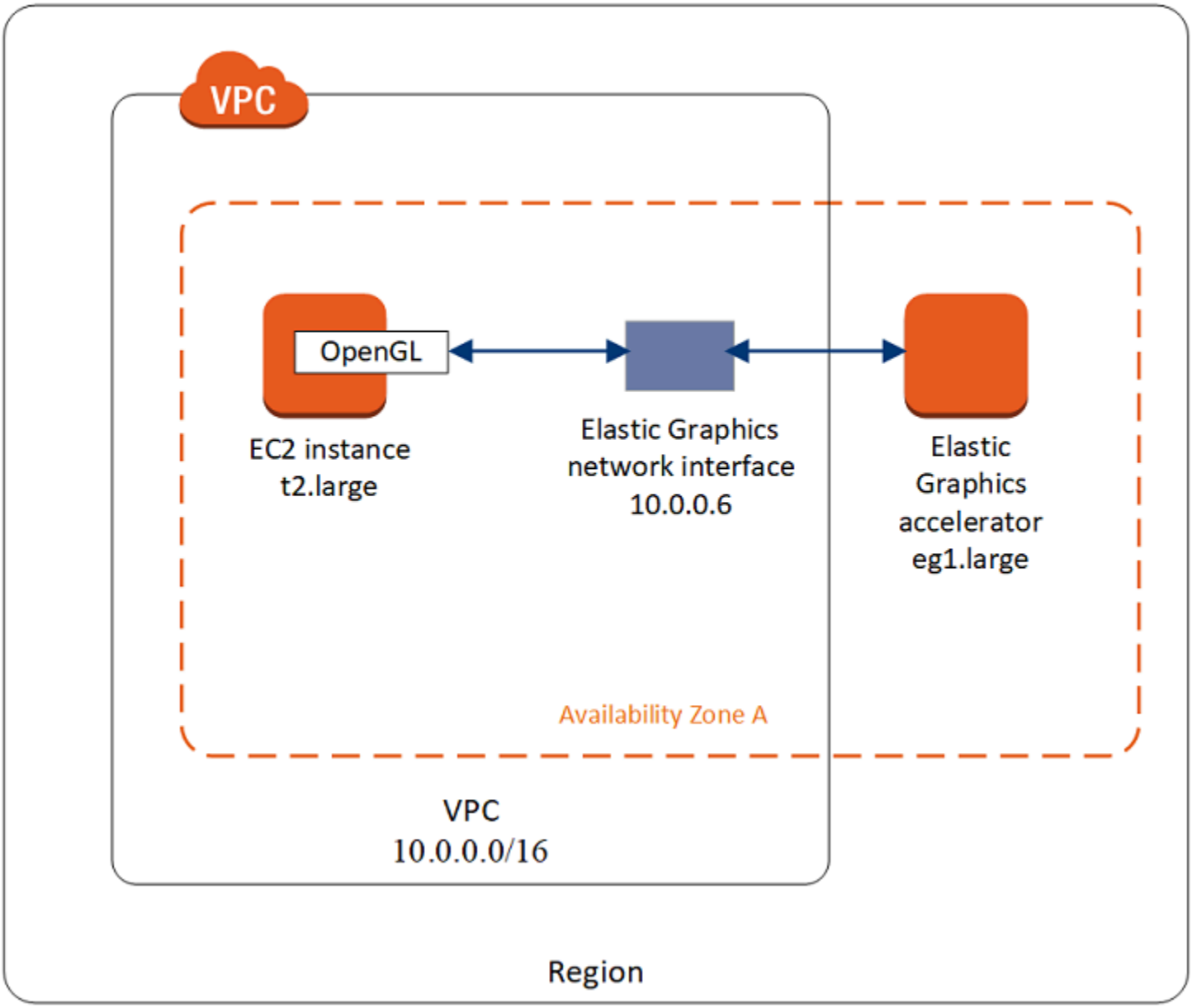
Die folgenden Elastic Graphics-Accelerators sind verfügbar. Sie können jeden beliebigen Elastic Graphics-Accelerator an jeden beliebigen unterstützten Instance-Typ anfügen.

Elastic Graphics Accelerator	Grafikspeicher (GB)
`eg1.medium`	1
`eg1.large`	2
`eg1.xlarge`	4

Elastic Graphics Accelerator	Grafikspeicher (GB)
`eg1.2xlarge`	8

Ein Elastic Graphics-Accelerator ist nicht Teil der Hardware Ihrer Instance. Stattdessen wird er über eine Netzwerkschnittstelle, die sogenannte Elastic Graphics-Netzwerkschnittstelle, an das Netzwerk angefügt. Wenn Sie eine Instance mit Grafikbeschleunigung starten oder neu starten, wird diese Elastic Graphics-Netzwerkschnittstelle in Ihrer VPC für Sie erstellt.

Die Elastic Graphics-Netzwerkschnittstelle wird im selben Subnetz und derselben VPC wie Ihre Instance erstellt und erhält von diesem Subnetz eine private IPv4-Adresse. Der mit Ihrer Amazon EC2-Instance verbundene Accelerator wird aus einem Pool verfügbarer Accelerators in derselben Availability Zone wie Ihre Instance zugewiesen.



Elastic Graphics-Accelerators unterstützen die API-Standards für OpenGL 4.3 API und frühere Versionen, die für Batch-Anwendungen oder die 3D-Grafikbeschleunigung verwendet werden können. Eine Amazon-optimierte OpenGL-Bibliothek auf Ihrer Instance erkennt den verbundenen Accelerator. Sie leitet OpenGL-API-Aufrufe von Ihrer Instance zum Accelerator, der dann die Anfragen verarbeitet und die Ergebnisse zurück gibt. Der Datenverkehr zwischen der Instance und dem Accelerator verwendet die gleiche Bandbreite wie der Netzwerkdatenverkehr der Instance. Sie sollten daher ausreichend Bandbreite zur Verfügung haben. Wenden Sie sich mit Fragen zur OpenGL-Compliance oder zu Versionen an Ihren Softwareanbieter.

Standardmäßig wird die Standardsicherheitsgruppe für Ihre VPC mit der Elastic Graphics-Netzwerkschnittstelle verbunden. Der Elastic Graphics-Netzwerkdatenverkehr verwendet das TCP-Protokoll und Port 2007. Stellen Sie sicher, dass die Sicherheitsgruppe für Ihre Instance dies zulässt. Weitere Informationen finden Sie unter Konfigurieren Ihrer Sicherheitsgruppen für.

Preise für Elastic Graphics

Sie zahlen für jede Sekunde, die ein Elastic Graphics-Accelerator mit einer Instance im Status `running` verbunden ist, wenn sich der Accelerator im Status `Ok` befindet. Sie zahlen nicht für einen Accelerator, der mit einer Instance im Status `pending`, `stopping`, `stopped`, `shutting-down` oder `terminated` verbunden ist. Sie zahlen auch nicht, wenn sich ein Accelerator im Status `Unknown` oder `Impaired` befindet.

Die Preise für Accelerators sind nur zu On-Demand-Tarifen verfügbar. Sie können einen Accelerator an eine Reserved Instance oder eine Spot-Instance anfügen. Der On-Demand-Preis gilt jedoch für den Accelerator.

Weitere Informationen finden Sie unter Amazon Elastic Graphics-Preise.

Elastic Graphics-Einschränkungen

Berücksichtigen Sie die folgenden Einschränkungen, bevor Sie Elastic Graphics-Accelerators verwenden:

- Sie können Accelerators nur mit Microsoft Windows Server 2012 R2 oder später an Windows-Instances anfügen. Linux-Instances werden derzeit nicht unterstützt.
- Sie können jeweils einen Accelerator an eine Instance anfügen.
- Sie können einen Accelerator nur während des Starts der Instance anfügen. Ein Accelerator kann nicht an eine vorhandene Instance angefügt werden.
- Sie können eine Instance mit angefügtem Accelerator nicht in den Ruhezustand versetzen.
- Accelerators können nicht von mehreren Instances verwendet werden.
- Sie können einen Accelerator nicht von einer Instance trennen oder auf eine andere Instance übertragen. Wenn Sie einen Accelerator nicht mehr benötigen, müssen Sie Ihre Instance beenden. Wenn Sie den Accelerator-Typ ändern möchten, erstellen Sie ein AMI von Ihrer Instance, beenden Sie die Instance und starten Sie eine neue Instance mit einer anderen Accelerator-Spezifikation.
- Es werden nur Versionen der OpenGL-API bis einschließlich 4.3 unterstützt. DirectX, CUDA und OpenCL werden nicht unterstützt.

- Der Elastic Graphics-Accelerator ist nicht über den Gerätemanager Ihrer Instance sichtbar oder zugänglich.
- Sie können Accelerator-Kapazität nicht reservieren oder planen.

Arbeiten mit Elastic Graphics

> **Important**
>
> Amazon Elastic Graphics hat am 8. Januar 2024 das Lebensende erreicht. Für Workloads, die Grafikbeschleunigung erfordern, empfehlen wir die Verwendung von Amazon EC2 G4ad-, G4dn- oder G5-Instances.

Sie können eine Instance starten und während des Starts einen Elastic Graphics-Accelerator damit verbinden. Anschließend müssen Sie auf Ihrer Instance manuell die erforderlichen Bibliotheken installieren, die die Kommunikation mit dem Accelerator ermöglichen. Einschränkungen finden Sie unter Elastic Graphics-Einschränkungen.

Aufgaben

- Konfigurieren Ihrer Sicherheitsgruppen für
- Starten einer Instance mit einem Elastic Graphics-Accelerator
- Installieren der erforderlichen Software für Elastic Graphics
- Prüfen der Elastic Graphics-Funktionalität auf Ihrer Instance
- Anzeigen der Informationen Elastic Graphics
- Einreichen von Feedback

Konfigurieren Ihrer Sicherheitsgruppen für

Elastic Graphics erfordert eine selbstbezügliche Sicherheitsgruppe, die allen ein- und ausgehenden Datenverkehr von und zur Sicherheitsgruppe zulässt. Die Sicherheitsgruppe muss die folgenden Regeln in Bezug auf eingehenden und ausgehenden Datenverkehr enthalten.

Eingehend

Typ	Protokoll	Port	Quelle
Elastic Graphics	TCP	2007	Die Sicherheitsgruppen-ID (ihre eigene Ressourcen-ID)

Ausgehend

Typ	Protocol (Protokoll)	Port-Bereich	Bestimmungsort
Elastic Graphics	TCP	2007	Die Sicherheitsgruppen-ID (ihre eigene Ressourcen-ID)

Wenn Sie die Amazon EC2 Konsole verwenden, um Ihre Instance mit einem Elastic Graphics-Accelerator zu starten, können Sie entweder dem Startinstance-Assistenten erlauben, die erforderlichen Sicherheitsgruppenregeln automatisch zu erstellen oder Sie können eine Sicherheitsgruppe auswählen, die Sie zuvor erstellt haben.

Wenn Sie Ihre Instance mit dem AWS CLI oder einem SDK starten, müssen Sie eine Sicherheitsgruppe angeben, die Sie zuvor erstellt haben.

So erstellen Sie eine Sicherheitsgruppe für Elastic Graphics

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) und anschließend Create Security Group (Sicherheitsgruppe erstellen) aus.
3. Führen Sie im Fenster Create Security Group Folgendes aus:

    a. Geben Sie für Security group name (Name der Sicherheitsgruppe) einen beschreibenden Namen für die Sicherheitsgruppe ein, wie etwa `Elastic Graphics security group`.

    b. (Optional:) Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Sicherheitsgruppe ein.

    c. Für VPC wählen Sie die VPC aus, in die Sie Elastic Graphics verwenden möchten.

    d. Wählen Sie Sicherheitsgruppe erstellen aus.

4. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus, wählen Sie die Sicherheitsgruppe, die Sie gerade erstellt haben, und kopieren Sie dann auf der Registerkarte Details die Sicherheitsgruppen-ID.
5. Wählen Sie auf der Registerkarte Inbound Rules (Regeln für eingehenden Datenverkehr) die Option Edit Inbound Rules (Regeln für eingehenden Datenverkehr bearbeiten) aus und gehen Sie wie folgt vor:

   a. Wählen Sie Regel hinzufügen aus.
   b. Wählen Sie für Typ die Option Elastic Graphics aus.
   c. Wählen Sie für den Source type (Quelltyp) die Option Custom (Benutzerdefiniert).
   d. Für Source fügen Sie die Sicherheitsgruppen-ID, die Sie zuvor kopiert haben, ein.
   e. Wählen Sie Save rules (Regeln speichern) aus.
6. Wählen Sie auf der Registerkarte Outbound Rules (Regeln für ausgehenden Datenverkehr) Edit Outbound Rules (Regeln für ausgehenden Datenverkehr bearbeiten) und gehen Sie wie folgt vor:

   a. Wählen Sie Regel hinzufügen aus.
   b. Wählen Sie für Typ die Option Elastic Graphics aus.
   c. Für Zieltyp wählen Sie Benutzerdefiniert aus.
   d. Für Ziel fügen Sie die Sicherheitsgruppen-ID, die Sie zuvor kopiert haben, ein.
   e. Wählen Sie Save rules (Regeln speichern) aus.

Weitere Informationen finden Sie unter Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances.

Starten einer Instance mit einem Elastic Graphics-Accelerator

Sie können während des Starts einen Elastic Graphics-Accelerator einer Instance zuweisen. Wenn der Start fehlschlägt, kommen folgende Ursachen dafür in Frage:

- Unzureichende Elastic Graphics-Accelerator-Kapazität
- Überschreitung der Grenzwerte für Elastic Graphics-Accelerators in der Region
- Unzureichende Zahl privater IPv4-Adressen in Ihrer VPC zur Erstellung einer Netzwerkschnittstelle für den Accelerator

Weitere Informationen finden Sie unter Elastic Graphics-Einschränkungen.

So weisen Sie während des Starts einer Instance (Konsole) einen Elastic Graphics-Accelerator zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard Launch Instance aus.
3. Geben Sie unter Name und Tags einen Wert für Name ein. Sie können optional Zusätzliche Tags hinzufügen wählen, um weitere Tags zu Ressourcen hinzuzufügen, die mit der Instance verknüpft sind, die Sie starten.
4. Wählen Sie unter Anwendungs- und Betriebssystemimages (Amazon Machine Image) ein Windows-AMI aus.
5. Wählen Sie unter Instance type (Instance-Typ) einen unterstützten Instance-Typ aus. Weitere Informationen finden Sie unter Elastic Graphics-Grundlagen.
6. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
7. Wählen Sie neben Netzwerkeinstellungen die Option Bearbeiten und geben Sie dann die Netzwerkeinstellungen an, die für Ihre Instance verwendet werden sollen.

   a. Wählen Sie unter Netzwerk eine VPC für Ihre Instance aus.
   b. Wählen Sie unter Subnetz ein Subnetz aus, in dem Sie Ihre Instance starten möchten.
   c. Für Firewall (Sicherheitsgruppen) können Sie die Sicherheitsgruppe verwenden, in der Sie manuell erstellt habenKonfigurieren Ihrer Sicherheitsgruppen für, oder die Konsole eine Sicherheitsgruppe mit den erforderlichen Regeln für eingehenden und ausgehenden Datenverkehr für Sie erstellen lassen. Fügen Sie nach Bedarf zusätzliche Sicherheitsgruppen hinzu.
8. (Optional) Konfigurieren Sie unter Speicher konfigurieren die Größe Ihres Root-Volumes und fügen Sie bei Bedarf weitere Volumes hinzu.
9. Erweitern Sie den Abschnitt Erweiterte Details.
10. Wählen Sie unter Erweiterte Details für Elastic GPU einen Elastic Graphics-Beschleunigertyp aus.
11. Wählen Sie in der Übersicht Launch instance (Instance starten) aus.

Zuweisen Sie eines Elastic Graphics-Accelerator beim Start einer Instance (AWS CLI)

Sie können den AWS CLI Befehl run-instances mit dem folgenden Parameter verwenden:

```
--elastic-gpu-specification Type=eg1.medium
```

Für den Parameter `--security-group-ids` müssen Sie eine Sicherheitsgruppe hinzufügen, die über die erforderlichen Regeln für ein- und ausgehenden Datenverkehr verfügt. Weitere Informationen finden Sie unter Konfigurieren Ihrer Sicherheitsgruppen für.

Um beim Start einer Instanz einen Elastic Graphics Accelerator zuzuordnen (Tools für Windows) PowerShell

Verwenden Sie den PowerShell Befehl New-EC2InstanceTools für Windows.

Installieren der erforderlichen Software für Elastic Graphics

Wenn Sie Ihre Instance mit einem aktuellen AWS Windows-AMI gestartet haben, wird die erforderliche Software beim ersten Start automatisch installiert. Wenn Sie Ihre Instance mit Windows-AMIs gestartet haben, bei denen die erforderliche Software nicht automatisch installiert wird, müssen Sie die erforderliche Software manuell auf der Instance installieren.

So installieren Sie die erforderliche Software für Elastic Graphics (falls erforderlich)

1. Stellen Sie eine Verbindung mit der Instance her.
2. Laden Sie das Installationsprogramm Elastic Graphics herunter und öffnen Sie es. Der Installationsmanager verbindet sich mit dem Elastic Graphics-Endpunkt und lädt die jeweils neueste Version der erforderlichen Software herunter.

   > **Note**
   >
   > Wenn der Download-Link nicht funktioniert, versuchen Sie es mit einem anderen Browser oder kopieren Sie die Linkadresse und fügen Sie sie in eine neue Browser-Registerkarte ein.

3. Starten Sie zur Prüfung die Instance erneut.

Prüfen der Elastic Graphics-Funktionalität auf Ihrer Instance

Die Elastic Graphics-Pakete auf Ihrer Instance enthalten Tools, mit denen Sie den Status des Accelerators anzeigen und prüfen können, ob die OpenGL-Befehle von Ihrer Instance zu dem Accelerator funktionieren.

Wenn Ihre Instance mit einem AMI ohne Vorinstallation der Elastic Graphics-Pakete gestartet wurde, können Sie diese selbst herunterladen und installieren. Weitere Informationen finden Sie unter Installieren der erforderlichen Software für Elastic Graphics.

Sie können die Elastic-Graphics-Funktionalität auf Ihrer Instance mit einer der folgenden Methoden überprüfen.

> **Note**
>
> Wenn der Statusmonitor oder das Befehlszeilen-Tool von Elastic Graphics ein unerwartetes Ergebnis zurückgibt, lesen Sie unter Beheben von Problemen mit fehlerhaftem Status nach.

Elastic Graphics status monitor

Mit dem Statusmonitortool können Sie Informationen zum Status eines angefügten Elastic Graphics-Accelerators anzeigen. Standardmäßig ist dieses Tool im Benachrichtigungsbereich der Taskleiste in Ihrer Windows-Instance verfügbar und zeigt den Status des Grafik-Accelerators an. Die folgenden Werte sind möglich:

Fehlerfrei

Der Elastic Graphics-Accelerator ist aktiviert und funktioniert korrekt.

Wird aktualisiert

Der Status des Elastic Graphics-Accelerators wird derzeit aktualisiert. Es kann einige Minuten dauern, bis der Status angezeigt wird.

Außer Betrieb

Der Elastic Graphics-Accelerator ist nicht in Betrieb. Um weitere Informationen zu dem Fehler anzuzeigen, gehen Sie zu Weitere Informationen.

Elastic Graphics command line tool

Sie können das Elastic Graphics-Befehlszeilentool, `egcli.exe`, zur Prüfung des Status des Accelerators verwenden. Gibt es ein Problem mit dem Accelerator, gibt das Tool einen Fehlercode zurück.

Öffnen Sie zum Starten des Tools eine Befehlszeile aus Ihrer Instance heraus und führen Sie folgenden Befehl aus:

```
C:\Program Files\Amazon\EC2ElasticGPUs\manager\egcli.exe
```

Das Tool unterstützt auch die folgenden Parameter:

`--json`, `-j`

Gibt an, ob die JSON-Meldung angezeigt werden soll. Die möglichen Werte sind `true` und `false`. Der Standardwert ist `true`.

`--imds`, `-i`

Gibt an, ob die Metadaten der Instance auf die Verfügbarkeit des Accelerators hin geprüft werden sollen. Die möglichen Werte sind `true` und `false`. Der Standardwert ist `true`.

Es folgt eine Beispielausgabe. Der Status `OK` zeigt an, dass der Accelerator aktiviert ist und korrekt funktioniert.

```
EG Infrastructure is available.
Instance ID egpu-f6d94dfa66df4883b284e96db7397ee6
Instance Type eg1.large
EG Version 1.0.0.885 (Manager) / 1.0.0.95 (OpenGL Library) / 1.0.0.69 (OpenGL
 Redirector)
EG Status: Healthy
JSON Message:
{
  "version": "2016-11-30",
  "status": "OK"
}
```

Folgende Werte sind für möglic `status`:

`OK`

Der Elastic Graphics-Accelerator ist aktiviert und funktioniert korrekt.

`UPDATING`

Der Elastic Graphics-Treiber wird aktualisiert.

`NEEDS_REBOOT`

Der Elastic Graphics-Treiber wurde aktualisiert und es ist ein Neustart der Amazon EC2-Instance erforderlich.

`LOADING_DRIVER`

Der Elastic Graphics-Treiber wird geladen.

`CONNECTING_EGPU`

Der Elastic Graphics-Treiber überprüft derzeit die Konnektivität mit dem Elastic Graphics-Accelerator.

`ERROR_UPDATE_RETRY`

Beim Aktualisieren des Elastic Graphics-Treibers ist ein Fehler aufgetreten. Ein neuer Aktualisierungsversuch erfolgt in Kürze.

`ERROR_UPDATE`

Beim Versuch, den Elastic Graphics-Treiber zu aktualisieren, ist ein nicht zu behebender Fehler aufgetreten.

`ERROR_LOAD_DRIVER`

Beim Laden des Elastic Graphics-Treibers ist ein Fehler aufgetreten.

`ERROR_EGPU_CONNECTIVITY`

Der Elastic Graphics-Accelerator ist nicht verfügbar.

Anzeigen der Informationen Elastic Graphics

Sie können Informationen zu dem Elastic Graphics-Accelerator anzeigen, der mit Ihrer Instance verknüpft ist.

So zeigen Sie Informationen zu einem Elastic Graphics-Accelerator (Konsole) an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Suchen Sie auf der Registerkarte Details nach Elastic Graphics ID. Wählen Sie die ID aus, um folgende Informationen über den Elastic Graphics-Accelerator anzuzeigen:

   - Anfügestatus
   - Typ
   - Gesundheitsstatus

Anzeigen von Informationen zu einem Elastic Graphics-Accelerator (AWS CLI)

Sie können den Befehl describe-elastic-gpus AWS CLI verwenden:

```
aws ec2 describe-elastic-gpus
```

Sie können den AWS CLI Befehl describe-network-interfaces verwenden und nach der Besitzer-ID filtern, um Informationen über die Elastic Graphics-Netzwerkschnittstelle anzuzeigen.

```
aws ec2 describe-network-interfaces --filters "Name=attachment.instance-owner-
id,Values=amazon-elasticgpus"
```

Um Informationen über einen Elastic Graphics Accelerator anzuzeigen (Tools für Windows) PowerShell

Verwenden Sie die folgenden Befehle:

- Get-EC2ElasticGpu
- Get-EC2NetworkInterface

So zeigen Sie Informationen zu einem Elastic Graphics-Accelerator mithilfe der Instance-Metadaten an

1. Erstellen Sie eine Verbindung zu der Windows-Instance, die einen Elastic Graphics-Accelerator verwendet.
2. Führen Sie eine der folgenden Aktionen aus:
   - Verwenden Sie von aus PowerShell das folgende Cmdlet:

     ```
     PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/elastic-
     gpus/associations/egpu-f6d94dfa66df4883b284e96db7397ee6
     ```

   - Geben Sie in Ihrem Web-Browser folgende URL in das Adressfeld ein:

     ```
     http://169.254.169.254/latest/meta-data/elastic-gpus/associations/egpu-
     f6d94dfa66df4883b284e96db7397ee6
     ```

Einreichen von Feedback

Sie können Feedback zu Ihren Erfahrungen mit Elastic Graphics übermitteln, damit das Team weitere Verbesserungen entwickeln kann.

So übermitteln Sie Feedback mit dem Elastic Graphics-Statusmonitor

1. Öffnen Sie im Benachrichtigungsbereich der Taskleiste in Ihrer Windows-Instance den Elastic Graphics-Statusmonitor.
2. Wählen Sie unten links Feedback aus.
3. Geben Sie Ihr Feedback ein, und wählen Sie Submit.

Elastic-Graphics-Verwaltung

> **Important**
>
> Amazon Elastic Graphics hat am 8. Januar 2024 das Lebensende erreicht. Für Workloads, die Grafikbeschleunigung erfordern, empfehlen wir die Verwendung von Amazon EC2 G4ad-, G4dn- oder G5-Instances.

AWS könnte in folgenden Fällen feststellen, dass sich ein Elastic Graphics-Beschleuniger in einem fehlerhaften Zustand befindet:

- ein Sicherheits- oder Infrastrukturupdate erforderlich ist
- ein Softwareupdate erforderlich ist
- ein Problem mit dem zugrunde liegenden Host vorliegt

Wenn AWS festgestellt wird, dass sich ein Elastic Graphics-Beschleuniger in einem fehlerhaften Zustand befindet, wird der Beschleuniger außer Betrieb genommen. AWS informiert Sie über die bevorstehende Außerbetriebnahme des Accelerators und informiert Sie über die erforderlichen Abhilfemaßnahmen.

Themen

Wie werde ich benachrichtigt?

Wenn die AWS Außerbetriebnahme eines Elastic Graphics Accelerators geplant ist, sendet dieser eine Mitteilung über die Außerbetriebnahme des Accelerators an Sie. AWS Health Dashboard AWS sendet außerdem eine E-Mail an die E-Mail-Adresse, die mit Ihrem AWS Konto verknüpft ist. Das ist dieselbe E-Mail-Adresse, mit der Sie sich bei der AWS Management Console anmelden.

> **Note**
>
> Wenn Sie ein E-Mail-Konto verwenden, das Sie nicht regelmäßig überprüfen, können Sie anhand des feststellen, ob einer Ihrer Elastic Graphics Accelerators eingestellt werden soll. AWS Health Dashboard Sie können die Kontaktinformationen für Ihr AWS Konto auch auf der Seite mit den Kontoeinstellungen ändern.

Die Benachrichtung zur Außerbetriebnahme umfasst Folgendes:

- Die ID der Instance, mit der der Accelerator verbunden ist
- Informationen über das Problem, von dem der Accelerator betroffen ist
- Das Datum der Außerbetriebnahme des Accelerators
- Die erforderlichen Korrekturmaßnahmen

Was muss ich tun?

Wenn Sie darüber informiert werden, dass für Ihren Elastic Graphics Accelerator eine Außerbetriebnahme geplant wurde, müssen Sie die mit dem Accelerator verbundene Instance anhalten und starten, damit der alte, fehlerhafte Accelerator durch einen neuen, fehlerfreien Accelerator ersetzt werden kann.

Wir empfehlen Ihnen, auf der Instance ausgeführte Grafikanwendungen zu schließen, bevor Sie die Instance anhalten und neu starten.

> **Important**
>
> Wenn Sie Ihre Instance nicht vor dem Datum der geplanten Außerbetriebnahme anhalten und starten, wird der mit Ihrer Instance verbundene Accelerator automatisch angehalten. Das kann dazu führen, dass Ihre Anwendungen nicht mehr funktionieren.

Sie müssen die Instance anhalten und starten. Ein Neustart der Instance ersetzt den fehlerhaften Accelerator nicht durch einen fehlerfreien Accelerator.

Was passiert am Datum der Außerbetriebnahme des Accelerators?

Wenn ein fehlerhafter Elastic Graphics Accelerator sein geplantes Auslaufdatum erreicht, wird er AWS dauerhaft beendet. Um einen Ersatz für Ihren fehlerhaften Accelerator zu erhalten (vor oder nach dem Datum der Außerbetriebnahme), müssen Sie die mit dem Accelerator verbundene Instance anhalten und starten.

Wenn Sie Ihre Instance nicht vor dem Datum der geplanten Außerbetriebnahme anhalten und starten, wird der mit Ihrer Instance verbundene Accelerator automatisch angehalten. Das kann dazu führen, dass Ihre Anwendungen nicht mehr funktionieren.

Verwenden Sie CloudWatch Metriken, um Elastic Graphics zu überwachen

Important

Amazon Elastic Graphics hat am 8. Januar 2024 das Lebensende erreicht. Für Workloads, die Grafikbeschleunigung erfordern, empfehlen wir die Verwendung von Amazon EC2 G4ad-, G4dn- oder G5-Instances.

Sie können Ihren Elastic Graphics Accelerator mithilfe von Amazon überwachen CloudWatch, das Messwerte über die Leistung Ihres Accelerators sammelt. Diese Statistiken werden für einen Zeitraum von zwei Wochen aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihr Service ausgeführt wird.

Standardmäßig senden Elastic Graphics-Beschleuniger Metrikdaten innerhalb von 5 Minuten CloudWatch an.

Weitere Informationen zu Amazon CloudWatch finden Sie im CloudWatch Amazon-Benutzerhandbuch.

Elastic Graphics-Metriken

Der `AWS/ElasticGPUs`-Namespace enthält die folgenden Metriken für Elastic Graphics.

Metrik	Beschreibung
GPU ConnectivityCheck ausgefallen	Meldet, ob die Verbindung zu dem Elastic Graphics-Accelerator aktiv ist oder fehlschlug. Der Wert Null (0) zeigt an, dass die Verbindung aktiv ist. Der Wert (1) zeigt einen Verbindungsfehlschlag an. Einheiten: Anzahl
GPU HealthCheck ausgefallen	Meldet, ob der Elastic Graphics-Accelerator in der vergangenen Minute einer Statusprüfung unterzogen wurde. Der Wert Null (0) gibt an, dass die Statusprüfung bestanden wurde. Der Wert (1) zeigt den Fehlschlag einer Statusprüfung an. Einheiten: Anzahl
GPU MemoryUtilization	Der verwendete GPU-Speicher. Einheiten: MiB

Elastic Graphics-Dimensionen

Sie können die Metrikdaten für Ihre Elastic Graphics-Accelerators mithilfe der folgenden Dimensionen filtern.

Dimension	Beschreibung
`EGPUId`	Filtert die Daten nach dem Elastic Graphics-Accelerator.
`InstanceId`	Filtert die Daten nach der Instance, mit der der Elastic Graphics-Accelerator verbunden ist.

CloudWatch Metriken für Elastic Graphics anzeigen

Metriken werden zuerst nach dem Service-Namespace und dann nach den unterstützten Dimensionen gruppiert. Sie können die folgenden Vorgehensweisen nutzen, um die Metriken für Ihre Elastic Graphics-Accelerators anzuzeigen.

Um Elastic Graphics-Metriken mit der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Ändern Sie, falls erforderlich, die Region. Wählen Sie auf der Navigationsleiste die Region aus, in der sich Ihr Elastic Graphics-Accelerator befindet. Weitere Informationen finden Sie unter - Regionen und Endpunkte.
3. Wählen Sie im Navigationsbereich Metrics aus.
4. Wählen Sie für All metrics (Alle Metriken) Elastic Graphics und Elastic Graphics Metrics (Elastic Graphics-Metriken) aus.

Anzeigen von Elastic Graphics-Metriken (AWS CLI)

Verwenden Sie den folgenden list-metrics-Befehl:

```
aws cloudwatch list-metrics --namespace "AWS/ElasticGPUs"
```

Erstellen Sie CloudWatch Alarme zur Überwachung von Elastic Graphics

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum und sendet eine Benachrichtigung an ein Amazon SNS-Thema, die vom Wert der Metrik im Verhältnis zu einem vorgegebenen Schwellenwert in einer Reihe von Zeiträumen abhängt.

Sie können beispielsweise einen Alarm erstellen, der den Zustand eines Elastic Graphics-Accelerators überwacht und eine Benachrichtigung sendet, wenn der Grafik-Accelerator in drei aufeinander folgenden 5-Minuten-Zeiträumen eine Statusprüfung nicht besteht.

So erstellen Sie einen Alarm für den Zustand eines Elastic Graphics-Accelerators

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Alarms und Create Alarm aus.
3. Wählen Sie für Select metrics (Metriken auswählen) Elastic Graphics und Elastic Graphics Metrics (Elastic Graphics-Metriken) aus.
4. Wählen Sie die Metrik GPU HealthCheck Failed aus und wählen Sie Metrik auswählen aus.
5. Konfigurieren Sie den Alarm wie folgt:

a. Geben Sie unter Alarm details (Alarmdetails) einen Namen und eine Beschreibung für Ihren Alarm ein. Wählen Sie für Whenever (Immer wenn) >= aus und geben Sie 1 ein.

b. Wählen Sie unter Aktionen eine vorhandene Benachrichtigungsliste oder die Option New list (Neue Liste) aus.

c. Wählen Sie Create Alarm aus.

Fehlerbehebung

> **Important**
>
> Amazon Elastic Graphics hat am 8. Januar 2024 das Lebensende erreicht. Für Workloads, die Grafikbeschleunigung erfordern, empfehlen wir die Verwendung von Amazon EC2 G4ad-, G4dn- oder G5-Instances.

Im Folgenden werden häufig auftretende Fehler und die entsprechenden Schritte zur Fehlerbehebung beschrieben.

Inhalt

Untersuchung von Problemen mit der Anwendungsleistung

Elastic Graphics verwendet das Instance-Netzwerk zum Senden von OpenGL-Befehlen an eine remote verbundene Grafikkarte. Dazu wird auf ein Desktop mit einer OpenGL-Anwendung mit einem Elastic Graphics-Accelerator typischerweise mithilfe einer Remote-Zugrifftechnologie zugegriffen. Es

ist wichtig, zwischen Leistungsproblemen aufgrund des OpenGL-Renderings und solchen aufgrund der Desktop-Fernzugriffstechnologie zu unterscheiden.

Probleme mit der Leistung des OpenGL-Renderings

Die Leistung des OpenGL-Renderings basiert auf der Anzahl der OpenGL-Befehle und Frames, die auf der Remote-Instance generiert werden.

Die Rendering-Leistung kann aufgrund der folgenden Faktoren variieren:

- Elastic Graphics-Accelerator-Leistung
- Netzwerkleistung
- CPU-Leistung
- Rendering-Modell, Szenariokomplexität
- Verhalten der OpenGL-Anwendung

Eine einfache Methode zur Leistungsbewertung besteht darin, die Zahl der gerenderten Frames auf der Remote-Instance anzuzeigen. Elastic Graphics-Accelerators zeigen maximal 25 FPS auf der Remote-Instance an, um die bestmögliche Qualität bei gleichzeitiger Reduzierung der Netzwerkauslastung zu bieten.

So zeigen Sie die Anzahl der produzierten Frames an:

1. Öffnen Sie die folgende Datei in einem Texteditor. Wenn die Datei nicht vorhanden ist, erstellen Sie sie.

   ```
   C:\Program Files\Amazon\EC2ElasticGPUs\conf\eg.conf
   ```

2. Identifizieren Sie den `[Application]`-Abschnitt oder fügen Sie ihn hinzu, und fügen Sie dann den folgenden Konfigurationsparameter hinzu:

   ```
   [Application]
   show_fps=1
   ```

3. Starten Sie die Anwendung neu, und prüfen Sie die FPS erneut.

Wenn der Wert bei der Aktualisierung der gerenderten Szene 15 - 25 FPS erreicht, bietet der Elastic Graphics-Accelerator Spitzenleistung. Alle weiteren bestehenden Leistungsprobleme basieren

möglicherweise auf dem Remote-Zugriff auf das Instance-Desktop. Wenn dies der Fall ist, vgl. den Abschnitt zu Problemen mit dem Fernzugriff.

Wenn der FPS-Wert unter 15 liegt, können Sie Folgendes versuchen:

- Verbessern Sie die Elastic Graphics-Accelerator-Leistung durch die Auswahl eines stärkeren Grafik-Accelerator-Typs.
- Verbessern Sie die allgemeine Netzwerkleistung mit folgenden Maßnahmen:
  - Prüfen Sie die ein- und ausgehende Bandbreite zu und von dem Endpunkt des Elastic Graphics-Accelerators. Der Elastic Graphics Accelerator-Endpunkt kann mit dem folgenden Befehl abgerufen werden: PowerShell

    ```
    PS C:\> (Invoke-WebRequest http://169.254.169.254/latest/meta-data/elastic-gpus/
    associations/[ELASTICGPU_ID]).content
    ```

  - Der Netzwerkdatenverkehr von der Instance zum Endpunkt des Elastic Graphics-Accelerators bezieht sich auf den Befehlsumfang, den die OpenGL-Anwendung produziert.
  - Der Netzwerkdatenverkehr vom Endpunkt des Elastic Graphics-Accelerators zur Instance bezieht sich auf die Anzahl der vom Grafik-Accelerator erstellten Frames.
  - Wenn Sie sehen, dass die Netzwerknutzung den maximalen Netzwerkdurchsatz der Instance erreicht, versuchen Sie, eine Instance mit einem höheren zulässigen Netzwerkdurchsatz zu verwenden.
- Verbessern der CPU-Leistung:
  - Anwendungen benötigen möglicherweise deutlich mehr CPU-Ressourcen als der Elastic Graphics-Accelerator. Wenn Windows Task Manager eine hohe Nutzung von CPU-Ressourcen meldet, versuchen Sie, eine Instance mit mehr CPU-Leistung zu verwenden.

Leistungsprobleme mit dem Fernzugriff

Eine Instance mit einem verbundenen Elastic Graphics-Accelerator ist über verschiedene Remote-Zugriffstechnologien zugänglich. Leistung und Qualität können variieren je nach:

- Fernzugriffstechnologie
- Instance-Leistung
- Client-Leistung
- Netzwerklatenz und Bandbreite zwischen Client und Instance

Wahlmöglichkeiten für das Fernzugriffsprotokoll sind etwa:

- Microsoft Remote Desktop Connection
- NICE DCV
- VNC

Für weitere Informationen zur Optimierung vgl. das spezifische Protokoll.

Beheben von Problemen mit fehlerhaftem Status

Wenn sich der Elastic Graphics-Accelerator in einem fehlerhaften Status befindet, verwenden Sie die folgenden Schritte zur Fehlerbehebung, um dieses Problem zu lösen.

Überprüfen der Instance-Konfiguration

Wenn das Elastic-Graphics-Befehlszeilen-Tool `egcli.exe` ein ähnliches Ergebnis wie das folgende zurückgibt, stellen Sie sicher, dass Ihre Sicherheitsgruppe ordnungsgemäß konfiguriert ist und dass Sie die Instance mit aktiviertem Instance-Metadatenservice gestartet haben.

```
EG Version 1.0.7.4240 (Manager) / N/A (OpenGL Library) / N/A (OpenGL Redirector)
EG Status: Out Of Service
Something prevented the EG Infrastructure to work properly.
```

Starten und Stoppen der Instance

Wenn sich der Elastic Graphics-Accelerator in einem fehlerhaften Status befindet, ist das Anhalten und erneute Starten der Instance die einfachste Option. Weitere Informationen finden Sie unter Stoppen und starten Sie Ihre Instances manuell.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Prüfen Sie die installierten Komponenten.

Öffnen Sie das Windows Control Panel, und prüfen Sie, ob die folgenden Komponenten installiert sind:

- Amazon Elastic Graphics Manager
- Amazon Elastic Graphics OpenGL Library
- Amazon EC2 Elastic GPUs OpenGL Redirector

Wenn eine dieser Komponenten fehlt, müssen Sie sie manuell installieren. Weitere Informationen finden Sie unter Installieren der erforderlichen Software für Elastic Graphics.

Überprüfen der Elastic Graphics-Protokolle

Öffnen Sie die Windows-Ereignisanzeige, erweitern Sie den Abschnitt Application and Services Logs (Anwendungs- und Dienstprotokolle) und suchen Sie in den folgenden Ereignisprotokollen nach Fehlern:

- EC2ElasticGPUs
- EC2ElasticGPUs-GUI

Warum sehe ich mehrere ENIs?

Wenn Sie eine EC2-Instance mit einem Elastic Graphics Accelerator aufrufen StartInstances, wird auf der Instance ein neues Elastic Network Interface (ENI) erstellt, damit OpenGL-Befehle an die remote angeschlossene Grafikkarte gesendet werden können.

Wenn Sie innerhalb eines kurzen Zeitraums (einige Sekunden oder weniger) StartInstancesmehrmals dieselbe EC2-Instance aufrufen, wird bei jedem Aufruf eine neue Netzwerkschnittstelle erstellt. Allerdings:

- Der Elastic-Graphics-Accelerator verwendet nur eine Netzwerkschnittstelle.
- Für zusätzliche Netzwerkschnittstellen fallen keine Gebühren an und sie werden innerhalb von 24 Stunden automatisch freigegeben.

Installieren des WSL auf Ihrer Windows-Instance

Windows Subsystem for Linux (WSL) kann kostenlos heruntergeladen werden und kann auf Ihrer Windows-Instance installiert werden. Durch die Installation des WSL können Sie native Linux-Befehlszeilen-Tools direkt auf Ihrer Windows-Instance ausführen und die Linux-Tools neben Ihrem herkömmlichen Windows-Desktop für Skripts verwenden. Sie können auf einer einzigen Windows-

Instance problemlos zwischen Linux und Windows wechseln, was in einer Entwicklungsumgebung sehr nützlich sein kann.

Weitere Informationen über WSL finden Sie in der Dokumentation zum Windows Subsystem for Linux auf der Microsoft Build Website.

Einschränkungen

- WSL ist in zwei Versionen erhältlich: WSL 1 und WSL 2.
  - Für `.metal`-EC2-Instances können Sie entweder WSL 1 oder WSL 2 installieren.
  - Für virtualisierte EC2-Instances müssen Sie WSL 1 installieren.
- Für Windows-Server-Betriebssysteme kann WSL nur auf Instances installiert werden, auf denen Folgendes ausgeführt wird:
  - Windows Server 2019
  - Windows Server 2022

Installieren des WSL

Die folgenden Anweisungen installieren WSL auf einer EC2-Instance, auf der Windows Server 2022 ausgeführt wird. Anweisungen zur Installation von WSL auf einer EC2-Instance, auf der Windows Server 2019 ausgeführt wird, finden Sie auf der Microsoft-Website unter Installieren von WSL auf früheren Versionen von Windows Server. Nachdem Sie diese Anweisungen befolgt haben, können Sie Schritt 3 der folgenden Anweisungen verwenden, um WSL für die Verwendung von WSL 1 zu konfigurieren.

Installieren Sie WSL 1

1. Um WSL zu installieren, führen Sie den folgenden Standardinstallationsbefehl auf Ihrer EC2-Instance aus, stellen Sie jedoch sicher, dass Sie WSL 1 aktivieren, indem Sie `--enable-wsl1` einschließen. Standardmäßig ist WSL 2 installiert. Wenn Ihre Instance mit einem virtualisierten Instance-Typ gestartet wurde, müssen Sie Schritt 3 in diesem Verfahren ausführen, um die Version auf WSL 1 festzulegen.

   ```
   wsl --install --enable-wsl1 --no-launch
   ```

2. Starten Sie Ihre EC2-Instance neu.

```
shutdown -r -t 20
```

3. Um WSL für die Verwendung von WSL 1 zu konfigurieren, führen Sie auf Ihrer Instance den folgenden Befehl aus. Weitere Informationen zum Festlegen der WSL-Version finden Sie unter Manuelle Installationsschritte für ältere Versionen von WSL auf der Microsoft Build Website.

```
wsl --set-default-version 1
```

4. Installieren Sie die Standarddistribution.

```
wsl --install
```

Installieren Sie WSL 2

- Um WSL zu installieren, führen Sie den folgenden Standardinstallationsbefehl auf Ihrer EC2-Instance aus. Standardmäßig ist WSL 2 installiert. Wenn Sie WSL auf einer `.metal`-Instance installieren, ist dies der einzige Schritt, den Sie ausführen müssen.

  ```
  wsl --install
  ```

  Weitere Informationen finden Sie unter Linux auf Windows mit WSL installieren auf der Microsoft Build Website.

Aktualisieren einer Amazon EC2-Instance unter Windows Server auf eine neuere Version von Windows

Es gibt zwei Methoden, um eine frühere Version von Windows Server zu aktualisieren, die auf einer Instanz ausgeführt wird: direktes Upgrade und Migration (auch side-by-side Upgrade genannt). Mit einem direkten Upgrade werden die Dateien des Betriebssystems aktualisiert, während Ihre persönlichen Einstellungen und Dateien intakt bleiben. Eine Migration umfasst die Erfassung von Einstellungen, Konfigurationen und Daten und deren Übertragung auf ein neueres Betriebssystem auf eine frische Amazon EC2-Instance.

Microsoft hat traditionell die Migration auf eine neuere Version von Windows Server anstelle eines Upgrades empfohlen. Die Migration kann zu weniger Fehlern oder Problemen beim Upgrade führen, sie dauert jedoch möglicherweise länger als ein direktes Upgrade, da eine

neue Instance bereitgestellt werden muss, Anwendungen geplant und übertragen und die Konfigurationseinstellungen auf der neuen Instance angepasst werden müssen. Ein direktes Upgrade kann schneller sein, Softwareinkompatibilität kann jedoch zu Fehlern führen.

Inhalt

Führen Sie ein direktes Upgrade auf Ihrer Windows-Instanz durch

Bevor Sie ein direktes Upgrade ausführen, müssen Sie ermitteln, welche Netzwerktreiber die Instance ausführt. PV-Netzwerktreiber ermöglichen Ihnen den Zugriff auf Ihre Instance per Remote-Desktop. Instances verwenden entweder AWS PV, Intel Network Adapter oder die Enhanced Networking-Treiber. Weitere Informationen finden Sie unter Paravirtual-Treiber für Windows-Instances.

Bevor Sie ein direktes Upgrade beginnen

Führen Sie die folgenden Aufgaben durch und beachten Sie die folgenden wichtigen Details, bevor Sie mit Ihrem direkten Upgrade beginnen.

- Lesen Sie die Microsoft-Dokumentation, um die Upgrade-Anforderungen, bekannte Probleme und Einschränkungen zu verstehen. Sie sollten auch die offiziellen Anweisungen für Upgrades überprüfen.
  - Upgradeoptionen für Windows Server 2012
  - Upgradeoptionen für Windows Server 2012 R2
  - Upgrade- und Konvertierungsoptionen für Windows Server 2016
  - Upgrade- und Konvertierungsoptionen für Windows Server 2019
  - Upgrade- und Konvertierungs-Optionen für Windows Server 2022
  - Windows Server Upgrade Center
- Wir empfehlen, für Instances mit mindestens zwei vCPUs und 4 GB RAM ein Betriebssystem-Upgrade durchzuführen. Bei Bedarf können Sie die Instance in eine andere Größe desselben

Typs ändern (z. B. t2.small in t2.large), das Upgrade durchführen und die Instance dann wieder in die Originalgröße ändern. Wenn Sie die Instance-Größe beibehalten müssen, können Sie den Fortschritt über den Instance-Konsolen-Screenshot überwachen. Weitere Informationen finden Sie unter Ändern des Instance-Typs.

- Stellen Sie sicher, dass das Stamm-Volume auf Ihrer Windows-Instance über genügend freien Speicherplatz verfügt. Das Windows Setup warnt Sie im Fall von unzureichendem Speicherplatz möglicherweise nicht. Informationen zur benötigten Menge an Speicherplatz für das Upgrade eines bestimmten Betriebssystems finden Sie in der Microsoft-Dokumentation. Wenn das Volume nicht über genügend Speicherplatz verfügt, kann es erweitert werden. Weitere Informationen finden Sie unter Amazon EBS Elastic Volumes im Amazon EBS-Benutzerhandbuch.
- Bestimmen Sie Ihren Upgrade-Pfad. Sie müssen das Betriebssystem auf dieselbe Architektur upgraden. Beispielsweise müssen Sie ein 32-Bit-System auf ein 32-Bit-System upgraden. Windows Server 2008 R2 und spätere Versionen sind nur 64-Bit.
- Deaktivieren Sie Antivirus- und Anti-Spyware-Software und Firewalls. Diese Arten von Software können Konflikte beim Upgrade-Prozess erzeugen. Aktivieren Sie Antivirus- und Anti-Spyware-Software und Firewalls nach dem Abschluss des Upgrades erneut.
- Installieren Sie die neuesten Treiber, so wie unter Migrieren Sie eine Windows-Instance zu einem Instance-Typ der aktuellen Generation beschrieben.
- Der Upgrade Helper Service unterstützt nur Instances, auf denen Citrix PV-Treiber ausgeführt werden. Wenn die Instance auf Red Hat-Treibern ausgeführt wird, müssen Sie zuerst diese Treiber manuell upgraden.

Führen Sie ein direktes Upgrade einer Instance mit den AWS Treibern PV, Intel Network Adapter oder Enhanced Networking durch

Verwenden Sie das folgende Verfahren, um eine Windows Server Instance mit einem AWS PV, Intel Network Adapter oder den Enhanced Networking-Treibern zu aktualisieren.

So führen Sie ein direktes Upgrade durch

1. Erstellen Sie ein AMI des Systems, das Sie entweder zu Backup- oder Testzwecken upgraden möchten. Sie können das Upgrade dann auf der Kopie ausführen, um eine Testumgebung zu simulieren. Wenn das Upgrade abgeschlossen wird, können Sie den Datenverkehr mit geringer Ausfallzeit zu dieser Instance umleiten. Wenn das Upgrade fehlschlägt, können Sie zum Backup zurückwechseln. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

2. Stellen Sie sicher, dass Ihre Windows-Server-Instance die neuesten Treiber verwendet.

   a. Informationen zum Aktualisieren Ihres AWS PV-Treibers finden Sie unterUpgraden von PV-Treibern auf Windows-Instances.

   b. Informationen zum Aktualisieren Ihres ENA-Treibers finden Sie unterInstallieren Sie den Elastic Network Adapter (ENA) -Treiber.

   c. Informationen zum Aktualisieren Ihrer Intel-Treiber finden Sie unter Aktivieren Sie Enhanced Networking mit der Intel 82599 VF-Schnittstelle auf Ihren EC2-Instances

3. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

4. Wählen Sie im Navigationsbereich Instances aus. Suchen Sie die Instance. Notieren Sie die Instance-ID und Availability Zone für die Instance. Diese Informationen werden später in diesem Verfahren benötigt.

5. Wenn Sie von Windows Server 2012 oder 2012 R2 auf Windows Server 2016, 2019 oder 2022 aktualisieren, führen Sie die folgenden Schritte auf Ihrer Instance durch, bevor Sie fortfahren:

   a. Deinstallieren Sie den EC2Config-Service. Weitere Informationen finden Sie unter Beenden, Neustarten, Löschen oder Deinstallieren von EC2Config.

   b. Installieren Sie EC2Launch v1 oder den EC2Launch-v2-Agenten. Weitere Informationen finden Sie unter Konfigurieren einer Windows-Instance mithilfe von EC2Launch und Konfigurieren einer Windows-Instance mithilfe von EC2Launch v2.

   c. Installieren Sie den AWS Systems Manager SSM-Agenten. Weitere Informationen finden Sie unter Arbeiten mit dem SSM Agent im AWS Systems Manager -Benutzerhandbuch.

6. Erstellen Sie ein neues Volume aus einem Windows Server-Installationsmedien-Snapshot.

   a. Wählen Sie im Navigationsbereich links unter Elastic Block Store die Option Snapshots.

   b. Wählen Sie in der Filterleiste Öffentliche Schnappschüsse.

   c. Geben Sie in der Suchleiste die folgenden Filter ein:

      - Wählen Sie Owner Alias, dann = und dann Amazon.
      - Wählen Sie Beschreibung und beginnen Sie dann mit der Eingabe**`Windows`**. Wählen Sie den Windows-Filter aus, der der Systemarchitektur und der bevorzugten Sprache entspricht, auf die Sie aktualisieren möchten. Wählen Sie zum Beispiel Windows 2019 English Installation Media für ein Upgrade auf Windows Server 2019.

d. Aktivieren Sie das Kontrollkästchen neben dem Snapshot, der der Systemarchitektur und den Spracheinstellungen entspricht, auf die Sie aktualisieren möchten, und wählen Sie dann Aktionen, Volume aus Snapshot erstellen.

e. Wählen Sie auf der Seite Volume erstellen die Availability Zone, die zu Ihrer Windows-Instance passt, und wählen Sie dann Volume erstellen.

7. Wählen Sie im Banner Erfolgreich erstelltes Volume vol-***1234567890Beispiel*** oben auf der Seite die ID des Volumes, das Sie gerade erstellt haben.

8. Wählen Sie Actions (Aktionen) und Attach Volume (Volume anfügen).

9. Wählen Sie auf der Seite Volume anhängen unter Instance die Instance-ID Ihrer Windows-Instance und wählen Sie dann Volume anhängen.

10. Machen Sie das neue Volume für die Nutzung verfügbar, indem Sie die Schritte unter Amazon EBS-Volume zur Nutzung verfügbar machen befolgen.

> **Important**
>
> Initialisieren Sie den Datenträger nicht, da dadurch die vorhandenen Daten gelöscht werden.

11. Wechseln Sie in Windows PowerShell zum neuen Volumenlaufwerk. Beginnen Sie das Upgrade, indem Sie das Installationsmedien-Volume öffnen, das Sie an die Instance angehängt haben.

    a. Wenn Sie ein Upgrade auf Windows Server 2016 oder höher installieren, führen Sie Folgendes aus:

```
.\setup.exe /auto upgrade /dynamicupdate disable
```

> **Note**
>
> Das Ausführen von setup.exe mit deaktivierter `/dynamicupdate`-Option verhindert, dass Windows während des Windows Server-Upgrade-Prozesses Updates installiert, da die Installation von Updates während des Upgrades zu Fehlern führen kann. Sie können Updates mit Windows Update installieren, nachdem das Upgrade abgeschlossen ist.

Wenn Sie ein Upgrade auf eine frühere Version von Windows Server installieren, führen Sie Folgendes aus:

```
Sources\setup.exe
```

b. Wählen Sie für Select the operating system you want to install die vollständige Installations-SKU für Ihre Windows Server-Instance und anschließend Next aus.

c. Wählen Sie für Which type of installation do you want? die Option Upgrade aus.

d. Schließen Sie den Assistenten ab.

Windows Server Setup kopiert und verarbeitet jetzt Dateien. Nach einigen Minuten wird Ihre Remote-Desktop-Sitzung beendet. Die für das Upgrade benötigte Zeit hängt von der Anzahl an Anwendungen und Serverrollen ab, die auf Ihrer Windows Server-Instance ausgeführt werden. Das Upgrade kann vielleicht nur 40 Minuten oder auch einige Stunden dauern. Während des Upgrades schlägt die Instance-Statusprüfung 1 von 2 fehl. Wenn das Upgrade abgeschlossen ist, verlaufen beide Statusprüfungen erfolgreich. Sie können das Systemprotokoll auf Konsolenausgaben überprüfen oder CloudWatch Amazon-Metriken für Festplatten- und CPU-Aktivität verwenden, um festzustellen, ob das Upgrade voranschreitet.

> **Note**
>
> Wenn Sie ein Upgrade auf Windows Server 2019 erstellen, können Sie nach Abschluss des Upgrades den Desktop-Hintergrund manuell ändern, um den vorherigen Namen des Betriebssystems bei Bedarf zu löschen.

Wenn nach einigen Stunden noch nicht beide Statusprüfungen auf der Instance erfolgreich beendet wurden, informieren Sie sich unter Beheben Sie Fehler bei einem Upgrade auf einer Windows-Instance.

Aufgaben nach dem Upgrade

1. Melden Sie sich bei der Instance an, um ein Upgrade für das .NET Framework zu initiieren, und starten Sie das System neu, wenn Sie dazu aufgefordert werden.
2. Falls Sie dies in einem vorherigen Schritt noch nicht getan haben, installieren Sie den EC2Launch v1- oder EC2Launch v2-Agenten. Weitere Informationen finden Sie unter

Konfigurieren einer Windows-Instance mithilfe von EC2Launch und Konfigurieren einer Windows-Instance mithilfe von EC2Launch v2.

3. Wenn Sie auf Windows Server 2012 R2 aktualisiert haben, empfehlen wir, die PV-Treiber auf AWS PV-Treiber zu aktualisieren. Wenn Sie auf einer Nitro-basierten Instance ein Upgrade durchgeführt haben, empfehlen wir Ihnen, die NVME- und ENA-Treiber zu installieren oder zu aktualisieren. Weitere Informationen finden Sie unter Windows Server 2012 R2, Installieren oder aktualisieren Sie NVMe-Treiber mit AWS PowerShell oder Aktivieren von Enhanced Networking unter Windows.
4. Aktivieren Sie die Antivirus- und Anti-Spyware-Software und Firewalls erneut.

Führen Sie ein automatisiertes Upgrade auf Ihrer Windows-Instanz durch

Mit AWS Systems Manager Automation-Runbooks können Sie ein automatisiertes Upgrade Ihrer Windows- und SQL Server-Instanzen durchführen. AWS

Inhalt

Zugehörige Services

Die folgenden AWS Dienste werden im automatisierten Upgrade-Prozess verwendet:

- AWS Systems Manager. AWS Systems Manager ist eine leistungsstarke, einheitliche Oberfläche für die zentrale Verwaltung Ihrer AWS Ressourcen. Weitere Informationen finden Sie im AWS Systems Manager -Benutzerhandbuch.
- AWS Systems Manager Agent (SSM Agent) ist Amazon-Software, die auf einer Amazon EC2-Instance, einem lokalen Server oder einer virtuellen Maschine (VM) installiert und konfiguriert werden kann. SSM Agent ermöglicht es Systems Manager, diese Ressourcen zu aktualisieren, zu verwalten und zu konfigurieren. Der Agent verarbeitet Anforderungen des Systems-Manager-Services in der AWS -Cloud und führt sie dann wie in der Anforderung angegeben aus. Weitere Informationen finden Sie unter Arbeiten mit SSM Agent im AWS Systems Manager -Benutzerhandbuch.

- AWS Systems Manager SSM-Runbooks. Ein SSM-Runbook definiert die Aktionen, die Systems Manager auf Ihren verwalteten Instances durchführt. SSM-Runbooks verwenden JavaScript Object Notation (JSON) oder YAML und enthalten Schritte und Parameter, die Sie angeben. Dieses Thema verwendet zwei Systems-Manager-SSM-Runbooks für die Automatisierung. Weitere Informationen finden Sie in der Referenz zum AWS Systems Manager -Automation-Runbook im AWS Systems Manager -Benutzerhandbuch.

Ausführungsoptionen

Wählen Sie erst Automation (Automatisierung) auf der Systems Manager-Konsole und dann Execute (Ausführen). Nachdem Sie ein Automation-Dokument ausgewählt haben, werden Sie aufgefordert, eine Option zur Automatisierungsausführung auszuwählen. Sie wählen aus den folgenden Optionen. In den Schritten für die in diesem Thema angegebenen Pfade verwenden wir die Option Simple execution (Einfache Ausführung).

Einfache Ausführung

Wählen Sie diese Option, wenn Sie eine einzelne Instance aktualisieren möchten, aber nicht jeden Automatisierungsschritt durchlaufen möchten, um die Ergebnisse zu prüfen. Diese Option wird in den folgenden Upgrade-Schritten näher erläutert.

Rate control (Ratenregelung)

Wählen Sie diese Option, wenn Sie das Upgrade auf mehr als eine Instance anwenden möchten. Sie definieren die folgenden Einstellungen.

- Parameter

  Diese Einstellung, die auch in den Einstellungen für Multi-Konto und Region festgelegt ist, definiert, wie Ihre Automatisierung verzweigt ist.
- Targets (Ziele)

  Wählen Sie das Ziel aus, auf das Sie die Automatisierung anwenden möchten. Diese Einstellung wird auch in den Einstellungen für Multi-Konto und Region festgelegt.
- Parameter Values (Parameterwerte)

  Verwenden Sie die Werte, die in den Parametern im Automatisierungsdokument definiert sind.
- Resource Group (Ressourcengruppe)

In ist eine Ressource eine Entität AWS, mit der Sie arbeiten können. Beispiele hierfür sind Amazon EC2 EC2-Instances, AWS CloudFormation Stacks oder Amazon S3 S3-Buckets. Wenn Sie mit mehreren Ressourcen arbeiten, kann es sinnvoll sein, sie als Gruppe zu verwalten, anstatt für jede Aufgabe von einem AWS Service zum anderen zu wechseln. In einigen Fällen möchten Sie vielleicht große Anzahlen an verwandten Ressourcen verwalten, wie EC2-Instances, die eine Anwendungsebene ausmachen. In diesem Fall müssen Sie wahrscheinlich Massenaktionen auf diesen Ressourcen gleichzeitig durchführen.

- Tags

  Mithilfe von Stichwörtern können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Diese Kategorisierung ist nützlich, wenn Sie viele Ressourcen desselben Typs haben. Sie können eine bestimmte Ressource mit den zugewiesenen Tags (Markierungen) schnell identifizieren.

- Rate Control (Ratenregelung)

  Die Ratenregelung wird auch in den Einstellungen für Multi-Konto und Region festgelegt. Wenn Sie die Parameter der Ratenregelung festlegen, definieren Sie, auf wie viel Ihrer Flotte die Automatisierung angewendet wird, und zwar entweder nach Zielanzahl oder Prozentzahl der Flotte.

Multi-Account and Region (Multi-Konto und Region)

Zusätzlich zu den unter der Ratenregelung angegebenen Parametern, die auch in den Einstellungen für Multi-Konto und Region verwendet werden, gibt es zwei zusätzliche Einstellungen:

- Accounts and organizational units (OUs) (Konten und Organisationseinheiten (OUs))

  Geben Sie mehrere Konten an, auf denen Sie die Automatisierung ausführen möchten.

- AWS-Regionen

  Geben Sie mehrere AWS-Regionen Orte an, an denen Sie die Automatisierung ausführen möchten.

Manuelle Ausführung

Diese Option ähnelt der Einfachen Ausführung, allerdings können Sie jeden Automatisierungsschritt durchlaufen und die Ergebnisse prüfen.

Aktualisieren von Windows Server

Das `AWSEC2-CloneInstanceAndUpgradeWindows`-Runbook erstellt ein Amazon Machine Image (AMI) von einer Windows-Server-Instance in Ihrem Konto und aktualisiert dieses AMI auf eine unterstützte Version Ihrer Wahl. Dieser mehrschrittige Prozess kann bis zu zwei Stunden dauern.

Es sind zwei AMIs im automatisierten Upgrade-Prozess enthalten:

- Aktuell ausgeführte Instance. Das erste AMI ist die aktuell ausgeführte Instance, die nicht aktualisiert wird. Diese AMI wird verwendet, um eine andere Instance zu starten, damit diese das direkte Upgrade ausführt. Wenn der Vorgang abgeschlossen ist, wird dieses AMI aus Ihrem Konto gelöscht, es sei denn, sie geben speziell an, dass Sie die Original-Instance behalten möchten. Diese Einstellung wird vom Parameter gehandhabt `KeepPreUpgradeImageBackUp` (der Standardwert ist `false`, was bedeutet, dass das AMI standardmäßig gelöscht wird).
- Aktualisiertes AMI. Dieses AMI ist das Ergebnis des Automatisierungsvorgangs.

Das Endergebnis ist ein AMI, welches die aktualisierte Instance des AMI ist.

Wenn das Upgrade abgeschlossen ist, können Sie die Anwendung testen, indem Sie das neue AMI in Ihrer Amazon VPC starten. Nachdem Sie den Test abgeschlossen haben und bevor Sie eine weitere Aktualisierung durchführen, planen Sie die Anwendungsausfallzeit ein, bevor Sie vollständig zu der aktualisierten Instance wechseln.

Voraussetzungen

Um Ihr Windows Server-Upgrade mit dem AWS Systems Manager Automatisierungsdokument zu automatisieren, müssen Sie die folgenden Aufgaben ausführen:

- Erstellen Sie eine IAM-Rolle mit den angegebenen IAM-Richtlinien, damit Systems Manager Automatisierungsaufgaben auf Ihren Amazon EC2-Instances durchführen und überprüfen kann, dass Sie die Voraussetzungen für die Verwendung von Systems Manager erfüllen. Weitere Informationen finden Sie im AWS Identity and Access Management Benutzerhandbuch unter Erstellen einer Rolle zum Delegieren von Berechtigungen für einen AWS Dienst.
- Wählen Sie die Option aus, wie die Automatisierung ausgeführt werden soll. Die Optionen für die Ausführung sind Simple execution (Einfache Ausführung), Rate control (Ratenregelung), Multi-account and Region (Multi-Konto und Region) und Manual execution (Manuelle Ausführung). Weitere Informationen zu diesen Optionen finden Sie unter Ausführungsoptionen.

- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Installation und Konfiguration von SSM Agent auf Amazon-EC2-Instances für Windows Server.
- Windows PowerShell 3.0 oder höher muss auf Ihrer Instanz installiert sein.
- Für Instances, die einer Microsoft Active Directory-Domain angehören, empfehlen wir, eine `SubnetId` anzugeben, die keine Verbindung zu Ihren Domain-Cntrollern aufweist, um Hostnamenkonflikte zu vermeiden.
- Das Instance-Subnetz muss über eine ausgehende Verbindung zum Internet verfügen, die Zugriff AWS-Services auf Amazon S3 und den Zugriff auf Download-Patches von Microsoft ermöglicht. Diese Anforderung ist erfüllt, wenn das Subnetz entweder ein öffentliches Subnetz ist und die Instance eine öffentliche IP-Adresse hat, oder wenn es sich bei dem Subnetz um ein privates Subnetz mit einer Route handelt, die Internetverkehr an ein öffentliches NAT-Gerät sendet.
- Diese Automatisierung funktioniert mit Instances, auf denen Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 und Windows Server 2019 ausgeführt wird.
- Stellen Sie sicher, dass die Instance 20 GB freien Speicherplatz auf dem Boot-Datenträger hat.
- Wenn die Instance keine Windows-Lizenz verwendet, die von bereitgestellt wird AWS, geben Sie eine Amazon EBS-Snapshot-ID an, die Windows Server 2012 R2-Installationsmedien enthält. So gehen Sie vor:
  1. Überprüfen Sie, ob die Amazon-EC2-Instance Windows Server 2012 oder höher ausführt.
  2. Erstellen Sie ein Amazon-EBS-Volume mit 6 GB in derselben Availability Zone, in der die Instance ausgeführt wird. Fügen Sie das Volume der Instance an. Mounten Sie dies beispielsweise als Laufwerk D.
  3. Klicken Sie mit der rechten Maustaste auf die ISO, und mounten Sie es für eine Instance, beispielsweise als Laufwerk E.
  4. Kopieren Sie den Inhalt der ISO von Laufwerk E:\ zu Laufwerk D:\.
  5. Erstellen Sie einen Amazon-EBS-Snapshot des 6 GB-Volumes, das Sie oben in Schritt 2 erstellt haben.

Einschränkungen für Windows Server Upgrade

Diese Automatisierung unterstützt keine Upgrades von Windows-Domain-Controllern, Clustern oder Windows-Desktopbetriebssystemen. Diese Automation unterstützt außerdem keine Amazon–EC2-Instances für Windows Server mit den folgenden installierten Rollen:

- Remote Desktop Session Host (RDSH)

- Remote Desktop Connection Broker (RDCB)
- Remote Desktop Virtualization Host (RDVH)
- Remote Desktop Web Access (RDWA)

Schritte zum Durchführen eines automatisierten Upgrades von Windows Server

Gehen Sie wie folgt vor, um Ihre Windows Server-Instance mithilfe des AWSECCloneInstanceAndUpgrade2-Windows-Automatisierungs-Runbooks zu aktualisieren.

1. Öffnen Sie Systems Manager von der AWS Management Console aus.
2. Wählen Sie im linken Navigationsbereich unter Änderungsmanagement Automatisierung aus.
3. Wählen Sie Execute automation (Automatisierung ausführen).
4. Suchen Sie nach dem Automatisierungsdokument mit der Bezeichnung `AWSEC2-CloneInstanceAndUpgradeWindows`.
5. Wenn der Dokumentenname angezeigt wird, wählen Sie ihn aus. Anschließend werden die Dokumentendetails angezeigt.
6. Klicken Sie auf Execute automation (Automatisierung ausführen), um die Parameter für dieses Dokument einzugeben. Lassen Sie Simple execution (Einfache Ausführung) oben auf der Seite ausgewählt.
7. Geben Sie die angeforderten Parameter basierend auf den folgenden Hinweisen ein.

   - `InstanceID`

     Typ: Zeichenfolge

     (Erforderlich) Die Instance, auf der Windows Server 2008 R2, 2012 R2, 2016, oder 2019 ausgeführt wird, auf der SSM Agent installiert ist.

   - `InstanceProfile`.

     Typ: Zeichenfolge

     (Erforderlich) Das IAM-Instance-Profil. Dies ist die IAM-Rolle, die verwendet wird, um die Systems Manager Manager-Automatisierung für die Amazon EC2 EC2-Instance und AWS AMIs durchzuführen. Weitere Informationen finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager im AWS Systems Manager -Benutzerhandbuch.

   - `TargetWindowsVersion`

Typ: Zeichenfolge

(Erforderlich) Wählen Sie die Windows-Zielversion aus.

- `SubnetId`

  Typ: Zeichenfolge

  (Erforderlich) Dies ist das Subnetz für den Upgrade-Prozess und der Ort, an dem sich Ihre Quell-EC2-Instance befindet. Stellen Sie sicher, dass das Subnetz ausgehende Verbindungen zu AWS Diensten wie Amazon S3 und auch zu Microsoft hat (um Patches herunterzuladen).

- `KeepPreUpgradedBackUp`

  Typ: Zeichenfolge

  (Optional) Wenn dieser Parameter auf `true` gesetzt ist, behält die Automatisierung das von der Instance erstellte Image bei. Die Standardeinstellung lautet `false`.

- `RebootInstanceBeforeTakingImage`

  Typ: Zeichenfolge

  (Optional) Der Standardwert ist `false` (kein Reboot). Wenn dieser Parameter auf `true` gesetzt ist, startet Systems Manager die Instance neu, bevor ein AMI für das Upgrade erstellt wird.

8. Nachdem Sie die Parameter eingegeben haben, wählen Sie Execute (Ausführen) aus. Wenn die Automatisierung beginnt, können Sie den Ausführungsfortschritt überwachen.
9. Wenn die Automatisierung abgeschlossen ist, sehen Sie die AMI-ID. Sie können das AMI starten, um zu überprüfen, ob das Windows-Betriebssystem aktualisiert wurde.

> **Note**
>
> Es ist nicht notwendig, dass die Automatisierung alle Schritte ausführt. Die Schritte basieren bedingt auf dem Verhalten der Automatisierung und der Instance. Der Systems Manager überspringt möglicherweise einige Schritte, die nicht erforderlich sind. Darüber hinaus können einige Schritte ausfallen. Systems Manager versucht, alle aktuellen Patches zu aktualisieren und zu installieren. Manchmal wird bei einigen Patches aber auch die Zeit basierend auf einer definierbaren Zeitüberschreitungs-Einstellung für diesen Schritt überschritten. Wenn dies geschieht, fährt die Systems

Manager-Automatisierung mit dem nächsten Schritt fort, um sicherzustellen, dass das interne Betriebssystem auf die Windows Server-Zielversion aktualisiert wird.

10. Nachdem die Automatisierung abgeschlossen wurde, können Sie eine Amazon EC2-Instance mit der AMI-ID starten, um Ihr Upgrade zu überprüfen. Weitere Informationen zum Erstellen einer Amazon EC2 EC2-Instance aus einem AWS AMI finden Sie unter Wie starte ich eine EC2-Instance von einem benutzerdefinierten AMI aus?

Upgrade von SQL Server

Das `AWSEC2-CloneInstanceAndUpgradeSQLServer`-Skript erstellt ein AMI aus einer Amazon-EC2-Instance, auf der SQL Server in Ihrem Konto ausgeführt wird, und aktualisiert dann das AMI auf eine aktuellere Version von SQL Server. Dieser mehrschrittige Prozess kann bis zu zwei Stunden dauern.

In diesem Workflow, die Automatisierung erstellt ein AMI aus der Instance und startet dann das neu erstellte AMI in dem Subnetz, das Sie bereitstellen. Die Automatisierung führt dann ein direktes Upgrade von SQL Server durch. Nach dem Upgrade erstellt die Automatisierung ein neues AMI, bevor die aktualisierte Instance beendet wird.

Es sind zwei AMIs im automatisierten Upgrade-Prozess enthalten:

- Aktuell ausgeführte Instance. Das erste AMI ist die aktuell ausgeführte Instance, die nicht aktualisiert wird. Diese AMI wird verwendet, um eine andere Instance zu starten, damit diese das direkte Upgrade ausführt. Wenn der Vorgang abgeschlossen ist, wird dieses AMI aus Ihrem Konto gelöscht, es sei denn, sie geben speziell an, dass Sie die Original-Instance behalten möchten. Diese Einstellung wird vom Parameter gehandhabt `KeepPreUpgradeImageBackUp` (der Standardwert ist `false`, was bedeutet, dass das AMI standardmäßig gelöscht wird).
- Aktualisiertes AMI. Dieses AMI ist das Ergebnis des Automatisierungsvorgangs.

Das Endergebnis ist ein AMI, welches die aktualisierte Instance des AMI ist.

Wenn das Upgrade abgeschlossen ist, können Sie die Anwendung testen, indem Sie das neue AMI in Ihrer Amazon VPC starten. Nachdem Sie den Test abgeschlossen haben und bevor Sie eine weitere Aktualisierung durchführen, planen Sie die Anwendungsausfallzeit ein, bevor Sie vollständig zu der aktualisierten Instance wechseln.

Voraussetzungen

Um Ihr SQL Server-Upgrade mit dem AWS Systems Manager Automatisierungsdokument zu automatisieren, müssen Sie die folgenden Aufgaben ausführen:

- Erstellen Sie eine IAM-Rolle mit den angegebenen IAM-Richtlinien, damit Systems Manager Automatisierungsaufgaben auf Ihren Amazon EC2-Instances durchführen und überprüfen kann, dass Sie die Voraussetzungen für die Verwendung von Systems Manager erfüllen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im AWS Identity and Access Management -Benutzerhandbuch.
- Wählen Sie die Option aus, wie die Automatisierung ausgeführt werden soll. Die Optionen für die Ausführung sind Simple execution (Einfache Ausführung), Rate control (Ratenregelung), Multi-account and Region (Multi-Konto und Region) und Manual execution (Manuelle Ausführung). Weitere Informationen zu diesen Optionen finden Sie unter Ausführungsoptionen.
- Die Amazon-EC2-Instance muss Windows Server 2008 R2 oder höher und SQL Server 2008 oder höher verwenden.
- Stellen Sie sicher, dass SSM Agent auf Ihrer Instance installiert ist. Weitere Informationen finden Sie unter Arbeiten mit SSM-Agent auf Amazon-EC2-Instances für Windows Server.
- Überprüfen Sie, ob die Instance über genügend freien Speicherplatz verfügt:
  - Wenn Sie ein Upgrade von Windows Server 2008 R2 auf 2012 R2 oder von Windows Server 2012 R2 auf ein neueres Betriebssystem durchführen, stellen Sie sicher, dass Sie über 20 GB freien Festplattenspeicher auf der Startdiskette der Instance verfügen.
  - Wenn Sie ein Upgrade von Windows Server 2008 R2 auf 2016 oder höher durchführen, stellen Sie sicher, dass die Instance über 40 GB freien Festplattenspeicher auf der Startdiskette der Instance verfügt.
- Für Instances, die eine Bring Your Own License (BYOL) SQL Server-Version verwenden, gelten die folgenden zusätzlichen Voraussetzungen:
  - Stellen Sie eine Amazon-EBS-Snapshot-ID mit den Installationsmedien des Ziel-SQL-Servers berei. So gehen Sie vor:
    1. Überprüfen Sie, ob die Amazon-EC2-Instance Windows Server 2008 R2 oder höher ausführt.
    2. Erstellen Sie ein Amazon-EBS-Volume mit 6 GB in derselben Availability Zone, in der die Instance ausgeführt wird. Fügen Sie das Volume der Instance an. Mounten Sie dies beispielsweise als Laufwerk D.
    3. Klicken Sie mit der rechten Maustaste auf die ISO, und mounten Sie es für eine Instance, beispielsweise als Laufwerk E.

4. Kopieren Sie den Inhalt der ISO von Laufwerk E:\ zu Laufwerk D:\.
5. Erstellen Sie einen Amazon-EBS-Snapshot des 6 GB-Volumes, das Sie in Schritt 2 erstellt haben.

Einschränkungen für automatisierte Upgrades von SQL Server

Die folgenden Einschränkungen gelten, wenn Sie das AWSECCloneInstanceAndUpgrade2-SQLServer-Runbook zur Durchführung eines automatisierten Upgrades verwenden:

- Das Upgrade ist nur auf einem SQL Server mit Windows-Authentifizierung möglich.
- Stellen Sie sicher, dass keine Sicherheits-Patch-Updates auf den Instances ausstehen. Öffnen Sie Control Panel (Systemsteuerung), und wählen Sie dann Check for updates (Auf Aktualisierungen prüfen).
- SQL Server-Bereitstellungen in HA und der Spiegelungsmodus werden nicht unterstützt.

Schritte zum Durchführen eines automatisierten Upgrades von SQL Server

Gehen Sie wie folgt vor, um Ihren SQL Server mithilfe des AWSECCloneInstanceAndUpgrade2-SQLServer-Automatisierungsrunbooks zu aktualisieren.

1. Wenn Sie dies nicht bereits getan haben, laden Sie die SQL Server 2016 .iso-Datei herunter und mounten Sie sie auf dem Quellserver.
2. Nachdem die .iso-Datei gemountet wurde, kopieren Sie alle Komponentendateien und platzieren Sie sie auf dem Volume Ihrer Wahl.
3. Erstellen Sie einen Amazon-EBS-Snapshot des Volumes und kopieren Sie die Snapshot-ID für eine spätere Verwendung in die Zwischenablage. Weitere Informationen finden Sie unter Erstellen von Amazon EBS-Snapshots im Amazon EBS-Benutzerhandbuch.
4. Fügen Sie das Instance-Profil an die Amazon-EC2-Quell-Instance an. Auf diese Weise kann Systems Manager mit der EC2-Instance kommunizieren und Befehle auf ihr ausführen, nachdem sie dem AWS Systems Manager Service hinzugefügt wurde. Für dieses Beispiel haben wir die Rolle `SSM-EC2-Profile-Role` genannt, wobei die `AmazonSSMManagedInstanceCore` -Richtlinie der Rolle angefügt ist. Informationen dazu finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager im AWS Systems Manager -Benutzerhandbuch.
5. Wählen Sie in der AWS Systems Manager Konsole im linken Navigationsbereich Managed Instances aus. Überprüfen Sie, dass sich Ihre EC2-Instance in der Liste der verwalteten

Instances befindet. Wenn Ihre Instance nach einigen Minuten nicht angezeigt wird, lesen Sie unter Wo sind meine Instances? im AWS Systems Manager -Benutzerhandbuch nach.

6. Wählen Sie im linken Navigationsbereich unter Änderungsmanagement Automatisierung aus.
7. Wählen Sie Execute automation (Automatisierung ausführen).
8. Suchen Sie nach dem Automatisierungsdokument mit der Bezeichnung `AWSEC2-CloneInstanceAndUpgradeSQLServer`.
9. Rufen Sie das `AWSEC2-CloneInstanceAndUpgradeSQLServer`-SSM-Dokument auf und wählen Sie dann Next (Weiter).
10. Stellen Sie sicher, dass die Option Simple execution (Einfache Ausführung) ausgewählt ist.
11. Geben Sie die angeforderten Parameter basierend auf den folgenden Hinweisen ein.

    - `InstanceId`

      Typ: Zeichenfolge

      (Erforderlich) Die Instance, die SQL Server 2008 R2 (oder höher) ausführt.

    - `IamInstanceProfile`

      Typ: Zeichenfolge

      (Erforderlich) Das IAM-Instance-Profil.

    - `SQLServerSnapshotId`

      Typ: Zeichenfolge

      (Erforderlich) Die Snapshot-ID für die Installationsmedien des Ziel-SQL-Servers. Dieser Parameter ist für Instances mit SQL-Server-Lizenzen nicht erforderlich.

    - `SubnetId`

      Typ: Zeichenfolge

      (Erforderlich) Dies ist das Subnetz für den Upgrade-Prozess und der Ort, an dem sich Ihre Quell-EC2-Instance befindet. Stellen Sie sicher, dass das Subnetz ausgehende Verbindungen zu AWS Diensten wie Amazon S3 und auch zu Microsoft hat (um Patches herunterzuladen).

    - `KeepPreUpgradedBackUp`

      Typ: Zeichenfolge

(Optional) Wenn dieser Parameter auf `true` gesetzt ist, behält die Automatisierung das von der Instance erstellte Image bei. Die Standardeinstellung lautet `false`.

- `RebootInstanceBeforeTakingImage`

  Typ: Zeichenfolge

  (Optional) Der Standardwert ist `false` (kein Reboot). Wenn dieser Parameter auf `true` gesetzt ist, startet Systems Manager die Instance neu, bevor ein AMI für das Upgrade erstellt wird.

- `TargetSQLVersion`

  Typ: Zeichenfolge

  (Optional) Die Zielversion von SQL Server. Der Standardwert ist `2016`.

12. Nachdem Sie die Parameter eingegeben haben, wählen Sie Execute (Ausführen) aus. Wenn die Automatisierung beginnt, können Sie den Ausführungsfortschritt überwachen.
13. Wenn der Execution Status (Ausführungsstatus) Success (Erfolg) anzeigt, erweitern Sie Outputs (Ausgaben), um die AMI-Informationen anzuzeigen. Sie können Ihre SQL-Server-Instance für die VPC Ihrer Wahl mit der AMI-ID starten.
14. Öffnen Sie die Amazon EC2-Konsole. Wählen Sie im linken Navigationsbereich AMIs aus. Das neue AMI sollte angezeigt werden.
15. Um zu überprüfen, ob die neue Version von SQL Server erfolgreich installiert wurde, wählen Sie das neue AMI aus und klicken Sie auf Launch (Starten).
16. Wählen Sie den Typ der Instance, den das AMI haben soll, die VPC und das Subnetz, in das Sie bereitstellen möchten, und den Speicher, den Sie verwenden möchten. Da Sie die neue Instance von einem AMI starten, werden Ihnen die Volumes als Option angeboten, die in die neue EC2-Instance, die Sie starten, aufgenommen werden kann. Sie können alle diese Volumes entfernen oder Volumes hinzufügen.
17. Fügen Sie ein Tag (Markierung) hinzu, damit Sie Ihre Instance leichter identifizieren können.
18. Fügen Sie die Sicherheitsgruppe oder Gruppen zur Instance hinzu.
19. Wählen Sie Launch Instance aus.
20. Wählen Sie den Tag (Markierung)-Namen für die Instance und anschließend Connect (Verbinden) im Dropdown-Menü Actions (Aktionen) aus.
21. Vergewissern Sie sich, dass die neue SQL-Server-Version die Datenbank-Engine auf der neuen Instance ist.

Migrieren Sie eine Windows-Instance zu einem Instance-Typ der aktuellen Generation

Die AWS Windows-AMIs werden mit den Standardeinstellungen konfiguriert, die von den Microsoft-Installationsmedien verwendet werden, mit einigen Anpassungen. Zu den Anpassungen gehören Treiber und Konfigurationen, die die Instance-Typen der neuesten Generation unterstützen. Dabei handelt es sich um Instances, die auf dem AWS Nitro-System basieren, wie z. B. M5 oder C5.

Bei der Migration zu Nitro-basierten Instances, einschließlich Bare-Metal-Instances, empfehlen wir Ihnen, die Schritte in diesem Thema in den folgenden Fällen auszuführen:

- Wenn Sie Instances von benutzerdefinierten Windows-AMIs starten
- Wenn Sie Instances von Windows-AMIs von Amazon starten, die vor August 2018 erstellt wurden

Weitere Informationen finden Sie unter Amazon EC2-Update – zusätzliche Instance-Typen, Nitro-System und CPU-Optionen.

> **Note**
>
> Die folgenden Migrationsverfahren können unter Windows Server Version 2008 R2 und höher ausgeführt werden. Informationen zur Migration von Linux-Instances zu Instance-Typen der neuesten Generation finden Sie unter. the section called “Ändern des Instance-Typs”

Inhalt

> **Note**
>
> Alternativ können Sie mit dem Automatisierungsdokument `AWSSupport-UpgradeWindowsAWSDrivers` die in Teil 1, Teil 2 und Teil 3 beschriebenen Verfahren automatisieren. Wenn Sie sich für das automatisierte Verfahren entscheiden, lesen Sie (Alternative) Aktualisieren Sie die AWS PV-, ENA- und NVMe-Treiber mit AWS Systems Manager. Fahren Sie dann mit Teil 4 und Teil 5 fort.

Bevor Sie beginnen

Bei diesem Verfahren wird davon ausgegangen, dass Sie derzeit auf einem Xen-basierten Instance-Typ der vorherigen Generation, wie z. B. einer M4 oder C4, laufen und dass Sie zu einer Instanz migrieren, die auf dem Nitro System basiert. AWS

Sie müssen PowerShell Version 3.0 oder höher verwenden, um das Upgrade erfolgreich durchzuführen.

> **Note**
>
> Wenn Sie auf Instances der aktuellen Generation migrieren, können die statische IP oder benutzerdefinierte DNS-Netzwerkeinstellungen der vorhandenen ENI verloren gehen, da die Instance zu einem neuen Enhanced Networking-Adaptergerät wechselt.

Bevor Sie die Schritte in diesem Verfahren durchführen, empfehlen wir das Erstellen eines Backups der Instance. Wählen Sie in der EC2-Konsole die Instance aus, die die Migration benötigt, und öffnen Sie das Kontextmenü (rechte Maustaste), wählen Sie die Option Instance-Status und dann Stopp.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Um Daten auf Instance-Speicher-Volumes zu erhalten, stellen Sie sicher, dass Sie die Daten in einem persistenten Speicher sichern.

Öffnen Sie das Kontextmenü (rechte Maustaste) für die Instance in der EC2-Konsole, wählen Sie die Option Image und dann Image erstellen.

> **Note**
>
> Die Teile 4 und 5 dieser Anweisungen können abgeschlossen werden, nachdem Sie den Instanztyp auf die neueste Generation migriert oder geändert haben. Wir empfehlen jedoch, dass Sie sie vor der Migration abschließen, wenn Sie speziell zu einem Bare-Metal-Instance-Typ migrieren.

Teil 1: AWS PV-Treiber installieren und aktualisieren

Obwohl AWS PV-Treiber im Nitro-System nicht verwendet werden, sollten Sie sie dennoch aktualisieren, wenn Sie frühere Versionen von Citrix PV oder AWS PV verwenden. Die neuesten AWS PV-Treiber beheben Bugs in früheren Versionen der Treiber, die möglicherweise im Nitro-System auftreten oder falls Sie zurück zu einer Xen-basierten Instance migrieren. Als bewährte Methode empfehlen wir, immer auf die neuesten Treiber für Windows-Instanzen zu AWS aktualisieren.

Gehen Sie wie folgt vor, um ein direktes Upgrade von AWS PV-Treibern durchzuführen oder um unter Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 oder Windows Server 2019 von Citrix AWS PV-Treibern auf PV-Treiber zu aktualisieren. Weitere Informationen finden Sie unter Upgraden von PV-Treibern auf Windows-Instances.

Informationen zum Upgrade eines Domain-Controllers finden Sie unter Führen Sie ein Upgrade eines Domänencontrollers durch (AWS PV-Upgrade).

Um ein Upgrade von oder auf AWS PV-Treibern durchzuführen

1. Stellen Sie über Remote Desktop eine Verbindung mit der Instance her und bereiten Sie die Instance für das Upgrade vor. Schalten Sie den Systemdatenträger offline, bevor Sie das Upgrade durchführen. Wenn Sie eine direkte Aktualisierung von AWS PV-Treibern durchführen, ist dieser Schritt nicht erforderlich. Setzen Sie die Start-Option für alle nicht erforderlichen Services in der Services-Konsole auf Manual.
2. Laden Sie das aktuelle Treiberpaket in die Instance herunter.
3. Extrahieren Sie den Inhalt des Ordners und führen Sie die Datei `AWSPVDriverSetup.msi` aus.

Wenn Sie die MSI-Datei ausgeführt haben, wird die Instance automatisch neu gestartet und das Upgrade des Treibers durchgeführt. Die Instance kann für die Dauer von bis zu 15 Minuten nicht verfügbar sein.

Wenn das Upgrade abgeschlossen wurde und die Instance beide Zustandsprüfungen in der Amazon EC2-Konsole bestanden hat, stellen Sie über Remote Desktop eine Verbindung mit der Instance her und prüfen Sie, ob der neue Treiber installiert wurde. Suchen Sie im Geräte-Manager unter Storage Controllers den AWS PV Storage Host Adapter. Vergewissern Sie sich, dass die Treiberversion identisch mit der aktuellen Version in der Tabelle für den Treiber-Versionsverlauf ist. Weitere Informationen finden Sie unter AWS Verlauf des PV-Treiberpakets.

Teil 2: Installieren und aktualisieren von ENA

Führen Sie ein Upgrade auf den Elastic Network Adapter-Treiber durch, um sicherzustellen, dass alle Netzwerkfeatures unterstützt werden. Wenn Sie Ihre Instance gestartet haben und sie nicht über ein bereits aktiviertes erweitertes Netzwerk verfügt, müssen Sie den erforderlichen Netzwerkadaptertreiber auf Ihre Instance herunterladen und installieren. Setzen Sie dann das Attribut der enaSupport-Instance auf activate enhanced networking. Sie können dieses Attribut nur aus unterstützten Instance-Typen und nur bei installiertem ENA-Treiber aktivieren. Weitere Informationen finden Sie unter Aktivieren Sie Enhanced Networking mit dem Elastic Network Adapter (ENA) auf Ihren EC2-Instances.

1. Laden Sie den aktuellen Treiber in die Instance herunter.
2. Extrahieren Sie die ZIP-Datei.
3. Installieren Sie den Treiber, indem Sie das `install.ps1` PowerShell Skript aus dem extrahierten Ordner ausführen.

   > **Note**
   >
   > Führen Sie das `install.ps1`-Skript als Administrator aus, um Fehler bei der Installation zu vermeiden.

4. Überprüfen Sie, ob für Ihr AMI enaSupport aktiviert ist. Wenn nicht, fahren Sie fort, indem Sie der Dokumentation in Aktivieren Sie Enhanced Networking mit dem Elastic Network Adapter (ENA) auf Ihren EC2-Instances folgen.

Teil 3: Aktualisieren Sie die AWS NVMe-Treiber

AWS NVMe-Treiber werden verwendet, um mit Amazon EBS- und SSD-Instance-Speicher-Volumes zu interagieren, die für eine bessere Leistung als NVMe-Blockgeräte im Nitro-System verfügbar gemacht werden.

> **Important**
>
> Die folgenden Anweisungen wurden speziell für die Installation oder das Upgrade von AWS NVMe auf einer Instance der vorherigen Generation mit der Absicht geändert, die Instance auf den Instance-Typ der neuesten Generation zu migrieren.

1. Laden Sie das aktuelle Treiberpaket in die Instance herunter.
2. Extrahieren Sie die ZIP-Datei.
3. Installieren Sie den Treiber durch Ausführen von `dpinst.exe`.
4. Öffnen Sie eine PowerShellSitzung und führen Sie den folgenden Befehl aus:

   ```
   PS C:\> start rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
   ```

   > **Note**
   >
   > Um den Befehl anzuwenden, müssen Sie die PowerShell Sitzung als Administrator ausführen. PowerShell (x86) -Versionen führen zu einem Fehler.
   > Dieser Befehl führt nur sysprep auf den Gerätetreibern aus. Es wird nicht die gesamte Sysprep-Vorbereitung ausgeführt.

5. Fahren Sie für Windows Server 2008 R2 und Windows Server 2012 die Instance herunter, ändern Sie den Instance-Typ in eine Instance der neuesten Generation und starten Sie diese. Fahren Sie dann mit Teil 4 fort. Falls Sie die Instance noch einmal auf einem Instance-Typ der früheren Generation starten, bevor Sie eine Migration zu einem Instance-Typ der neuesten Generation durchgeführt haben, wird sie nicht gestartet. Bei anderen unterstützten Windows-AMIs können Sie den Instance-Typ nach dem sysprep-Befehl für das Gerät jederzeit ändern.

Teil 4: Aktualisieren von EC2Config und EC2Launch

Für Windows-Instances bieten EC2Config und EC2Launch zusätzliche Funktionen und Informationen bei Ausführung im Nitro-System, einschließlich EC2 Bare Metal. Der EC2Config-Service ist standardmäßig in AMIs für Windows Server-Versionen vor Windows Server 2016 enthalten. EC2Launch ersetzt den EC2Config-Service auf AMIs mit Windows Server 2016 und höher.

Wenn der EC2Config- und der EC2Launch-Service aktualisiert werden, verfügen neue Windows-AMIs in AWS über die aktuelle Version des Service. Sie müssen jedoch Ihre eigenen Windows-AMIs und Instances mit der aktuellen Version von EC2Config und EC2Launch aktualisieren.

So installieren oder aktualisieren Sie EC2Config

1. Laden Sie das EC2Config-Installationsprogramm herunter und entzippen Sie es.
2. Führen Sie `EC2Install.exe`. Eine vollständige Liste der verfügbaren Optionen erhalten Sie, wenn Sie `EC2Install` mit der Option `/?` ausführen. Standardmäßig werden Eingabeaufforderungen angezeigt. Um den Befehl ohne Eingabeaufforderungen auszuführen, verwenden Sie die Option `/quiet`.

Weitere Informationen finden Sie unter Installieren der neuesten Version von EC2Config.

So installieren oder aktualisieren Sie EC2Launch

1. Wenn Sie EC2Launch bereits auf einer Instance installiert und konfiguriert haben, erstellen Sie ein Backup der EC2Launch-Konfigurationsdatei. Beim Installationsprozess werden Änderungen an dieser Datei nicht übernommen. Standardmäßig befindet sich die Datei im Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.
2. Laden Sie die Datei EC2-Windows-Launch.zip in ein Verzeichnis auf der Instance herunter.
3. Laden Sie die Datei install.ps1 in dasselbe Verzeichnis herunter, in das Sie `EC2-Windows-Launch.zip` heruntergeladen haben.
4. Führen Sie `install.ps1`.

> **Note**
>
> Führen Sie das `install.ps1`-Skript als Administrator aus, um Fehler bei der Installation zu vermeiden.

5. Wenn Sie ein Backup der EC2Launch-Konfigurationsdatei erstellt haben, kopieren Sie sie in das Verzeichnis `C:\ProgramData\Amazon\EC2-Windows\Launch\Config`.

Weitere Informationen finden Sie unter Konfigurieren einer Windows-Instance mithilfe von EC2Launch.

Teil 5: Installieren des Treibers für den seriellen Port für Bare Metal-Instances

Der `i3.metal`-Instance-Typ nutzt anstelle eines auf dem I/O-Port basierenden seriellen Geräts ein PCI-basiertes serielles Gerät. Die neuesten Windows-AMIs verwenden automatisch PCI-basierte serielle Geräte und haben den Treiber für den seriellen Port installiert. Falls Sie keine Instance verwenden, die über eine von Amazon bereitgestellte Windows-AMI mit Datum vom 2018.04.11 oder später gestartet wurde, müssen Sie den Treiber für den seriellen Port installieren, um das serielle Gerät für EC2-Features zu aktivieren, wie etwa Passwortgenerierung und Konsolenausgabe. Die neuesten EC2Config- und EC2Launch-Utilities unterstützen auch i3.metal und bieten zusätzliche Funktionen. Folgen Sie den Schritten in Teil 4, wenn Sie dies noch nicht getan haben.

So installieren Sie den Treiber für die serielle Schnittstelle

1. Laden Sie das Paket für den seriellen Treiber in die Instance herunter.
2. Extrahieren Sie die Inhalte des Ordners, klicken Sie mit der rechten Maustaste auf `aws_ser.INF` und wählen Sie Installieren aus.
3. Klicken Sie auf Okay.

Teil 6: Aktualisieren der Energieverwaltungseinstellungen

Mit der folgenden Aktualisierung werden die Energiespareinstellungen so konfiguriert, dass Bildschirme nie ausgeschaltet werden. So kann das Betriebssystem auf Nitro-Systemen korrekt heruntergefahren werden. Alle von Amazon seit 2018.11.28 bereitgestellten Windows-AMIs verfügen bereits über diese Standardkonfiguration.

1. Öffnen Sie eine Eingabeaufforderung oder eine PowerShell Sitzung.
2. Führen Sie die folgenden Befehle aus:

```
powercfg /setacvalueindex 381b4222-f694-41f0-9685-ff5bb260df2e 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex 8c5e7fda-e8bf-4a96-9a85-a6e23a8c635c 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
powercfg /setacvalueindex a1841308-3541-4fab-bc81-f71556f20b4a 7516b95f-
f776-4464-8c53-06167f40cc99 3c0bc021-c8a8-4e07-a973-6b14cbcb2b7e 0
```

Teil 7: Aktualisieren von Intel-Chipsatz-Treibern für neue Instance-Typen

Bei den Instance-Typen `u-6tb1.metal`, `u-9tb1.metal` und `u-12tb1.metal` wird Hardware verwendet, für die Chipsatz-Treiber erforderlich sind, die zuvor nicht auf Windows-AMIs installiert waren. Falls Sie keine Instance verwenden, die über ein von Amazon bereitgestelltes Windows-AMI mit der Datumsangabe 2018.11.19 oder später gestartet wurde, müssen Sie die Treiber mit Intel Chipset INF Utility installieren.

So installieren Sie die Chipsatz-Treiber

1. Laden Sie das Chipsatz-Hilfsprogramm auf die Instance herunter.
2. Extrahieren Sie die Dateien.
3. Führen Sie `SetupChipset.exe`.
4. Akzeptieren Sie die Software-Lizenzvereinbarung von Intel und installieren Sie die Chipsatz-Treiber.
5. Starten Sie die Instance neu.

(Alternative) Aktualisieren Sie die AWS PV-, ENA- und NVMe-Treiber mit AWS Systems Manager

Das Automatisierungsdokument `AWSSupport-UpgradeWindowsAWSDrivers` automatisiert die in Teil 1, Teil 2 und Teil 3 beschriebenen Schritte. Diese Methode kann auch eine Instance reparieren, bei der die Treiber-Upgrades fehlgeschlagen sind.

Das `AWSSupport-UpgradeWindowsAWSDrivers` Automatisierungsdokument aktualisiert oder repariert Speicher- und AWS Netzwerktreiber auf der angegebenen EC2-Instance. In dem Dokument wird versucht, die neuesten AWS Treiberversionen online zu installieren, indem der AWS Systems Manager Agent (SSM-Agent) aufgerufen wird. Wenn der SSM-Agent nicht erreichbar ist, kann das Dokument auf ausdrücklichen Wunsch eine Offline-Installation der AWS Treiber durchführen.

> **Note**
>
> Dieses Verfahren schlägt auf einem Domain-Controller fehl. Weitere Informationen zum Aktualisieren der Treiber auf einem Domain-Controller finden Sie unter Führen Sie ein Upgrade eines Domänencontrollers durch (AWS PV-Upgrade).

Um die AWS PV-, ENA- und NVMe-Treiber automatisch zu aktualisieren, verwenden Sie AWS Systems Manager

1. Öffnen Sie die Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager.
2. Wählen Sie Automation und dann Execute Automation.
3. Suchen Sie nach dem AWSSupport UpgradeWindows AWSDrivers Automatisierungsdokument, wählen Sie es aus und wählen Sie dann Automatisierung ausführen aus.
4. Konfigurieren Sie im Abschnitt Eingabeparameter die folgenden Optionen:

   Instance-ID

   Geben Sie die eindeutige ID der zu aktualisierenden Instance ein.

   AllowOffline

   (Optional) Wählen Sie eine der folgenden Optionen:

   - `True` — Wählen Sie diese Option, um eine Offline-Installation durchzuführen. Die Instance wird während des Upgrade-Prozesses gestoppt und neu gestartet.

     > **Warning**
     >
     > Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Um Daten auf Instance-Speicher-Volumes zu erhalten, stellen Sie sicher, dass Sie die Daten in einem persistenten Speicher sichern.

   - `False` — (Default (Standard)) Lassen Sie diese Option aktiviert. um eine Online-Installation durchzuführen. Die Instance wird während des Upgrade-Prozesses neu gestartet.

     > **Important**
     >
     > Online- und Offline-Upgrades erstellen ein AMI, bevor sie den Upgrade-Vorgang durchführen. Das AMI bleibt auch nach Abschluss der Automatisierung erhalten. Sichern Sie sich Ihren Zugriff auf das AMI oder löschen Sie es, wenn es nicht mehr benötigt wird.

SubnetId

(Optional) Geben Sie einen der folgenden Werte ein:

- `SelectedInstanceSubnet` (Default (Standard)) Der Upgrade-Prozess startet die Instance helper im selben Subnetz wie die zu aktualisierende Instance. Das Subnetz muss die Kommunikation zu den Systems Manager-Endpunkten (`ssm.*`) ermöglichen.
- `CreateNewVPC` — Der Upgrade-Prozess startet die Instance helper in einer neuen VPC. Verwenden Sie diese Option, wenn Sie nicht sicher sind, ob das Subnetz der Ziel-Instance die Kommunikation mit den `ssm.*`-Endpunkten zulässt. Ihr -Benutzer muss die Berechtigung haben, eine VPC zu erstellen.
- Eine bestimmte Subnetz-ID — Geben Sie die ID eines bestimmten Subnetzes an, in dem die Instance helper gestartet werden soll. Das Subnetz muss sich in der gleichen Availability Zone wie die zu aktualisierende Instance befinden und die Kommunikation mit den `ssm.*`-Endpunkten ermöglichen.

5. Wählen Sie Execute (Ausführen).
6. Warten Sie auf den Abschluss des Upgrades. Es kann bis zu 10 Minuten dauern, ein Online-Upgrade durchzuführen. Es kann bis zu 25 Minuten dauern, ein Offline-Upgrade durchzuführen.

Migrieren Sie eine Windows-Instanz von Nitro zu Xen-Instanztypen

Beim folgenden Verfahren wird davon ausgegangen, dass Sie derzeit auf einem Nitro-basierten Instanztyp arbeiten und dass Sie zu einer Instanz migrieren, die auf dem Xen-System basiert, z. B. M4 oder C4. Spezifikationen für Instance-Typen finden Sie im Amazon EC2 Instance Types Guide. Führen Sie vor der Migration die folgenden Schritte durch, um Fehler während des Startvorgangs zu vermeiden.

Um von Nitro zu Xen zu migrieren

1. Sichern Sie Ihre Daten.
2. Vergewissern Sie sich, dass Ihre Windows-SAN-Richtlinie es zulässt, dass Speichervolumes, die keine Root-Dateien sind, online geschaltet werden.
3. AWS PV-Treiber müssen auf einer Nitro-Instanz installiert und aktualisiert werden, bevor Sie zu einer Xen-Instanz migrieren. Schritte zur Installation und Aktualisierung von AWS PV-Treibern finden Sie unterTeil 1: AWS PV-Treiber installieren und aktualisieren.

4. Auf die neueste EC2Launch v2-Version aktualisieren. Die Schritte finden Sie unter Migrieren zu EC2Launch v2.
5. Öffnen Sie eine PowerShell Sitzung und führen Sie als Administrator den folgenden Befehl aus, um die Gerätetreiber zu sysprep zu konfigurieren. Durch die Ausführung von sysprep wird sichergestellt, dass die für den Start von Xen-Instances erforderlichen frühen Boot-Speichertreiber ordnungsgemäß bei Windows registriert sind.

   > **Note**
   >
   > Die Ausführung des Befehls mit PowerShell (x86-) Versionen führt zu einem Fehler. Dieser Befehl fügt der kritischen Gerätedatenbank nur die bootkritischen Gerätetreiber hinzu. Es wird nicht die gesamte Sysprep-Vorbereitung ausgeführt.

   ```
   Start-Process rundll32.exe sppnp.dll,Sysprep_Generalize_Pnp -wait
   ```

6. Führen Sie die Migration auf einen Xen-Instance-Typ durch, wenn der Sysprep-Prozess abgeschlossen ist.

Assistent zur Umstellung von Windows auf Linux für Microsoft SQL Server-Datenbanken

Informationen zur Platformierung von Microsoft SQL Server-Datenbanken von Windows auf Linux finden Sie unter Windows to Linux Replatforming Assistant for Microsoft SQL Server Databases im Microsoft SQL Server on Amazon EC2 EC2-Benutzerhandbuch.

Beheben Sie Fehler bei einem Upgrade auf einer Windows-Instance

AWS bietet Upgrade-Support bei Problemen oder Problemen mit dem Upgrade Helper Service, einem AWS Hilfsprogramm, mit dem Sie direkte Upgrades mit Citrix PV-Treibern durchführen können.

Nach dem Upgrade verzeichnet die Instance möglicherweise eine überdurchschnittlich hohe CPU-Nutzung, während der .NET Runtime Optimization Service das .Net Framework optimiert. Dieses Verhalten wird erwartet.

Wenn nach einigen Stunden noch nicht beide Statusprüfungen auf der Instance erfolgreich beendet wurden, überprüfen Sie Folgendes.

- Wenn Sie ein Upgrade auf Windows Server 2008 vorgenommen haben und nach einigen Stunden beide Statusprüfungen fehlschlagen, ist das Upgrade möglicherweise fehlgeschlagen und die Eingabeaufforderung Click OK zum Bestätigen des Zurücksetzens wird angezeigt. Da in diesem Status nicht auf die Konsole zugegriffen werden kann, ist es nicht möglich, auf die Schaltfläche zu klicken. Führen Sie einen Neustart über die Amazon EC2-Konsole oder API aus, um dies zu umgehen. Die Initiierung des Neustarts dauert zehn Minuten oder länger. Die Instance ist möglicherweise nach 25 Minuten verfügbar.
- Entfernen Sie Anwendungen oder Serverrollen vom Server und versuchen Sie es erneut.

Wenn nach dem Entfernen der Anwendungen oder Serverrollen vom Server nicht beide Statusprüfungen auf der Instance erfolgreich beendet werden, führen Sie die folgenden Schritte aus.

- Beenden Sie die Instance und fügen Sie das Stamm-Volume an eine andere Instance an. Weitere Informationen finden Sie in der Beschreibung zum Beenden und Anfügen des Stamm-Volumes an eine andere Instance in Warten auf Metadaten-Service.
- Analysieren Sie die Windows-Setup-Protokolldateien und -Ereignisprotokolle hinsichtlich Fehlern.

Bei anderen Fehlern oder Problemen mit einem Betriebssystem-Upgrade oder der Migration empfehlen wir die Lektüre der in Bevor Sie ein direktes Upgrade beginnen aufgelisteten Artikel.

EC2-Flotte und Spot-Flotte

EC2-Flotte und Spot-Flotte sind als nützliche Methode zum Starten einer Flotte oder einer Gruppe von Instances mit AWS konzipiert. Jede Instance in einer Flotte basiert auf einer Startvorlage oder einer Reihe von Startparametern, die Sie beim Start manuell konfigurieren.

Flottenpläne bieten die folgenden Features und Vorteile. Diese Vorteile ermöglichen es Ihnen, Ihre Kosteneinsparungen zu maximieren und Verfügbarkeit und Leistung zu optimieren, wenn Sie Anwendungen auf mehreren EC2-Instances ausführen.

Mehrere Instance-Typen und Kaufoptionen

In einem einzigen API-Aufruf kann eine Flotte mehrere Instance-Typen und Kaufoptionen (Spot- und On-Demand-Instances) starten, sodass Sie die Kosten durch Spot-Instance-Nutzung optimieren können. Sie können auch Rabatte für Reserved Instances und Savings Plan nutzen, indem Sie sie in Verbindung mit On-Demand-Instances in der Flotte verwenden.

Aufteilen von Instances in mehrere Availability Zones

Eine Flotte versucht automatisch, Instances gleichmäßig auf mehrere Availability Zones zu verteilen, um eine hohe Verfügbarkeit zu gewährleisten. Dies bietet Ausfallsicherheit für den Fall, dass eine Availability Zone nicht verfügbar ist.

Automatischer Ersatz von Spot Instances

Wenn Ihre Flotte Spot Instances umfasst, kann sie automatisch Ersatz-Spot-Kapazität anfordern, falls Ihre Spot Instances aufgrund einer Änderung des Instance-Zustands unterbrochen oder beeinträchtigt werden. Durch den Kapazitätsausgleich kann eine Flotte auch Ihre Spot Instances überwachen und proaktiv ersetzen, die einem erhöhten Risiko einer Unterbrechung ausgesetzt sind.

EC2 Fleet ist eine gute Option, wenn Sie Flexibilität bei der Verwaltung von Aspekten des Instance-Lebenszyklus oder der Skalierungsmechanismen benötigen. Sie können auch Spot-Flotte verwenden, aber wir raten Ihnen davon ab, dies zu tun, da es sich um eine veraltete API ohne geplante Investitionen handelt. Wenn Sie Spot-Flotte jedoch bereits verwenden, können Sie es weiterhin verwenden. Spot-Flotte und EC2-Flotte bieten dieselbe Kernfunktionalität.

> **Tip**
>
> Als allgemeine bewährte Methode empfehlen wir, lieber Flotten von Spot- und On-Demand-Instances mit Amazon EC2 Auto Scaling zu starten, da es zusätzliche Funktionen bietet, mit denen Sie Ihre Flotte verwalten können. Die Liste der zusätzlichen Features umfasst den automatischen Ersatz von Zustandsprüfungen für Spot und On-Demand-Instances, anwendungsbasierte Zustandsprüfungen und eine Integration mit Elastic Load Balancing, um eine gleichmäßige Verteilung des Anwendungsverkehrs auf Ihre fehlerfreien Instances sicherzustellen. Sie können Auto Scaling Scaling-Gruppen auch verwenden, wenn Sie AWS Dienste wie Amazon ECS, Amazon EKS (selbstverwaltete Knotengruppen) und Amazon VPC Lattice verwenden. Weitere Informationen hierzu finden Sie im Amazon EC2 Auto Scaling-Benutzerhandbuch.

Themen

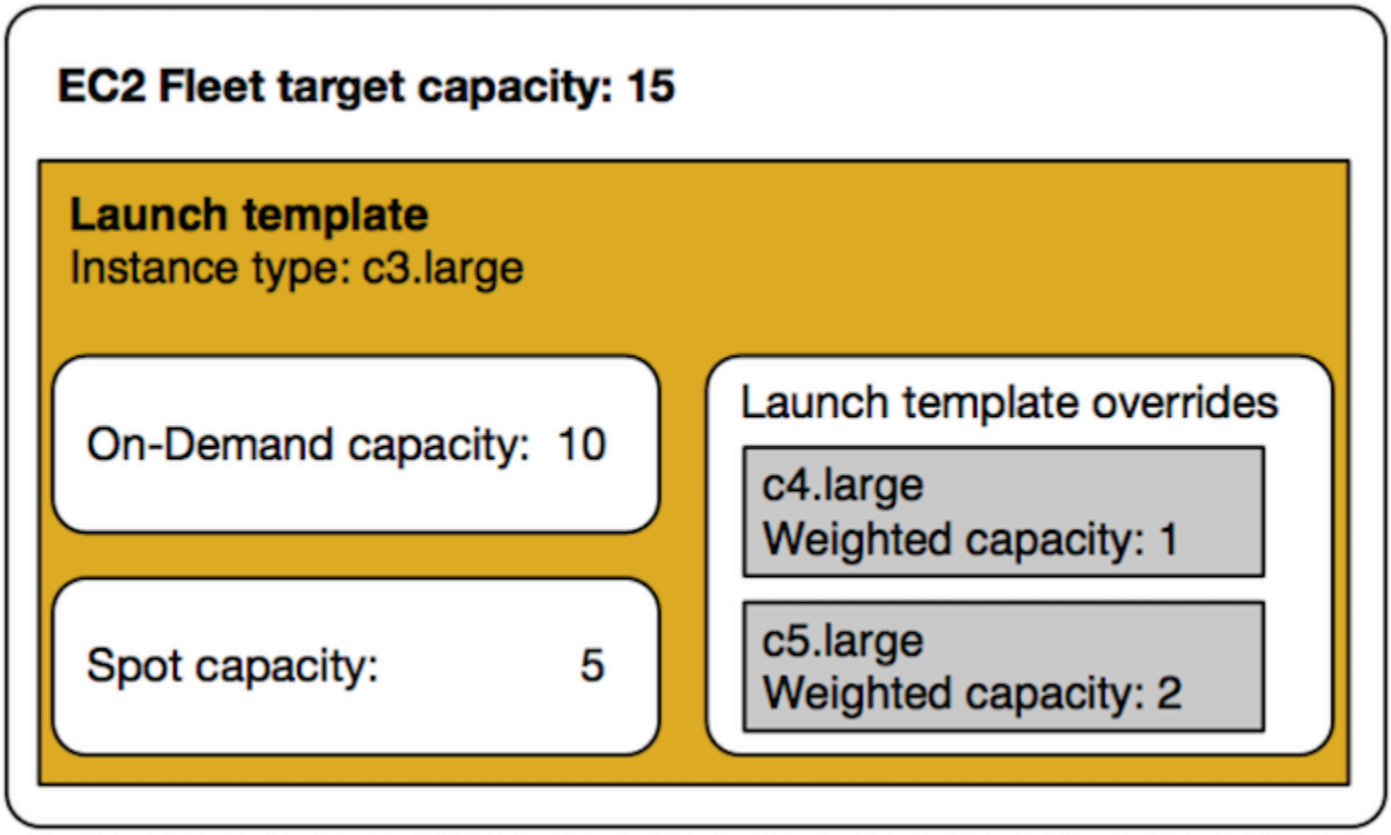
EC2-Flotte

Eine EC2-Flotte enthält die Konfigurationsinformationen zum Starten einer Flotte von Instances. In einem einzigen API-Aufruf kann eine Flotte mehrere Instance-Typen über mehrere Availability Zones hinweg mit der Spot Instance, On-Demand-Instance-, Reserved-Instance- und Savings-Plan-Kaufoptionen starten. Mit EC2-Flotte können Sie:

- Separate Ziele für Spot- und On-Demand-Kapazitäten und den Höchstbetrag, den Sie pro Stunde zu zahlen bereit sind, definieren
- Den Instance-Typ angeben, der sich für Ihre Anwendungen am besten eignet
- Angeben, wie Amazon EC2 im Rahmen der einzelnen Kaufoptionen Ihre Flottenkapazität verteilen soll

Sie können auch festlegen, wie viel Sie maximal pro Stunden für Ihre Flotte bereit sind zu zahlen. Dann startet EC2-Flotte Instances, bis der Maximalbetrag verbraucht ist. Wenn der Maximalbetrag erreicht ist, den Sie bereit sind zu zahlen, startet die Flotte keine Instances mehr, auch wenn die Zielkapazität noch nicht erreicht ist.

Das EC2-Flotte versucht, die Anzahl der Instances zu starten, die erforderlich sind, um die in Ihrer Anfrage angegebene Zielkapazität zu erreichen. Wenn Sie einen Maximalpreis pro Stunde angegeben haben, wird die Kapazität erfüllt, bis die Summe erreicht ist, die Sie maximal bereit sind zu zahlen. Die Flotte kann auch versuchen, ihre Ziel-Spot-Kapazität zu erhalten, wenn Ihre Spot-Instances unterbrochen sind. Weitere Informationen finden Sie unter Funktionsweise von Spot-Instances.



Sie können eine unbegrenzte Anzahl von Instance-Typen pro EC2-Flotte angeben. Diese Instance-Typen können sowohl mit Spot- als auch mit On-Demand-Kaufoptionen bereitgestellt werden. Sie können auch mehrere Availability Zones angeben, unterschiedliche maximale Spot-Preise für jede Instance festlegen und zusätzliche Spot-Optionen für jede Flotte angeben. Amazon EC2 verwendet die angegebenen Optionen zur Bereitstellung von Kapazität, wenn die Flotte gestartet wird.

Wenn Amazon EC2 eine Spot-Instance wegen einer Preiserhöhung oder eines Instance-Ausfalls zurückfordert, während die Flotte ausgeführt wird, kann die EC2-Flotte versuchen, die Instances

durch einen der von Ihnen angegebenen Instance-Typen zu ersetzen. Dies erleichtert die Wiedererlangung der Kapazität während eines Anstiegs der Spot-Preise. Sie können für jede Flotte eine flexible und elastische Beschaffungsstrategie entwickeln. Beispielsweise können Sie innerhalb bestimmter Flotten Ihre Primärkapazität bei Bedarf durch weniger teure Spotkapazität ergänzen, wenn diese verfügbar ist.

Wenn Sie Reserved Instances haben und Sie On-Demand-Instances in Ihrer Flotte angeben, verwendet EC2-Flotte Ihre Reserved Instances. Wenn Ihre Flotte beispielsweise eine On-Demand-Instance als `c4.large` angibt und Sie Reserved Instances für `c4.large` haben, erhalten Sie die Reserved Instance-Preise. Das Gleiche gilt, wenn Sie einen Savings Plan verwenden.

Für die Nutzung von EC2-Flotte fallen keine zusätzlichen Gebühren an. Sie zahlen nur für die EC2 Instances, die die Flotte für Sie startet.

Inhalt

EC2-Flotte-Einschränkungen

Die folgenden Einschränkungen gelten für EC2-Flotte:

- EC2-Flotte ist nur über Amazon EC2-API, AWS CLI, AWS -SDKs und AWS CloudFormation verfügbar.
- Eine EC2-Flottenanfrage kann sich nicht über mehrere Regionen erstrecken. AWS Sie müssen für jede Region eine eigene EC2-Flotte anlegen.
- Eine EC2-Flotte-Anfrage darf sich nicht über verschiedene Subnetze in derselben Availability Zone erstrecken.

Instances mit Spitzenlastleistung

Wenn Sie Ihre Spot-Instances mit einem Typ von Burstable Performance Instance starten, und wenn Sie planen, Ihre Spot-Instances mit Spitzenlastleistung sofort und für eine kurze Dauer zu

verwenden, ohne Leerlaufzeit für die Anrechnung von CPU-Guthaben, empfiehlt sich, diese im Standard mode (Standardmodus) zu starten, um höhere Kosten zu vermeiden. Wenn Sie die Spot-Instances mit Spitzenlastleistung im Unlimited mode (Unbegrenzten Modus) starten und die Spitzenlastleistung der CPU sofort nutzen, geben Sie überschüssiges Guthaben für Spitzen aus. Wenn Sie die Instance für eine kurze Zeit nutzen, hat die Instance keine Zeit, CPU-Guthaben zu sammeln, um das überschüssige Guthaben zu bezahlen. Das überschüssige Guthaben wir beim Beenden der Instance abgerechnet.

Der unbegrenzte Modus für Spot-Instances mit Spitzenlastleistung ist nur dann geeignet, wenn die Instance lange genug läuft, um CPU-Guthaben für Spitzen zu erhalten. Andernfalls macht das Bezahlen für überzähliges Guthaben die Spot-Instances mit Spitzenlastleistung teurer als die Verwendung anderer Instances. Weitere Informationen finden Sie unter Verwendung des unbegrenzten Modus im Vergleich zu einer festen CPU.

Startguthaben sollen eine produktive erste Starterfahrung für T2-Instances bieten, indem sie ausreichende Rechenressourcen zur Verfügung gestellt werden, um die Instance zu konfigurieren. Wiederholte Starts von T2-Instances, um neue Startguthaben zu erhalten, sind nicht zulässig. Wenn Sie dauerhaft eine CPU benötigen, können Sie Guthaben verdienen (durch Leerlauf über einen gewissen Zeitraum), Unbegrenzten Modus für T2 Spot-Instances verwenden oder einen Instance-Typ mit dedizierter CPU verwenden.

EC2-Flotte-Anforderungstypen

Es gibt drei Arten von EC2-Flotte-Anforderungen:

`instant`

Wenn Sie den Anforderungstyp als `instant` konfigurieren, erstellt EC2-Flotte eine einmalige, synchrone Anforderung für Ihre gewünschte Kapazität. In der API-Antwort gibt er die gestarteten Instances zurück sowie die Fehler für Instances, die nicht gestartet werden konnten. Weitere Informationen finden Sie unter Verwenden einer EC2-Flotte des Typs „Instant“.

`request`

Wenn Sie den Anforderungstyp als `request` konfigurieren, erstellt EC2-Flotte eine einmalige, asynchrone Anforderung für Ihre gewünschte Kapazität. Dann versucht die Flotte nicht, Spot-Instances aufzufüllen, wenn die Kapazität aufgrund von Spot-Unterbrechungen verringert ist, und sie stellt keine Anträge in alternativen Spot-Kapazitätspools, wenn die Kapazität nicht verfügbar ist.

`maintain`

(Standard) Wenn Sie den Anforderungstyp als `maintain` konfigurieren, erstellt EC2-Flotte eine asynchrone Anforderung für Ihre gewünschte Kapazität und erhält die Kapazität aufrecht, indem sie alle unterbrochenen Spot-Instances automatisch auffüllt.

Alle drei Anfragetypen profitieren von einer Zuweisungsstrategie. Weitere Informationen finden Sie unter Zuweisungsstrategien für Spot-Instances.

Verwenden einer EC2-Flotte des Typs „Instant“

Die EC2-Flotte des Typs Instant ist eine einmalige, synchrone Anforderung, die nur einen Versuch macht, die gewünschte Kapazität zu starten. Die API-Antwort gibt die gestarteten Instances zurück sowie die Fehler für Instances, die nicht gestartet werden konnten. Die Verwendung einer EC2-Flotte des Typs Instant, die in diesem Artikel beschrieben werden, hat mehrere Vorzüge. Beispielkonfigurationen finden Sie am Ende des Artikels.

Für Workloads, die eine reine Start-API zum Starten von EC2-Instances benötigen, können Sie die API verwenden. RunInstances Mit können Sie RunInstances jedoch nur On-Demand-Instances oder Spot-Instances starten, aber nicht beide in derselben Anfrage. Wenn Sie RunInstances Spot-Instances starten, ist Ihre Spot-Instance-Anfrage außerdem auf einen Instance-Typ und eine Availability Zone beschränkt. Dies zielt auf einen Spot-Kapazitätspool ab (eine Reihe von unbenutzten Instances mit gleichem Instance-Typ und gleicher Availability Zone). Wenn der Spot-Kapazitätspool nicht über genügend Spot-Instance-Kapazität für Ihre Anfrage verfügt, schlägt der RunInstances Anruf fehl.

Anstatt Spot-Instances RunInstances zum Starten von Spot-Instances zu verwenden, empfehlen wir Ihnen, die CreateFleet API mit dem `type` Parametersatz auf zu zu verwenden, `instant` um die folgenden Vorteile zu erzielen:

- Launchen von On-Demand-Instances und Spot Instances in einer Anforderung. Eine EC2-Flotte kann On-Demand-Instances, Spot-Instances oder beides starten. Die Anforderung für Spot-Instances ist erfüllt, wenn ausreichend Kapazität verfügbar ist und der maximale Preis pro Stunde für Ihre Anforderung den Spot-Preis überschreitet.
- Erhöhen Sie die Verfügbarkeit von Spot Instances. Durch die Verwendung einer EC2-Flotte des Typs `instant` können Sie Spot-Instances nach den Bewährte Methoden für Spot mit den daraus resultierenden Vorteilen starten:
  - Bewährte Methoden für Spot: Flexibel sein bei Instance-Typen und Availability Zones.

Vorteil: Durch die Angabe mehrerer Instance-Typen und Availability Zones erhöhen Sie die Anzahl der Spot-Kapazitätspools. Dies gibt dem Spot-Dienst eine bessere Chance, die gewünschte Spot-Rechenkapazität zu finden und zuzuweisen. Eine gute Faustregel besteht darin, für jeden Workload über mindestens 10 Instance-Typen hinweg flexibel zu sein und sicherzustellen, dass alle Availability Zones für die Verwendung in Ihrer VPC konfiguriert sind.

- Bewährte Methode für Spot: Verwenden Sie die price-capacity-optimized Zuweisungsstrategie.

  Vorteil: Die `price-capacity-optimized` Zuweisungsstrategie identifiziert Instances aus den Spot-Kapazitätspools mit der höchsten Verfügbarkeit und stellt dann automatisch Instances aus den kostengünstigsten dieser Pools bereit. Da Ihre Spot-Instance-Kapazität aus Pools mit optimaler Kapazität bezogen wird, verringert dies die Möglichkeit, dass Ihre Spot-Instances unterbrochen werden, wenn Amazon EC2 die Kapazität zurück braucht.

- Erhalten Sie Zugriff auf eine breitere Palette von Funktionen. Verwenden Sie für Workloads, die eine API nur für den Start benötigen und bei denen Sie es vorziehen, den Lebenszyklus Ihrer Instance zu verwalten, anstatt ihn von EC2 Fleet für Sie verwalten zu lassen, den Typ EC2 Fleet anstelle der API. `instant` RunInstances EC2 Fleet bietet ein breiteres Spektrum an Funktionen als RunInstances, wie in den folgenden Beispielen gezeigt. Für alle anderen Workloads sollten Sie Amazon EC2 Auto Scaling verwenden, da es ein umfassenderes Feature-Umfang für eine Vielzahl von Workloads bietet, wie beispielsweise ELB-unterstützte Anwendungen, containerisierte Workloads und Warteschlangenverarbeitungsaufträge.

Sie können eine EC2-Flotte vom Typ instant verwenden, um Instances in Kapazitätsblöcken zu starten. Weitere Informationen finden Sie unter Tutorial: Starten von Instances in Kapazitätsblöcken.

AWS Dienste wie Amazon EC2 Auto Scaling und Amazon EMR verwenden EC2 Fleet vom Typ Instant, um EC2-Instances zu starten.

Voraussetzungen für EC2-Flotte des Typs Instant

Informationen zu den Voraussetzungen für das Erstellen einer EC2-Flotte finden Sie unter EC2-Flotte-Voraussetzungen.

So funktioniert die Instant-EC2-Flotte

Bei der Arbeit mit einer EC2-Flotte des Typs `instant` lautet die Ereignisabfolge wie folgt:

1. Konfigurieren Sie den Anfragetyp CreateFleetals. `instant` Weitere Informationen finden Sie unter Erstellen einer EC2-Flotte. Beachten Sie, dass Sie den API-Aufruf nicht ändern können, nachdem Sie ihn machen.
2. Wenn Sie den API-Aufruf durchführen, erstellt EC2-Flotte eine einmalige, synchrone Anforderung für Ihre gewünschte Kapazität.
3. Die API-Antwort gibt die gestarteten Instances zurück sowie die Fehler für Instances, die nicht gestartet werden konnten.
4. Sie können Ihre EC2-Flotte beschreiben, die mit Ihrer EC2-Flotte verknüpften Instances auflisten und den Verlauf Ihrer EC2-Flotte anzeigen.
5. Nach dem Start Ihrer Instances können Sie die Flottenanfrage löschen. Wenn Sie die Flottenanforderung löschen, können Sie auch die zugeordneten Instances beenden oder diese laufen lassen.
6. Sie können die Instances jederzeit beenden.

Beispiele

In den folgenden Beispielen wird gezeigt, wie Sie eine EC2-Flotte des Typs `instant` für verschiedene Anwendungsfälle nutzen. Weitere Informationen zur Verwendung der CreateFleet EC2-API-Parameter finden Sie CreateFleetin der Amazon EC2 EC2-API-Referenz.

Beispiele

- Beispiel 1: Starten von Spot-Instances mit der kapazitätsoptimierten Zuweisungsstrategie
- Beispiel 2: Starten einer einzelnen Spot-Instance mit der kapazitätsoptimierten Zuweisungsstrategie
- Beispiel 3: Starten einer Spot-Instance mit Instance-Gewichtung
- Beispiel 4: Starten von Spot-Instances innerhalb einer einzelnen Availability Zone
- Beispiel 5: Starten von Spot-Instances eines einzelnen Instance-Typs innerhalb einer Availability Zone
- Beispiel 6: Spot-Instances nur starten, wenn minimale Zielkapazität gestartet werden kann
- Beispiel 7: Starten Sie Spot-Instances nur, wenn die minimale Zielkapazität desselben Instance-Typs in einer einzigen Availability Zone gestartet werden kann
- Beispiel 8: Starten von Instances mit mehreren Startvorlagen
- Beispiel 9: Starten von Spot-Instance mit einer Basis von On-Demand-Instances

- Beispiel 10: Starten von Spot-Instances mit kapazitätsoptimierter Zuweisungsstrategie mit einer Basis von On-Demand-Instances unter Verwendung von Kapazitätsreservierungen und der priorisierten Zuweisungsstrategie
- Beispiel 11: Starten Sie Spot-Instances mithilfe einer capacity-optimized-prioritized Zuweisungsstrategie

Beispiel 1: Starten von Spot-Instances mit der kapazitätsoptimierten Zuweisungsstrategie

Das folgende Beispiel gibt die Parameter an, die in einer EC2-Flotte des Typs `instant` benötigt werden: eine Startvorlage, eine Zielkapazität, eine Standard-Kaufoption und Startvorlagenüberschreibungen.

- Die Startvorlage wird durch ihren Startvorlagennamen und die Versionsnummer identifiziert.
- In den 12 Startvorlagenüberschreibungen werden 4 verschiedene Instance-Typen und 3 verschiedene Subnetze angegeben, die sich jeweils in einer separaten Availability Zone befinden. Jeder Instance-Typ und jede Subnetzkombination definiert einen Spot-Kapazitätspool, der zu 12 Spot-Kapazitätspools führt.
- Die Mindest-Zielkapazität für die Flotte ist 20 Instances.
- Die standardmäßige Kaufoption ist `spot`, wodurch die Flotte versucht, 20 Spot-Instances in dem Spot-Kapazitätspool zu starten, der über die optimale Kapazität für die Anzahl der zu startenden Instances verfügt.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
```

```
            "InstanceType":"c5.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.large",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.large",
            "SubnetId":"subnet-49e41922"
         }
      ]
```

```
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 2: Starten einer einzelnen Spot-Instance mit der kapazitätsoptimierten Zuweisungsstrategie

Sie können jeweils eine Spot-Instance optimal starten, indem Sie mehrere EC2 Fleet API-Aufrufe des Typs ausführen`instant`, indem Sie den TotalTargetCapacity Wert auf 1 setzen.

Das folgende Beispiel gibt die Parameter an, die in einer EC2-Flotte des Typs Instant benötigt werden: eine Startvorlage, eine Zielkapazität, eine Standard-Kaufoption und Startvorlagenüberschreibungen. Die Startvorlage wird durch ihren Startvorlagennamen und die Versionsnummer identifiziert. Die 12 Startvorlagenüberschreibungen haben 4 verschiedene Instance-Typen und 3 verschiedene Subnetze, die sich jeweils in einer separaten Availability Zone befinden. Die Zielkapazität für die Flotte beträgt 1 Instance und die Standardeinkaufoption ist Spot, was dazu führt, dass die Flotte versucht, eine Spot-Instance aus einem der 12 Spot-Kapazitätspools basierend auf der kapazitätsoptimierten Zuweisungsstrategie zu starten, um eine Spot-Instance aus dem am meisten verfügbaren Kapazitätspool zu starten.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab"
```

```
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
   ],
```

```
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 3: Starten einer Spot-Instance mit Instance-Gewichtung

Die folgenden Beispiele verwenden die Instance-Gewichtung, d. h. der Preis versteht sich pro Einheitsstunde anstatt pro Instance-Stunde. Jede Startkonfiguration listet einen anderen Instance-Typ und eine andere Gewichtung auf, je nachdem, wie viele Einheiten des Workloads auf der Instance ausgeführt werden können, sofern eine Einheit der Workload 15 GB Arbeitsspeicher und 4 vCPUs benötigt. Zum Beispiel kann ein m5.xlarge (4 vCPUs und 16 GB Speicher) eine Einheit ausführen und ist gewichtet 1, m5.2xlarge (8 vCPUs und 32 GB Speicher) kann 2 Einheiten ausführen und ist gewichtet 2 usw. Die gesamte Zielkapazität wird auf 40 Einheiten eingestellt. Die Standardeinkaufoption ist vor Ort, und die Allokationsstrategie ist kapazitätsoptimiert, was entweder 40 m5.xlarge (40 geteilt durch 1), 20 m5.2xlarge (40 geteilt durch 2), 10 m5.4xlarge (40 geteilt durch 4), 5 m5.8xlarge (40 geteilt durch 8) oder eine Mischung der Instance-Typen mit Gewichtungen, die zu den gewünschten Kapazität basierend auf der kapazitätsoptimierten Zuweisungsstrategie.

Weitere Informationen finden Sie unter EC2-Flotte-Instance-Gewichtung.

```
{
   "SpotOptions":{
      "AllocationStrategy":"capacity-optimized"
   },
   "LaunchTemplateConfigs":[
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":1
            },
            {
               "InstanceType":"m5.xlarge",
               "SubnetId":"subnet-e7188bab",
```

```
            "WeightedCapacity":1
         },
         {
            "InstanceType":"m5.xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":1
         },
         {
            "InstanceType":"m5.2xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":2
         },
         {
            "InstanceType":"m5.2xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":2
         },
         {
            "InstanceType":"m5.2xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":2
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":4
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":4
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":4
         },
         {
            "InstanceType":"m5.8xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":8
         },
         {
            "InstanceType":"m5.8xlarge",
```

```
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":8
            },
            {
               "InstanceType":"m5.8xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":8
            }
         ]
      }
   ],
   "TargetCapacitySpecification":{
      "TotalTargetCapacity":40,
      "DefaultTargetCapacityType":"spot"
   },
   "Type":"instant"
}
```

Beispiel 4: Starten von Spot-Instances innerhalb einer einzelnen Availability Zone

Sie können eine Flotte so konfigurieren, dass alle Instances in einer einzigen Availability Zone gestartet werden, indem Sie die Spot-Optionen SingleAvailabilityZone auf true setzen.

Die 12 Startvorlagenüberschreibungen haben unterschiedliche Instance-Typen und Subnetze (jeweils in einer separaten Availability Zone), aber die gleiche gewichtete Kapazität. Die Gesamtzielkapazität beträgt 20 Instances, die voreingestellte Kaufoption ist spot und die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die EC2-Flotte startet 20 Spot-Instances in einem einzigen AZ, aus dem Spot-Kapazitätspool (s) mit optimaler Kapazität unter Verwendung der Launch-Spezifikationen.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
```

```
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.4xlarge",
```

```
                "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 5: Starten von Spot-Instances eines einzelnen Instance-Typs innerhalb einer Availability Zone

Sie können eine Flotte so konfigurieren, dass alle Instances desselben Instance-Typs und in einer einzigen Availability Zone gestartet werden, indem Sie die SpotOptions SingleInstanceType Option auf true und SingleAvailabilityZone auf true setzen.

Die 12 Startvorlagenüberschreibungen haben unterschiedliche Instance-Typen und Subnetze (jeweils in einer separaten Availability Zone), aber die gleiche gewichtete Kapazität. Die Gesamtzielkapazität beträgt 20 Instances, die voreingestellte Kaufoption ist spot, die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die EC2-Flotte startet 20 Spot-Instances desselben Instance-Typs in einem einzigen AZ aus dem Spot-Instance-Pool mit optimaler Kapazität unter Verwendung der Startspezifikationen.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
```

```
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 6: Spot-Instances nur starten, wenn minimale Zielkapazität gestartet werden kann

Sie können eine Flotte so konfigurieren, dass Instances nur gestartet werden, wenn die Mindestzielkapazität gestartet werden kann, indem Sie die Spot-Optionen MinTargetCapacity auf die Mindestzielkapazität setzen, die Sie zusammen starten möchten.

Die 12 Startvorlagenüberschreibungen haben unterschiedliche Instance-Typen und Subnetze (jeweils in einer separaten Availability Zone), aber die gleiche gewichtete Kapazität. Die gesamte Zielkapazität und die minimale Zielkapazität sind beide auf 20 Instances festgelegt, die Standardeinkaufoption ist Spot, die Spot-Allokationsstrategie ist kapazitätsoptimiert. Die EC2-Flotte startet 20 Spot-Instances aus dem Spot-Kapazitätspool mit optimaler Kapazität unter Verwendung der Startvorlagenüberschreibungen nur, wenn alle 20 Instances gleichzeitig gestartet werden können.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5.4xlarge",
```

```
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"c5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5.4xlarge",
            "SubnetId":"subnet-49e41922"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-fae8c380"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-e7188bab"
         },
         {
            "InstanceType":"m5d.4xlarge",
            "SubnetId":"subnet-49e41922"
         }
      ]
   }
```

```
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 7: Starten Sie Spot-Instances nur, wenn die minimale Zielkapazität desselben Instance-Typs in einer einzigen Availability Zone gestartet werden kann

Sie können eine Flotte so konfigurieren, dass Instances nur gestartet werden, wenn die Mindestzielkapazität mit einem einzigen Instance-Typ in einer einzigen Availability Zone gestartet werden kann, indem Sie die Spot-Optionen MinTargetCapacity auf die Mindestzielkapazität setzen, die Sie zusammen mit den SingleAvailabilityZone Optionen SingleInstanceType und starten möchten.

Die 12 Startspezifikationen, die die Startvorlage überschreiben, haben unterschiedliche Instance-Typen und Subnetze (jede in einer separaten Availability Zone), aber die gleiche gewichtete Kapazität. Die Gesamtzielkapazität und die minimale Zielkapazität sind beide auf 20 Instances festgelegt, die Standardkaufoption ist Spot, die Spot-Zuweisungsstrategie ist kapazitätsoptimiert, das SingleInstanceType ist wahr und SingleAvailabilityZone ist wahr. Die EC2-Flotte startet 20 Spot-Instances desselben Instance-Typs in einem einzigen AZ aus dem Spot-Kapazitätspool mit optimaler Kapazität unter Verwendung der Startspezifikationen nur, wenn alle 20 Instances gleichzeitig gestartet werden können.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 20
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"c5d.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5.4xlarge",
               "SubnetId":"subnet-49e41922"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-fae8c380"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.4xlarge",
               "SubnetId":"subnet-49e41922"
```

```
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 8: Starten von Instances mit mehreren Startvorlagen

Sie können eine Flotte so konfigurieren, dass Instances mit unterschiedlichen Startspezifikationen für verschiedene Instance-Typen oder eine Gruppe von Instance-Typen gestartet werden, indem Sie mehrere Startvorlagen angeben. In diesem Beispiel wollen wir verschiedene EBS-Volume-Größen für verschiedene Instance-Typen haben und wir haben das in den Launch-Vorlagen ec2-fleet-lt-4xl, ec2-fleet-lt-9xl und ec2-fleet-lt-18xl konfiguriert.

In diesem Beispiel verwenden wir 3 verschiedene Startvorlagen für die 3 Instance-Typen, die auf ihrer Größe basieren. Die Startspezifikations-Überschreibungen für alle Startvorlagen verwenden Instance-Gewichtungen basierend auf den vCPUs des Instance-Typs. Die Gesamtzielkapazität beträgt 144 Einheiten, die voreingestellte Kaufoption ist Spot und die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die EC2-Flotte kann entweder 9 c5n.4xlarge (144 geteilt durch 16) mit der Startvorlage ec2-fleet-4xl oder 4 c5n.9xlarge (144 geteilt durch 36) mit der Startvorlage ec2-fleet-9xl oder 2 c5n.18xlarge (144 geteilt durch 72) mit der Startvorlage ec2-fleet-18xl oder eine Mischung der Instance-Typen mit Gewichtungen bis zur gewünschten Kapazität basierend auf der kapazitätsoptimierten Allokationsstrategie starten.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt-18xl",
            "Version":"$Latest"
         },
         "Overrides":[
            {
```

```
            "InstanceType":"c5n.18xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":72
         },
         {
            "InstanceType":"c5n.18xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":72
         },
         {
            "InstanceType":"c5n.18xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":72
         }
      ]
   },
   {
      "LaunchTemplateSpecification":{
         "LaunchTemplateName":"ec2-fleet-lt-9xl",
         "Version":"$Latest"
      },
      "Overrides":[
         {
            "InstanceType":"c5n.9xlarge",
            "SubnetId":"subnet-fae8c380",
            "WeightedCapacity":36
         },
         {
            "InstanceType":"c5n.9xlarge",
            "SubnetId":"subnet-e7188bab",
            "WeightedCapacity":36
         },
         {
            "InstanceType":"c5n.9xlarge",
            "SubnetId":"subnet-49e41922",
            "WeightedCapacity":36
         }
      ]
   },
   {
      "LaunchTemplateSpecification":{
         "LaunchTemplateName":"ec2-fleet-lt-4xl",
         "Version":"$Latest"
      },
```

```
         "Overrides":[
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-fae8c380",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-e7188bab",
               "WeightedCapacity":16
            },
            {
               "InstanceType":"c5n.4xlarge",
               "SubnetId":"subnet-49e41922",
               "WeightedCapacity":16
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 144,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 9: Starten von Spot-Instance mit einer Basis von On-Demand-Instances

Das folgende Beispiel gibt die Gesamtzielkapazität von 20 Instances für die Flotte und eine Zielkapazität von 5 On-Demand-Instances an. Die Standard-Kaufoption ist Spot. Die Flotte startet 5 On-Demand-Instances wie angegeben, muss aber noch 15 weitere Instance starten, um die gesamte Zielkapazität zu erreichen. Die Kaufoption für die Differenz wird wie TotalTargetCapacity — OnDemandTargetCapacity = berechnet DefaultTargetCapacityType, was dazu führt, dass die Flotte 15 Spot-Instances startet, die einen der 12 Spot-Kapazitätspools bilden, die auf der kapazitätsoptimierten Zuweisungsstrategie basieren.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "LaunchTemplateConfigs": [
      {
```

```
        "LaunchTemplateSpecification":{
           "LaunchTemplateName":"ec2-fleet-lt1",
           "Version":"$Latest"
        },
        "Overrides":[
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"c5d.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-fae8c380"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-e7188bab"
           },
           {
              "InstanceType":"m5.large",
              "SubnetId":"subnet-49e41922"
           },
           {
              "InstanceType":"m5d.large",
              "SubnetId":"subnet-fae8c380"
```

```
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab"
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922"
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 10: Starten von Spot-Instances mit kapazitätsoptimierter Zuweisungsstrategie mit einer Basis von On-Demand-Instances unter Verwendung von Kapazitätsreservierungen und der priorisierten Zuweisungsstrategie

Sie können eine Flotte so konfigurieren, dass sie zuerst On-Demand-Kapazitätsreservierungen verwendet, wenn Sie eine Basis von On-Demand-Instances mit dem standardmäßigen Zielkapazitätstyp Spot starten, indem Sie die Nutzungsstrategie für Kapazitätsreservierungen auf einstellen. use-capacity-reservations-first Und wenn mehrere Instance-Pools nicht verwendete Kapazitätsreservierungen haben, wird die gewählte On-Demand-Zuordnungsstrategie angewendet. In diesem Beispiel ist die On-Demand-Zuordnungsstrategie prioritisiert.

In diesem Beispiel sind 6 nicht verwendete Kapazitätsreservierungen verfügbar. Dies ist geringer als die On-Demand-Zielkapazität der Flotte von 10 On-Demand-Instances.

Das Konto hat die folgenden 6 nicht verwendeten Kapazitätsreservierungen in 2 Pools. Die Anzahl der Kapazitätsreservierungen in jedem Pool wird durch angegeben AvailableInstanceCount.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
```

```
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Die folgende Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die On-Demand-Zuweisungsstrategie hat Priorität, und die Nutzungsstrategie für Kapazitätsreservierungen hat Priorität use-capacity-reservations-first. Die Spot-Zuweisungsstrategie ist kapazitätsoptimiert. Die Gesamtzielkapazität beträgt 20, die On-Demand-Zielkapazität beträgt 10 und der voreingestellte Zielkapazitätstyp ist Spot.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized"
    },
    "OnDemandOptions":{
       "CapacityReservationOptions": {
         "UsageStrategy": "use-capacity-reservations-first"
       },
       "AllocationStrategy":"prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
            },
```

```
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 4.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 5.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 6.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 7.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 8.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 9.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 10.0
```

```
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 11.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 12.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity": 10,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Nachdem Sie die Instant-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 20 Instances gestartet, um die Zielkapazität zu erreichen:

- 7 c5.large On-Demand-Instances in us-east-1a – c5.large in us-east-1a wird zuerst priorisiert und es gibt drei verfügbare, nicht verwendete c5.large-Kapazitätsreservierungen. Die Kapazitätsreservierungen werden zuerst verwendet, um 3 On-Demand-Instances zu starten; dazu werden vier zusätzliche On-Demand-Instances gemäß der On-Demand-Zuordnungsstrategie gestartet, die in diesem Beispiel priorisiert sind.
- 3 m5.large On-Demand-Instances in us-east-1a – m5.large in us-east-1a wird zweitrangig priorisiert und es gibt drei verfügbare, nicht verwendete c3.large-Kapazitätsreservierungen.
- 10 Spot-Instances aus einem der 12 Spot-Kapazitätspools mit der optimalen Kapazität gemäß der kapazitätsoptimierten Zuweisungsstrategie.

Nachdem die Flotte gestartet wurde, können Sie describe-capacity-reservations ausführen, um zu sehen, wie viele nicht verwendete Kapazitätsreservierungen noch übrig sind. In diesem Beispiel sollten Sie die folgende Antwort sehen, die zeigt, dass alle c5.large- und m5.large-Kapazitätsreservierungen verwendet wurden.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.large",
    "AvailableInstanceCount": 0
}
```

Beispiel 11: Starten Sie Spot-Instances mithilfe einer capacity-optimized-prioritized Zuweisungsstrategie

Das folgende Beispiel gibt die Parameter an, die in einer EC2-Flotte des Typs Instant benötigt werden: eine Startvorlage, eine Zielkapazität, eine Standard-Kaufoption und Startvorlagenüberschreibungen. Die Startvorlage wird durch ihren Startvorlagennamen und die Versionsnummer identifiziert. Die 12 Startspezifikationen, die die Startvorlage außer Kraft setzen, haben 4 verschiedene Instance-Typen mit einer zugeordneten Priorität und 3 verschiedene Subnetze je in einer separaten Availability Zone. Die Zielkapazität für die Flotte beträgt 20 Instances, und die Standardkaufoption ist Spot. Dies führt dazu, dass die Flotte versucht, 20 Spot-Instances aus einem der 12 Spot-Kapazitätspools auf der Grundlage der capacity-optimized-prioritized Zuweisungsstrategie zu starten, bei der Prioritäten nach bestem Wissen implementiert werden, aber zuerst die Kapazität optimiert wird.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
    },
    "LaunchTemplateConfigs": [
      {
         "LaunchTemplateSpecification":{
            "LaunchTemplateName":"ec2-fleet-lt1",
            "Version":"$Latest"
         },
         "Overrides":[
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 1.0
```

```
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 1.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 2.0
            },
            {
               "InstanceType":"c5d.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 2.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-fae8c380",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-e7188bab",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5.large",
               "SubnetId":"subnet-49e41922",
               "Priority": 3.0
            },
            {
               "InstanceType":"m5d.large",
               "SubnetId":"subnet-fae8c380",
```

```
                "Priority": 4.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-e7188bab",
                "Priority": 4.0
            },
            {
                "InstanceType":"m5d.large",
                "SubnetId":"subnet-49e41922",
                "Priority": 4.0
            }
         ]
      }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

EC2-Flotte-Konfigurationsstrategien

Eine EC2-Flotte ist eine Gruppe von On-Demand-Instances und Spot-Instances. Bei der EC2-Flotte kann es sich auch um eine Gruppe von Instances mit Kapazitätsblöcken handeln.

On-Demand-Instances und Spot Instances

Das EC2-Flotte versucht, die Anzahl der Instances zu starten, die erforderlich sind, um die in Ihrer Flottenanforderung angegebene Zielkapazität zu erreichen. Die Flotte kann nur On-Demand-Instances, nur Spot-Instances oder eine Kombination aus On-Demand-Instances und Spot-Instances umfassen. Die Anforderung für Spot-Instances ist erfüllt, wenn ausreichend Kapazität verfügbar ist und der maximale Preis pro Stunde für Ihre Anforderung den Spot-Preis überschreitet. Die Flotte versucht zudem ihre Ziel-Spot-Kapazität zu erhalten, wenn Ihre Spot-Instances unterbrochen sind.

Sie können auch festlegen, wie viel Sie maximal pro Stunden für Ihre Flotte bereit sind zu zahlen. Dann startet EC2-Flotte Instances, bis der Maximalbetrag verbraucht ist. Wenn der Maximalbetrag erreicht ist, den Sie bereit sind zu zahlen, startet die Flotte keine Instances mehr, auch wenn die Zielkapazität noch nicht erreicht ist.

Ein Spot-Kapazitätspool ist eine Reihe von unbenutzten EC2-Instances mit demselben Instance-Typ und Availability Zone. Wenn Sie eine EC2-Flotte erstellen, können Sie mehrere Startspezifikationen angeben, die je nach Instance-Typ, Availability Zone, Subnetz und Höchstpreis variieren. Die Flotte wählt die Spot-Kapazitätspools aus, die zur Erfüllung der Anfrage verwendet werden, basierend auf den in Ihrer Anfrage enthaltenen Startspezifikationen und der Konfiguration der Anfrage. Die Spot-Instances stammen aus den ausgewählten Pools.

Mit einer EC2-Flotte können Sie große Mengen an EC2-Kapazität bereitstellen, die für Ihre Anwendung aufgrund der Anzahl der Kerne oder Instances oder des Speicherplatzes sinnvoll sind. Sie können beispielsweise eine EC2-Flotte angeben, um eine Zielkapazität von 200 Instances zu starten, von denen 130 On-Demand-Instances und der Rest Spot-Instances sind.

Instances mit Kapazitätsblöcken

Mit Kapazitätsblöcken für ML können Sie GPU-Instances für einen späteren Zeitpunkt reservieren, um kurzfristige Workloads für Machine Learning (ML) zu unterstützen. Instances, die in einem Kapazitätsblock ausgeführt werden, werden in Amazon EC2 UltraClusters automatisch nahe beieinander platziert. Weitere Informationen zu Kapazitätsblöcken finden Sie unter Kapazitätsblöcke für ML.

Verwenden Sie die entsprechenden Konfigurationsstrategien, um eine EC2-Flotte zu erstellen, die Ihren Anforderungen entspricht.

Inhalt

Planung einer EC2-Flotte

Bei der Planung Ihrer EC2-Flotte empfehlen wir Ihnen Folgendes:

- Legen Sie fest, ob Sie eine EC2-Flotte erstellen möchten, die eine einmalige, synchrone oder asynchrone Anforderung für die gewünschte Zielkapazität übermittelt oder eine, die die Zielkapazität dauerhaft beibehält. Weitere Informationen finden Sie unter EC2-Flotte-Anforderungstypen.
- Ermitteln Sie die Instance-Typen, die Ihre Anwendungsanforderungen am besten erfüllen.
- Wenn Sie vorhaben, Spot-Instances in Ihre EC2-Flotte aufzunehmen, lesen Sie sich bitte die Bewährten Methoden für Spot durch, bevor Sie die Flotte erstellen. Nutzen Sie diese bewährten Methoden bei der Planung Ihrer Flotte, damit Sie die Instances zum niedrigstmöglichen Preis bereitstellen können.
- Bestimmen Sie die Zielkapazität für Ihre EC2-Flotte. Sie können die Zielkapazität in Instances oder in benutzerdefinierten Einheiten angeben. Weitere Informationen finden Sie unter EC2-Flotte-Instance-Gewichtung.
- Bestimmen Sie, welcher Anteil der EC2-Flotte-Zielkapazität On-Demand-Kapazität und Spot-Kapazität sein muss. Sie können 0 für On-Demand-Kapazität oder Spot-Kapazität oder beides angeben.
- Legen Sie Ihren Preis pro Einheitsstunde fest, wenn Sie die Instance-Gewichtung verwenden. Zum Berechnen des Preises pro Einheit teilen Sie den Preis pro Instance-Stunde durch die Anzahl an Einheiten (oder Gewichtung), die diese Instance darstellt. Wenn Sie die Instance-Gewichtung nicht verwenden, entspricht der Standard-Preis pro Einheit dem Preis pro Instance-Stunde.
- Bestimmen Sie die maximale Summe pro Stunde, die Sie bereit sind, für Ihre Flotte zu bezahlen. Weitere Informationen finden Sie unter Kontrolle der Aufwendungen.
- Überprüfen Sie die möglichen Optionen für Ihre EC2-Flotte. Informationen zu den Flottenparametern finden Sie unter create-fleet in der AWS CLI -Befehlsreferenz. EC2-Flotte-Konfigurationsbeispiele finden Sie unter EC2-Flotte-Beispielkonfigurationen.

Zuweisungsstrategien für Spot-Instances

Ihre Startkonfiguration bestimmt alle möglichen Spot-Kapazitätspools (Instance-Typen und Availability Zones), aus denen EC2-Flotte Spot Instances starten kann. Beim Starten von Instances nutzt EC2-Flotte jedoch die von Ihnen angegebene Zuweisungsstrategie, um die jeweiligen Pools aus allen möglichen Pools auszuwählen.

> **Note**
>
> (Nur Linux-Instances) Wenn Sie Ihre Spot-Instance so konfigurieren, dass sie mit aktiviertem AMD SEV-SNP gestartet wird, wird Ihnen eine zusätzliche Nutzungsgebühr pro Stunde

berechnet, die 10% des On-Demand-Stundensatzes für den ausgewählten Instance-Typ entspricht. Wenn die Zuweisungsstrategie den Preis als Eingabe verwendet, berücksichtigt die EC2-Flotte diese zusätzliche Gebühr nicht. Es wird nur der Spot-Preis verwendet.

Zuweisungsstrategien

Sie können eine der folgenden Zuweisungsstrategien für Spot Instances angeben:

`price-capacity-optimized`(empfohlen)

Die EC2-Flotte identifiziert die Pools mit der höchsten Kapazitätsverfügbarkeit für die Anzahl der Instances, die gestartet werden. Das bedeutet, dass wir Spot-Instances aus den Pools anfordern werden, von denen wir glauben, dass sie in naher Zukunft die geringste Wahrscheinlichkeit einer Unterbrechung haben. Die EC2-Flotte fordert dann Spot Instances aus dem günstigsten dieser Pools an.

Die `price-capacity-optimized`-Zuweisungsstrategie ist die beste Wahl für die meisten Spot-Workloads, z. B. statuslose containerisierte Anwendungen, Microservices, Webanwendungen, Daten- und Analytikaufträge sowie Batchverarbeitung.

`capacity-optimized`

Die EC2-Flotte identifiziert die Pools mit der höchsten Kapazitätsverfügbarkeit für die Anzahl der Instances, die gestartet werden. Das bedeutet, dass wir Spot-Instances aus den Pools anfordern werden, von denen wir glauben, dass sie in naher Zukunft die geringste Wahrscheinlichkeit einer Unterbrechung haben. Sie können optional eine Priorität für jeden Instance-Typ in Ihrer Flotte mit festlege `capacity-optimized-prioritized`. Die EC2-Flotte optimiert zuerst die Kapazität, beachtet jedoch die Prioritäten der Instance-Typen so gut wie möglich.

Im Fall von Spot-Instances ändern sich die Preise allmählich im Lauf der Zeit, basierend auf langfristigen Trends bei Angebot und Nachfrage. Die Kapazität fluktuiert jedoch in Echtzeit. Bei Anwendung der Strategie `capacity-optimized` wird Spot-Instances automatisch zu den am besten verfügbaren Pools gestartet, indem Echtzeitdaten zur Kapazität analysiert werden und prognostiziert wird, welche Pools am besten verfügbar sind. Diese Strategie ist gut für Workloads, bei denen Unterbrechungen aufgrund von Neustarts von Aufgaben höhere Kosten verursachen, wie Continuous Integration (CI), Image- und Medien-Rendering, Deep Learning und High Performance Compute (HPC)-Workloads, bei denen Unterbrechungen höhere Kosten verursachen, da Aufgaben neu gestartet werden müssen. Da die `capacity-optimized`-

Strategie die Zahl der Unterbrechungen reduzieren kann, trägt sie zur Senkung der Gesamtkosten Ihrer Workload bei.

Alternativ können Sie die `capacity-optimized-prioritized`-Zuweisungsstrategie mit einem Prioritätsparameter verwenden, um die Instance-Typen von der höchsten zur niedrigsten Priorität zu ordnen. Sie können die gleiche Priorität für verschiedene Instance-Typen festlegen. Die EC2-Flotte wird zuerst für die Kapazität optimiert, berücksichtigt jedoch so gut wie möglich die Prioritäten der Instance-Typen (wenn z. B. die Berücksichtigung der Prioritäten keinen wesentlichen Einfluss auf die Fähigkeit der EC2-Flotte zur Bereitstellung optimaler Kapazität hat). Dies ist eine gute Option für Workloads, bei denen die Möglichkeit von Unterbrechungen minimiert werden muss und die Präferenz für bestimmte Instance-Typen wichtig ist. Beachten Sie Folgendes: Wenn Sie die Priorität für `capacity-optimized-prioritized` festlegen, wird die gleiche Priorität auch auf Ihre On-Demand-Instances angewendet, wenn die On-Demand-`AllocationStrategy` auf `prioritized` eingestellt ist.

`diversified`

Spot-Instances werden auf alle Spot-Kapazitätspools verteilt.

`lowest-price`(nicht empfohlen)

> **Warning**
>
> Wir empfehlen die `lowest-price` Zuweisungsstrategie nicht, da sie das höchste Unterbrechungsrisiko für Ihre Spot-Instances birgt.

Die Spot-Instances kommen aus dem preisgünstigsten Pool mit verfügbarer Kapazität. Dies ist die Standardstrategie. Es wird jedoch empfohlen, die Standardeinstellung zu überschreiben, indem Sie die `price-capacity-optimized`-Zuweisungsstrategie angeben.

Wenn der günstigste Pool keine verfügbare Kapazität aufweist, kommen die Spot Instances aus dem nächstgünstigsten Pool mit verfügbarer Kapazität.

Wenn in einem Pool die Kapazität zu Neige geht, bevor Ihre gewünschte Kapazität erreicht ist, wird Ihre Anforderung von der EC2-Flotte über den nächstgünstigsten Pool erfüllt. Damit die gewünschte Kapazität auf jeden Fall erreicht wird, erhalten Sie möglicherweise Spot-Instances aus mehreren Pools.

Da bei dieser Strategie nur der Instance-Preis und nicht die Kapazitätsverfügbarkeit berücksichtigt wird, kann es zu hohen Unterbrechungsraten kommen.

`InstancePoolsToUseCount`

Die Anzahl der Spot-Pools, über die Ihre Spot-Zielkapazität zugewiesen werden soll. Ist nur gültig, wenn die Zuweisungsstrategie auf `lowest-price` eingestellt ist. Die EC2-Flotte wählt die günstigsten Spot-Pools aus und weist Ihre Spot-Zielkapazität gleichmäßig über die von Ihnen angegebene Anzahl von Spot-Pools zu.

Beachten Sie, dass die EC2-Flotte versucht, Spot-Instances aus der Anzahl der Pools zu ziehen, die Sie nach bestem Aufwand angeben. Wenn einem Pool die Spot-Kapazität ausgeht, bevor Ihre Zielkapazität erreicht ist, wird die EC2-Flotte Ihre Anfrage weiterhin erfüllen, indem sie sie aus dem nächsten preisgünstigsten Pool zieht. Um sicherzustellen, dass Ihre Zielkapazität erreicht wird, erhalten Sie möglicherweise Spot-Instances von mehr als der von Ihnen angegebenen Anzahl von Pools. Wenn die meisten Pools keine Spot-Kapazität haben, erhalten Sie Ihre volle Zielkapazität möglicherweise von weniger als der von Ihnen angegebenen Anzahl von Pools.

Auswählen der geeigneten Zuweisungsstrategie

Sie können Ihre Flotte für Ihren Anwendungsfall optimieren, indem Sie die entsprechende Spot-Zuweisungsstrategie wählen. Als On-Demand-Instance-Zielkapazität wählt die EC2-Flotte stets den kostengünstigsten Instance-Typ aus, basierend auf dem öffentlichen On-Demand-Preis. Gleichzeitig wird die Zuweisungsstrategie (entweder `price-capacity-optimized`, `capacity-optimized`, `diversified` oder `lowest-price` – für Spot Instances) weiter befolgt.

Gleichgewicht zwischen niedrigstem Preis und Kapazitätsverfügbarkeit

Um die Kompromisse zwischen den Spot-Kapazitätspools mit dem niedrigsten Preis und den Spot-Kapazitätspools mit der höchsten Kapazitätsverfügbarkeit auszugleichen, empfehlen wir, die `price-capacity-optimized`-Zuweisungsstrategie zu verwenden. Bei dieser Strategie werden Entscheidungen darüber getroffen, von welchen Pools Spot Instances angefordert werden sollen, sowohl auf der Grundlage des Preises der Pools als auch der Kapazitätsverfügbarkeit der Spot Instances in diesen Pools. Das bedeutet, dass wir Spot Instances aus den Pools anfordern werden, von denen wir glauben, dass die Wahrscheinlichkeit einer kurzfristigen Unterbrechung am geringsten ist, wobei der Preis weiterhin berücksichtigt wird.

Wenn Ihre Flotte belastbare und statuslose Workloads ausführt, einschließlich containerisierter Anwendungen, Microservices, Webanwendungen, Daten- und Analysejobs sowie Stapelverarbeitung, dann sollten Sie die `price-capacity-optimized`-Zuweisungsstrategie verwenden, um optimale Kosteneinsparungen und Kapazitätsverfügbarkeit zu erzielen.

Wenn Ihre Flotte Workloads ausführt, bei denen Unterbrechungen aufgrund von Neustarts von Aufgaben höhere Kosten verursachen, sollten Sie Checkpointing implementieren, damit die Anwendungen von dem Punkt aus neu gestartet werden können, an dem sie unterbrochen wurden. Durch die Verwendung von Checkpointing passen Sie die `price-capacity-optimized`-Zuweisungsstrategie an diese Workloads an, da sie Kapazität aus den Pools mit dem niedrigsten Preis zuweist, die auch eine niedrige Spot Instance-Unterbrechungsrate bieten.

Eine Beispielkonfiguration, die die `price-capacity-optimized`-Zuweisungsstrategie verwendet, finden Sie unter Beispiel 10: Starten Sie Spot-Instances in einer Flotte price-capacity-optimized .

Wenn Workloads mit hohen Unterbrechungskosten verbunden sind

Sie können die `capacity-optimized`-Strategie optional verwenden, wenn Sie Workloads ausführen, die entweder Instance-Typen mit ähnlichen Preisen verwenden oder bei denen die Kosten einer Unterbrechung so hoch sind, dass jegliche Kostenersparnis im Vergleich zu einer geringfügigen Zunahme der Unterbrechungen nicht ausreicht. Bei dieser Strategie wird die Kapazität aus den am besten verfügbaren Spot-Kapazitätspools zugewiesen, die die Möglichkeit von weniger Unterbrechungen bieten, was die Gesamtkosten Ihres Workloads senken kann. Eine Beispielkonfiguration, die die `capacity-optimized`-Zuweisungsstrategie verwendet, finden Sie unter Beispiel 8: Starten Sie Spot-Instances in einer kapazitätsoptimierten Flotte.

Wenn die Möglichkeit von Unterbrechungen minimiert werden muss, aber die Präferenz für bestimmte Instance-Typen wichtig ist, können Sie Ihre Pool-Prioritäten ausdrücken, indem Sie die `capacity-optimized-prioritized`-Zuweisungsstrategie verwenden und dann die Reihenfolge der zu verwendenden Instance-Typen von der höchsten zur niedrigsten Priorität festlegen. Eine Beispielkonfiguration finden Sie unter Beispiel 9: Starten Sie Spot-Instances in einer kapazitätsoptimierten Flotte mit Prioritäten.

Beachten Sie Folgendes: Wenn Sie Prioritäten für `capacity-optimized-prioritized` festlegen, werden die gleichen Prioritäten auch auf Ihre On-Demand-Instances angewendet, wenn die On-Demand-`AllocationStrategy` auf `prioritized` eingestellt ist.

Wenn Ihr Workload zeitlich flexibel ist und die Kapazitätsverfügbarkeit kein Faktor ist

Wenn Ihre Flotte klein ist oder nur für einen kurzen Zeitraum ausgeführt wird, können Sie `price-capacity-optimized` nutzen, um die Kosteneinsparungen zu maximieren und dabei die Kapazitätsverfügbarkeit zu berücksichtigen.

Wenn Ihre Flotte groß ist oder lange läuft

Wenn Ihre Flotte groß ist oder für einen langen Zeitraum ausgeführt wird, können Sie die Verfügbarkeit Ihrer Flotte verbessern, indem Sie die Spot-Instances mit der `diversified`-Strategie über mehrere Pools verteilen. Wenn Ihre EC2-Flotte beispielsweise 10 Pools und eine Zielkapazität von 100 Instances angibt, startet die Flotte 10 Spot-Instances pro Pool. Wenn der Spot-Preis für einen Pool Ihren Höchstpreis für diesen Pool übersteigt, sind nur 10 % Ihrer Flotte betroffen. Bei dieser Strategie reagiert Ihre Flotte außerdem weniger empfindlich auf Steigerungen des Spot-Preises für die verschiedenen Pools im Laufe der Zeit. Die `diversified` startet bei einer EC2-Flotte-Strategie keine Spot-Instances in Pools mit Spot-Preisen, die auf dem Niveau des On-Demand-Preises oder darüber liegen.

Erhalten der Zielkapazität

Wenn Spot-Instances aufgrund einer Änderung in Bezug auf den Spot-Preis oder die verfügbare Kapazität eines Spot-Kapazitätspools beendet werden, startet eine EC2-Flotte vom Typ `maintain` Ersatz-Spot-Instances. Die Zuweisungsstrategie bestimmt die Pools, von denen aus die Ersatz-Instances gestartet werden, wie folgt:

- Wenn die Zuweisungsstrategie `price-capacity-optimized` ist, startet die Flotte Ersatz-Instances in den Pools mit der größten Spot-Instance-Kapazitätsverfügbarkeit. Dabei wird auch der Preis berücksichtigt und die günstigsten Pools mit hoher Kapazitätsverfügbarkeit identifiziert.
- Wenn die Zuweisungsstrategie `capacity-optimized` ist, startet die Flotte Ersatz-Instances in den Pools mit der größten verfügbaren Spot Instance-Kapazität.
- Wenn die Zuweisungsstrategie `diversified` lautet, verteilt die Flotte die Ersatz-Spot-Instances über die verbleibenden Pools.

Attributbasierte Auswahl von Instance-Typen für EC2-Flotte

Wenn Sie eine EC2-Flotte erstellen, müssen Sie mindestens einen Instance-Typ für die Konfiguration der On-Demand-Instances und Spot-Instances in der Flotte angeben. Alternativ zur manuellen Angabe der Instance-Typen können Sie die Attribute angeben, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen. Dies ist bekannt als attributbasierte Instance-Typauswahl. Sie können beispielsweise die minimale und maximale Anzahl von vCPUs angeben, die für Ihre Instances erforderlich sind, und die EC2-Flotte startet die Instances mit allen verfügbaren Instance-Typen, die diese vCPU-Anforderungen erfüllen.

Die attributbasierte Auswahl von Instance-Typen ist ideal für Workloads und Frameworks, die hinsichtlich der verwendeten Instance-Typen flexibel sein können, etwa beim Ausführen von Containern oder Web-Flotten, beim Verarbeiten von Big Data und der Implementierung von Tools zur fortlaufenden Integration und Bereitstellung (CI/CD).

Vorteile

Die Auswahl des attributbasierten Instance-Typs bietet folgende Vorteile:

- Verwenden Sie ganz einfach die richtigen Instance-Typen — Bei so vielen verfügbaren Instance-Typen kann es zeitaufwändig sein, die richtigen Instance-Typen für Ihren Workload zu finden. Wenn Sie Instance-Attribute angeben, haben die Instance-Typen automatisch die erforderlichen Attribute für Ihre Workload.
- Vereinfachte Konfiguration — Um mehrere Instance-Typen für eine EC2-Flotte manuell anzugeben, müssen Sie für jeden Instance-Typ eine separate Überschreibung der Startvorlage erstellen. Bei der attributbasierten Auswahl von Instance-Typen müssen Sie jedoch nur die Instance-Attribute in der Startvorlage oder in einer Startvorlagen-Überschreibung angeben, um mehrere Instance-Typen bereitzustellen.
- Automatische Verwendung neuer Instance-Typen — Wenn Sie Instance-Attribute anstelle von Instance-Typen angeben, kann Ihre Flotte Instance-Typen der neueren Generation verwenden, sobald sie veröffentlicht werden, was die Konfiguration der Flotte „zukunftssicher“ macht.
- Flexibilität beim Instance-Typ — Wenn Sie Instance-Attribute anstelle von Instance-Typen angeben, kann EC2 Fleet für den Start von Spot-Instances aus einer Vielzahl von Instance-Typen wählen. Dies entspricht der Spot-Best Practice zur Flexibilität von Instance-Typen.

Themen

Attributbasierte Auswahl von Instance-Typen

Um die attributbasierte Auswahl von Instance-Typen in Ihrer Flottenkonfiguration zu verwenden, ersetzen Sie die Liste der Instance-Typen durch eine Liste von Instance-Attributen, die Ihre Instances erfordern. Die EC2-Flotte startet Instances für alle verfügbaren Instance-Typen mit den angegebenen Instance-Attributen.

Themen

Arten von Instance-Attributen

Es gibt mehrere Instance-Attribute, die Sie angeben können, um Ihre Rechenanforderungen auszudrücken, wie zum Beispiel:

- vCPU-Anzahl — Die minimale und maximale Anzahl von vCPUs pro Instanz.
- Arbeitsspeicher — Das Minimum und das Maximum an Arbeitsspeicher GiBs pro Instanz.
- Lokaler Speicher — Ob EBS- oder Instance-Speicher-Volumes für den lokalen Speicher verwendet werden sollen.
- Spitzenleistung — Ob die T-Instance-Familie verwendet werden soll, einschließlich der Typen T4g, T3a, T3 und T2.

Eine Beschreibung der einzelnen Attribute und der Standardwerte finden Sie InstanceRequirementsin der Amazon EC2 API-Referenz.

Wo wird die attributbasierte Auswahl von Instance-Typen konfiguriert?

Je nachdem, ob Sie die Konsole oder die verwenden AWS CLI, können Sie die Instance-Attribute für die attributbasierte Auswahl des Instance-Typs wie folgt angeben:

In der Konsole können Sie die Instance-Attribute in einer oder beiden der folgenden Flottenkonfigurationskomponenten angeben:

- In einer Startvorlage. Verweisen Sie dann in der Flottenanforderung auf die Startvorlage

In der AWS CLI können Sie die Instance-Attribute in einer oder allen der folgenden Flottenkonfigurationskomponenten angeben:

- In einer Startvorlage. Verweisen Sie dann in der Flottenanforderung auf die Startvorlage
- In einer Startvorlagen-Überschreibung

  Wenn Sie eine Mischung aus Instances wünschen, die verschiedene AMIs verwenden, können Sie Instance-Attribute in mehreren Startvorlagen-Überschreibungen angeben. Zum Beispiel können verschiedene Instance-Typen x86- und ARM-basierte Prozessoren verwenden.

Wie die EC2-Flotte bei der Bereitstellung einer Flotte die attributbasierte Auswahl von Instance-Typen verwendet

Die EC2-Flotte stellt eine Flotte auf folgende Weise bereit:

- Die EC2-Flotte identifiziert die Instance-Typen mit den angegebenen Attributen.
- Die EC2-Flotte bestimmt anhand des Preisschutzes, welche Instance-Typen ausgeschlossen werden sollen.
- EC2 Fleet bestimmt anhand der AWS Regionen oder Availability Zones, die über die entsprechenden Instance-Typen verfügen, die Kapazitätspools, aus denen der Start der Instances in Betracht gezogen wird.
- Die EC2-Flotte wendet die angegebene Zuweisungsstrategie an, um zu bestimmen, aus welchen Kapazitätspools die Instances gestartet werden sollen.

  Beachten Sie, dass die attributbasierte Auswahl von Instance-Typen nicht die Kapazitätspools auswählt, aus denen die Flotte bereitgestellt werden soll. Dies ist die Aufgabe der Zuweisungsstrategien.

  Wenn Sie eine Zuweisungsstrategie angeben, startet die EC2-Flotte Instances gemäß der angegebenen Zuweisungsstrategie.

  - Bei Spot Instances unterstützt die attributbasierte Auswahl von Instance-Typen die `price-capacity-optimized`-, `capacity-optimized`- und `lowest-price`-Zuweisungsstrategien. Beachten Sie, dass wir die `lowest-price` Spot-Zuweisungsstrategie nicht empfehlen, da sie das höchste Unterbrechungsrisiko für Ihre Spot-Instances birgt.
  - Für On-Demand-Instances unterstützt die attributbasierte Auswahl von Instance-Typen die `lowest-price`-Zuweisungsstrategie.

- Wenn es keine Kapazität für die Instance-Typen mit den angegebenen Instance-Attributen gibt, können keine Instances gestartet werden und die Flotte gibt einen Fehler zurück.

Preisschutz

Der Preisschutz ist ein Feature, die verhindert, dass Ihre EC2-Flotte Instance-Typen verwendet, die Sie für zu teuer halten würden, selbst wenn sie den von Ihnen angegebenen Attributen entsprechen. Um den Preisschutz zu nutzen, legen Sie einen Preisgrenzwert fest. Wenn Amazon EC2 dann Instance-Typen mit Ihren Attributen auswählt, schließt es Instance-Typen aus, deren Preis über Ihrem Schwellenwert liegt.

Amazon EC2 berechnet den Preisschwellenwert wie folgt:

- Amazon EC2 identifiziert zunächst den Instance-Typ mit dem niedrigsten Preis aus den Instance-Typen, die Ihren Attributen entsprechen.
- Amazon EC2 nimmt dann den Wert (ausgedrückt als Prozentsatz), den Sie für den Preisschutzparameter angegeben haben, und multipliziert ihn mit dem Preis des identifizierten Instance-Typs. Das Ergebnis ist der Preis, der als Preisschwellenwert verwendet wird.

Es gibt separate Preisschwellen für On-Demand-Instances und Spot-Instances.

Wenn Sie eine Flotte mit attributbasierter Instance-Typauswahl erstellen, ist der Preisschutz standardmäßig aktiviert. Sie können die Standardwerte beibehalten oder eigene Werte angeben.

Sie können den Preisschutz auch deaktivieren. Um anzugeben, dass es keinen Schwellenwert für den Preisschutz gibt, geben Sie einen hohen Prozentwert an, z. 999999 B.

Themen

Wie wird der Instance-Typ mit dem niedrigsten Preis identifiziert

Amazon EC2 bestimmt den Preis, auf dem der Preisschwellenwert basieren soll, indem es den Instance-Typ mit dem niedrigsten Preis aus den Instance-Typen identifiziert, die Ihren angegebenen Attributen entsprechen. Dies geschieht auf folgende Weise:

- Zunächst werden die Instance-Typen C, M oder R der aktuellen Generation betrachtet, die Ihren Attributen entsprechen. Wenn es Übereinstimmungen findet, wird der Instance-Typ mit dem niedrigsten Preis identifiziert.
- Wenn es keine Übereinstimmung gibt, sucht es nach allen Instance-Typen der aktuellen Generation, die Ihren Attributen entsprechen. Wenn es Übereinstimmungen findet, wird der Instance-Typ mit dem niedrigsten Preis identifiziert.
- Wenn es keine Übereinstimmung gibt, sucht es nach allen Instance-Typen der vorherigen Generation, die Ihren Attributen entsprechen, und identifiziert den Instance-Typ mit dem niedrigsten Preis.

Preisschutz für On-Demand-Instances

Der Schwellenwert für den Preisschutz für On-Demand-Instance-Typen wird als Prozentsatz berechnet, der über dem identifizierten On-Demand-Instance-Typ mit dem niedrigsten Preis liegt (`OnDemandMaxPricePercentageOverLowestPrice`). Sie geben den höheren Prozentsatz an, den Sie bereit sind zu zahlen. Wenn Sie diesen Parameter nicht angeben, `20` wird der Standardwert von verwendet, um einen Preisschutzschwellenwert zu berechnen, der 20% über dem identifizierten Preis liegt.

Wenn der identifizierte On-Demand-Instance-Preis beispielsweise`0.4271`, und Sie angeben`25`, liegt der Preisschwellenwert 25% über`0.4271`. Er wird wie folgt berechnet:`0.4271 * 1.25 = 0.533875`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für On-Demand-Instances zu zahlen. In diesem Beispiel schließt Amazon EC2 alle On-Demand-Instance-Typen aus, die mehr als `0.533875` kosten.

Preisschutz für Spot-Instances

Standardmäßig wendet Amazon EC2 automatisch den optimalen Spot-Instance-Preisschutz an, sodass konsistent aus einer Vielzahl von Instance-Typen ausgewählt werden kann. Sie können den Preisschutz auch manuell selbst festlegen. Wenn Sie dies jedoch Amazon EC2 für Sie erledigen lassen, können Sie die Wahrscheinlichkeit erhöhen, dass Ihre Spot-Kapazität ausgeschöpft ist.

Sie können den Preisschutz mithilfe einer der folgenden Optionen manuell angeben. Wenn Sie den Preisschutz manuell festlegen, empfehlen wir, die erste Option zu verwenden.

- Ein Prozentsatz des identifizierten On-Demand-Instance-Typs mit dem niedrigsten Preis [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Wenn der angegebene Preis für den On-Demand-Instance-Typ `0.4271` beispielsweise ist und Sie angeben`60`, liegt der Preisgrenzwert bei 60% von`0.4271`. Er wird wie folgt berechnet:`0.4271 * 0.60 = 0.25626`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für Spot-Instances zu zahlen. In diesem Beispiel schließt Amazon EC2 alle Spot-Instance-Typen aus, die mehr als `0.25626` kosten.
- Ein Prozentsatz, der höher ist als der identifizierte Spot-Instance-Typ mit dem niedrigsten Preis [] `SpotMaxPricePercentageOverLowestPrice`

  Wenn der Preis für den identifizierten Spot-Instance-Typ beispielsweise und Sie angeben`25`, liegt der Preisschwellenwert 25% über`0.1808`. `0.1808` Er wird wie folgt berechnet:`0.1808 * 1.25 = 0.226`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für Spot-Instances zu zahlen. In diesem Beispiel schließt Amazon EC2 alle Spot-Instance-Typen aus, die mehr als `0.266` kosten. Wir empfehlen, diesen Parameter nicht zu verwenden, da die Spot-Preise schwanken können und daher auch Ihr Preisschutzschwellenwert schwanken kann.

Geben Sie die Preisschutzschwelle an

Schwellenwert für Preisschutz angeben

Konfigurieren Sie beim Erstellen der EC2-Flotte die Flotte für eine attributbasierte Auswahl des Instance-Typs und gehen Sie dann folgendermaßen vor:

- Zum Angeben des Schwellenwerts zum Preisschutz für On-Demand-Instances geben Sie in der JSON-Konfigurationsdatei in der `InstanceRequirements`-Struktur für `OnDemandMaxPricePercentageOverLowestPrice` den Preisschutzschwellenwert als Prozentsatz ein.
- Um den Schwellenwert für den Preisschutz der Spot-Instance anzugeben, geben Sie in der JSON-Konfigurationsdatei in der `InstanceRequirements` Struktur einen der folgenden Parameter an:
  - Geben Sie für `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice` den Schwellenwert für den Preisschutz als Prozentsatz ein.

- Geben Sie für `SpotMaxPricePercentageOverLowestPrice` den Preisschutzschwellenwert als Prozentsatz ein.

Weitere Informationen zum Erstellen der Flotte finden Sie unter Erstellen einer EC2-Flotte mit attributbasierter Auswahl von Instance-Typen.

> **Note**
>
> Wenn Sie beim Erstellen der EC2-Flotte `TargetCapacityUnitType` auf `vcpu` oder `memory-mib` festlegen, wird der Schwellenwert für den Preisschutz anhand des Preises pro vCPU oder pro Arbeitsspeicher anstelle des Preises pro Instance angewendet.

Überlegungen

- Sie können entweder Instance-Typen oder Instance-Attribute in einer EC2-Flotte angeben, aber nicht beides gleichzeitig.

  Wenn Sie die CLI verwenden, überschreiben die Startvorlagen-Überschreibungen die Startvorlage. Wenn die Startvorlage beispielsweise einen Instance-Typ enthält und die Startvorlagen-Überschreibung Instance-Attribute enthält, überschreiben die Instances, die durch die Instance-Attribute identifiziert werden, den Instance-Typ in der Startvorlage.
- Wenn Sie die CLI verwenden und Instance-Attribute als Überschreibungen angeben, können Sie nicht auch Gewichtungen oder Prioritäten angeben.
- Sie können maximal vier `InstanceRequirements`-Strukturen in einer Anforderungskonfiguration angeben.

Erstellen einer EC2-Flotte mit attributbasierter Auswahl von Instance-Typen

Sie können mithilfe der AWS CLI eine Flotte so konfigurieren, dass sie die attributbasierte Auswahl von Instance-Typen verwendet.

Erstellen einer EC2-Flotte mit attributbasierter Auswahl von Instance-Typen (AWS CLI)

Verwenden Sie den Befehl create-fleet (AWS CLI), um eine EC2-Flotte zu erstellen. Geben Sie die Flottenkonfiguration in einer JSON-Datei an.

```
aws ec2 create-fleet \
```

```
    --region us-east-1 \
    --cli-input-json file://file_name.json
```

file_name.json-Beispieldatei

Das folgende Beispiel enthält Parameter, mit denen eine EC2-Flotte für attributbasierte Instance-Typauswahl konfiguriert wird, gefolgt von einer Texterklärung.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Die Attribute für die attributbasierte Auswahl von Instance-Typen werden in der `InstanceRequirements`-Struktur angegeben. In diesem Beispiel werden zwei Attribute angegeben:

- `VCpuCount` – Es sind mindestens 2 vCPUs angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.

- `MemoryMiB` – Es werden mindestens 4 MiB Arbeitsspeicher angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.

Alle Instance-Typen mit 2 oder mehr vCPUs und 4 MiB oder mehr Arbeitsspeicher werden identifiziert. Der Preisschutz und die Zuweisungsstrategie könnten jedoch einige Instance-Typen ausschließen, wenn die EC2-Flotte die Flotte bereitstellt.

Eine Liste und Beschreibungen aller möglichen Attribute, die Sie angeben können, finden Sie InstanceRequirementsin der Amazon EC2 API-Referenz.

> **Note**
>
> Wenn `InstanceRequirements` in der Flottenkonfiguration enthalten ist, müssen `InstanceType` und `WeightedCapacity` ausgeschlossen werden. Sie können die Flottenkonfiguration nicht gleichzeitig mit den Instance-Attributen bestimmen.

Die JSON-Datei enthält auch die folgende Flottenkonfiguration:

- `"AllocationStrategy": "price-capacity-optimized"` – Die Zuweisungsstrategie für die Spot Instances in der Flotte.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"` – Die Startvorlage enthält einige Informationen zur Instance-Konfiguration. Wenn jedoch Instance-Typen angegeben sind, werden diese durch die in `InstanceRequirements` angegebenen Attribute überschrieben.
- `"TotalTargetCapacity": 20` – Die Zielkapazität beträgt 20 Instances.
- `"DefaultTargetCapacityType": "spot"` – Die Standardkapazität beträgt Spot Instances.
- `"Type": "instant"` – Der Anforderungstyp für die Flotte ist `instant`.

Beispiele für Konfigurationen, die gültig und ungültig sind

Wenn Sie den verwenden AWS CLI , um eine EC2-Flotte zu erstellen, müssen Sie sicherstellen, dass Ihre Flottenkonfiguration gültig ist. Die folgenden Beispiele zeigen gültige und ungültige Konfigurationen.

Konfigurationen gelten als ungültig, wenn sie Folgendes enthalten:

- Eine einzelne `Overrides`-Struktur mit `InstanceRequirements` und `InstanceType`

- Zwei `Overrides`-Strukturen, eine mit `InstanceRequirements` und die andere mit `InstanceType`
- Zwei `InstanceRequirements`-Strukturen mit sich überlappenden Attributwerten innerhalb derselben `LaunchTemplateSpecification`

Beispielkonfigurationen

- Gültige Konfiguration: Einzelstartvorlage mit Überschreibungen
- Gültige Konfiguration: Einzelne Startvorlage mit mehreren InstanceRequirements
- Gültige Konfiguration: Zwei Startvorlagen, jede mit Überschreibungen
- Gültige Konfiguration: Nur InstanceRequirements angegeben, keine überlappenden Attributwerte
- Die Konfiguration ist nicht gültig: Overrides enthalten InstanceRequirements und InstanceType.
- Konfiguration ungültig: Zwei Overrides enthalten InstanceRequirements und InstanceType
- Konfiguration ungültig: Überlappende Attributwerte

Gültige Konfiguration: Einzelstartvorlage mit Überschreibungen

Die folgende Konfiguration ist gültig. Sie enthält eine Startvorlage und eine `Overrides`-Struktur mit einer `InstanceRequirements`-Struktur. Eine Texterklärung der Beispielkonfiguration folgt.

```
{
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
```

```
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5000,
        "DefaultTargetCapacityType": "spot",
        "TargetCapacityUnitType": "vcpu"
        }
    }
}
```

`InstanceRequirements`

Um die attributbasierte Instance-Auswahl zu verwenden, müssen Sie die `InstanceRequirements`-Struktur in Ihre Flottenkonfiguration aufnehmen und die gewünschten Attribute für die Instances in der Flotte angeben.

Im vorhergehenden Beispiel werden die folgenden Instance-Attribute angegeben:

- `VCpuCount` – Die Instance-Typen müssen mindestens 2 und höchstens 8 vCPUs aufweisen.
- `MemoryMiB` – Die Instance-Typen müssen maximal 10240 MiB Speicher haben. Ein Minimum von 0 bedeutet, dass kein Mindestwert vorhanden ist.
- `MemoryGiBPerVCpu` – Die Instance-Typen müssen maximal 10 000 GiB Speicher pro vCPU haben. Der Parameter `Min` ist optional. Indem Sie ihn weglassen, geben Sie kein Mindestlimit an.

`TargetCapacityUnitType`

Der `TargetCapacityUnitType`-Parameter gibt die Einheit für die Zielkapazität an. Im Beispiel ist die Zielkapazität `5000` und der Typ der Zielkapazitätseinheit `vcpu`. Zusammen geben Sie eine gewünschte Zielkapazität von 5 000 vCPUs an. Die EC2-Flotte wird genügend Instances starten, damit die Gesamtzahl der vCPUs in der Flotte 5 000 vCPUs beträgt.

Gültige Konfiguration: Einzelne Startvorlage mit mehreren InstanceRequirements

Die folgende Konfiguration ist gültig. Sie enthält eine Startvorlage und eine `Overrides`-Struktur mit zwei `InstanceRequirements`-Strukturen. Die in `InstanceRequirements` angegebenen Attribute

sind gültig, da sich die Werte nicht überschneiden – die erste `InstanceRequirements`-Struktur gibt eine `VCpuCount` von 0-2 vCPUs an, während die zweite `InstanceRequirements`-Struktur 4-8 vCPUs angibt.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Gültige Konfiguration: Zwei Startvorlagen, jede mit Überschreibungen

Die folgende Konfiguration ist gültig. Sie enthält zwei Startvorlagen mit jeweils einer `Overrides`-Struktur, die eine `InstanceRequirements`-Struktur enthält. Diese Konfiguration ist nützlich für `arm`- und `x86`-Architekturunterstützung in derselben Flotte.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
```

```
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Gültige Konfiguration: Nur **`InstanceRequirements`** angegeben, keine überlappenden Attributwerte

Die folgende Konfiguration ist gültig. Sie enthält zwei `LaunchTemplateSpecification`-Strukturen, jeweils mit einer Startvorlage und einer `Overrides`-Struktur, die eine `InstanceRequirements`-Struktur enthält. Die in `InstanceRequirements` angegebenen Attribute sind gültig, da sich die Werte nicht überschneiden – die erste `InstanceRequirements`-Struktur gibt eine `VCpuCount` von 0-2 vCPUs an, während die zweite `InstanceRequirements`-Struktur 4-8 vCPUs angibt.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
```

```
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Die Konfiguration ist nicht gültig: **`Overrides`** enthalten **`InstanceRequirements`** und **`InstanceType`**.

Die folgende Konfiguration ist ungültig. Die `Overrides`-Struktur enthält `InstanceRequirements` und `InstanceType`. Sie können für `Overrides` `InstanceRequirements` oder `InstanceType` angeben, aber nicht beides.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
```

```
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Konfiguration ungültig: Zwei **`Overrides`** enthalten **`InstanceRequirements`** und **`InstanceType`**

Die folgende Konfiguration ist ungültig. Die `Overrides`-Strukturen enthalten `InstanceRequirements` und `InstanceType`. Sie können entweder `InstanceRequirements` oder `InstanceType` angeben, aber nicht beides, auch wenn sie sich in unterschiedlichen `Overrides`-Strukturen befinden.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
```

```
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
         "TargetCapacitySpecification": {
            "TotalTargetCapacity": 1,
            "DefaultTargetCapacityType": "spot"
        }
    }
}
```

Konfiguration ungültig: Überlappende Attributwerte

Die folgende Konfiguration ist ungültig. Die beiden `InstanceRequirements`-Strukturen enthalten jeweils `"VCpuCount": {"Min": 0, "Max": 2}`. Die Werte für diese Attribute überschneiden sich, was zu doppelten Kapazitätspools führt.

```
{
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
```

```
                        "Min": 0
                    }
                },
                {
                  "InstanceRequirements": {
                      "VCpuCount": {
                          "Min": 0,
                          "Max": 2
                      },
                      "MemoryMiB": {
                          "Min": 0
                      }
                  }
              }
            }
          ]
        }
      ],
       "TargetCapacitySpecification": {
          "TotalTargetCapacity": 1,
          "DefaultTargetCapacityType": "spot"
      }
  }
}
```

Vorschau von Instance-Typen mit bestimmten Attributen

Sie können den AWS CLI Befehl get-instance-types-from-instance-requirements verwenden, um eine Vorschau der Instance-Typen anzuzeigen, die den von Ihnen angegebenen Attributen entsprechen. Dies ist besonders nützlich, um herauszufinden, welche Attribute in Ihrer Anforderungskonfiguration angegeben werden sollen, ohne Instances zu starten. Beachten Sie, dass der Befehl die verfügbare Kapazität nicht berücksichtigt.

Um eine Vorschau einer Liste von Instanztypen anzuzeigen, geben Sie Attribute mit dem AWS CLI

1. (Optional) Um alle möglichen Attribute zu generieren, die angegeben werden können, verwenden Sie den Befehl get-instance-types-from-instance-requirements und den `--generate-cli-skeleton`-Parameter. Sie können die Ausgabe optional in eine Datei umleiten, um sie mit mit `input > attributes.json` zu speichern.

   ```
   aws ec2 get-instance-types-from-instance-requirements \
       --region us-east-1 \
   ```

```
    --generate-cli-skeleton input > attributes.json
```

Erwartete Ausgabe

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "i386"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
```

```
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Erstellen Sie eine JSON-Konfigurationsdatei mit der Ausgabe des vorherigen Schritts und konfigurieren Sie sie wie folgt:

> **Note**
>
> Sie müssen Werte für `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` und `MemoryMiB` angeben. Sie können die anderen Attribute weglassen. In diesem Fall werden die Standardwerte verwendet.
> Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-instance-types-from-instance-requirements in der Amazon-EC2-Befehlszeilenreferenz.

a. Geben Sie für `ArchitectureTypes` mindestes einen Prozessorarchitekturtyp an.

b. Geben Sie für `VirtualizationTypes` mindestens eine Art von Virtualisierung an.

c. Geben Sie für `VCpuCount` die minimale und maximale Anzahl von vCPUs an. Wenn Sie keine Mindestgrenze angeben möchten, geben Sie `0` für `Min` an. Wenn Sie keine Maximalgrenze angeben möchten, lassen Sie den `Max`-Parameter weg.

d. Geben Sie für `MemoryMiB` den Mindest- und Höchstwert für Speicher in MiB an. Wenn Sie keine Mindestgrenze angeben möchten, geben Sie `0` für `Min` an. Wenn Sie keine Maximalgrenze angeben möchten, lassen Sie den `Max`-Parameter weg.

e. Sie können optional eines oder mehrere der anderen Attribute angeben, um die Liste der zurückgegebenen Instance-Typen weiter einzuschränken.

3. Um eine Vorschau der Instance-Typen anzuzeigen, die die von Ihnen in der JSON-Datei angegebenen Attribute aufweisen, verwenden Sie den Befehl get-instance-types-from-instance-requirements und geben Sie mithilfe des `--cli-input-json`-Parameters den Namen und Pfad zu Ihrer JSON-Datei an. Sie können die Ausgabe optional so formatieren, dass sie in einem Tabellenformat angezeigt wird.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Beispiel-Datei *`Attribute.json`*

In diesem Beispiel sind die erforderlichen Attribute in der JSON-Datei enthalten. Sie lauten `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount`, und `MemoryMiB`. Darüber hinaus ist das optionale `InstanceGenerations`-Attribut ebenfalls enthalten. Beachten Sie,

dass für `MemoryMiB` der `Max`-Wert weggelassen werden kann, um anzuzeigen, dass kein Grenzwert vorhanden ist.

```
{

    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Beispielausgabe

```
-----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+---------------------------------------+
||            InstanceTypes            ||
|+-------------------------------------+|
||            InstanceType             ||
|+-------------------------------------+|
||  c4.xlarge                          ||
||  c5.xlarge                          ||
||  c5a.xlarge                         ||
||  c5ad.xlarge                        ||
||  c5d.xlarge                         ||
||  c5n.xlarge                         ||
||  d2.xlarge                          ||
...
```

4. Nachdem Sie Instance-Typen identifiziert haben, die Ihren Anforderungen entsprechen, notieren Sie die Instance-Attribute, die Sie verwendet haben, damit Sie sie beim Konfigurieren Ihrer Flottenanforderung verwenden können.

Konfigurieren von EC2-Flotte für On-Demand-Backup

Wenn Sie einen dringenden, unvorhersehbaren Skalierungsbedarf haben, wie z. B. eine Nachrichten-Website, die während eines großen Nachrichtenereignisses oder Spielstarts skaliert werden muss, empfehlen wir Ihnen, alternative Instance-Typen für Ihre On-Demand-Instances anzugeben, falls Ihre bevorzugte Option nicht über genügend verfügbare Kapazität verfügt. Zum Beispiel könnten Sie `c5.2xlarge`-On-Demand-Instances vorziehen, aber wenn die verfügbare Kapazität nicht ausreicht, sind Sie bereit, ein paar `c4.2xlarge`-Instances während der Spitzenlast hinzuzufügen. In diesem Fall versucht EC2-Flotte, alle Ihre Zielkapazitäten mit Hilfe von `c5.2xlarge`-Instances zu erfüllen, aber wenn die Kapazität nicht ausreicht, werden automatisch `c4.2xlarge`-Instances gestartet, um die Zielkapazität zu erfüllen.

Themen

- Priorisieren von Instance-Typen für On-Demand-Kapazität
- Verwenden von Kapazitätsreservierungen für On-Demand-Instances

Priorisieren von Instance-Typen für On-Demand-Kapazität

Wenn die EC2-Flotte versucht, Ihre On-Demand-Kapazität zu erfüllen, startet sie standardmäßig zuerst den kostengünstigsten Instance-Typ. Wenn `AllocationStrategy` auf `prioritized` eingestellt ist, bestimmt die EC2-Flotte anhand der Priorität, welcher Instance-Typ bei der Erfüllung der On-Demand-Kapazität zuerst verwendet werden soll. Die Priorität wird der Startvorlagen-Überschreibung zugewiesen, und die höchste Priorität wird zuerst gestartet.

Beispiel: Priorisieren von Instance-Typen

In diesem Bespiel konfigurieren Sie drei Startvorlagen-Überschreibungen, jede mit einem anderen Instance-Typ.

Der On-Demand-Preis für die Instance-Typen variiert. Im Folgenden sind die in diesem Beispiel verwendeten Instance-Typen nach Preisen aufgeführt, beginnend mit dem günstigsten Instance-Typ:

- `m4.large` – am günstigsten
- `m5.large`

- `m5a.large`

Wenn Sie die Reihenfolge nicht anhand der Priorität bestimmen, startet die Flotte zur Erfüllung der On-Demand-Kapazität mit dem günstigsten Instance-Typ.

Nehmen wir jedoch an, Sie hätten ungenutzte `m5.large` Reserved Instances, die Sie zuerst verwenden möchten. Sie können die Startvorlagen-Überschreibungspriorität so einstellen, dass die Instance-Typen wie folgt in der Reihenfolge ihrer Priorität verwendet werden:

- `m5.large` – Priorität 1
- `m4.large` – Priorität 2
- `m5a.large` – Priorität 3

Verwenden von Kapazitätsreservierungen für On-Demand-Instances

Mit On-Demand-Kapazitätsreservierungen können Sie Rechenkapazität für Ihre On-Demand-Instances in einer bestimmten Availability Zone für eine beliebige Dauer reservieren. Sie können eine EC2-Flotte so konfigurieren, dass sie die Kapazitätsreservierungen beim Starten von On-Demand-Instances zuerst verwendet.

Kapazitätsreservierungen werden entweder als `open` oder `targeted` konfiguriert. EC2-Flotte kann On-Demand-Instances entweder in `open`- oder `targeted`-Kapazitätsreservierungen wie folgt starten:

- Wenn eine Kapazitätsreservierung `open` ist, werden On-Demand-Instances mit übereinstimmenden Attributen automatisch in der reservierten Kapazität ausgeführt.
- Wenn die Kapazitätsreservierung `targeted` ist, müssen die On-Demand-Instances speziell für die Ausführung in der reservierten Kapazität ausgerichtet sein. Dies ist nützlich, um bestimmte Kapazitätsreservierungen zu verwenden oder um zu kontrollieren, wann bestimmte Kapazitätsreservierungen verwendet werden sollen.

Wenn Sie `targeted`-Kapazitätsreservierungen in Ihrer EC2-Flotte verwenden, müssen genügend Kapazitätsreservierungen vorhanden sein, um die angeforderte On-Demand-Kapazität zu erfüllen, andernfalls schlägt der Start fehl. Um zu vermeiden, dass ein Start fehlschlägt, fügen Sie stattdessen die `targeted`-Kapazitätsreservierungen einer Ressourcengruppe hinzu, und richten Sie dann die Ressourcengruppe an. Die Ressourcengruppe muss nicht über ausreichende Kapazitätsreservierungen verfügen. Wenn die Kapazitätsreservierungen ausgehen, bevor die Ziel-

On-Demand-Kapazität erfüllt ist, kann die Flotte die verbleibende Zielkapazität in reguläre On-Demand-Kapazität starten.

So verwenden Sie Kapazitätsreservierungen mit EC2-Flotte

1. Konfigurieren Sie die Flotte als Typ `instant`. Sie können Kapazitätsreservierungen für Flotten anderer Art nicht verwenden.
2. Konfigurieren Sie die Nutzungsstrategie für Kapazitätsreservierungen als `use-capacity-reservations-first`.
3. Wählen Sie in der Startvorlage für Kapazitätsreservierung entweder Öffnen oder Ziel nach Gruppe aus. Wenn Sie Ziel nach Gruppe wählen, geben Sie die Ressourcengruppen-ID für Kapazitätsreservierungen an.

Wenn die Flotte versucht, die On-Demand-Kapazität zu erfüllen, und wenn sie feststellt, dass mehrere Instance-Pools über ungenutzte übereinstimmende Kapazitätsreservierungen verfügen, bestimmt sie die Pools, in denen die On-Demand-Instances gestartet werden sollen, basierend auf der On-Demand-Zuordnungsstrategie (`lowest-price` oder `prioritized`).

Beispiele für die Konfiguration einer Flotte für die Verwendung von Kapazitätsreservierungen zur Erfüllung von On-Demand-Kapazitäten finden Sie unter EC2-Flotte-Beispielkonfigurationen, insbesondere Beispiele 5 bis 7.

Weitere Informationen zum Konfigurieren von Kapazitätsreservierungen finden Sie unter On-Demand Capacity Reservations und Häufig gestellte Fragen zur On-Demand-Kapazitätsreservierung.

Kapazitätsausgleich

Sie können die EC2-Flotte so konfigurieren, dass eine Ersatz-Spot-Instance gestartet wird, wenn Amazon EC2 eine Neuausgleichsempfehlung ausgibt, um Sie darüber zu informieren, dass für eine Spot-Instance ein erhöhtes Unterbrechungsrisiko besteht. Der Kapazitätsausgleich hilft Ihnen, die Verfügbarkeit von Workloads aufrechtzuerhalten, indem Sie Ihre Flotte proaktiv um eine neue Spot-Instance erweitern, bevor eine ausgeführte Instance durch Amazon EC2 unterbrochen wird. Weitere Informationen finden Sie unter Empfehlung zum Neuausgleich einer EC2-Instance.

Um die EC2-Flotte für den Start einer Ersatz-Spot-Instance zu konfigurieren, verwenden Sie den Befehl create-fleet (AWS CLI) und die relevanten Parameter in der `MaintenanceStrategies`-Struktur. Weitere Informationen finden Sie in der Beispielstartkonfiguration.

Einschränkungen

- Die Kapazitätsanpassung ist nur für Flotten des Typs `maintain` verfügbar.
- Wenn die Flotte läuft, können Sie die Kapazitätsausgleichs-Einstellung nicht ändern. Um die Einstellung Kapazitätsausgleich zu ändern, müssen Sie die Flotte löschen und eine neue Flotte erstellen.

Konfigurationsoptionen

`ReplacementStrategy` für die EC2-Flotte unterstützt die folgenden beiden Werte:

`launch-before-terminate`

Amazon EC2 kann die Spot Instances beenden, die eine Neuausgleichsbenachrichtigung erhalten, nachdem neue Ersatz-Spot-Instances gestartet wurden. Wenn Sie `launch-before-terminate` angeben, müssen Sie auch einen Wert für `termination-delay` angeben. Nachdem die neuen Ersatz-Instances gestartet wurden, wartet Amazon EC2 während der Dauer des `termination-delay` und beendet dann die alten Instances. Für `termination-delay` beträgt das Minimum 120 Sekunden (2 Minuten) und das Maximum 7 200 Sekunden (2 Stunden).

Wir empfehlen die Verwendung von `launch-before-terminate` nur, wenn Sie vorhersagen können, wie lange Ihre Verfahren zum Herunterfahren der Instances dauern werden. Dadurch wird sichergestellt, dass die alten Instances erst beendet werden, wenn die Verfahren zum Herunterfahren abgeschlossen sind. Beachten Sie, dass Amazon EC2 die alten Instances mit einer zweiminütigen Warnung vor der `termination-delay` unterbrechen kann.

Wir raten dringend davon ab, die `lowest-price`-Zuweisungsstrategie in Kombination mit `launch-before-terminate` zu verwenden, um Ersatz-Spot-Instances zu vermeiden, die ebenfalls einem erhöhten Unterbrechungsrisiko ausgesetzt sind.

`launch`

Amazon EC2 startet Ersatz-Spot-Instances, wenn eine Neuausgleichsbenachrichtigung für bestehende Spot-Instances ausgegeben wird. Amazon EC2 beendet nicht die Instances, die eine Neuausgleichsbenachrichtigung erhalten. Sie können die alten Instances beenden oder laufen lassen. Ihnen werden alle Instances in Rechnung gestellt, während sie ausgeführt werden.

Überlegungen

Wenn Sie EC2-Flotte für Kapazitätsausgleich konfigurieren, sollten Sie Folgendes berücksichtigen:

Stellen Sie so viele Spot-Kapazitätspools wie möglich in der Anfrage bereit

Konfigurieren Sie Ihre EC2-Flotte für die Verwendung mehrerer Instance-Typen und Availability Zones. Dies bietet die Flexibilität, Spot-Instances in verschiedenen Spot-Kapazitätspools zu starten. Weitere Informationen finden Sie unter Flexibel sein bei Instance-Typen und Availability Zones.

Vermeiden Sie ein erhöhtes Risiko einer Unterbrechung von Ersatz-Spot-Instances

Ihre Ersatz-Spot-Instances haben möglicherweise ein erhöhtes Risiko einer Unterbrechung, wenn Sie die `lowest-price`-Zuweisungsstrategie verwenden. Dies liegt daran, dass Amazon EC2 immer Instances im preisgünstigsten Pool startet, der zu diesem Zeitpunkt verfügbare Kapazität hat, auch wenn Ihre Ersatz-Spot-Instances wahrscheinlich kurz nach dem Start unterbrochen werden. Um ein erhöhtes Unterbrechungsrisiko zu vermeiden, wird davon abgeraten, die `lowest-price`-Zuweisungsstrategie zu verwenden, stattdessen empfehlen wir die `capacity-optimized`- oder `capacity-optimized-prioritized`-Zuweisungsstrategie. Diese Strategien stellen sicher, dass Ersatz-Spot-Instances in den optimalen Spot-Kapazitätspools gestartet werden und ihre Unterbrechung in naher Zukunft daher weniger wahrscheinlich ist. Weitere Informationen finden Sie unter Nutzen der preis- und kapazitätsoptimierten Zuweisungsstrategie.

Amazon EC2 startet eine neue Instance nur dann, wenn die Verfügbarkeit gleich oder besser ist

Eines der Ziele des Kapazitätsausgleichs ist die Verbesserung der Verfügbarkeit einer Spot Instance. Wenn eine vorhandene Spot Instance eine Neuausgleichsempfehlung erhält, startet Amazon EC2 nur dann eine neue Instance, wenn die neue Instance dieselbe oder eine bessere Verfügbarkeit als die vorhandene Instance bietet. Wenn das Risiko einer Unterbrechung einer neuen Instance größer ist als das der vorhandenen Instance, startet Amazon EC2 keine neue Instance. Amazon EC2 wird die Spot-Kapazitätspools jedoch weiterhin bewerten und eine neue Instance starten, falls sich die Verfügbarkeit verbessert.

Es besteht die Möglichkeit, dass Ihre vorhandene Instance unterbrochen wird, ohne dass Amazon EC2 pro-aktiv eine neue Instance startet. In diesem Fall versucht Amazon EC2, eine neue Instance zu starten, sobald die Unterbrechungsmeldung für eine Spot Instance eingeht, unabhängig davon, ob bei der neuen Instance ein hohes Unterbrechungsrisiko besteht.

Capacity Rebalancing erhöht nicht die Unterbrechungsrate Ihrer Spot-Instance

Wenn Sie Capacity Rebalancing aktivieren, wird Ihre Spot-Instance-Unterbrechungsrate (die Anzahl der Spot-Instances, die zurückgefordert werden, wenn Amazon EC2 die Kapazität zurück

benötigt) nicht erhöht. Wenn der Kapazitätsausgleich jedoch feststellt, dass bei einer Instance das Risiko einer Unterbrechung besteht, versucht Amazon EC2 sofort, eine neue Instance zu starten. Das Ergebnis ist, dass möglicherweise mehr Instances ersetzt werden, als wenn Sie darauf gewartet hätten, dass Amazon EC2 eine neue Instance startet, nachdem die gefährdete Instance unterbrochen wurde.

Sie können zwar mehr Instances mit aktiviertem Capacity Rebalancing ersetzen, jedoch Sie profitieren davon, dass Sie eher proaktiv als reaktiv sind, indem Sie mehr Zeit haben, Maßnahmen zu ergreifen, bevor Ihre Instances unterbrochen werden. Mit einer Spot-Instance-Unterbrechungsbenachrichtigung haben Sie normalerweise nur bis zu zwei Minuten Zeit, um Ihre Instance ordnungsgemäß herunterzufahren. Wenn Capacity Rebalancing eine neue Instance im Voraus startet, geben Sie bestehenden Prozessen eine bessere Chance, sie auf Ihrer gefährdeten Instance abzuschließen. Sie können mit dem Herunterfahren Ihrer Instance beginnen und verhindern, dass neue Arbeiten für Ihre gefährdete Instance geplant werden. Sie können auch damit beginnen, die neu gestartete Instance für die Übernahme der Anwendung vorzubereiten. Mit dem proaktiven Ersetzen durch Capacity Rebalancing profitieren Sie von einer reibungslosen Kontinuität.

Betrachten Sie als theoretisches Beispiel zur Demonstration der Risiken und Vorteile des Einsatzes von Capacity Rebalancing das folgende Szenario:

- 14:00 Uhr – Für Instance-A wird eine Empfehlung zum erneuten Ausgleich empfangen und Amazon EC2 versucht sofort, eine Ersatz-Instance-B zu starten, sodass Sie Zeit haben, Ihre Shutdown-Verfahren zu starten.*
- 14:30 Uhr — Für Instance-B wird eine Empfehlung zum erneuten Ausgleich empfangen, die durch Instance-C ersetzt wird, sodass Sie Zeit haben, Ihre Shutdown-Verfahren zu starten.*
- 14:32 Uhr — Wenn Capacity Rebalancing nicht aktiviert wäre und um 14:32 Uhr eine Benachrichtigung über eine Unterbrechung der Spot-Instance für Instance-A eingegangen wäre, hätten Sie nur bis zu zwei Minuten Zeit gehabt, um Maßnahmen zu ergreifen, währenddessen Instance-A allerdings bis zu diesem Zeitpunkt hochgefahren wäre.

* Wenn `launch-before-terminate` angegeben ist, beendet Amazon EC2 die gefährdete Instance, nachdem die Ersatz-Instance online geschaltet wurde.

Amazon EC2 kann einen neuen Ersatz Spot-Instances starten, bis die erfüllte Kapazität die doppelte Zielkapazität hat

Wenn ein EC2-Flotte für den Kapazitätsausgleich konfiguriert ist, versucht die Flotte, eine neue Ersatz-Spot-Instance für jede Spot-Instance zu starten, die eine Ausgleichsempfehlung erhält.

Nachdem eine Spot-Instance eine Neuausgleichsempfehlung erhalten hat, wird sie nicht mehr als Teil der erfüllten Kapazität gezählt. Je nach Ersetzungsstrategie beendet Amazon EC2 die Instance entweder nach einer vorkonfigurierten Beendigungsverzögerung oder lässt sie laufen. Dies gibt Ihnen die Möglichkeit, Neuausgleichsaktionen für die Instance durchzuführen.

Wenn Ihre Flotte die doppelte Zielkapazität erreicht, wird sie keine neuen Ersatz-Instances mehr starten, selbst wenn die Ersatz-Instances selbst eine Empfehlung zum Neuausgleich erhalten.

Beispielsweise erstellen Sie eine EC2-Flotte mit einer Zielkapazität von 100 Spot-Instances. Alle Spot Instances erhalten eine Neuausgleichsempfehlung, die dazu führt, dass Amazon EC2 100 Ersatz-Spot-Instances startet. Dadurch wird die Anzahl der erfüllten Spot-Instances auf 200 erhöht, was der doppelten Zielkapazität entspricht. Einige der Ersatz-Instances erhalten eine Neuausgleichsempfehlung, es werden jedoch keine Ersatz-Instances mehr gestartet, da die Flotte die doppelte Zielkapazität nicht überschreiten kann.

Beachten Sie, dass Ihnen alle Instances in Rechnung gestellt werden, während sie ausgeführt werden.

Wir empfehlen Ihnen, die EC2-Flotte so zu konfigurieren, dass Spot-Instances beendet werden, die eine Neuausgleichsempfehlung erhalten.

Wenn Sie Ihre EC2-Flotte für den Kapazitätsausgleich konfigurieren, empfehlen wir Ihnen, `launch-before-terminate` mit einer angemessenen Beendigungsverzögerung nur dann auszuwählen, wenn Sie vorhersagen können, wie lange die Verfahren zum Herunterfahren der Instances dauern werden. Dadurch wird sichergestellt, dass die alten Instances erst beendet werden, wenn die Verfahren zum Herunterfahren abgeschlossen sind.

Wenn Sie die für die Neuausgleichsempfehlung empfohlenen Instances selbst beenden möchten, empfehlen wir Ihnen, das Signal für die Neuausgleichsempfehlung zu überwachen, das von den Spot-Instances in der Flotte empfangen wird. Durch die Überwachung des Signals können Sie schnell Neuausgleichsaktionen für die betroffenen Instances durchführen, bevor Amazon EC2 sie unterbricht, und dann können Sie sie manuell beenden. Wenn Sie die Instances nicht beenden, bezahlen Sie weiterhin für sie, während sie ausgeführt werden. Amazon EC2 beendet die Instances, die eine Neuausgleichsempfehlung erhalten, nicht automatisch.

Sie können Benachrichtigungen mithilfe von Amazon EventBridge - oder Instance-Metadaten einrichten. Weitere Informationen finden Sie unter Überwachen von Signalen für Neuausgleichsempfehlungen.

EC2-Flotte zählt keine Instances, die bei der Berechnung der erfüllten Kapazität bei einer Verringerung oder Vergrößerung eine Neuausgleichsempfehlung erhalten

Wenn Ihr EC2-Flotte für den Kapazitätsausgleich konfiguriert ist und Sie die Zielkapazität so ändern, dass sie entweder verringert oder vergrößert wird, zählt die Flotte die Instances nicht, die für den Ausgleich markiert sind, wie folgt:

- Abskalieren – Wenn Sie die gewünschte Zielkapazität verringern, beendet Amazon EC2 Instances, die nicht für eine Neuverteilung markiert sind, bis die gewünschte Kapazität erreicht ist. Die Instances, die für einen Neuausgleich markiert sind, werden nicht auf die erfüllte Kapazität angerechnet.

  Ein Beispiel: Angenommen, Sie erstellen eine EC2-Flotte mit einer Zielkapazität von 100 Spot Instances. 10 Instances erhalten eine Neuausgleichsempfehlung. Amazon EC2 startet also 10 neue Ersatz-Instances, was zu einer erfüllten Kapazität von 110 Instances führt. Sie reduzieren dann die Zielkapazität auf 50 (abskalieren), aber die erfüllte Kapazität beträgt tatsächlich 60 Instances, da die 10 Instances, die für einen Neuausgleich markiert sind, nicht von Amazon EC2 beendet werden. Sie müssen diese Instances manuell beenden oder Sie können sie laufen lassen.
- Aufskalieren – Wenn Sie Ihre gewünschte Zielkapazität erhöhen, startet Amazon EC2 neue Instances, bis die gewünschte Kapazität erreicht ist. Die Instances, die für einen Neuausgleich markiert sind, werden nicht auf die erfüllte Kapazität angerechnet.

  Ein Beispiel: Angenommen, Sie erstellen eine EC2-Flotte mit einer Zielkapazität von 100 Spot-Instances. 10 Instances erhalten eine Neuausgleichsempfehlung. Die Flotte startet also 10 neue Ersatz-Instances, was zu einer erfüllten Kapazität von 110 Instances führt. Sie erhöhen dann die Zielkapazität auf 200 (Erweiterung), aber die erfüllte Kapazität beträgt tatsächlich 210 Instances, da die 10 Instances, die für einen Neuausgleich markiert sind, nicht von der Flotte als Teil der Zielkapazität gezählt werden. Sie müssen diese Instances manuell beenden oder Sie können sie laufen lassen.

Außerkraftsetzungen des Höchstpreises

Jede EC2-Flotte kann einen globalen Höchstpreis enthalten oder den Standardpreis (den On-Demand-Preis) verwenden. Die Flotte verwendet diesen Preis als Standard-Höchstpreis für die einzelnen Startspezifikationen.

Sie können optional einen Höchstpreis in einer oder mehreren Startspezifikationen angeben. Dieser Preis gilt speziell für die Startspezifikation. Wenn eine Startspezifikation einen spezifischen Preis

beinhaltet, verwendet die EC2-Flotte diesen Höchstpreis, wodurch der globale Höchstpreis außer Kraft gesetzt wird. Alle anderen Startspezifikationen, die keinen spezifischen Höchstpreis enthalten, verwenden weiterhin den globalen Höchstpreis.

Kontrolle der Aufwendungen

EC2-Flotte stoppt das Starten von Instances, wenn einer der folgenden Parameter erfüllt ist: `TotalTargetCapacity` oder `MaxTotalPrice` (die maximale Summe, die Sie bereit sind zu zahlen). Zur Kontrolle der Kosten, die Sie für Ihre Flotte zahlen, können Sie den `MaxTotalPrice` angeben. Ist die maximale Summe erreicht, stoppt EC2-Flotte das Starten von Instances auch dann, wenn die Zielkapazität noch nicht erreicht ist.

Im folgenden Beispiel werden zwei verschiedene Szenarien gezeigt. Im ersten Szenario stoppt EC2-Flotte das Starten von Instances, wenn die Zielkapazität erreicht ist. Im zweiten Szenario stoppt EC2-Flotte das Starten von Instances, wenn die maximale Summe erreicht ist, die Sie bereit sind zu zahlen (`MaxTotalPrice`).

Beispiel: Kein Starten mehr von Instances, wenn die Zielkapazität erreicht ist

Bei einer Anforderung für `m4.large` On-Demand-Instances mit:

- On-Demand-Preis: 0,10 USD pro Stunde
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 1,50 USD

EC2-Flotte startet 10 On-Demand-Instances, da der Gesamtpreis von 1,00 USD (10 Instances x 0,10 USD) den `MaxTotalPrice` von 1,50 USD für On-Demand-Instances nicht überschreitet.

Beispiel: Kein Starten mehr von Instances, wenn der Höchstpreis erreicht ist

Bei einer Anforderung für `m4.large` On-Demand-Instances mit:

- On-Demand-Preis: 0,10 USD pro Stunde
- `OnDemandTargetCapacity`: 10
- `MaxTotalPrice`: 0,80 USD

Wenn EC2-Flotte die On-Demand-Zielkapazität (10 On-Demand-Instances) startet, betragen die Gesamtkosten pro Stunde 1,00 USD. Dies überschreitet die Summe (0,80 USD), die als `MaxTotalPrice` für On-Demand-Instances festgelegt ist. Damit Sie nicht mehr ausgeben, als Sie

möchten, startet EC2-Flotte nur 8 On-Demand-Instances (weniger als die On-Demand-Zielkapazität), da sonst der `MaxTotalPrice` für On-Demand-Instances überschritten werden würde.

EC2-Flotte-Instance-Gewichtung

Wenn Sie eine EC2-Flotte erstellen, können Sie die Kapazitätseinheiten definieren, die jeder Instance-Typ zur Leistung Ihrer Anwendung beiträgt. Sie können dann den Höchstpreis für die einzelnen Startspezifikationen über die Instance-Gewichtung anpassen.

Standardmäßig gilt der von Ihnen angegebene Preis pro Instance-Stunde. Wenn Sie das Feature der Instance-Gewichtung verwenden, gilt der von Ihnen angegebene Preis pro Einheitsstunde. Der Preis pro Einheitsstunde lässt sich errechnen, indem Sie Ihren Preis für einen Instance-Typ durch die Anzahl der Einheiten dividieren, die er darstellt. Die EC2-Flotte berechnet die Anzahl der zu startenden Instances, indem die Zielkapazität durch die Instance-Gewichtung geteilt wird. Wenn es sich bei dem Ergebnis nicht um eine Ganzzahl handelt, rundet die Flotte dieses auf die nächste Ganzzahl auf, sodass die Größe Ihrer Flotte nicht unter der Zielkapazität liegt. Die Flotte kann alle Pools auswählen, die Sie in Ihrer Startspezifikation angeben, selbst wenn die Kapazität der gestarteten Instances die angeforderte Zielkapazität übersteigt.

Die folgende Tabelle enthält Beispiele für die Berechnung des Preises pro Einheit für eine EC2-Flotte mit einer Zielkapazität von 10.

Instance-Typ	Instance-Gewichtung	Zielkapazität	Anzahl an gestarteten Instances	Preis pro Instance-Stunde	Preis pro Einheitsstunde
`r3.xlarge`	2	10	5 (10 geteilt durch 2)	$0.05	0,025 USD (0,05 geteilt durch 2)
`r3.8xlarge`	8	10	2 (10 geteilt durch 8, Ergebnis aufgerundet)	$0.10	0,0125 USD (0,10 geteilt durch 8)

Verwenden Sie EC2-Flotte Instance-Gewichtung wie folgt, um die gewünschte Zielkapazität in den Pools mit dem niedrigsten Preis pro Einheit zum Zeitpunkt der Erfüllung bereitzustellen:

1. Geben Sie die Zielkapazität für Ihre EC2-Flotte entweder in Instances (Standard) oder in den Einheiten Ihrer Wahl an, z. B. virtuelle CPUs, Arbeitsspeicher, Speicher oder Durchsatz.
2. Legen Sie den Preis pro Einheit fest.
3. Geben Sie für jede Startspezifikation die Gewichtung an, d. h. die Anzahl der Einheiten, die der Instance-Typ für die Zielkapazität darstellt.

Beispiel für die Instance-Gewichtung

Stellen Sie sich eine EC2-Flotte-Anfrage mit der folgenden Konfiguration vor:

- Eine Zielkapazität von 24
- Eine Startspezifikation mit dem Instance-Typ `r3.2xlarge` und der Gewichtung 6
- Eine Startspezifikation mit dem Instance-Typ `c3.xlarge` und der Gewichtung 5

Die Gewichtung stellt die Anzahl an Einheiten dar, die der Instance-Typ hinsichtlich der Zielkapazität darstellt. Wenn die erste Startspezifikation den niedrigsten Preis pro Einheit (Preis für `r3.2xlarge` pro Instance-Stunde geteilt durch 6) bereitstellt, würde die EC2-Flotte vier dieser Instances starten (24 geteilt durch 6).

Wenn die zweite Startspezifikation den niedrigsten Preis pro Einheit (Preis für `c3.xlarge` pro Instance-Stunde geteilt durch 5) bereitstellt, würde die EC2-Flotte fünf dieser Instances starten (24 geteilt durch 5, Ergebnis aufgerundet).

Instance-Gewichtung und Zuweisungsstrategie

Stellen Sie sich eine EC2-Flotte-Anfrage mit der folgenden Konfiguration vor:

- Eine Zielkapazität von 30 Spot-Instances
- Eine Startspezifikation mit dem Instance-Typ `c3.2xlarge` und der Gewichtung 8
- Eine Startspezifikation mit dem Instance-Typ `m3.xlarge` und der Gewichtung 8
- Eine Startspezifikation mit dem Instance-Typ `r3.xlarge` und der Gewichtung 8

Die EC2-Flotte würde vier Instances starten (30 geteilt durch 8, Ergebnis aufgerundet). Bei der `diversified`-Strategie startet die Flotte eine Instance in jedem der drei Pools und die vierte Instance in dem Pool, für den der niedrigste Preis pro Einheit anfällt.

Arbeiten mit EC2-Flotten

Um mit EC2-Flotte zu beginnen, erstellen Sie eine Anforderung mit der Gesamtzielkapazität, der On-Demand-Kapazität, der Spot-Kapazität und einer oder mehreren Startspezifikationen für die Instances sowie dem Höchstpreis, den Sie zu zahlen bereit sind. Die Flottenanforderung muss eine Startvorlage enthalten, die die Informationen definiert, die die Flotte benötigt, um eine Instance zu starten, z. B. eine AMI, einen Instance-Typ, ein Subnetz oder eine Availability Zone, und eine oder mehrere Sicherheitsgruppen. Sie können für den Instance-Typ, das Subnetz, die Availability Zone und den Höchstpreis, den Sie zu zahlen bereit sind, Startspezifikationen überschreiben und Sie können jeder Startspezifikation eine gewichtete Kapazität zuweisen.

Die EC2-Flotte startet On-Demand-Instances, wenn freie Kapazität vorhanden ist, und startet Spot-Instances, wenn Ihr Höchstpreis den Spot-Preis übersteigt und Kapazität verfügbar ist.

Wenn Ihre Flotte Spot-Instances enthält, kann Amazon EC2 versuchen, Ihre Flotten-Zielkapazität aufrechtzuerhalten, wenn sich die Spot-Preise ändern.

Eine EC2-Flotte-Anforderung vom Typ `maintain` oder `request` bleibt solange aktiv, bis sie abläuft oder Sie sie löschen. Wenn Sie eine Flotte vom Typ `maintain` oder `request` löschen, können Sie angeben, ob das Löschen die Instances dieser Flotte beendet. Anderenfalls werden die On-Demand-Instances so lange ausgeführt, bis Sie sie beenden. Die Spot-Instances werden ausgeführt, bis sie unterbrochen oder von Ihnen beendet werden.

Inhalt

- Löschen einer EC2-Flotte

EC2-Flotte-Anforderungsstatus

Eine EC2-Flotte-Anfrage kann die folgenden Zustände aufweisen:

`submitted`

Die EC2-Flotte-Anforderung wird evaluiert und Amazon EC2 bereitet den Start der Zielanzahl von Instances vor. Die Anfrage kann On-Demand-Instances, Spot-Instances oder beides enthalten. Wenn eine Anforderung Ihre Flottenlimits überschreiten würde, wird sie sofort gelöscht.

`active`

Die EC2-Flotte-Anfrage wurde validiert und Amazon EC2 versucht, die Zielanzahl der laufenden Instances beizubehalten. Die Anforderung bleibt so lange in diesem Zustand, bis sie geändert oder gelöscht wird.

`modifying`

Die EC2-Flotte-Anforderung wird geändert. Die Anforderung bleibt in diesem Zustand, bis die Änderung vollständig bearbeitet oder die Anforderung gelöscht wird. Nur ein `maintain`-Flottentyp kann geändert werden. Dieser Status gilt nicht für die anderen Anforderungstypen.

`deleted_running`

Die EC2-Flotte-Anforderung wird gelöscht und startet keine weiteren Instances. Die bestehenden Instances laufen weiter, bis sie unterbrochen oder manuell beendet werden. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances unterbrochen oder beendet wurden. Nur ein EC2-Flotte vom Typ `maintain` oder `request` kann laufende Instances haben, nachdem die EC2-Flotte-Anforderung gelöscht wurde. Eine gelöschte `instant`-Flotte mit laufenden Instances wird nicht unterstützt. Dieser Status gilt nicht für `instant`-Flotten.

`deleted_terminating`

Die EC2-Flotte-Anforderung wird gelöscht und die zugehörigen Instances werden beendet. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances beendet wurden.

`deleted`

Die EC2-Flotte wird gelöscht und hat keine laufenden Instances. Die Anforderung wird zwei Tage nach Beendigung der zugehörigen Instances gelöscht.

EC2-Flotte-Voraussetzungen

Um eine EC2-Flotte zu erstellen, müssen die folgenden Voraussetzungen erfüllt sein:

- Startvorlage
- Serviceverknüpfte Rolle für EC2-Flotte
- Gewähren von Zugriff auf von Kunden verwaltete Schlüssel zur Verwendung mit verschlüsselten AMIs und EBS-Snapshots
- Berechtigungen für EC2-Flotten-Benutzer

Startvorlage

Eine Startvorlage enthält Informationen über die zu startenden Instances, wie den Instance-Typ, die Availability Zone und den Höchstpreis, den Sie zu zahlen bereit sind. Weitere Informationen finden Sie unter Starten einer Instance über eine Startvorlage.

Serviceverknüpfte Rolle für EC2-Flotte

Die `AWSServiceRoleForEC2Fleet`-Rolle gewährt der EC2-Flotte die Berechtigung, in Ihrem Namen Instances anzufordern, zu launchen, zu beenden und zu markieren. Amazon EC2 verwendet diese serviceverknüpfte Rolle, um die folgenden Aktionen durchzuführen:

- `ec2:RunInstances` – Instances starten.
- `ec2:RequestSpotInstances` – Spot-Instances anfragen.
- `ec2:TerminateInstances` – Instances beenden.
- `ec2:DescribeImages` – Amazon Machine Images (AMI) für die Spot-Instances beschreiben.
- `ec2:DescribeInstanceStatus` – Status der Spot-Instances beschreiben.
- `ec2:DescribeSubnets` – Subnetze für Spot-Instances beschreiben.
- `ec2:CreateTags` – Tags zu den EC2-Flotte, Instances und Volumes hinzufügen.

Stellen Sie sicher, dass diese Rolle vorhanden ist, bevor Sie die AWS CLI oder eine API verwenden, um eine EC2-Flotte zu erstellen.

> **Note**
>
> Ein `instant` EC2-Flotte erfordert diese Rolle nicht.

Um die Rolle anzulegen, verwenden Sie die IAM-Konsole wie folgt.

Um die AWSServiceRoleForEC2Fleet Rolle für die EC2-Flotte zu erstellen

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rollen) und dann Create role (Rolle erstellen).
3. Gehen Sie auf der Seite Typ der vertrauenswürdigen Entität auswählen wie folgt vor:
   a. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS -Service aus.
   b. Wählen Sie unter Anwendungsfall für Service oder Anwendungsfall die Option EC2 — Fleet aus.

      > **Tip**
      >
      > Achten Sie darauf, EC2 — Fleet auszuwählen. Wenn Sie EC2 wählen, wird der Anwendungsfall EC2 — Fleet nicht in der Liste der Anwendungsfälle angezeigt. Im Anwendungsfall EC2 — Fleet wird automatisch eine Richtlinie mit den erforderlichen IAM-Berechtigungen erstellt und AWSServiceRoleForEC2Fleetals Rollennamen vorgeschlagen.

   c. Wählen Sie Next (Weiter).
4. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
5. Wählen Sie auf der Seite Benennen, Überprüfen und Erstellen die Option Rolle erstellen aus.

Wenn Sie EC2 Fleet nicht mehr verwenden müssen, empfehlen wir Ihnen, die Rolle zu löschen. AWSServiceRoleForEC2Fleet Nachdem diese Rolle aus Ihrem Konto gelöscht wurde, können Sie die Rolle erneut anlegen, wenn Sie eine andere Flotte anlegen.

Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im -IAM-Benutzerhandbuch.

Gewähren von Zugriff auf von Kunden verwaltete Schlüssel zur Verwendung mit verschlüsselten AMIs und EBS-Snapshots

Wenn Sie in Ihrer EC2-Flotte ein verschlüsseltes AMI oder einen verschlüsselten Amazon EBS-Snapshot angeben und einen AWS KMS Schlüssel für die Verschlüsselung verwenden, müssen Sie der AWSServiceRoleForEC2FleetRolle die Berechtigung zur Verwendung des vom Kunden

verwalteten Schlüssels erteilen, damit Amazon EC2 Instances in Ihrem Namen starten kann. Dazu müssen Sie dem vom Kunden verwalteten Schlüssel eine Erteilung hinzufügen, wie im Folgenden gezeigt:

Bei der Einrichtung von Berechtigungen ist die Erteilung von Berechtigung eine Alternative zu Schüsselrichtlinien. Weitere Informationen finden Sie unter Verwenden von Erteilungen und Verwenden von Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

Um der AWSServiceRoleForEC2Fleet Rolle Berechtigungen zur Verwendung des vom Kunden verwalteten Schlüssels zu erteilen

- Verwenden Sie den Befehl create-grant, um dem vom Kunden verwalteten Schlüssel einen Zuschuss hinzuzufügen und den Prinzipal (die AWSServiceRoleForEC2Fleetdienstbezogene Rolle) anzugeben, dem die Berechtigung erteilt wird, die durch die Gewährung erlaubten Operationen auszuführen. Der vom Kunden verwaltete Schlüssel wird durch den `key-id`-Parameter und den ARN des vom Kunden verwalteten Schlüssels angegeben.
  Der Principal wird durch den `grantee-principal` Parameter und den ARN der AWSServiceRoleForEC2Fleetdienstverknüpften Rolle angegeben.

  ```
  aws kms create-grant \
      --region us-east-1 \
      --key-id arn:aws:kms:us-
  east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
      --grantee-principal arn:aws:iam::111122223333:role/AWSServiceRoleForEC2Fleet \
      --operations "Decrypt" "Encrypt" "GenerateDataKey"
   "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
   "ReEncryptTo"
  ```

Berechtigungen für EC2-Flotten-Benutzer

Wenn Ihre Benutzer eine EC2-Flotte erstellen oder verwalten, stellen Sie sicher, dass Sie ihnen die erforderlichen Berechtigungen gewähren.

So erstellen Sie eine Richtlinie für EC2-Flotte

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Policies aus.
3. Wählen Sie Richtlinie erstellen aus.

4. Wählen Sie auf der Seite Create policy (Richtlinie erstellen) die Registerkarte JSON, ersetzen Sie den Text durch den im Folgenden gezeigten Text, und wählen Sie Review policy (Richtlinie überprüfen).

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
              "iam:ListRoles",
              "iam:PassRole",
              "iam:ListInstanceProfiles"
            ],
            "Resource":"arn:aws:iam::123456789012:role/DevTeam*"
        }
    ]
}
```

`ec2:*` erteilt einem Benutzer die Berechtigung, alle Amazon-EC2-API-Aktionen aufzurufen. Sie können die Berechtigung eines Benutzer auf bestimmte Amazon EC2-API-Aktionen beschränken, indem Sie diese Aktionen stattdessen explizit angeben.

Der Benutzer muss über die Berechtigung verfügen, die folgenden Aktionen aufzurufen: `iam:ListRoles`, um vorhandene IAM-Rollen aufzulisten, `iam:PassRole`, um die Rolle für die EC2-Flotte anzugeben und `iam:ListInstanceProfiles`, um vorhandene Instance-Profile aufzulisten.

(Optional) Um einem Benutzer das Erstellen von Rollen oder Instance-Profilen mithilfe der IAM-Konsole zu ermöglichen, müssen Sie der Richtlinie auch die folgenden Aktionen hinzufügen:

- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`

- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

5. Geben Sie auf der Seite Review policy (Richtlinie überprüfen) einen Richtliniennamen und eine Beschreibung ein und wählen Sie anschließend Create policy (Richtlinie erstellen) aus.
6. Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

   - Benutzer und Gruppen in AWS IAM Identity Center:

     Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
   - Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

     Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
   - IAM-Benutzer:
     - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
     - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

EC2-Flotte-Zustandsprüfungen

EC2-Flotte überprüft den Zustand der Instances in der Flotte alle zwei Minuten. Der Zustand einer Instance lautet entweder `healthy` oder `unhealthy`.

EC2-Flotte bestimmt den Zustand einer Instance mit den von Amazon EC2 bereitgestellten Zustandsprüfungen. Eine Instance wird als `unhealthy` bestimmt, wenn der Status der Instance-Statusprüfung oder der Systemstatusprüfung für drei aufeinanderfolgende Zustandsprüfungen `impaired` ist. Weitere Informationen finden Sie unter Statusprüfungen für Ihre Instances.

Sie können Ihre Flotte so konfigurieren, dass nicht voll funktionsfähige Spot-Instances ersetzt werden. Nach der Festlegung von `ReplaceUnhealthyInstances` auf `true` wird eine Spot

Instance ersetzt, wenn sie als `unhealthy` gemeldet wird. Die Flotte kann die Zielkapazität einige Minuten lang unterschreiten, während eine nicht voll funktionsfähige Spot-Instance ersetzt wird.

Voraussetzungen

- Die Ersetzung im Zuge von Zustandsprüfungen wird nur für EC2-Flotten unterstützt, die eine Zielkapazität (Flotten vom Typ `maintain`) beibehalten und nicht für Flotten vom Typ `request` oder `instant`.
- Der Austausch von Zustandsprüfungen wird nur für Spot-Instances unterstützt. Diese Feature wird für On-Demand-Instances nicht unterstützt.
- Sie können Ihre EC2-Flotte nur beim Erstellen so konfigurieren, dass nicht voll funktionsfähige Instances ersetzt werden.
- Benutzer können die Ersetzung im Rahmen von Zustandsprüfungen nur verwenden, wenn sie über die Berechtigung zum Aufrufen der `ec2:DescribeInstanceStatus`-Aktion verfügen.

So konfigurieren Sie ein EC2-Flotte, um nicht voll funktionsfähige Spot-Instances zu ersetzen

1. Befolgen Sie die Schritte zum Erstellen von EC2-Flotte. Weitere Informationen finden Sie unter Erstellen einer EC2-Flotte.
2. Um die Flotte so zu konfigurieren, dass sie nicht voll funktionsfähige Spot-Instances ersetzt, geben Sie in der JSON-Datei für `ReplaceUnhealthyInstances` `true` ein.

Erzeugen einer EC2-Flotte-JSON-Konfigurationsdatei

Um die vollständige Liste der EC2-Flottenkonfigurationsparameter anzuzeigen, können Sie eine JSON-Datei erzeugen. Eine Beschreibung aller Parameter finden Sie unter create-fleet in der AWS CLI -Befehlsreferenz.

So erzeugen Sie eine JSON-Datei mit allen verfügbaren EC2-Flotte-Parametern über die Befehlszeile

- Verwenden Sie den Befehl create-fleet (AWS CLI) und den `--generate-cli-skeleton`-Parameter, um eine EC2-Flotten-JSON-Datei zu erzeugen und die Ausgabe zum Speichern in eine Datei umzuleiten.

```
aws ec2 create-fleet \
    --generate-cli-skeleton input > ec2createfleet.json
```

Beispielausgabe


```
{
    "DryRun": true,
    "ClientToken": "",
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch"
            }
        },
        "InstanceInterruptionBehavior": "hibernate",
        "InstancePoolsToUseCount": 0,
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "OnDemandOptions": {
        "AllocationStrategy": "prioritized",
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        },
        "SingleInstanceType": true,
        "SingleAvailabilityZone": true,
        "MinTargetCapacity": 0,
        "MaxTotalPrice": ""
    },
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "",
                "LaunchTemplateName": "",
                "Version": ""
            },
            "Overrides": [
                {
                    "InstanceType": "r5.metal",
                    "MaxPrice": "",
                    "SubnetId": "",
                    "AvailabilityZone": "",
```

```
                    "WeightedCapacity": 0.0,
                    "Priority": 0.0,
                    "Placement": {
                        "AvailabilityZone": "",
                        "Affinity": "",
                        "GroupName": "",
                        "PartitionNumber": 0,
                        "HostId": "",
                        "Tenancy": "dedicated",
                        "SpreadDomain": "",
                        "HostResourceGroupArn": ""
                    },
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "MemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        },
                        "CpuManufacturers": [
                            "amd"
                        ],
                        "MemoryGiBPerVCpu": {
                            "Min": 0.0,
                            "Max": 0.0
                        },
                        "ExcludedInstanceTypes": [
                            ""
                        ],
                        "InstanceGenerations": [
                            "previous"
                        ],
                        "SpotMaxPricePercentageOverLowestPrice": 0,
                        "OnDemandMaxPricePercentageOverLowestPrice": 0,
                        "BareMetal": "included",
                        "BurstablePerformance": "required",
                        "RequireHibernateSupport": true,
                        "NetworkInterfaceCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "LocalStorage": "excluded",
```

```
                        "LocalStorageTypes": [
                            "ssd"
                        ],
                        "TotalLocalStorageGB": {
                            "Min": 0.0,
                            "Max": 0.0
                        },
                        "BaselineEbsBandwidthMbps": {
                            "Min": 0,
                            "Max": 0
                        },
                        "AcceleratorTypes": [
                            "inference"
                        ],
                        "AcceleratorCount": {
                            "Min": 0,
                            "Max": 0
                        },
                        "AcceleratorManufacturers": [
                            "amd"
                        ],
                        "AcceleratorNames": [
                            "a100"
                        ],
                        "AcceleratorTotalMemoryMiB": {
                            "Min": 0,
                            "Max": 0
                        }
                    }
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 0,
        "OnDemandTargetCapacity": 0,
        "SpotTargetCapacity": 0,
        "DefaultTargetCapacityType": "on-demand",
        "TargetCapacityUnitType": "memory-mib"
    },
    "TerminateInstancesWithExpiration": true,
    "Type": "instant",
    "ValidFrom": "1970-01-01T00:00:00",
    "ValidUntil": "1970-01-01T00:00:00",
```

```
    "ReplaceUnhealthyInstances": true,
    "TagSpecifications": [
        {
            "ResourceType": "fleet",
            "Tags": [
                {
                    "Key": "",
                    "Value": ""
                }
            ]
        }
    ],
    "Context": ""
}
```

Erstellen einer EC2-Flotte

Um eine EC2-Flotte zu erstellen, müssen Sie nur die folgenden Parameter angeben:

- `LaunchTemplateId` oder `LaunchTemplateName` – Gibt die zu verwendende Startvorlage an (die die Parameter für die zu startenden Instances enthält, wie den Instance-Typ, die Availability Zone und den Höchstpreis, den Sie bereit sind zu zahlen)
- `TotalTargetCapacity` – Gibt die Gesamtzielkapazität für die Flotte an
- `DefaultTargetCapacityType` – Gibt an, ob die Standardkaufoption On-Demand oder Spot ist

Sie können mehrere Startspezifikationen angeben, die die Startvorlage überschreiben. Die Startspezifikationen können je nach Instance-Typ, Availability Zone, Subnetz und Höchstpreis variieren und eine andere gewichtete Kapazität enthalten. Alternativ können Sie die Attribute angeben, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen. Weitere Informationen finden Sie unter Attributbasierte Auswahl von Instance-Typen für EC2-Flotte.

Wenn Sie keinen Parameter angeben, verwendet die Flotte den Standardwert für den Parameter.

Geben Sie die Flottenparameter in einer JSON-Datei an. Weitere Informationen finden Sie unter Erzeugen einer EC2-Flotte-JSON-Konfigurationsdatei.

Derzeit wird das Erstellen einer EC2-Flotte in der Konsole nicht unterstützt.

So erstellen Sie eine EC2-Flotte (AWS CLI)

- Verwenden Sie den Befehl create-fleet (AWS CLI), um eine EC2-Flotte zu erstellen, und geben Sie die JSON-Datei an, die die Flottenkonfigurationsparameter enthält.

```
aws ec2 create-fleet --cli-input-json file://file_name.json
```

Beispiel-Konfigurationsdateien finden Sie unter EC2-Flotte-Beispielkonfigurationen.

Es folgt eine Beispielausgabe für eine Flotte des Typs `request` oder `maintain`:

```
{
    "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE"
}
```

Es folgt eine Beispielausgabe für eine Flotte des Typs `instant`, die die Zielkapazität gestartet hat:

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ],
      "InstanceType": "c5.large",
      "Platform": null
    },
    {
```

```
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-5678901234abcdef0",
        "i-5432109876abcdef9"
      ]
  ]
}
```

Es folgt eine Beispielausgabe für eine Flotte des Typs `instant`, die die Zielkapazität teilweise mit Fehlern für Instances gestartet hat, die nicht gestartet wurden:

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientInstanceCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": [
    {
      "LaunchTemplateAndOverrides": {
```

```
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a"
        }
      },
      "Lifecycle": "on-demand",
      "InstanceIds": [
        "i-1234567890abcdef0",
        "i-9876543210abcdef9"
      ]
  ]
}
```

Es folgt eine Beispielausgabe für eine Flotte des Typs `instant`, die keine Instances gestartet hat:

```
{
  "FleetId": "fleet-12a34b55-67cd-8ef9-ba9b-9208dEXAMPLE",
  "Errors": [
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
        "Overrides": {
          "InstanceType": "c4.xlarge",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
    {
      "LaunchTemplateAndOverrides": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "lt-01234a567b8910abcEXAMPLE",
          "Version": "1"
        },
```

```
        "Overrides": {
          "InstanceType": "c5.large",
          "AvailabilityZone": "us-east-1a",
        }
      },
      "Lifecycle": "on-demand",
      "ErrorCode": "InsufficientCapacity",
      "ErrorMessage": ""
    },
  ],
  "Instances": []
}
```

Markieren einer EC2-Flotte

Um die Kategorisierung und Verwaltung Ihrer EC2-Flotte-Anforderungen zu vereinfachen, können Sie sie mit benutzerdefinierten Metadaten markieren. Sie können einer EC2-Flotte-Anforderung beim Erstellen oder danach ein Tags (Markierungen) zuweisen.

Wenn Sie eine Flottenanforderung markieren, werden die Instances und Volumes, die von der Flotte gestartet werden, nicht automatisch markiert. Sie müssen die von der Flotte gestarteten Instances und Volumes explizit markieren. Sie können festlegen, dass Tags (Markierungen) nur der Flottenanforderung, nur den Instances, die von der Flotte gestartet werden oder nur den Volumes zugewiesen werden, die den Instances zugeordnet sind, die von der Flotte gestartet wurden oder allen drei.

> **Note**
>
> Bei `instant`-Flottentypen können Sie Volumes markieren, die an On-Demand-Instances und Spot-Instances angehängt sind. Bei `request`- oder `maintain`-Flottentypen können Sie nur Volumes markieren, die an On-Demand-Instances angehängt sind.

Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

Voraussetzung

Gewähren Sie dem Benutzer die Berechtigung zum Markieren von Ressourcen. Weitere Informationen finden Sie unter Beispiel: Markieren von Ressourcen.

So gewähren Sie einem Benutzer die Berechtigung zum Markieren von Ressourcen

Erstellen Sie eine IAM-Richtlinie, die Folgendes beinhaltet:

- Die Aktion `ec2:CreateTags`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen von Tags.
- Die Aktion `ec2:CreateFleet`. Dadurch wird dem Benutzer die Berechtigung zum Erstellen einer EC2-Flotten-Anfrage gewährt.
- Für `Resource` wird empfohlen, dass Sie `"*"` angeben. Dadurch können Benutzer alle Ressourcentypen markieren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagEC2FleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:CreateFleet"
            ],
            "Resource": "*"
}
```

Important

Derzeit unterstützen wir keine Berechtigungen auf Ressourcenebene für die `create-fleet`-Ressource. Wenn Sie `create-fleet` als Ressource angeben, erhalten Sie eine nicht autorisierte Ausnahme, wenn Sie versuchen, die Flotte zu markieren. Das folgende Beispiel veranschaulicht, wie die Richtlinie nicht festgelegt wird.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:CreateFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:create-fleet/*"
```

```
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

So markieren Sie eine neue EC2-Flotte-Anforderung

Um eine EC2-Flotte-Anforderungen beim Erstellen zu markieren, geben Sie das Schlüssel-Wert-Paar in der JSON-Datei an, mit der die Flotte erstellt wird. Der Wert für `ResourceType` muss `fleet` sein. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.

So markieren Sie Instances und Volumes, die durch eine EC2-Flotte gestartet werden

Um Instances und Volumes mit Tags zu markieren, wenn sie durch die Flotte gestartet werden, geben Sie die Tags in der Startvorlage an, auf die in der EC2-Flotte-Anforderung verwiesen wird.

> **Note**
>
> Sie können keine an Spot-Instances angehängt Volumes markieren, die von einem `request`- oder `maintain`-Flottentyp gestartet werden.

So markieren Sie eine vorhandene EC2-Flotten-Anforderung oder Instance oder ein vorhandenes Volume (AWS CLI)

Verwenden Sie den Befehl create-Tags, um vorhandene Ressourcen zu markieren.

```
aws ec2 create-tags \
    --resources fleet-12a34b55-67cd-8ef9-
ba9b-9208dEXAMPLE i-1234567890abcdef0 vol-1234567890EXAMPLE \
    --tags Key=purpose,Value=test
```

Beschreiben der EC2-Flotte

Sie können Ihre EC2-Flottenkonfiguration, die Instances in Ihrer EC2-Flotte und den Ereignisverlauf Ihrer EC2-Flotte beschreiben.

EC2-Flotten beschreiben (AWS CLI)

Verwenden Sie den Befehl describe-fleets, um Ihre EC2-Flotten zu beschreiben:

```
aws ec2 describe-fleets
```

Important

Wenn eine Flotte vom Typ `instant` ist, müssen Sie die Flotten-ID angeben. Anderenfalls wird sie in der Antwort nicht angezeigt. Schließen Sie `--fleet-ids` wie folgt ein:

```
aws ec2 describe-fleets --fleet-ids fleet-8a22eee4-f489-ab02-06b8-832a7EXAMPLE
```

Beispielausgabe

```
{
    "Fleets": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2022-02-09T03:35:52+00:00",
            "FleetId": "fleet-364457cd-3a7a-4ed9-83d0-7b63e51bb1b7",
            "FleetState": "active",
            "ExcessCapacityTerminationPolicy": "termination",
```

```
            "FulfilledCapacity": 2.0,
            "FulfilledOnDemandCapacity": 0.0,
            "LaunchTemplateConfigs": [
                {
                    "LaunchTemplateSpecification": {
                        "LaunchTemplateName": "my-launch-template",
                        "Version": "$Latest"
                    }
                }
            ],
            "TargetCapacitySpecification": {
                "TotalTargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "SpotTargetCapacity": 2,
                "DefaultTargetCapacityType": "spot"
            },
            "TerminateInstancesWithExpiration": false,
            "Type": "maintain",
            "ReplaceUnhealthyInstances": false,
            "SpotOptions": {
                "AllocationStrategy": "capacity-optimized",
                "InstanceInterruptionBehavior": "terminate"
            },
            "OnDemandOptions": {
                "AllocationStrategy": "lowestPrice"
            }
        }
    ]
}
```

Verwenden Sie den Befehl describe-fleet-instances, um die Instances für die angegebene EC2-Flotte zu beschreiben: Die zurückgegebene Liste der laufenden Instances wird regelmäßig aktualisiert und kann veraltet sein.

```
aws ec2 describe-fleet-instances  --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Beispielausgabe

```
{
    "ActiveInstances": [
        {
            "InstanceId": "i-09cd595998cb3765e",
```

```
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-86k84j6p"
        },
        {
            "InstanceId": "i-09cf95167ca219f17",
            "InstanceHealth": "healthy",
            "InstanceType": "m4.large",
            "SpotInstanceRequestId": "sir-dvxi7fsm"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Verwenden Sie den Befehl describe-fleet-history, um den Verlauf für die angegebene EC2-Flotte im angegebenen Zeitraum zu beschreiben:

```
aws ec2 describe-fleet-history --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE --start-time 2018-04-10T00:00:00Z
```

Beispielausgabe

```
{
    "HistoryRecords": [
        {
            "EventInformation": {
                "EventSubType": "submitted"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:05.000Z"
        },
        {
            "EventInformation": {
                "EventSubType": "active"
            },
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:15.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "t2.small, ami-07c8bc5c1ce9598c3, ...",
                "EventSubType": "progress"
            },
```

```
            "EventType": "fleetRequestChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-083a1c446e66085d2"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        },
        {
            "EventInformation": {
                "EventDescription": "{\"instanceType\":\"t2.small\", ...}",
                "EventSubType": "launched",
                "InstanceId": "i-090db02406cc3c2d6"
            },
            "EventType": "instanceChange",
            "Timestamp": "2020-09-01T18:26:17.000Z"
        }
    ],
    "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
    "LastEvaluatedTime": "1970-01-01T00:00:00.000Z",
    "StartTime": "2018-04-09T23:53:20.000Z"
}
```


Ändern einer EC2-Flotte

Sie können eine EC2-Flotte ändern, die sich im Zustand `submitted` oder `active` befindet. Wenn Sie eine Flotte ändern, wird sie in den `modifying`-Zustand versetzt.

Sie können nur ein EC2-Flotte mit dem Typ `maintain` ändern. Sie können ein EC2-Flotte des Typs `request` oder `instant` nicht ändern.

Sie können die folgenden Parameter einer EC2-Flotte ändern:

- `target-capacity-specification` – Zielkapazität für `TotalTargetCapacity`, `OnDemandTargetCapacity` und `SpotTargetCapacity` erhöhen oder verringern.
- `excess-capacity-termination-policy` – Ob laufende Instances beendet werden sollen, wenn die Gesamtzielkapazität der EC2-Flotte unter die aktuelle Flottengröße gesenkt wird. Gültige Werte sind `no-termination` und `termination`.

Wenn Sie die Zielkapazität erhöhen, startet die EC2-Flotte die zusätzlichen Instances entsprechend der Instance-Kaufoption, die für den `DefaultTargetCapacityType` angegeben wurde, die entweder On-Demand-Instances oder Spot-Instances sind.

Wenn ja `DefaultTargetCapacityTypespot`, startet die EC2-Flotte die zusätzlichen Spot-Instances entsprechend ihrer Zuweisungsstrategie.

Wenn Sie die Zielkapazität verringern, löscht die EC2-Flotte alle offenen Anfragen, die die neue Zielkapazität überschreiten. Sie können anfordern, dass die Flotte Instances beendet, bis die Größe der Flotte die neue Zielkapazität erreicht hat. Wenn die Zuweisungsstrategie `lowest-price` lautet, beendet die Flotte die Instances mit dem höchsten Preis pro Einheit. Wenn die Zuweisungsstrategie `diversified` lautet, beendet die Flotte Instances in allen Pools. Alternativ können Sie anfordern, dass die EC2-Flotte ihre aktuelle Größe beibehält, dabei jedoch keine Spot-Instances ersetzt, die unterbrochen werden, und keine Instances, die Sie manuell beenden.

Wenn eine EC2-Flotte eine Spot-Instance aufgrund einer Verringerung der Zielkapazität beendet, erhält die Instance eine Benachrichtigung über die Unterbrechung einer Spot-Instance.

So ändern Sie eine EC2-Flotte (AWS CLI)

Verwenden Sie den Befehl modify-fleet, um die Zielkapazität der angegebenen EC2-Flotte zu aktualisieren:

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=20
```

Wenn Sie die Zielkapazität verringern, die aktuelle Größe der Flotte jedoch beibehalten möchten, können Sie den vorherigen Befehl wie folgt ändern:

```
aws ec2 modify-fleet \
    --fleet-id fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity-specification TotalTargetCapacity=10 \
    --excess-capacity-termination-policy no-termination
```

Löschen einer EC2-Flotte

Wenn Sie eine EC2-Flotte nicht mehr benötigen, können Sie sie löschen. Nachdem Sie eine Flotte gelöscht haben, werden alle der Flotte zugeordneten Spot-Anfragen abgebrochen, sodass keine neuen Spot-Instances gestartet werden.

Wenn Sie eine EC2-Flotte löschen, müssen Sie auch angeben, ob Sie alle ihre Instances beenden möchten. Dazu gehören sowohl On-Demand-Instances als auch Spot-Instances. Bei `instant` Flotten muss EC2 Fleet die Instances beenden, wenn die Flotte gelöscht wird. Eine gelöschte `instant`-Flotte mit laufenden Instances wird nicht unterstützt.

Wenn Sie angeben, dass die Instances beim Löschen der Flotte beendet werden müssen, wird die Flotte in den `deleted_terminating`-Status versetzt. Andernfalls befindet sie sich im `deleted_running`-Zustand und die Instances werden weiter ausgeführt, bis sie unterbrochen oder von Ihnen manuell beendet werden.

Einschränkungen

- Sie können bis zu 25 Flotten des Typs `instant` in einer einzigen Anfrage löschen.
- Sie können bis zu 100 Flotten des Typs `maintain` oder `request` in einer einzigen Anfrage löschen.
- Sie können bis zu 125 Flotten in einer einzigen Anfrage löschen, sofern Sie das oben angegebene Kontingent für jeden Flottentyp nicht überschreiten.
- Wenn Sie die angegebene Anzahl an zu löschenden Flotten überschreiten, werden keine Flotten gelöscht.
- Bis zu 1000 Instances können in einer einzigen Anfrage zum Löschen von `instant`-Flotten beendet werden.

So löschen Sie eine EC2-Flotte und beenden ihre Instances (AWS CLI)

Verwenden Sie den delete-fleets-Befehl und den `--terminate-instances`-Parameter, um die angegebene EC2-Flotte zu löschen und die zugehörigen Instances zu beenden.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Beispielausgabe

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_terminating",
```

```
            "PreviousFleetState": "active",
            "FleetId": "fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
        }
    ]
}
```

So löschen Sie eine EC2-Flotte, ohne deren Instances zu beenden (AWS CLI)

Sie können den vorherigen Befehl mit dem `--no-terminate-instances`-Parameter ändern, um die angegebene EC2-Flotte zu löschen, ohne die zugehörigen Instances zu beenden.

> **Note**
>
> `--no-terminate-instances` wird nicht für `instant`-Flotten unterstützt.

```
aws ec2 delete-fleets \
    --fleet-ids fleet-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Beispielausgabe

```
{
    "UnsuccessfulFleetDeletions": [],
    "SuccessfulFleetDeletions": [
        {
            "CurrentFleetState": "deleted_running",
            "PreviousFleetState": "active",
            "FleetId": "fleet-4b8aaae8-dfb5-436d-a4c6-3dafa4c6b7dcEXAMPLE"
        }
    ]
}
```

Beheben von Fehlern, wenn eine Flotte nicht gelöscht werden kann

Wenn ein EC2-Flotte nicht gelöscht werden kann, gibt `UnsuccessfulFleetDeletions` in der Ausgabe die ID des EC2-Flotte, einen Fehlercode und eine Fehlermeldung zurück.

Die Fehlercodes sind:

- `ExceededInstantFleetNumForDeletion`

- `fleetIdDoesNotExist`
- `fleetIdMalformed`
- `fleetNotInDeletableState`
- `NoTerminateInstancesNotSupported`
- `UnauthorizedOperation`
- `unexpectedError`

Fehlerbehebung für **`ExceededInstantFleetNumForDeletion`**

Wenn Sie versuchen, mehr als 25 `instant`-Flotten in einer einzigen Anfrage zu löschen, wird der `ExceededInstantFleetNumForDeletion`-Fehler zurückgegeben. Es folgt eine Beispielausgabe für diesen Fehler.

```
{
    "UnsuccessfulFleetDeletions": [
     {
          "FleetId": " fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
          "Error": {
                 "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
           }
     },
     {
           "FleetId": "fleet-9a941b23-0286-5bf4-2430-03a029a07e31",
           "Error": {
                 "Message": "Can’t delete more than 25 instant fleets in a single
 request.",
                 "Code": "ExceededInstantFleetNumForDeletion"
            }
     }
     .
     .
     .
     ],
     "SuccessfulFleetDeletions": []
}
```

Fehlerbehebung bei **`NoTerminateInstancesNotSupported`**

Wenn Sie angeben, dass die Instances in einer `instant`-Flotte beim Löschen der Flotte nicht beendet werden dürfen, wird der `NoTerminateInstancesNotSupported`-Fehler zurückgegeben. `--no-terminate-instances` wird nicht für `instant`-Flotten unterstützt. Es folgt eine Beispielausgabe für diesen Fehler.

```
{
      "UnsuccessfulFleetDeletions": [
            {
                  "FleetId": "fleet-5d130460-0c26-bfd9-2c32-0100a098f625",
                  "Error": {
                         "Message": "NoTerminateInstances option is not supported for
 instant fleet",
                         "Code": "NoTerminateInstancesNotSupported"
                   }
            }
       ],
       "SuccessfulFleetDeletions": []
```

Fehlerbehebung bei **`UnauthorizedOperation`**

Wenn Sie keine Berechtigung zum Beenden von Instances haben, erhalten Sie den `UnauthorizedOperation`-Fehler beim Löschen einer Flotte, die ihre Instances beenden muss. Das Folgende ist die Fehlerantwort.

```
<Response><Errors><Error><Code>UnauthorizedOperation</Code><Message>You are not
 authorized to perform this
operation. Encoded authorization failure message: VvuncIxj7Z_CPGNYXWqnuFV-
YjByeAU66Q9752NtQ-I3-qnDLWs6JLFd
KnSMMiq5s6cGqjjPtEDpsnGHzzyHasFHOaRYJpaDVravoW25azn6KNkUQQlFwhJyujt2dtNCdduJfrqcFYAjlEiRMkfDHt7
BHturzDK6A560Y2nDSUiMmAB1y9UNtqaZJ9SNe5sNxKMqZaqKtjRbk02RZu5V2vn9VMk6fm2aMVHbY9JhLvGypLcMUjtJ76
VPiU5v2s-
UgZ7h0p2yth6ysUdhlONg6dBYu8_y_HtEI54invCj4CoK0qawqzMNe6rcmCQHvtCxtXsbkgyaEbcwmrm2m01-
EMhekLFZeJLr
DtYOpYcEl4_nWFX1wtQDCnNNCmxnJZAoJvb3VMDYpDTsxjQv1PxODZuqWHs23YXWVywzgnLtHeRf2o4lUhGBw17mXsS07k7
PT9vrHtQiILor5VVTsjSPWg7edj__1rsnXhwPSu8gI48ZLRGrPQqFq0RmKO_QIE8N8s6NWzCK4yoX-9gDcheurOGpkprPIC
</Message></Error></Errors><RequestID>89b1215c-7814-40ae-a8db-41761f43f2b0</
RequestID></Response>
```

Um den Fehler zu beheben, müssen Sie die `ec2:TerminateInstances`-Aktion der IAM-Richtlinie hinzufügen, wie im folgenden Beispiel gezeigt.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
         {
             "Sid": "DeleteFleetsAndTerminateInstances",
             "Effect": "Allow",
             "Action": [
                    "ec2:DeleteFleets"
                    "ec2:TerminateInstances"
             ],
             "Resource": "*"
         }
    ]
}
```

Spot-Flotte

Eine Spot-Flotte ist eine Reihe von Spot-Instances und optional auch On-Demand-Instances, die basierend auf von Ihnen festgelegten Kriterien gestartet wird. Die Spot-Flotte wählt die Spot-Kapazitätspools aus, die Ihre Anforderungen erfüllen, und startet Spot-Instances, um die Zielkapazität für die Flotte zu erfüllen. Spot-Flotten sind standardmäßig so eingestellt, dass sie die Zielkapazität aufrechterhalten, indem nach der Beendigung von Spot-Instances in der Flotte Ersatz-Instances gestartet werden. Sie können eine Spot-Flotte als einmalige Anforderung übermitteln; diese wird nicht beibehalten, nachdem die Instances beendet wurden. Sie können On-Demand-Instance-Anforderungen in einer Spot-Flotten-Anforderung einschließen.

> **Note**
>
> Wenn Sie eine Konsole verwenden möchten, um eine Flotte zu erstellen, die Spot Instances enthält, empfehlen wir, eine Auto-Scaling-Gruppe anstelle der Spot-Flotte zu verwenden. Weitere Informationen finden Sie unter Auto-Scaling-Gruppen mit mehreren Instance-Typen und Kaufoptionen im Amazon EC2 Auto Scaling-Benutzerhandbuch.
> Wenn Sie die verwenden möchten, um eine Flotte AWS CLI zu erstellen, die Spot-Instances enthält, empfehlen wir, anstelle einer Spot-Flotte entweder eine Auto Scaling-Gruppe oder eine EC2-Flotte zu verwenden. Die RequestSpotFleet API, auf der Spot Fleet basiert, ist eine ältere API ohne geplante Investitionen.
> Für weitere Informationen zu den empfohlenen APIs, siehe Was ist die beste Spot-Request-Methode?

Themen

Spot-Flotte-Anforderungstypen

Es gibt zwei Arten von Spot-Flotten-Anforderungen:

`request`

Wenn Sie den Anforderungstyp als `request` konfigurieren, erstellt Spot-Flotte eine einmalige, asynchrone Anforderung für Ihre gewünschte Kapazität. Dann versucht die Flotte nicht, Spot-Instances aufzufüllen, wenn die Kapazität aufgrund von Spot-Unterbrechungen verringert ist, und sie stellt keine Anträge in alternativen Spot-Kapazitätspools, wenn die Kapazität nicht verfügbar ist.

`maintain`

Wenn Sie den Anforderungstyp als `maintain` konfigurieren, erstellt Spot-Flotte eine asynchrone Anforderung für Ihre gewünschte Kapazität und erhält die Kapazität aufrecht, indem sie alle unterbrochenen Spot-Instances automatisch auffüllt.

Um den Typ der Anforderung in der Amazon EC2 Konsole anzugeben, gehen Sie beim Erstellen einer Spot-Fleet-Anforderung wie folgt vor:

- Um eine Spot-Flotte des Typs `request` zu erstellen, löschen Sie das Kontrollkästchen Erhalten der Zielkapazität.
- Um eine Spot-Flotte des Typs `maintain` zu erstellen, wählen Sie das Kontrollkästchen Erhalten der Zielkapazität aus.

Weitere Informationen finden Sie unter Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole).

Beide Anfragetypen profitieren von einer Zuweisungsstrategie. Weitere Informationen finden Sie unter Zuweisungsstrategien für Spot-Instances.

Spot-Flotte-Konfigurationsstrategien

Eine Spot-Flotte ist eine Sammlung oder Flotte von Spot-Instances und optional auch On-Demand-Instances.

Die Spot-Flotte versucht, die Anzahl an Spot-Instances und On-Demand-Instances zu starten, um die in Ihrer Spot-Flotten-Anforderung angegebene Zielkapazität zu erreichen. Die Anforderung von Spot-Instances ist erfüllt, wenn der Höchstpreis, den Sie in der Anfrage angegeben haben, den aktuellen Spot-Preis übersteigt und freie Kapazität vorhanden ist. Die Spot-Flotte versucht auch, ihre Ziel-Kapazitätsflotte beizubehalten, wenn Ihre Spot-Instances unterbrochen werden.

Sie können auch einen Maximalbetrag pro Stunde festlegen, den Sie für Ihre Flotte zu zahlen bereit sind. Dann startet die Spot-Flotte Instances, bis der Maximalbetrag erreicht ist. Wenn der Maximalbetrag erreicht ist, den Sie bereit sind zu zahlen, startet die Flotte keine Instances mehr, auch wenn die Zielkapazität noch nicht erreicht ist.

Ein Spot-Kapazitätspool ist ein Satz von ungenutzten EC2-Instances mit demselben Instance-Typ (z. B. `m5.large`), Betriebssystem sowie derselben Availability Zone und Netzwerkplattform. Wenn Sie eine Spot-Flotten-Anforderung erstellen, können Sie mehrere Startspezifikationen einschließen, die sich in Bezug auf den Instance-Typ, das AMI, die Availability Zone oder das Subnetz unterscheiden. Die Spot-Flotte wählt die Spot-Kapazitätspools aus, die zur Erfüllung der Anfrage verwendet werden, basierend auf den in Ihrer Spot-Flotten-Anfrage enthaltenen Startspezifikationen und der Konfiguration der Spot-Flotten-Anfrage. Die Spot-Instances stammen aus den ausgewählten Pools.

Inhalt

Planen einer Spot-Flotten-Anforderung

Bevor Sie eine Spot-Flotten-Anforderung erstellen, lesen Sie bitte Spot – Best Practices. Verwenden Sie diese bewährten Methoden beim Planen Ihrer Spot-Flotten-Anforderung, damit Sie die gewünschten Instance-Typen zu einem möglichst niedrigen Preis bereitstellen können. Wir empfehlen außerdem Folgendes:

- Legen Sie fest, ob Sie eine Spot-Flotte erstellen möchten, die eine einmalige Anforderung für die gewünschte Zielkapazität übermittelt oder eine, die eine Zielkapazität dauerhaft aufrechterhält.
- Ermitteln Sie die Instance-Typen, die Ihre Anwendungsanforderungen am besten erfüllen.
- Legen Sie die Zielkapazität für Ihre Spot-Flotten-Anforderung fest. Sie können die Zielkapazität in Instances oder in benutzerdefinierten Einheiten angeben. Weitere Informationen finden Sie unter Instance-Gewichtung für Spot-Flotten.

- Bestimmen Sie, welcher Anteil der Spot-Flotten-Zielkapazität On-Demand-Kapazität sein muss. Sie können für "On-Demand-Kapazität" 0 angeben.
- Legen Sie Ihren Preis pro Einheitsstunde fest, wenn Sie die Instance-Gewichtung verwenden. Zum Berechnen des Preises pro Einheit teilen Sie den Preis pro Instance-Stunde durch die Anzahl an Einheiten (oder Gewichtung), die diese Instance darstellt. Wenn Sie die Instance-Gewichtung nicht verwenden, entspricht der Standard-Preis pro Einheit dem Preis pro Instance-Stunde.
- Prüfen Sie die möglichen Optionen für Ihre Spot-Flotten-Anforderung. Weitere Informationen finden Sie unter dem Befehl request-spot-fleet in der AWS CLI -Befehlsreferenz. Weitere Beispiele finden Sie unter Beispielkonfigurationen für Spot-Flotte.

Zuweisungsstrategien für Spot-Instances

Ihre Startkonfiguration bestimmt alle möglichen Spot-Kapazitätspools (Instance-Typen und Availability Zones), aus denen Spot Fleet Spot-Instances starten kann. Beim Starten von Instances nutzt Spot Fleet jedoch die von Ihnen angegebene Zuweisungsstrategie, um die jeweiligen Pools aus allen möglichen Pools auszuwählen.

> **Note**
>
> (Nur Linux-Instances) Wenn Sie Ihre Spot-Instance so konfigurieren, dass sie mit aktiviertem AMD SEV-SNP gestartet wird, wird Ihnen eine zusätzliche Nutzungsgebühr pro Stunde berechnet, die 10% des On-Demand-Stundensatzes für den ausgewählten Instance-Typ entspricht. Wenn die Zuweisungsstrategie den Preis als Eingabe verwendet, berücksichtigt die EC2-Flotte diese zusätzliche Gebühr nicht. Es wird nur der Spot-Preis verwendet.

Zuweisungsstrategien

Sie können eine der folgenden Zuweisungsstrategien für Spot Instances angeben:

`priceCapacityOptimized`(empfohlen)

Spot-Flotte identifiziert die Pools mit der höchsten Kapazitätsverfügbarkeit für die Anzahl der gestarteten Instances. Das bedeutet, dass wir Spot-Instances aus den Pools anfordern werden, von denen wir glauben, dass sie in naher Zukunft die geringste Wahrscheinlichkeit einer Unterbrechung haben. Die Spot-Flotte fordert dann Spot-Instances aus dem günstigsten dieser Pools an.

Die `priceCapacityOptimized`-Zuweisungsstrategie ist die beste Wahl für die meisten Spot-Workloads, z. B. statuslose containerisierte Anwendungen, Microservices, Webanwendungen, Daten- und Analytikaufträge sowie Batchverarbeitung.

`capacityOptimized`

Die Spot-Flotte identifiziert die Pools mit der höchsten Kapazitätsverfügbarkeit für die Anzahl der Instances, die gestartet werden. Das bedeutet, dass wir Spot Instances aus den Pools anfordern werden, von denen wir glauben, dass die Wahrscheinlichkeit einer kurzfristigen Unterbrechung am geringsten ist. Sie können optional eine Priorität für jeden Instance-Typ in Ihrer Flotte mit festlege `capacityOptimizedPrioritized`. Die Spot-Flotte optimiert zuerst die Kapazität, beachtet jedoch die Prioritäten der Instance-Typen so gut wie möglich.

Im Fall von Spot-Instances ändern sich die Preise allmählich im Lauf der Zeit, basierend auf langfristigen Trends bei Angebot und Nachfrage. Die Kapazität fluktuiert jedoch in Echtzeit. Bei Anwendung der Strategie `capacityOptimized` wird Spot-Instances automatisch zu den am besten verfügbaren Pools gestartet, indem Echtzeitdaten zur Kapazität analysiert werden und prognostiziert wird, welche Pools am besten verfügbar sind. Diese Strategie ist gut für Workloads, bei denen Unterbrechungen aufgrund von Neustarts von Aufgaben höhere Kosten verursachen, wie Continuous Integration (CI), Image- und Medien-Rendering, Deep Learning und High Performance Compute (HPC)-Workloads, bei denen Unterbrechungen höhere Kosten verursachen, da Aufgaben neu gestartet werden müssen. Da die `capacityOptimized`-Strategie die Zahl der Unterbrechungen reduzieren kann, trägt sie zur Senkung der Gesamtkosten Ihrer Workload bei.

Alternativ können Sie die `capacityOptimizedPrioritized`-Zuweisungsstrategie mit einem Prioritätsparameter verwenden, um die Instance-Typen von der höchsten zur niedrigsten Priorität zu ordnen. Sie können die gleiche Priorität für verschiedene Instance-Typen festlegen. Die Spot-Flotte wird zuerst für die Kapazität optimiert, berücksichtigt jedoch so gut wie möglich die Prioritäten der Instance-Typen (wenn z. B. die Berücksichtigung der Prioritäten keinen wesentlichen Einfluss auf die Fähigkeit der Spot-Flotte zur Bereitstellung optimaler Kapazität hat). Dies ist eine gute Option für Workloads, bei denen die Möglichkeit von Unterbrechungen minimiert werden muss und die Präferenz für bestimmte Instance-Typen wichtig ist. Die Verwendung von Prioritäten wird nur unterstützt, wenn Ihre Flotte eine Startvorlage verwendet. Beachten Sie Folgendes: Wenn Sie die Priorität für `capacityOptimizedPrioritized` festlegen, wird die gleiche Priorität auch auf Ihre On-Demand-Instances angewendet, wenn die On-Demand-`AllocationStrategy` auf `prioritized` eingestellt ist.

`diversified`

Die Spot-Instances sind über alle Pools verteilt.

Auswahl einer geeigneten Zuweisungsstrategie

Sie können Ihre Flotte für Ihren Anwendungsfall optimieren, indem Sie die entsprechende Spot-Zuweisungsstrategie wählen. Für die Zielkapazität von On-Demand-Instances wählt Spot Fleet immer den günstigsten Instance-Typ auf der Grundlage des öffentlichen On-Demand-Preises aus und folgt dabei der Zuweisungsstrategie — entweder `priceCapacityOptimizedcapacityOptimized`, oder `diversified` — für Spot-Instances.

Gleichgewicht zwischen niedrigstem Preis und Kapazitätsverfügbarkeit

Um die Kompromisse zwischen den Spot-Kapazitätspools mit dem niedrigsten Preis und den Spot-Kapazitätspools mit der höchsten Kapazitätsverfügbarkeit auszugleichen, empfehlen wir, die `priceCapacityOptimized`-Zuweisungsstrategie zu verwenden. Bei dieser Strategie werden Entscheidungen darüber getroffen, von welchen Pools Spot Instances angefordert werden sollen, sowohl auf der Grundlage des Preises der Pools als auch der Kapazitätsverfügbarkeit der Spot Instances in diesen Pools. Das bedeutet, dass wir Spot Instances aus den Pools anfordern werden, von denen wir glauben, dass die Wahrscheinlichkeit einer kurzfristigen Unterbrechung am geringsten ist, wobei der Preis weiterhin berücksichtigt wird.

Wenn Ihre Flotte belastbare und statuslose Workloads ausführt, einschließlich containerisierter Anwendungen, Microservices, Webanwendungen, Daten- und Analysejobs sowie Stapelverarbeitung, dann sollten Sie die `priceCapacityOptimized`-Zuweisungsstrategie verwenden, um optimale Kosteneinsparungen und Kapazitätsverfügbarkeit zu erzielen.

Wenn Ihre Flotte Workloads ausführt, bei denen Unterbrechungen aufgrund von Neustarts von Aufgaben höhere Kosten verursachen, sollten Sie Checkpointing implementieren, damit die Anwendungen von dem Punkt aus neu gestartet werden können, an dem sie unterbrochen wurden. Durch die Verwendung von Checkpointing passen Sie die `priceCapacityOptimized`-Zuweisungsstrategie an diese Workloads an, da sie Kapazität aus den Pools mit dem niedrigsten Preis zuweist, die auch eine niedrige Spot Instance-Unterbrechungsrate bieten.

Eine Beispielkonfiguration, die die `priceCapacityOptimized`-Zuweisungsstrategie verwendet, finden Sie unter Beispiel 9: Starten Sie Spot-Instances in einer kapazitätsoptimierten Flotte mit Prioritäten.

Wenn Workloads mit hohen Unterbrechungskosten verbunden sind

Sie können die `capacityOptimized`-Strategie optional verwenden, wenn Sie Workloads ausführen, die entweder Instance-Typen mit ähnlichen Preisen verwenden oder bei denen die Kosten einer Unterbrechung so hoch sind, dass jegliche Kostenersparnis im Vergleich zu einer geringfügigen Zunahme der Unterbrechungen nicht ausreicht. Bei dieser Strategie wird die Kapazität aus den am besten verfügbaren Spot-Kapazitätspools zugewiesen, die die Möglichkeit von weniger Unterbrechungen bieten, was die Gesamtkosten Ihres Workloads senken kann. Eine Beispielkonfiguration, die die `capacityOptimized`-Zuweisungsstrategie verwendet, finden Sie unter Beispiel 7: Konfigurieren Sie den Kapazitätsausgleich, um Ersatz-Spot-Instances zu starten.

Wenn die Möglichkeit von Unterbrechungen minimiert werden muss, aber die Präferenz für bestimmte Instance-Typen wichtig ist, können Sie Ihre Pool-Prioritäten ausdrücken, indem Sie die `capacityOptimizedPrioritized`-Zuweisungsstrategie verwenden und dann die Reihenfolge der zu verwendenden Instance-Typen von der höchsten zur niedrigsten Priorität festlegen. Eine Beispielkonfiguration finden Sie unter Beispiel 8: Starten Sie Spot-Instances in einer kapazitätsoptimierten Flotte.

Beachten Sie, dass die Verwendung von Prioritäten nur unterstützt wird, wenn Ihre Flotte eine Startvorlage verwendet. Beachten Sie außerdem: Wenn Sie Prioritäten für `capacityOptimizedPrioritized` festlegen, werden die gleichen Prioritäten auch auf Ihre On-Demand-Instances angewendet, wenn die On-Demand-`AllocationStrategy` auf `prioritized` eingestellt ist.

Wenn Ihr Workload zeitlich flexibel ist und die Kapazitätsverfügbarkeit kein Faktor ist

Wenn Ihre Flotte klein ist oder nur für einen kurzen Zeitraum ausgeführt wird, können Sie `priceCapacityOptimized` nutzen, um die Kosteneinsparungen zu maximieren und dabei die Kapazitätsverfügbarkeit zu berücksichtigen.

Wenn Ihre Flotte groß ist oder lange läuft

Wenn Ihre Flotte groß ist oder für einen langen Zeitraum ausgeführt wird, können Sie die Verfügbarkeit Ihrer Flotte verbessern, indem Sie die Spot-Instances mit der `diversified`-Strategie über mehrere Pools verteilen. Wenn Ihre Spot-Flotten-Anforderung beispielsweise 10 Pools und eine Zielkapazität von 100 Instances angibt, startet die Flotte 10 Spot-Instances pro Pool. Wenn der Spot-Preis für einen Pool Ihren Höchstpreis für diesen Pool übersteigt, sind nur 10 % Ihrer Flotte betroffen. Bei dieser Strategie reagiert Ihre Flotte außerdem weniger empfindlich auf Steigerungen des Spot-Preises für die verschiedenen Pools im Laufe der Zeit. Bei der `diversified`-Strategie

startet die Spot-Flotte keine Spot-Instances in Pools mit einem Spot-Preis, der auf dem Niveau des On-Demand-Preises oder darüber liegt.

Erhalten der Zielkapazität

Wenn Spot Instances aufgrund einer Änderung in Bezug auf den Spot-Preis oder die verfügbare Kapazität eines Spot-Kapazitätspools beendet werden, startet eine Spot-Flotte vom Typ `maintain` Ersatz-Spot-Instances. Die Zuweisungsstrategie bestimmt die Pools, von denen aus die Ersatz-Instances gestartet werden, wie folgt:

- Wenn die Zuweisungsstrategie `priceCapacityOptimized` ist, startet die Flotte Ersatz-Instances in den Pools mit der größten Spot-Instance-Kapazitätsverfügbarkeit. Dabei wird auch der Preis berücksichtigt und die günstigsten Pools mit hoher Kapazitätsverfügbarkeit identifiziert.
- Wenn die Zuweisungsstrategie `capacityOptimized` ist, startet die Flotte Ersatz-Instances in den Pools mit der größten verfügbaren Spot Instance-Kapazität.
- Wenn die Zuweisungsstrategie `diversified` lautet, verteilt die Flotte die Ersatz-Spot-Instances über die verbleibenden Pools.

Attributbasierte Auswahl von Instance-Typen für Spot-Flotte

Wenn Sie eine Spot-Flotte erstellen, müssen Sie mindestens einen Instance-Typ für die Konfiguration der On-Demand-Instances und Spot-Instances in der Flotte angeben. Alternativ zur manuellen Angabe der Instance-Typen können Sie die Attribute angeben, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen. Dies ist bekannt als attributbasierte Instance-Typauswahl. Sie können beispielsweise die minimale und maximale Anzahl von vCPUs angeben, die für Ihre Instances erforderlich sind, und die Spot-Flotte startet die Instances mit allen verfügbaren Instance-Typen, die diese vCPU-Anforderungen erfüllen.

Die attributbasierte Auswahl von Instance-Typen ist ideal für Workloads und Frameworks, die hinsichtlich der verwendeten Instance-Typen flexibel sein können, etwa beim Ausführen von Containern oder Web-Flotten, beim Verarbeiten von Big Data und der Implementierung von Tools zur fortlaufenden Integration und Bereitstellung (CI/CD).

Vorteile

Die Auswahl des attributbasierten Instance-Typs bietet folgende Vorteile:

- Einfache Verwendung der richtigen Instance-Typen — Bei so vielen verfügbaren Instance-Typen kann es zeitaufwändig sein, die richtigen Instance-Typen für Ihren Workload zu finden. Wenn Sie

Instance-Attribute angeben, haben die Instance-Typen automatisch die erforderlichen Attribute für Ihre Workload.

- Vereinfachte Konfiguration — Um mehrere Instance-Typen für eine Spot-Flotte manuell anzugeben, müssen Sie für jeden Instance-Typ eine separate Überschreibung der Startvorlage erstellen. Bei der attributbasierten Auswahl von Instance-Typen müssen Sie jedoch nur die Instance-Attribute in der Startvorlage oder in einer Startvorlagen-Überschreibung angeben, um mehrere Instance-Typen bereitzustellen.
- Automatische Verwendung neuer Instance-Typen — Wenn Sie Instance-Attribute anstelle von Instance-Typen angeben, kann Ihre Flotte Instance-Typen der neueren Generation verwenden, sobald sie veröffentlicht werden, was die Konfiguration der Flotte „zukunftssicher“ macht.
- Flexibilität beim Instance-Typ — Wenn Sie Instance-Attribute anstelle von Instance-Typen angeben, kann Spot Fleet für den Start von Spot-Instances aus einer Vielzahl von Instance-Typen wählen. Dies entspricht den bewährten Methoden von Spot zur Flexibilität von Instance-Typen.

Themen

Attributbasierte Auswahl von Instance-Typen

Um die attributbasierte Auswahl von Instance-Typen in Ihrer Flottenkonfiguration zu verwenden, ersetzen Sie die Liste der Instance-Typen durch eine Liste von Instance-Attributen, die Ihre Instances erfordern. Die Spot-Flotte startet Instances für alle verfügbaren Instance-Typen mit den angegebenen Instance-Attributen.

Themen

Arten von Instance-Attributen

Es gibt mehrere Instance-Attribute, die Sie angeben können, um Ihre Rechenanforderungen auszudrücken, wie zum Beispiel:

- vCPU-Anzahl — Die minimale und maximale Anzahl von vCPUs pro Instanz.
- Arbeitsspeicher — Das Minimum und das Maximum an Arbeitsspeicher GiBs pro Instanz.
- Lokaler Speicher — Ob EBS- oder Instance-Speicher-Volumes für den lokalen Speicher verwendet werden sollen.
- Spitzenleistung — Ob die T-Instance-Familie verwendet werden soll, einschließlich der Typen T4g, T3a, T3 und T2.

Eine Beschreibung der einzelnen Attribute und der Standardwerte finden Sie InstanceRequirementsin der Amazon EC2 API-Referenz.

Wo wird die attributbasierte Auswahl von Instance-Typen konfiguriert?

Je nachdem, ob Sie die Konsole oder die verwenden AWS CLI, können Sie die Instance-Attribute für die attributbasierte Auswahl des Instance-Typs wie folgt angeben:

In der Konsole können Sie die Instance-Attribute in einer oder beiden der folgenden Flottenkonfigurationskomponenten angeben:

- In einer Startvorlage. Verweisen Sie dann in der Flottenanforderung auf die Startvorlage
- In der Flottenanforderung

In der AWS CLI können Sie die Instance-Attribute in einer oder allen der folgenden Flottenkonfigurationskomponenten angeben:

- In einer Startvorlage. Verweisen Sie in der Flottenanforderung auf die Startvorlage.
- In einer Startvorlagen-Überschreibung

  Wenn Sie eine Mischung aus Instances wünschen, die verschiedene AMIs verwenden, können Sie Instance-Attribute in mehreren Startvorlagen-Überschreibungen angeben. Zum Beispiel können verschiedene Instance-Typen x86- und ARM-basierte Prozessoren verwenden.
- In einer Startspezifikation

Wie die Spot-Flotte bei der Bereitstellung einer Flotte die attributbasierte Auswahl von Instance-Typen verwendet

Die Spot-Flotte stellt eine Flotte auf folgende Weise bereit:

- Die Spot-Flotte identifiziert die Instance-Typen mit den angegebenen Attributen.
- Die Spot-Flotte bestimmt anhand des Preisschutzes, welche Instance-Typen ausgeschlossen werden sollen.
- Spot Fleet bestimmt anhand der AWS Regionen oder Availability Zones, die über die entsprechenden Instance-Typen verfügen, die Kapazitätspools, aus denen der Start der Instances in Betracht gezogen wird.
- Die Spot-Flotte wendet die angegebene Zuweisungsstrategie an, um zu bestimmen, aus welchen Kapazitätspools die Instances gestartet werden sollen.

  Beachten Sie, dass die attributbasierte Auswahl von Instance-Typen nicht die Kapazitätspools auswählt, aus denen die Flotte bereitgestellt werden soll. Dies ist die Aufgabe der Zuweisungsstrategien. Es kann eine große Anzahl von Instance-Typen mit den angegebenen Attributen geben und einige von ihnen sind unter Umständen teuer.

  Wenn Sie eine Zuweisungsstrategie angeben, startet die Spot-Flotte Instances gemäß der angegebenen Zuweisungsstrategie.

  - Bei Spot-Instances unterstützt die attributbasierte Auswahl von Instance-Typen die `capacityOptimizedPrioritized`- und `capacityOptimized`- Zuweisungsstrategien.
  - Bei On-Demand-Instances unterstützt die attributbasierte Auswahl des Instance-Typs die `lowestPrice` Zuweisungsstrategie, die garantiert, dass Spot Fleet On-Demand-Instances aus den kostengünstigsten Kapazitätspools startet.
- Wenn es keine Kapazität für die Instance-Typen mit den angegebenen Instance-Attributen gibt, können keine Instances gestartet werden und die Flotte gibt einen Fehler zurück.

Preisschutz

Der Preisschutz ist ein Feature, die verhindert, dass Ihre Spot-Flotte Instance-Typen verwendet, die Sie für zu teuer halten würden, selbst wenn sie den von Ihnen angegebenen Attributen entsprechen. Um den Preisschutz zu nutzen, legen Sie einen Preisgrenzwert fest. Wenn Amazon EC2 dann Instance-Typen mit Ihren Attributen auswählt, schließt es Instance-Typen aus, deren Preis über Ihrem Schwellenwert liegt.

Amazon EC2 berechnet den Preisschwellenwert wie folgt:

- Amazon EC2 identifiziert zunächst den Instance-Typ mit dem niedrigsten Preis aus den Instance-Typen, die Ihren Attributen entsprechen.
- Amazon EC2 nimmt dann den Wert (ausgedrückt als Prozentsatz), den Sie für den Preisschutzparameter angegeben haben, und multipliziert ihn mit dem Preis des identifizierten Instance-Typs. Das Ergebnis ist der Preis, der als Preisschwellenwert verwendet wird.

Es gibt separate Preisschwellen für On-Demand-Instances und Spot-Instances.

Wenn Sie eine Flotte mit attributbasierter Instance-Typauswahl erstellen, ist der Preisschutz standardmäßig aktiviert. Sie können die Standardwerte beibehalten oder eigene Werte angeben.

Sie können den Preisschutz auch deaktivieren. Um anzugeben, dass es keinen Schwellenwert für den Preisschutz gibt, geben Sie einen hohen Prozentwert an, z. 999999 B.

Themen

Wie wird der Instance-Typ mit dem niedrigsten Preis identifiziert

Amazon EC2 bestimmt den Preis, auf dem der Preisschwellenwert basieren soll, indem es den Instance-Typ mit dem niedrigsten Preis aus den Instance-Typen identifiziert, die Ihren angegebenen Attributen entsprechen. Dies geschieht auf folgende Weise:

- Zunächst werden die Instance-Typen C, M oder R der aktuellen Generation betrachtet, die Ihren Attributen entsprechen. Wenn es Übereinstimmungen findet, wird der Instance-Typ mit dem niedrigsten Preis identifiziert.
- Wenn es keine Übereinstimmung gibt, sucht es nach allen Instance-Typen der aktuellen Generation, die Ihren Attributen entsprechen. Wenn es Übereinstimmungen findet, wird der Instance-Typ mit dem niedrigsten Preis identifiziert.
- Wenn es keine Übereinstimmung gibt, sucht es nach allen Instance-Typen der vorherigen Generation, die Ihren Attributen entsprechen, und identifiziert den Instance-Typ mit dem niedrigsten Preis.

Preisschutz für On-Demand-Instances

Der Schwellenwert für den Preisschutz für On-Demand-Instance-Typen wird als Prozentsatz berechnet, der über dem identifizierten On-Demand-Instance-Typ mit dem niedrigsten Preis liegt (`OnDemandMaxPricePercentageOverLowestPrice`). Sie geben den höheren Prozentsatz an, den Sie bereit sind zu zahlen. Wenn Sie diesen Parameter nicht angeben, `20` wird der Standardwert von verwendet, um einen Preisschutzschwellenwert zu berechnen, der 20% über dem identifizierten Preis liegt.

Wenn der identifizierte On-Demand-Instance-Preis beispielsweise`0.4271`, und Sie angeben`25`, liegt der Preisschwellenwert 25% über`0.4271`. Er wird wie folgt berechnet:`0.4271 * 1.25 = 0.533875`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für On-Demand-Instances zu zahlen. In diesem Beispiel schließt Amazon EC2 alle On-Demand-Instance-Typen aus, die mehr als `0.533875` kosten.

Preisschutz für Spot-Instances

Standardmäßig wendet Amazon EC2 automatisch den optimalen Spot-Instance-Preisschutz an, sodass konsistent aus einer Vielzahl von Instance-Typen ausgewählt werden kann. Sie können den Preisschutz auch manuell selbst festlegen. Wenn Sie dies jedoch Amazon EC2 für Sie erledigen lassen, können Sie die Wahrscheinlichkeit erhöhen, dass Ihre Spot-Kapazität ausgeschöpft ist.

Sie können den Preisschutz mithilfe einer der folgenden Optionen manuell angeben. Wenn Sie den Preisschutz manuell festlegen, empfehlen wir, die erste Option zu verwenden.

- Ein Prozentsatz des identifizierten On-Demand-Instance-Typs mit dem niedrigsten Preis [`MaxSpotPriceAsPercentageOfOptimalOnDemandPrice`]

  Wenn der angegebene Preis für den On-Demand-Instance-Typ `0.4271` beispielsweise ist und Sie angeben`60`, liegt der Preisgrenzwert bei 60% von`0.4271`. Er wird wie folgt berechnet:`0.4271 * 0.60 = 0.25626`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für Spot-Instances zu zahlen. In diesem Beispiel schließt Amazon EC2 alle Spot-Instance-Typen aus, die mehr als `0.25626` kosten.
- Ein Prozentsatz, der höher ist als der identifizierte Spot-Instance-Typ mit dem niedrigsten Preis [] `SpotMaxPricePercentageOverLowestPrice`

  Wenn der Preis für den identifizierten Spot-Instance-Typ beispielsweise und Sie angeben`25`, liegt der Preisschwellenwert 25% über`0.1808`. `0.1808` Er wird wie folgt berechnet:`0.1808 * 1.25 = 0.226`. Der berechnete Preis ist der Höchstbetrag, den Sie bereit sind, für Spot-

Instances zu zahlen. In diesem Beispiel schließt Amazon EC2 alle Spot-Instance-Typen aus, die mehr als `0.266` kosten. Wir empfehlen, diesen Parameter nicht zu verwenden, da die Spot-Preise schwanken können und daher auch Ihr Preisschutzschwellenwert schwanken kann.

Geben Sie die Preisschutzschwelle an

Schwellenwert für Preisschutz angeben

Konfigurieren Sie beim Erstellen der Spot-Flotte die Flotte für eine attributbasierte Auswahl des Instance-Typs und gehen Sie dann folgendermaßen vor:

- Konsole

  Zur Eingabe des Schwellenwerts für On-Demand-Instance-Preisschutz wählen Sie unter Additional instance attribute (Zusätzliches Instance-Attribut) die Option On-demand price protection (On-Demand-Preisschutz) aus. Wählen Sie dann Add attribute (Attribut hinzufügen) aus. Geben Sie bei On-Demand price protection percentage (Prozentsatz des On-Demand-Preisschutzes) den Preisschutzschwellenwert als Prozentsatz ein.

  Zur Eingabe des Schwellenwerts für Spot-Instance-Preisschutz wählen Sie unter Additional instance attribute (Zusätzliches Instance-Attribut) die Option Sport price protection (Spot-Preisschutz) aus. Wählen Sie dann Add attribute (Attribut hinzufügen) aus. Wählen Sie einen Parameter und geben Sie den Preisschutzschwellenwert als Prozentsatz ein.
- AWS CLI

  Zum Angeben des Schwellenwerts zum Preisschutz für On-Demand-Instances geben Sie in der JSON-Konfigurationsdatei in der `InstanceRequirements`-Struktur für `OnDemandMaxPricePercentageOverLowestPrice` den Preisschutzschwellenwert als Prozentsatz ein.

  Um den Schwellenwert für den Preisschutz der Spot-Instance anzugeben, geben Sie in der JSON-Konfigurationsdatei in der `InstanceRequirements` Struktur einen der folgenden Parameter an:

  - Geben Sie für `MaxSpotPriceAsPercentageOfOptimalOnDemandPrice` den Schwellenwert für den Preisschutz als Prozentsatz ein.
  - Geben Sie für `SpotMaxPricePercentageOverLowestPrice` den Preisschutzschwellenwert als Prozentsatz ein.

Weitere Informationen zum Erstellen der Flotte finden Sie unter Erstellen einer Spot-Flotte mit attributbasierter Auswahl von Instance-Typen.

> **Note**
>
> Wenn Sie beim Erstellen der Spot-Flotte Total target capacity (Gesamtzielkapazität) auf vCPUs oder Memory (MiB) (Arbeitsspeicher (MiB)) (Konsole) oder `TargetCapacityUnitType` auf `vcpu` oder `memory-mib` (AWS CLI) festlegen, wird der Preisschutzschwellenwert anhand des Preises pro vCPU oder pro Arbeitsspeicher anstelle des Preises pro Instance angewendet.

Überlegungen

- Sie können entweder Instance-Typen oder Instance-Attribute in einer Spot-Flotte angeben, aber nicht beides gleichzeitig.

  Wenn Sie die CLI verwenden, überschreiben die Startvorlagen-Überschreibungen die Startvorlage. Wenn die Startvorlage beispielsweise einen Instance-Typ enthält und die Startvorlagen-Überschreibung Instance-Attribute enthält, überschreiben die Instances, die durch die Instance-Attribute identifiziert werden, den Instance-Typ in der Startvorlage.
- Wenn Sie die CLI verwenden und Instance-Attribute als Überschreibungen angeben, können Sie nicht auch Gewichtungen oder Prioritäten angeben.
- Sie können maximal vier `InstanceRequirements`-Strukturen in einer Anforderungskonfiguration angeben.

Erstellen einer Spot-Flotte mit attributbasierter Auswahl von Instance-Typen

Sie können mithilfe der Amazon-EC2-Konsole oder der AWS CLI eine Flotte so konfigurieren, dass sie die attributbasierte Auswahl von Instance-Typen verwendet.

Themen

- Erstellen einer Spot-Flotte mit der Konsole
- Erstellen Sie eine Spot-Flotte mit dem AWS CLI

Erstellen einer Spot-Flotte mit der Konsole

So konfigurieren Sie eine Spot-Flotte für die attributbasierte Auswahl von Instance-Typen (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Spot-Anforderungen und wählen Sie die Spot-Instances anfordern aus.
3. Befolgen Sie die Schritte zum Erstellen einer Spot-Flotte. Weitere Informationen finden Sie unter Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole).

   Konfigurieren Sie beim Erstellen der Spot-Flotte wie folgt die Flotte für die attributbasierte Auswahl von Instance-Typen:

   a. Wählen Sie für Instance type requirements (Anforderungen hinsichtlich des Instance-Typs) die Option Specify instance attributes that match your compute requirements (Instance-Attribute angeben, die Ihren Computinganforderungen entsprechen) aus.
   b. Geben Sie für vCPUs die gewünschte minimale und maximale Anzahl der vCPUs ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beides.
   c. Geben Sie für Arbeitsspeicher (GiB) den gewünschten Mindest- und Höchstwert ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beide Optionen aus.
   d. (Optional) Für Zusätzliche Instance-Attribute können Sie optional ein oder mehrere Attribute angeben, um Ihre Computinganforderungen genauer auszudrücken. Jedes zusätzliche Attribut fügt Ihrer Anfrage weitere Einschränkungen hinzu.
   e. (Optional) Um die Instance-Typen mit Ihren angegebenen Attributen anzuzeigen, erweitern Sie Vorschau der übereinstimmenden Instance-Typen.

Erstellen Sie eine Spot-Flotte mit dem AWS CLI

So konfigurieren Sie eine Spot-Flotte für die attributbasierte Auswahl von Instance-Typen (AWS CLI)

Verwenden Sie den Befehl request-spot-fleet (AWS CLI), um eine Spot-Flottenanforderung zu erstellen. Geben Sie die Flottenkonfiguration in einer JSON-Datei an.

```
aws ec2 request-spot-fleet \
    --region us-east-1 \
    --spot-fleet-request-config file://file_name.json
```

file_name.json-Beispieldatei

Das folgende Beispiel enthält Parameter, mit denen eine Spot-Flotte für attributbasierte Instance-Typauswahl konfiguriert wird, gefolgt von einer Texterklärung.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Die Attribute für die attributbasierte Auswahl von Instance-Typen werden in der `InstanceRequirements`-Struktur angegeben. In diesem Beispiel werden zwei Attribute angegeben:

- `VCpuCount` – Es sind mindestens 2 vCPUs angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.
- `MemoryMiB` – Es werden mindestens 4 MiB Arbeitsspeicher angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.

Alle Instance-Typen mit 2 oder mehr vCPUs und 4 MiB oder mehr Arbeitsspeicher werden identifiziert. Der Preisschutz und die Zuweisungsstrategie könnten jedoch einige Instance-Typen ausschließen, wenn die Spot-Flotte die Flotte bereitstellt.

Eine Liste und Beschreibungen aller möglichen Attribute, die Sie angeben können, finden Sie InstanceRequirementsin der Amazon EC2 API-Referenz.

> **Note**
>
> Wenn `InstanceRequirements` in der Flottenkonfiguration enthalten ist, müssen `InstanceType` und `WeightedCapacity` ausgeschlossen werden. Sie können die Flottenkonfiguration nicht gleichzeitig mit den Instance-Attributen bestimmen.

Die JSON-Datei enthält auch die folgende Flottenkonfiguration:

- `"AllocationStrategy": "priceCapacityOptimized"` – Die Zuweisungsstrategie für die Spot Instances in der Flotte.
- `"LaunchTemplateName": "my-launch-template", "Version": "1"` – Die Startvorlage enthält einige Informationen zur Instance-Konfiguration. Wenn jedoch Instance-Typen angegeben sind, werden diese durch die in `InstanceRequirements` angegebenen Attribute überschrieben.
- `"TargetCapacity": 20` – Die Zielkapazität beträgt 20 Instances.
- `"Type": "request"` – Der Anforderungstyp für die Flotte ist `request`.

Beispiele für Konfigurationen, die gültig und ungültig sind

Wenn Sie den verwenden AWS CLI , um eine Spot-Flotte zu erstellen, müssen Sie sicherstellen, dass Ihre Flottenkonfiguration gültig ist. Die folgenden Beispiele zeigen gültige und ungültige Konfigurationen.

Konfigurationen gelten als ungültig, wenn sie Folgendes enthalten:

- Eine einzelne `Overrides`-Struktur mit `InstanceRequirements` und `InstanceType`
- Zwei `Overrides`-Strukturen, eine mit `InstanceRequirements` und die andere mit `InstanceType`
- Zwei `InstanceRequirements`-Strukturen mit sich überlappenden Attributwerten innerhalb derselben `LaunchTemplateSpecification`

Beispielkonfigurationen

- Gültige Konfiguration: Einzelstartvorlage mit Überschreibungen
- Gültige Konfiguration: Einzelne Startvorlage mit mehreren InstanceRequirements
- Gültige Konfiguration: Zwei Startvorlagen, jede mit Überschreibungen
- Gültige Konfiguration: Nur InstanceRequirements angegeben, keine überlappenden Attributwerte

- Die Konfiguration ist nicht gültig: Overrides enthalten InstanceRequirements und InstanceType.
- Konfiguration ungültig: Zwei Overrides enthalten InstanceRequirements und InstanceType
- Konfiguration ungültig: Überlappende Attributwerte

Gültige Konfiguration: Einzelstartvorlage mit Überschreibungen

Die folgende Konfiguration ist gültig. Sie enthält eine Startvorlage und eine `Overrides`-Struktur mit einer `InstanceRequirements`-Struktur. Eine Texterklärung der Beispielkonfiguration folgt.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "My-launch-template",
                "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 2,
                            "Max": 8
                        },
                        "MemoryMib": {
                            "Min": 0,
                            "Max": 10240
                        },
                        "MemoryGiBPerVCpu": {
                            "Max": 10000
                        },
                        "RequireHibernateSupport": true
                    }
                }
            ]
        }
    ],
        "TargetCapacity": 5000,
```

```
            "OnDemandTargetCapacity": 0,
            "TargetCapacityUnitType": "vcpu"
    }
}
```

`InstanceRequirements`

Um die attributbasierte Instance-Auswahl zu verwenden, müssen Sie die `InstanceRequirements`-Struktur in Ihre Flottenkonfiguration aufnehmen und die gewünschten Attribute für die Instances in der Flotte angeben.

Im vorhergehenden Beispiel werden die folgenden Instance-Attribute angegeben:

- `VCpuCount` – Die Instance-Typen müssen mindestens 2 und höchstens 8 vCPUs aufweisen.
- `MemoryMiB` – Die Instance-Typen müssen maximal 10240 MiB Speicher haben. Ein Minimum von 0 bedeutet, dass kein Mindestwert vorhanden ist.
- `MemoryGiBPerVCpu` – Die Instance-Typen müssen maximal 10 000 GiB Speicher pro vCPU haben. Der Parameter `Min` ist optional. Indem Sie ihn weglassen, geben Sie kein Mindestlimit an.

`TargetCapacityUnitType`

Der `TargetCapacityUnitType`-Parameter gibt die Einheit für die Zielkapazität an. Im Beispiel ist die Zielkapazität `5000` und der Typ der Zielkapazitätseinheit `vcpu`. Zusammen geben Sie eine gewünschte Zielkapazität von 5 000 vCPUs an. Die Spot-Flotte wird genügend Instances starten, damit die Gesamtzahl der vCPUs in der Flotte 5 000 vCPUs beträgt.

Gültige Konfiguration: Einzelne Startvorlage mit mehreren InstanceRequirements

Die folgende Konfiguration ist gültig. Sie enthält eine Startvorlage und eine `0verrides`-Struktur mit zwei `InstanceRequirements`-Strukturen. Die in `InstanceRequirements` angegebenen Attribute sind gültig, da sich die Werte nicht überschneiden – die erste `InstanceRequirements`-Struktur gibt eine `VCpuCount` von 0-2 vCPUs an, während die zweite `InstanceRequirements`-Struktur 4-8 vCPUs angibt.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
```

```
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Gültige Konfiguration: Zwei Startvorlagen, jede mit Überschreibungen

Die folgende Konfiguration ist gültig. Sie enthält zwei Startvorlagen mit jeweils einer `Overrides`-Struktur, die eine `InstanceRequirements`-Struktur enthält. Diese Konfiguration ist nützlich für `arm`- und `x86`-Architekturunterstützung in derselben Flotte.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "armLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "x86LaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
```

```
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Gültige Konfiguration: Nur **`InstanceRequirements`** angegeben, keine überlappenden Attributwerte

Die folgende Konfiguration ist gültig. Sie enthält zwei `LaunchTemplateSpecification`-Strukturen, jeweils mit einer Startvorlage und einer `Overrides`-Struktur, die eine `InstanceRequirements`-Struktur enthält. Die in `InstanceRequirements` angegebenen Attribute sind gültig, da sich die Werte nicht überschneiden – die erste `InstanceRequirements`-Struktur gibt eine `VCpuCount` von 0-2 vCPUs an, während die zweite `InstanceRequirements`-Struktur 4-8 vCPUs angibt.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
```

```
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 4,
                            "Max": 8
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Die Konfiguration ist nicht gültig: **`Overrides`** enthalten **`InstanceRequirements`** und **`InstanceType`**.

Die folgende Konfiguration ist ungültig. Die `Overrides`-Struktur enthält `InstanceRequirements` und `InstanceType`. Sie können für `Overrides` `InstanceRequirements` oder `InstanceType` angeben, aber nicht beides.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
```

```
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                },
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Konfiguration ungültig: Zwei **`Overrides`** enthalten **`InstanceRequirements`** und **`InstanceType`**

Die folgende Konfiguration ist ungültig. Die `Overrides`-Strukturen enthalten `InstanceRequirements` und `InstanceType`. Sie können entweder `InstanceRequirements` oder `InstanceType` angeben, aber nicht beides, auch wenn sie sich in unterschiedlichen `Overrides`-Strukturen befinden.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
```

```
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    }
                }
              ]
            },
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyOtherLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceType": "m5.large"
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Konfiguration ungültig: Überlappende Attributwerte

Die folgende Konfiguration ist ungültig. Die beiden `InstanceRequirements`-Strukturen enthalten jeweils `"VCpuCount": {"Min": 0, "Max": 2}`. Die Werte für diese Attribute überschneiden sich, was zu doppelten Kapazitätspools führt.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
```

```
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "MyLaunchTemplate",
                    "Version": "1"
                },
                "Overrides": [
                {
                    "InstanceRequirements": {
                        "VCpuCount": {
                            "Min": 0,
                            "Max": 2
                        },
                        "MemoryMiB": {
                            "Min": 0
                        }
                    },
                    {
                      "InstanceRequirements": {
                          "VCpuCount": {
                              "Min": 0,
                              "Max": 2
                          },
                          "MemoryMiB": {
                              "Min": 0
                          }
                      }
                  }
                }
              ]
            }
        ],
        "TargetCapacity": 1,
        "OnDemandTargetCapacity": 0,
        "Type": "maintain"
    }
}
```

Vorschau von Instance-Typen mit bestimmten Attributen

Sie können den AWS CLI Befehl get-instance-types-from-instance-requirements verwenden, um eine Vorschau der Instance-Typen anzuzeigen, die den von Ihnen angegebenen Attributen entsprechen. Dies ist besonders nützlich, um herauszufinden, welche Attribute in Ihrer Anforderungskonfiguration angegeben werden sollen, ohne Instances zu starten. Beachten Sie, dass der Befehl die verfügbare Kapazität nicht berücksichtigt.

Um eine Vorschau einer Liste von Instanztypen anzuzeigen, geben Sie Attribute mit dem AWS CLI

1. (Optional) Um alle möglichen Attribute zu generieren, die angegeben werden können, verwenden Sie den Befehl get-instance-types-from-instance-requirements und den `--generate-cli-skeleton`-Parameter. Sie können die Ausgabe optional in eine Datei umleiten, um sie mit mit `input > attributes.json` zu speichern.

```
aws ec2 get-instance-types-from-instance-requirements \
    --region us-east-1 \
    --generate-cli-skeleton input > attributes.json
```

Erwartete Ausgabe

```
{
    "DryRun": true,
    "ArchitectureTypes": [
        "i386"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 0,
            "Max": 0
        },
        "MemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "CpuManufacturers": [
            "intel"
        ],
```

```
        "MemoryGiBPerVCpu": {
            "Min": 0.0,
            "Max": 0.0
        },
        "ExcludedInstanceTypes": [
            ""
        ],
        "InstanceGenerations": [
            "current"
        ],
        "SpotMaxPricePercentageOverLowestPrice": 0,
        "OnDemandMaxPricePercentageOverLowestPrice": 0,
        "BareMetal": "included",
        "BurstablePerformance": "included",
        "RequireHibernateSupport": true,
        "NetworkInterfaceCount": {
            "Min": 0,
            "Max": 0
        },
        "LocalStorage": "included",
        "LocalStorageTypes": [
            "hdd"
        ],
        "TotalLocalStorageGB": {
            "Min": 0.0,
            "Max": 0.0
        },
        "BaselineEbsBandwidthMbps": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorTypes": [
            "gpu"
        ],
        "AcceleratorCount": {
            "Min": 0,
            "Max": 0
        },
        "AcceleratorManufacturers": [
            "nvidia"
        ],
        "AcceleratorNames": [
            "a100"
        ],
```

```
        "AcceleratorTotalMemoryMiB": {
            "Min": 0,
            "Max": 0
        },
        "NetworkBandwidthGbps": {
            "Min": 0.0,
            "Max": 0.0
        },
        "AllowedInstanceTypes": [
            ""
        ]
    },
    "MaxResults": 0,
    "NextToken": ""
}
```

2. Erstellen Sie eine JSON-Konfigurationsdatei mit der Ausgabe des vorherigen Schritts und konfigurieren Sie sie wie folgt:

> **Note**
>
> Sie müssen Werte für `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount` und `MemoryMiB` angeben. Sie können die anderen Attribute weglassen. In diesem Fall werden die Standardwerte verwendet.
> Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-instance-types-from-instance-requirements in der Amazon-EC2-Befehlszeilenreferenz.

a. Geben Sie für `ArchitectureTypes` mindestes einen Prozessorarchitekturtyp an.

b. Geben Sie für `VirtualizationTypes` mindestens eine Art von Virtualisierung an.

c. Geben Sie für `VCpuCount` die minimale und maximale Anzahl von vCPUs an. Wenn Sie keine Mindestgrenze angeben möchten, geben Sie `0` für `Min` an. Wenn Sie keine Maximalgrenze angeben möchten, lassen Sie den `Max`-Parameter weg.

d. Geben Sie für `MemoryMiB` den Mindest- und Höchstwert für Speicher in MiB an. Wenn Sie keine Mindestgrenze angeben möchten, geben Sie `0` für `Min` an. Wenn Sie keine Maximalgrenze angeben möchten, lassen Sie den `Max`-Parameter weg.

e. Sie können optional eines oder mehrere der anderen Attribute angeben, um die Liste der zurückgegebenen Instance-Typen weiter einzuschränken.

3. Um eine Vorschau der Instance-Typen anzuzeigen, die die von Ihnen in der JSON-Datei angegebenen Attribute aufweisen, verwenden Sie den Befehl get-instance-types-from-instance-requirements und geben Sie mithilfe des `--cli-input-json`-Parameters den Namen und Pfad zu Ihrer JSON-Datei an. Sie können die Ausgabe optional so formatieren, dass sie in einem Tabellenformat angezeigt wird.

```
aws ec2 get-instance-types-from-instance-requirements \
    --cli-input-json file://attributes.json \
    --output table
```

Beispiel-Datei *Attribute.json*

In diesem Beispiel sind die erforderlichen Attribute in der JSON-Datei enthalten. Sie lauten `ArchitectureTypes`, `VirtualizationTypes`, `VCpuCount`, und `MemoryMiB`. Darüber hinaus ist das optionale `InstanceGenerations`-Attribut ebenfalls enthalten. Beachten Sie, dass für `MemoryMiB` der `Max`-Wert weggelassen werden kann, um anzuzeigen, dass kein Grenzwert vorhanden ist.

```
{
    "ArchitectureTypes": [
        "x86_64"
    ],
    "VirtualizationTypes": [
        "hvm"
    ],
    "InstanceRequirements": {
        "VCpuCount": {
            "Min": 4,
            "Max": 6
        },
        "MemoryMiB": {
            "Min": 2048
        },
        "InstanceGenerations": [
            "current"
        ]
    }
}
```

Beispielausgabe

```
----------------------------------------
|GetInstanceTypesFromInstanceRequirements|
+----------------------------------------+
||             InstanceTypes            ||
|+--------------------------------------+|
||             InstanceType             ||
|+--------------------------------------+|
||  c4.xlarge                           ||
||  c5.xlarge                           ||
||  c5a.xlarge                          ||
||  c5ad.xlarge                         ||
||  c5d.xlarge                          ||
||  c5n.xlarge                          ||
||  c6a.xlarge                           ||
...
```

4. Nachdem Sie Instance-Typen identifiziert haben, die Ihren Anforderungen entsprechen, notieren Sie die Instance-Attribute, die Sie verwendet haben, damit Sie sie beim Konfigurieren Ihrer Flottenanforderung verwenden können.

On-Demand-Kapazität in Spot-Flotten

Um sicherzustellen, dass Sie immer über Instance-Kapazität verfügen, können Sie eine Anforderung nach On-Demand-Kapazität in Ihre Spot-Flotten-Anforderung aufnehmen. In Ihrer Spot-Flotten-Anforderung geben Sie Ihre gewünschte Zielkapazität an und wie viel von dieser Kapazität On-Demand sein muss. Die Bilanz umfasst die Spot-Kapazität, die gestartet wird, wenn Amazon EC2-Kapazität und -Verfügbarkeit vorhanden sind. Wenn Sie z. B. in Ihrer Spot-Flotten-Anforderung die Zielkapazität als 10 und die On-Demand-Kapazität als 8 angeben, startet Amazon EC2 8 Kapazitätseinheiten als On-Demand und 2 Kapazitätseinheiten (10–8=2) als Spot.

Priorisieren von Instance-Typen für On-Demand-Kapazität

Wenn die Spot-Flotte versucht, Ihre On-Demand-Kapazität zu erfüllen, startet sie standardmäßig zuerst den kostengünstigsten Instance-Typ. Wenn `OnDemandAllocationStrategy` auf `prioritized` eingestellt ist, bestimmt die Spot-Flotte anhand der Priorität, welcher Instance-Typ zur Erfüllung der On-Demand-Kapazität zuerst verwendet werden soll.

Die Priorität wird der Startvorlagen-Überschreibung zugewiesen, und die höchste Priorität wird zuerst gestartet.

Beispiel: Priorisieren von Instance-Typen

In diesem Bespiel konfigurieren Sie drei Startvorlagen-Überschreibungen, jede mit einem anderen Instance-Typ.

Der On-Demand-Preis für die Instance-Typen variiert. Im Folgenden sind die in diesem Beispiel verwendeten Instance-Typen nach Preisen aufgeführt, beginnend mit dem günstigsten Instance-Typ:

- `m4.large`- günstigster
- `m5.large`
- `m5a.large`

Wenn Sie die Reihenfolge nicht anhand der Priorität bestimmen, startet die Flotte zur Erfüllung der On-Demand-Kapazität mit dem günstigsten Instance-Typ.

Nehmen wir jedoch an, Sie hätten ungenutzte `m5.large` Reserved Instances, die Sie zuerst verwenden möchten. Sie können die Startvorlagen-Überschreibungspriorität so einstellen, dass die Instance-Typen wie folgt in der Reihenfolge ihrer Priorität verwendet werden:

- `m5.large` – Priorität 1
- `m4.large` – Priorität 2
- `m5a.large` – Priorität 3

Kapazitätsausgleich

Sie können die Spot-Flotte so konfigurieren, dass eine Ersatz-Spot-Instance gestartet wird, wenn Amazon EC2 eine Neuausgleichsempfehlung ausgibt, um Sie darüber zu informieren, dass für eine Spot-Instance ein erhöhtes Unterbrechungsrisiko besteht. Der Kapazitätsausgleich hilft Ihnen, die Verfügbarkeit von Workloads aufrechtzuerhalten, indem Sie Ihre Flotte proaktiv um eine neue Spot-Instance erweitern, bevor eine ausgeführte Instance durch Amazon EC2 unterbrochen wird. Weitere Informationen finden Sie unter Empfehlung zum Neuausgleich einer EC2-Instance.

Um die Spot-Flotte so zu konfigurieren, dass eine Ersatz-Spot-Instance gestartet wird, können Sie die Amazon EC2 Konsole oder die AWS CLI verwenden.

- Amazon EC2-Konsole: Sie müssen das Kontrollkästchen Capacity rebalance (Kapazitätsneuausgleich) aktivieren, wenn Sie die Spot-Flotte erstellen. Weitere Informationen

finden Sie in Schritt 6.d unter Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole).

- AWS CLI: Verwenden Sie den Befehl request-spot-fleet und die relevanten Parameter in der `SpotMaintenanceStrategies`-Struktur. Weitere Informationen finden Sie in der Beispielstartkonfiguration.

Einschränkungen

- Die Kapazitätsanpassung ist nur für Flotten des Typs `maintain` verfügbar.
- Wenn die Flotte läuft, können Sie die Kapazitätsausgleichs-Einstellung nicht ändern. Um die Einstellung Kapazitätsausgleich zu ändern, müssen Sie die Flotte löschen und eine neue Flotte erstellen.

Konfigurationsoptionen

`ReplacementStrategy` für die Spot-Flotte unterstützt die folgenden beiden Werte:

`launch-before-terminate`

Amazon EC2 kann die Spot Instances beenden, die eine Neuausgleichsbenachrichtigung erhalten, nachdem neue Ersatz-Spot-Instances gestartet wurden. Wenn Sie `launch-before-terminate` angeben, müssen Sie auch einen Wert für `termination-delay` angeben. Nachdem die neuen Ersatz-Instances gestartet wurden, wartet Amazon EC2 während der Dauer des `termination-delay` und beendet dann die alten Instances. Für `termination-delay` beträgt das Minimum 120 Sekunden (2 Minuten) und das Maximum 7 200 Sekunden (2 Stunden).

Wir empfehlen die Verwendung von `launch-before-terminate` nur, wenn Sie vorhersagen können, wie lange Ihre Verfahren zum Herunterfahren der Instances dauern werden. Dadurch wird sichergestellt, dass die alten Instances erst beendet werden, wenn die Verfahren zum Herunterfahren abgeschlossen sind. Beachten Sie, dass Amazon EC2 die alten Instances mit einer zweiminütigen Warnung vor der `termination-delay` unterbrechen kann.

`launch`

Amazon EC2 startet Ersatz-Spot-Instances, wenn eine Neuausgleichsbenachrichtigung für bestehende Spot-Instances ausgegeben wird. Amazon EC2 beendet nicht die Instances, die eine Neuausgleichsbenachrichtigung erhalten. Sie können die alten Instances beenden oder laufen lassen. Ihnen werden alle Instances in Rechnung gestellt, während sie ausgeführt werden.

Überlegungen

Beachten Sie Folgendes, wenn Sie eine Spot-Flotte für Kapazitätsneuausgleich konfigurieren:

Stellen Sie so viele Spot-Kapazitätspools wie möglich in der Anfrage bereit

Konfigurieren Sie Ihre Spot-Flotte für die Verwendung mehrerer Instance-Typen und Availability Zones. Dies bietet die Flexibilität, Spot-Instances in verschiedenen Spot-Kapazitätspools zu starten. Weitere Informationen finden Sie unter Flexibel sein bei Instance-Typen und Availability Zones.

Vermeiden Sie ein erhöhtes Risiko einer Unterbrechung von Ersatz-Spot-Instances

Um ein erhöhtes Risiko einer Unterbrechung zu vermeiden, empfehlen wir die `capacityOptimizedPrioritized` Zuweisungsstrategie `capacityOptimized` oder. Diese Strategien stellen sicher, dass Ersatz-Spot-Instances in den optimalen Spot-Kapazitätspools gestartet werden und ihre Unterbrechung in naher Zukunft daher weniger wahrscheinlich ist. Weitere Informationen finden Sie unter Nutzen der preis- und kapazitätsoptimierten Zuweisungsstrategie.

Amazon EC2 startet eine neue Instance nur dann, wenn die Verfügbarkeit gleich oder besser ist

Eines der Ziele des Kapazitätsausgleichs ist die Verbesserung der Verfügbarkeit einer Spot Instance. Wenn eine vorhandene Spot Instance eine Neuausgleichsempfehlung erhält, startet Amazon EC2 nur dann eine neue Instance, wenn die neue Instance dieselbe oder eine bessere Verfügbarkeit als die vorhandene Instance bietet. Wenn das Risiko einer Unterbrechung einer neuen Instance größer ist als das der vorhandenen Instance, startet Amazon EC2 keine neue Instance. Amazon EC2 wird die Spot-Kapazitätspools jedoch weiterhin bewerten und eine neue Instance starten, falls sich die Verfügbarkeit verbessert.

Es besteht die Möglichkeit, dass Ihre vorhandene Instance unterbrochen wird, ohne dass Amazon EC2 pro-aktiv eine neue Instance startet. In diesem Fall versucht Amazon EC2, eine neue Instance zu starten, sobald die Unterbrechungsmeldung für eine Spot Instance eingeht, unabhängig davon, ob bei der neuen Instance ein hohes Unterbrechungsrisiko besteht.

Capacity Rebalancing erhöht nicht die Unterbrechungsrate Ihrer Spot-Instance

Wenn Sie Capacity Rebalancing aktivieren, wird Ihre Spot-Instance-Unterbrechungsrate (die Anzahl der Spot-Instances, die zurückgefordert werden, wenn Amazon EC2 die Kapazität zurück benötigt) nicht erhöht. Wenn der Kapazitätsausgleich jedoch feststellt, dass bei einer Instance das Risiko einer Unterbrechung besteht, versucht Amazon EC2 sofort, eine neue Instance zu starten. Das Ergebnis ist, dass möglicherweise mehr Instances ersetzt werden, als wenn Sie

darauf gewartet hätten, dass Amazon EC2 eine neue Instance startet, nachdem die gefährdete Instance unterbrochen wurde.

Sie können zwar mehr Instances mit aktiviertem Capacity Rebalancing ersetzen, jedoch Sie profitieren davon, dass Sie eher proaktiv als reaktiv sind, indem Sie mehr Zeit haben, Maßnahmen zu ergreifen, bevor Ihre Instances unterbrochen werden. Mit einer Spot-Instance-Unterbrechungsbenachrichtigung haben Sie normalerweise nur bis zu zwei Minuten Zeit, um Ihre Instance ordnungsgemäß herunterzufahren. Wenn Capacity Rebalancing eine neue Instance im Voraus startet, geben Sie bestehenden Prozessen eine bessere Chance, sie auf Ihrer gefährdeten Instance abzuschließen. Sie können mit dem Herunterfahren Ihrer Instance beginnen und verhindern, dass neue Arbeiten für Ihre gefährdete Instance geplant werden. Sie können auch damit beginnen, die neu gestartete Instance für die Übernahme der Anwendung vorzubereiten. Mit dem proaktiven Ersetzen durch Capacity Rebalancing profitieren Sie von einer reibungslosen Kontinuität.

Betrachten Sie als theoretisches Beispiel zur Demonstration der Risiken und Vorteile des Einsatzes von Capacity Rebalancing das folgende Szenario:

- 14:00 Uhr – Für Instance-A wird eine Empfehlung zum erneuten Ausgleich empfangen und Amazon EC2 versucht sofort, eine Ersatz-Instance-B zu starten, sodass Sie Zeit haben, Ihre Shutdown-Verfahren zu starten.*
- 14:30 Uhr — Für Instance-B wird eine Empfehlung zum erneuten Ausgleich empfangen, die durch Instance-C ersetzt wird, sodass Sie Zeit haben, Ihre Shutdown-Verfahren zu starten.*
- 14:32 Uhr — Wenn Capacity Rebalancing nicht aktiviert wäre und um 14:32 Uhr eine Benachrichtigung über eine Unterbrechung der Spot-Instance für Instance-A eingegangen wäre, hätten Sie nur bis zu zwei Minuten Zeit gehabt, um Maßnahmen zu ergreifen, währenddessen Instance-A allerdings bis zu diesem Zeitpunkt hochgefahren wäre.

* Wenn `launch-before-terminate` angegeben ist, beendet Amazon EC2 die gefährdete Instance, nachdem die Ersatz-Instance online geschaltet wurde.

Amazon EC2 kann einen neuen Ersatz Spot-Instances starten, bis die erfüllte Kapazität die doppelte Zielkapazität hat

Wenn ein Spot-Flotte für Kapazitätsneuausgleich konfiguriert wird, versucht Amazon EC2, für jede Spot-Instance, die eine Neuausgleichsempfehlung erhält, eine neue Ersatz-Spot-Instance zu starten. Nachdem eine Spot-Instance eine Neuausgleichsempfehlung erhalten hat, wird sie nicht mehr als Teil der erfüllten Kapazität gezählt. Je nach Ersetzungsstrategie beendet Amazon EC2 die Instance entweder nach einer vorkonfigurierten Beendigungsverzögerung oder lässt sie laufen. Dies gibt Ihnen die Möglichkeit, Neuausgleichsaktionen für die Instance durchzuführen.

Wenn Ihre Flotte die doppelte Zielkapazität erreicht, wird sie keine neuen Ersatz-Instances mehr starten, selbst wenn die Ersatz-Instances selbst eine Empfehlung zum Neuausgleich erhalten.

Angenommen, Sie erstellen Sie eine Spot-Flotte mit einer Zielkapazität von 100 Spot-Instances. Alle Spot Instances erhalten eine Neuausgleichsempfehlung, die dazu führt, dass Amazon EC2 100 Ersatz-Spot-Instances startet. Dadurch wird die Anzahl der erfüllten Spot-Instances auf 200 erhöht, was der doppelten Zielkapazität entspricht. Einige der Ersatz-Instances erhalten eine Neuausgleichsempfehlung, es werden jedoch keine Ersatz-Instances mehr gestartet, da die Flotte die doppelte Zielkapazität nicht überschreiten kann.

Beachten Sie, dass Ihnen alle Instances in Rechnung gestellt werden, während sie ausgeführt werden.

Wir empfehlen Ihnen, die Spot-Flotte so zu konfigurieren, dass Spot-Instances beendet werden, die eine Neuausgleichsempfehlung erhalten.

Wenn Sie Ihre Spot-Flotte für den Kapazitätsausgleich konfigurieren, empfehlen wir Ihnen, `launch-before-terminate` mit einer angemessenen Beendigungsverzögerung nur dann auszuwählen, wenn Sie vorhersagen können, wie lange die Verfahren zum Herunterfahren der Instances dauern werden. Dadurch wird sichergestellt, dass die alten Instances erst beendet werden, wenn die Verfahren zum Herunterfahren abgeschlossen sind.

Wenn Sie die für die Neuausgleichsempfehlung empfohlenen Instances selbst beenden möchten, empfehlen wir Ihnen, das Signal für die Neuausgleichsempfehlung zu überwachen, das von den Spot-Instances in der Flotte empfangen wird. Durch die Überwachung des Signals können Sie schnell Neuausgleichsaktionen für die betroffenen Instances durchführen, bevor Amazon EC2 sie unterbricht, und dann können Sie sie manuell beenden. Wenn Sie die Instances nicht beenden, bezahlen Sie weiterhin für sie, während sie ausgeführt werden. Amazon EC2 beendet die Instances, die eine Neuausgleichsempfehlung erhalten, nicht automatisch.

Sie können Benachrichtigungen mithilfe von Amazon EventBridge - oder Instance-Metadaten einrichten. Weitere Informationen finden Sie unter Überwachen von Signalen für Neuausgleichsempfehlungen.

Die Spot-Flotte zählt bei der Berechnung der erfüllten Kapazität beim Auf- oder Abskalieren keine Instances, die eine Neuausgleichs-Empfehlung erhalten

Wenn Ihre Spot-Flotte für Kapazitätsneuausgleich konfiguriert ist und Sie die Zielkapazität auf Scale-in oder Scale-out ändern, zählt die Flotte die Instances, die für Neuausgleich markiert sind, nicht zur erfüllten Kapazität.

- Abskalieren – Wenn Sie die gewünschte Zielkapazität verringern, beendet Amazon EC2 Instances, die nicht für eine Neuverteilung markiert sind, bis die gewünschte Kapazität erreicht ist. Die Instances, die für einen Neuausgleich markiert sind, werden nicht auf die erfüllte Kapazität angerechnet.

  Ein Beispiel: Angenommen, Sie erstellen eine Spot-Flotte mit einer Zielkapazität von 100 Spot Instances. 10 Instances erhalten eine Neuausgleichsempfehlung. Amazon EC2 startet also 10 neue Ersatz-Instances, was zu einer erfüllten Kapazität von 110 Instances führt. Sie reduzieren dann die Zielkapazität auf 50 (abskalieren), aber die erfüllte Kapazität beträgt tatsächlich 60 Instances, da die 10 Instances, die für einen Neuausgleich markiert sind, nicht von Amazon EC2 beendet werden. Sie müssen diese Instances manuell beenden oder Sie können sie laufen lassen.
- Aufskalieren – Wenn Sie Ihre gewünschte Zielkapazität erhöhen, startet Amazon EC2 neue Instances, bis die gewünschte Kapazität erreicht ist. Die Instances, die für einen Neuausgleich markiert sind, werden nicht auf die erfüllte Kapazität angerechnet.

  Ein Beispiel: Angenommen, Sie erstellen eine Spot-Flotte mit einer Zielkapazität von 100 Spot Instances. 10 Instances erhalten eine Neuausgleichsempfehlung. Amazon EC2 startet also 10 neue Ersatz-Instances, was zu einer erfüllten Kapazität von 110 Instances führt. Sie erhöhen dann die Zielkapazität auf 200 (Erweiterung), aber die erfüllte Kapazität beträgt tatsächlich 210 Instances, da die 10 Instances, die für einen Neuausgleich markiert sind, nicht von der Flotte als Teil der Zielkapazität gezählt werden. Sie müssen diese Instances manuell beenden oder Sie können sie laufen lassen.

Außerkraftsetzungen des Spot-Preises

Jede Spot-Flotten-Anforderung kann einen globalen Höchstpreis enthalten oder den Standardpreis (den On-Demand-Preis) verwenden. Die Spot-Flotte verwendet diesen Preis als Standard-Höchstpreis für jede ihrer Startspezifikationen.

Sie können optional einen Höchstpreis in einer oder mehreren Startspezifikationen angeben. Dieser Preis gilt speziell für die Startspezifikation. Wenn eine Startspezifikation einen spezifischen Preis umfasst, verwendet die Spot-Flotte diesen Höchstpreis, sodass der globale Höchstpreis überschrieben wird. Alle anderen Startspezifikationen, die keinen spezifischen Höchstpreis enthalten, verwenden weiterhin den globalen Höchstpreis.

Kontrolle der Aufwendungen

Die Spot-Flotte stoppt das Starten von Instances, wenn entweder die Zielkapazität oder der Maximalbetrag erreicht ist, den Sie zu zahlen bereit sind. Zur Kontrolle der Kosten, die Sie für Ihre Flotte zahlen, können Sie den `SpotMaxTotalPrice` für Spot-Instances und den `OnDemandMaxTotalPrice` für On-Demand-Instances angeben. Ist der maximale Gesamtpreis erreicht, stoppt die Spot-Flotte das Starten von Instances auch dann, wenn die Zielkapazität noch nicht erreicht ist.

Im folgenden Beispiel werden zwei verschiedene Szenarien gezeigt. Im ersten Szenario stoppt die Spot-Flotte das Starten von Instances, wenn die Zielkapazität erreicht ist. Im zweiten Szenario stoppt die Spot-Flotte das Starten von Instances, wenn der Maximalbetrag erreicht ist, den Sie zu zahlen bereit sind.

Beispiel: Kein Starten mehr von Instances, wenn die Zielkapazität erreicht ist

Bei einer Anforderung für `m4.large` On-Demand-Instances mit:

- On-Demand-Preis: 0,10 USD pro Stunde
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 1,50 USD

Die Spot-Flotte launcht 10 On-Demand-Instances, da der Gesamtpreis von 1,00 USD (10 Instances x 0,10 USD) den `OnDemandMaxTotalPrice` von 1,50 USD nicht überschreitet.

Beispiel: Kein Starten mehr von Instances, wenn der Höchstpreis erreicht ist

Bei einer Anforderung für `m4.large` On-Demand-Instances mit:

- On-Demand-Preis: 0,10 USD pro Stunde
- `OnDemandTargetCapacity`: 10
- `OnDemandMaxTotalPrice`: 0,80 USD

Wenn die Spot-Flotte die On-Demand-Zielkapazität (10 On-Demand-Instances) startet, betragen die Gesamtkosten pro Stunde 1,00 USD. Dies überschreitet die Summe (0,80 USD), die für `OnDemandMaxTotalPrice` festgelegt ist. Damit Sie nicht mehr ausgeben, als Sie möchten, launcht die Spot-Flotte nur 8 On-Demand-Instances (weniger als die On-Demand-Zielkapazität), da sonst der `OnDemandMaxTotalPrice` überschritten würde.

Instance-Gewichtung für Spot-Flotten

Wenn Sie eine Flotte von Spot-Instances anfordern, können Sie definieren, wie viele Kapazitätseinheiten jeder Instance-Typ zu der Leistung Ihrer Anwendung beitragen soll, und Ihren Höchstpreis für die einzelnen Spot-Kapazitätspools mit der Instance-Gewichtung entsprechend anpassen.

Standardmäßig gilt der von Ihnen angegebene Preis pro Instance-Stunde. Wenn Sie das Feature der Instance-Gewichtung verwenden, gilt der von Ihnen angegebene Preis pro Einheitsstunde. Der Preis pro Einheitsstunde lässt sich errechnen, indem Sie Ihren Preis für einen Instance-Typ durch die Anzahl der Einheiten dividieren, die er darstellt. Die Spot-Flotte berechnet die Anzahl der zu startenden Spot-Instances, indem die Zielkapazität durch die Instance-Gewichtung dividiert wird. Wenn es sich beim Ergebnis nicht um eine Ganzzahl handelt, rundet die Spot-Flotte es auf die nächste Ganzzahl auf, damit die Größe Ihrer Flotte nicht unter der Zielkapazität liegt. Die Spot-Flotte kann alle Pools auswählen, die Sie in Ihrer Startspezifikation angeben, auch wenn die Kapazität der gestarteten Instances die angeforderte Zielkapazität übersteigt.

Die folgenden Tabellen enthalten Beispiele für die Berechnung des Preises pro Einheit für eine Spot-Flotten-Anforderung mit einer Zielkapazität von 10.

Instance-Typ	Instance-Gewichtung	Preis pro Instance-Stunde	Preis pro Einheitsstunde	Anzahl an gestarteten Instances
`r3.xlarge`	2	$0.05	0,025 (0,05 geteilt durch 2)	5 (10 geteilt durch 2)

Instance-Typ	Instance-Gewichtung	Preis pro Instance-Stunde	Preis pro Einheitsstunde	Anzahl an gestarteten Instances
`r3.8xlarge`	8	$0.10	0,0125	2

Instance-Typ	Instance-Gewichtung	Preis pro Instance-Stunde	Preis pro Einheitsstunde	Anzahl an gestarteten Instances
			(0,10 geteilt durch 8)	(10 geteilt durch 8, Ergebnis aufgerundet)

Verwenden Sie die Spot-Flotten-Instance-Gewichtung wie folgt, um die gewünschte Zielkapazität in den Pools mit dem niedrigsten Preis pro Einheit zum Zeitpunkt der Erfüllung bereitzustellen:

1. Geben Sie die Zielkapazität für Ihre Spot-Flotte entweder in Instances (Standard) oder in den Einheiten Ihrer Wahl an, z. B. virtuelle CPUs, Arbeitsspeicher, Speicher oder Durchsatz.
2. Legen Sie den Preis pro Einheit fest.
3. Geben Sie für alle Startkonfigurationen die Gewichtung an, d. h. die Anzahl an Einheiten, die der Instance-Typ hinsichtlich der Zielkapazität darstellt.

Beispiel für die Instance-Gewichtung

Stellen Sie sich eine Spot-Flotten-Anforderung mit der folgenden Konfiguration vor:

- Eine Zielkapazität von 24
- Eine Startspezifikation mit dem Instance-Typ `r3.2xlarge` und der Gewichtung 6
- Eine Startspezifikation mit dem Instance-Typ `c3.xlarge` und der Gewichtung 5

Die Gewichtung stellt die Anzahl an Einheiten dar, die der Instance-Typ hinsichtlich der Zielkapazität darstellt. Wenn die erste Startspezifikation den niedrigsten Preis pro Einheit (Preis für `r3.2xlarge` pro Instance-Stunde geteilt durch 6) bereitstellt, würde die Spot-Flotte vier dieser Instances starten (24 geteilt durch 6).

Wenn die zweite Launch-Spezifikation den niedrigsten Preis pro Einheit (Preis für `c3.xlarge` pro Instance-Stunde geteilt durch 5) bereitstellt, würde die Spot-Flotte fünf dieser Instances launchen (24 geteilt durch 5, Ergebnis aufgerundet).

Instance-Gewichtung und Zuweisungsstrategie

Stellen Sie sich eine Spot-Flotten-Anforderung mit der folgenden Konfiguration vor:

- Eine Zielkapazität von 30
- Eine Startspezifikation mit dem Instance-Typ `c3.2xlarge` und der Gewichtung 8
- Eine Startspezifikation mit dem Instance-Typ `m3.xlarge` und der Gewichtung 8
- Eine Startspezifikation mit dem Instance-Typ `r3.xlarge` und der Gewichtung 8

Die Spot-Flotte würde vier Instances starten (30 geteilt durch 8, Ergebnis aufgerundet). Bei der `diversified`-Strategie launcht die Spot-Flotte eine Instance in jedem der drei Pools und die vierte Instance in dem Pool, für den der niedrigste Preis pro Einheit anfällt.

Arbeiten mit Spot-Flotten

Zum Verwenden einer Spot-Flotte erstellen Sie eine Spot-Flotten-Anforderung mit der Gesamtzielkapazität, einem optionalen On-Demand-Anteil, einer oder mehreren Startspezifikationen für die Instances und dem Höchstpreis, den Sie zu zahlen bereit sind. Die Flottenanforderung muss eine Startspezifikation enthalten, die die Informationen definiert, die die Flotte benötigt, um eine Instance zu starten, z. B. eine AMI, einen Instance-Typ, ein Subnetz oder eine Availability Zone, und eine oder mehrere Sicherheitsgruppen.

Wenn Ihre Flotte Spot-Instances enthält, kann Amazon EC2 versuchen, Ihre Flotten-Zielkapazität aufrechtzuerhalten, wenn sich die Spot-Preise ändern.

Die Zielkapazität einer einmaligen Anfrage kann nach der Übermittlung nicht mehr geändert werden. Um die Zielkapazität zu ändern, muss die Anforderung abgebrochen und eine neue übermittelt werden.

Eine Spot-Flotten-Anforderung bleibt so lange aktiv, bis sie abläuft oder Sie sie abbrechen. Wenn Sie eine Flotten-Anforderung abbrechen, können Sie angeben, ob mit dem Abbrechen der Anforderung die Spot-Instances in dieser Flotte beendet werden sollen.

Inhalt

- Ändern einer Spot-Flotten-Anforderung
- Abbrechen einer Spot-Flotten-Anforderung

Status von Spot-Flotten-Anforderungen

Eine Spot-Flotten-Anforderung einen der folgenden Status aufweisen:

- `submitted` – Die Spot-Flotten-Anforderung wird evaluiert und Amazon EC2 bereitet den Launch der gewünschten Anzahl von Instances vor. Wenn eine Anforderung Ihre Spot-Flottenlimits überschreiten würde, wird sie sofort abgebrochen.
- `active` – Die Spot-Flotte wurde validiert und Amazon EC2 versucht, die gewünschte Anzahl an ausgeführten Spot Instances aufrechtzuerhalten. Die Anforderung bleibt so lange in diesem Zustand, bis sie geändert oder abgebrochen wird.
- `modifying` – Die Spot-Flotten-Anforderung wird geändert. Die Anforderung bleibt in diesem Zustand, bis die Änderung vollständig verarbeitet ist oder die Spot-Flotte abgebrochen wird. Eine einmalige `request` kann nicht geändert werden. Dieser Zustand trifft daher nicht auf solche Spot-Anforderungen zu.
- `cancelled_running` – Die Spot-Flotte wird abgebrochen und startet keine weiteren Spot Instances. Die bestehenden Spot-Instances laufen weiter, bis sie unterbrochen oder beendet werden. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances unterbrochen oder beendet wurden.
- `cancelled_terminating` – Die Spot-Flotte wird abgebrochen und ihre Spot Instances werden beendet. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances beendet wurden.
- `cancelled` – Die Spot-Flotte wird abgebrochen und weist keine laufenden Spot Instances auf. Die Spot-Flotten-Anforderung wird zwei Tage nach dem Beenden der zugehörigen Instances gelöscht.

Zustandsprüfungen von Spot-Flotten

Die Spot-Flotte überprüft den Zustand der Spot-Instances in der Flotte alle zwei Minuten. Der Zustand einer Instance lautet entweder `healthy` oder `unhealthy`.

Die Spot-Flotte ermittelt den Zustand einer Instance anhand der von Amazon EC2 bereitgestellten Zustandsprüfungen. Wenn der Status der Instance-Statusprüfung oder der Systemstatusprüfung während drei aufeinanderfolgenden Zustandsprüfungen `impaired` lautet, ist der Zustand der Instance `unhealthy`. Weitere Informationen finden Sie unter Statusprüfungen für Ihre Instances.

Sie können Ihre Flotte so konfigurieren, dass nicht voll funktionsfähige Spot-Instances ersetzt werden. Nach dem Aktivieren von Ersetzungen in Zuge von Zustandsprüfungen wird eine Spot Instance ersetzt, wenn sie als `unhealthy` gemeldet wird. Die Flotte kann die Zielkapazität einige Minuten lang unterschreiten, während eine nicht voll funktionsfähige Spot-Instance ersetzt wird.

Voraussetzungen

- Der Ersetzung von Zustandsprüfungen wird nur für Spot-Flotten unterstützt, welche eine Zielkapazität (Flotten vom Typ `maintain`) aufrechterhalten, nicht für einmalige Spot-Flotten (Flotten des Typs `request`).
- Der Austausch von Zustandsprüfungen wird nur für Spot-Instances unterstützt. Dieses Feature wird für On-Demand-Instances nicht unterstützt.
- Sie können Ihre Spot-Flotte nur beim Erstellen so konfigurieren, dass nicht voll funktionsfähige Instances ersetzt werden.
- Benutzer können die Ersetzung im Rahmen von Zustandsprüfungen nur verwenden, wenn sie über die Berechtigung zum Aufrufen der `ec2:DescribeInstanceStatus`-Aktion verfügen.

Console

So konfigurieren Sie eine Spot-Flotte mit der Konsole dafür, dass nicht voll funktionsfähige Spot-Instances ersetzt werden:

1. Befolgen Sie die Schritte zum Erstellen einer Spot-Flotte. Weitere Informationen finden Sie unter Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole).
2. Zum Konfigurieren der Flotte, um fehlerhafte Spot-Instances zu ersetzen, wählen Sie für Health check (Zustandsprüfung) die Option Replace unhealthy instances (Fehlerhafte Instances ersetzen) aus. Zum Aktivieren dieser Option müssen Sie zuerst Maintain target capacity (Zielkapazität erhalten) auswählen.

AWS CLI

So konfigurieren Sie eine Spot-Flotte mit der AWS CLI dafür, dass nicht voll funktionsfähige Spot Instances ersetzt werden

1. Befolgen Sie die Schritte zum Erstellen einer Spot-Flotte. Weitere Informationen finden Sie unter Erstellen Sie eine Spot-Flotte mit dem AWS CLI.

2. Um die Flotte so zu konfigurieren, dass sie nicht voll funktionsfähige Spot-Instances ersetzt, geben Sie für `ReplaceUnhealthyInstances` `true` ein.

Spot-Flotten-Berechtigungen

Wenn Ihre Benutzer eine Spot-Flotte erstellen oder verwalten sollen, müssen Sie diesen die erforderlichen Berechtigungen gewähren.

Wenn Sie die Amazon EC2-Konsole zum Erstellen einer Spot-Flotte verwenden, erstellt sie zwei serviceverknüpfte Rollen namens `AWSServiceRoleForEC2SpotFleet` und `AWSServiceRoleForEC2Spot` und eine Rolle namens `aws-ec2-spot-fleet-tagging-role`, die der Spot-Flotte die Berechtigungen zum Anfordern, Launchen, Beenden und Markieren von Ressourcen in Ihrem Namen erteilen. Wenn Sie die AWS CLI oder eine API verwenden, müssen Sie sicherstellen, dass diese Rollen vorhanden sind.

Verwenden Sie die folgenden Anweisungen, um die erforderlichen Berechtigungen zu erteilen und die Rollen zu erstellen.

Berechtigungen und Rollen

- Benutzern die Berechtigung für Spot-Flotte gewähren
- Serviceverknüpfte Rolle für Spot-Flotte
- Serviceverknüpfte Rolle für Spot-Instances
- IAM-Rolle zum Markieren einer Spot-Flotte

Benutzern die Berechtigung für Spot-Flotte gewähren

Wenn Ihre Benutzer eine Spot-Flotte erstellen oder verwalten, stellen Sie sicher, dass Sie ihnen die erforderlichen Berechtigungen gewähren.

So erstellen Sie eine Richtlinie für Spot-Flotte

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Policies und Create policy aus.
3. Wählen Sie auf der Seite Richtlinie erstellen die Option JSON aus und ersetzen Sie den Text durch Folgendes.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances",
                "ec2:CreateTags",
                "ec2:RequestSpotFleet",
                "ec2:ModifySpotFleetRequest",
                "ec2:CancelSpotFleetRequests",
                "ec2:DescribeSpotFleetRequests",
                "ec2:DescribeSpotFleetInstances",
                "ec2:DescribeSpotFleetRequestHistory"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::*:role/aws-ec2-spot-fleet-tagging-role"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles",
                "iam:ListInstanceProfiles"
            ],
            "Resource": "*"
        }
    ]
}
```

Die vorangehende Beispielrichtlinie gewährt einem Benutzer die Berechtigungen, die für die meisten Spot-Flotten-Anwendungsfälle erforderlich sind. Um den Benutzer auf bestimmte API-Aktionen zu beschränken, geben Sie stattdessen nur diese API-Aktionen an.

Erforderliche EC2- und IAM-APIs

Die folgenden APIs müssen in der Richtlinie enthalten sein:

- `ec2:RunInstances` – erforderlich zum Launchen von Instances in einer Spot-Flotte

- `ec2:CreateTags` – erforderlich zum Markieren der Spot-Flotten-Anforderung, der Instances oder der Volumes
- `iam:PassRole` – erforderlich, um die Spot-Flotten-Rolle anzugeben
- `iam:CreateServiceLinkedRole` – erforderlich zum Erstellen der serviceverknüpften Rolle
- `iam:ListRoles` – erforderlich zum Aufzählen vorhandener IAM-Rollen
- `iam:ListInstanceProfiles` – erforderlich zum Aufzählen vorhandener Instance-Profile

> **Important**
>
> Wenn Sie in der Startspezifikation oder Startvorlage eine Rolle für das IAM-Instance-Profil angeben, müssen Sie dem Benutzer die Berechtigung gewähren, die Rolle an den Service zu übergeben. Schließen Sie hierzu in der IAM-Richtlinie `"arn:aws:iam::*:role/`*`IamInstanceProfile-role`*`"` als Ressource für die Aktion `iam:PassRole` ein. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erteilen von Benutzerberechtigungen zur Übergabe einer Rolle an einen AWS Service.

APIs für Spot-Flotten

Fügen Sie Ihrer Richtlinie bei Bedarf die folgenden Spot Fleet API-Aktionen hinzu:

- `ec2:RequestSpotFleet`
- `ec2:ModifySpotFleetRequest`
- `ec2:CancelSpotFleetRequests`
- `ec2:DescribeSpotFleetRequests`
- `ec2:DescribeSpotFleetInstances`
- `ec2:DescribeSpotFleetRequestHistory`

Optionale IAM-APIs

(Optional) Um einem Benutzer das Erstellen von Rollen oder Instance-Profilen mithilfe der IAM-Konsole zu ermöglichen, müssen Sie der Richtlinie die folgenden Aktionen hinzufügen:

- `iam:AddRoleToInstanceProfile`

- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetRole`
- `iam:ListPolicies`

4. Wählen Sie Review policy (Richtlinie prüfen) aus.
5. Geben Sie auf der Seite Review policy (Richtlinie überprüfen) einen Richtlinienamen und eine Beschreibung ein und wählen Sie anschließend Create policy (Richtlinie erstellen) aus.
6. Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

   - Benutzer und Gruppen in AWS IAM Identity Center:

     Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

   - Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

     Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

   - IAM-Benutzer:
     - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
     - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Serviceverknüpfte Rolle für Spot-Flotte

Amazon EC2 nutzt serviceverknüpfte Rollen für die Berechtigungen, die für den Aufruf anderer AWS -Services in Ihrem Namen benötigt werden. Eine dienstverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit einem AWS Dienst verknüpft ist. Mit Diensten verknüpfte Rollen bieten eine sichere Möglichkeit, Berechtigungen an AWS Dienste zu delegieren, da nur der verknüpfte Dienst eine dienstbezogene Rolle übernehmen kann. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen im -IAM-Benutzerhandbuch.

Amazon EC2 verwendet die angegebene serviceverknüpfte Rolle AWSServiceRoleForEC2SpotFleet, um Instances in Ihrem Namen zu starten und zu verwalten.

> **Important**
>
> Wenn Sie in Ihrer Spot-Flotte ein verschlüsseltes AMI oder einen verschlüsselten Amazon EBS-Snapshot angeben, müssen Sie der AWSServiceRoleForEC2SpotFleetRolle die Berechtigung zur Verwendung des CMK erteilen, damit Amazon EC2 Instances in Ihrem Namen starten kann. Weitere Informationen finden Sie unter Gewähren von Zugriff auf CMKs für die Verwendung mit verschlüsselten AMIs und EBS-Snapshots.

Berechtigungen erteilt von AWSServiceRoleForEC2SpotFleet

Amazon EC2 verwendet AWSServiceRoleForEC2SpotFleet, um die folgenden Aktionen durchzuführen:

- `ec2:RequestSpotInstances` - Spot-Instances-Anforderung
- `ec2:RunInstances` – Starten von Instances
- `ec2:TerminateInstances` – Beenden von Instances
- `ec2:DescribeImages` – Beschreiben von Amazon Machine Images (AMIs) für die Instances
- `ec2:DescribeInstanceStatus` – Beschreiben des Status der Instances
- `ec2:DescribeSubnets` – Beschreiben der Subnetze für die Instances
- `ec2:CreateTags` – Hinzufügen von Tags zur Spot-Flotten-Anforderung, zu Instances und zu Volumes
- `elasticloadbalancing:RegisterInstancesWithLoadBalancer` – Hinzufügen der angegebenen Instances zum angegebenen Load Balancer
- `elasticloadbalancing:RegisterTargets` – Registrieren der die angegebenen Ziele bei der angegebenen Zielgruppe

Erstellen der serviceverknüpften Rolle

Größtenteils müssen Sie die serviceverknüpfte Rolle nicht manuell erstellen. Amazon EC2 erstellt die AWSServiceRoleForEC2SpotFleetserviceverknüpfte Rolle, wenn Sie zum ersten Mal eine Spot-Flotte mithilfe der Konsole erstellen.

Wenn Sie vor Oktober 2017, als Amazon EC2 begann, diese servicebezogene Rolle zu unterstützen, eine aktive Spot-Flotte-Anfrage hatten, hat Amazon EC2 die AWSServiceRoleForEC2SpotFleetRolle in Ihrem Konto erstellt. AWS Weitere Informationen finden Sie unter Eine neue Rolle wurde in meinem AWS Konto angezeigt im IAM-Benutzerhandbuch.

Wenn Sie die AWS CLI oder eine API verwenden, um eine Spot-Flotte zu erstellen, müssen Sie zunächst sicherstellen, dass diese Rolle existiert.

Um AWSServiceRoleForEC2SpotFleet mit der Konsole zu erstellen

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rolle) aus.
3. Wählen Sie Rolle erstellen aus.
4. Gehen Sie auf der Seite Select trusted entity (Vertrauenswürdige Entität auswählen) wie folgt vor:
    a. Wählen Sie unter Vertrauenswürdiger Entitätstyp die Option AWS -Service aus.
    b. Wählen Sie unter Anwendungsfall für Service oder Anwendungsfall die Option EC2 aus.
    c. Wählen Sie als Anwendungsfall EC2 — Spot Fleet aus.
    d. Wählen Sie Next (Weiter).
5. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.
6. Wählen Sie auf der Seite Benennen, Überprüfen und Erstellen die Option Rolle erstellen aus.

Um zu erstellen AWSServiceRoleForEC2SpotFleet mit dem AWS CLI

Verwenden Sie den Befehl create-service-linked-role wie folgt.

```
aws iam create-service-linked-role --aws-service-name spotfleet.amazonaws.com
```

Wenn Sie Spot Fleet nicht mehr verwenden müssen, empfehlen wir Ihnen, die AWSServiceRoleForEC2SpotFleetRolle zu löschen. Nachdem diese Rolle in Ihrem Konto gelöscht wurde, erstellt Amazon EC2 die Rolle erneut, wenn Sie eine Spot-Flotte über die Konsole anfordern. Weitere Informationen finden Sie unter Löschen einer serviceverknüpften Rolle im IAM-Benutzerhandbuch.

Gewähren von Zugriff auf CMKs für die Verwendung mit verschlüsselten AMIs und EBS-Snapshots

Wenn Sie in Ihrer Spot-Flottenanfrage ein verschlüsseltes AMI oder einen verschlüsselten Amazon EBS-Snapshot angeben und einen vom Kunden verwalteten Schlüssel für die Verschlüsselung verwenden, müssen Sie der AWSServiceRoleForEC2SpotFleetRolle die Berechtigung zur Verwendung des CMK erteilen, damit Amazon EC2 Instances in Ihrem Namen starten kann. Dazu müssen Sie eine Erteilung zum CMK hinzufügen, wie im Folgenden gezeigt:

Bei der Einrichtung von Berechtigungen ist die Erteilung von Berechtigung eine Alternative zu Schüsselrichtlinien. Weitere Informationen finden Sie unter Verwenden von Erteilungen und Verwenden von Schlüsselrichtlinien in AWS KMS im Developer-Handbuch für AWS Key Management Service .

Um der AWSServiceRoleForEC2SpotFleet Rolle Berechtigungen zur Verwendung des CMK zu erteilen

- Verwenden Sie den Befehl create-grant, um dem CMK einen Grant hinzuzufügen und den Principal (die mit dem AWSServiceRoleForEC2SpotFleetService verknüpfte Rolle) anzugeben, dem die Berechtigung erteilt wird, die mit dem Grant erlaubten Operationen auszuführen. Der CMK wird durch den Parameter `key-id` und den ARN des CMK spezifiziert. Der Principal wird durch den `grantee-principal` Parameter und den ARN der AWSServiceRoleForEC2SpotFleetdienstverknüpften Rolle angegeben.

```
aws kms create-grant \
    --region us-east-1 \
    --key-id arn:aws:kms:us-
east-1:444455556666:key/1234abcd-12ab-34cd-56ef-1234567890ab \
    --grantee-principal arn:aws:iam::111122223333:role/
AWSServiceRoleForEC2SpotFleet \
    --operations "Decrypt" "Encrypt" "GenerateDataKey"
 "GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"
 "ReEncryptTo"
```

Serviceverknüpfte Rolle für Spot-Instances

Amazon EC2 verwendet die angegebene serviceverknüpfte Rolle AWSServiceRoleForEC2Spot, um Spot-Instances in Ihrem Namen zu starten und zu verwalten. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für Spot-Instance-Anforderungen.

IAM-Rolle zum Markieren einer Spot-Flotte

Die IAM-Rolle `aws-ec2-spot-fleet-tagging-role` gewährt der Spot-Flotte die Berechtigung, die Spot-Flotten-Anforderung, -Instances und -Volumes zu markieren. Weitere Informationen finden Sie unter Markieren einer Spot-Flotte.

> **Important**
>
> Wenn Sie sich dafür entscheiden, Instances in der Flotte zu markieren und gleichzeitig die Zielkapazität beizubehalten (die Spot-Flotten-Anfrage ist vom Typ `maintain`), können die Unterschiede in den Berechtigungen, die für den Benutzer und die `IamFleetRole` festgelegt sind, zu einem inkonsistenten Tag-Verhalten der Instances in der Flotte führen. Wenn `IamFleetRole` die `CreateTags`-Berechtigung nicht enthält, werden einige der von der Flotte gestarteten Instances möglicherweise nicht markiert. Während wir daran arbeiten, diese Inkonsistenz zu beheben, um sicherzustellen, dass alle Instances, die von der Flotte gestartet werden, markiert sind, empfehlen wir, die `aws-ec2-spot-fleet-tagging-role`-Rolle für die `IamFleetRole` zu verwenden. Um eine bestehende Rolle zu verwenden, können Sie alternativ die `AmazonEC2SpotFleetTaggingRole` AWS verwaltete Richtlinie an die bestehende Rolle anhängen. Andernfalls müssen Sie die `CreateTags`-Berechtigung manuell zu Ihrer vorhandenen Richtlinie hinzufügen.

So erstellen Sie die IAM-Rolle zum Markieren einer Spot-Flotte:

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Roles (Rolle) aus.
3. Wählen Sie Rolle erstellen aus.
4. Wählen Sie auf der Seite Select trusted entity (Auswahl der vertrauenswürdigen Entität) unter Trusted entity type (Auswahl der vertrauenswürdigen Entität) die Option AWS service (-Service) aus.
5. Wählen Sie unter Anwendungsfall unter Anwendungsfälle für andere AWS Dienste die Option EC2 und dann EC2 — Spot Fleet Tagging aus.
6. Wählen Sie Next (Weiter).
7. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die Option Next (Weiter) aus.

8. Geben Sie auf der Seite Name, review, and create (Benennen, überprüfen und erstellen) für Role name (Rollenname) einen Namen für die Rolle ein (z. B. **`aws-ec2-spot-fleet-tagging-role`**).
9. Überprüfen Sie die Informationen auf der Seite, und wählen Sie dann Create role (Rolle erstellen) aus.

Serviceübergreifende Confused-Deputy-Prävention

Das Confused-Deputy-Problem ist ein Sicherheitsproblem, bei dem eine Entität, die nicht über die Berechtigung zum Ausführen einer Aktion verfügt, eine Entität mit größeren Rechten zwingen kann, die Aktion auszuführen. Wir empfehlen, dass Sie die globalen Bedingungskontext-Schlüssel `aws:SourceArn` und `aws:SourceAccount` in der `aws-ec2-spot-fleet-tagging-role`-Vertrauensrichtlinie verwenden, um die Berechtigungen, welche die Spot-Flotte einem anderen Service erteilt, auf eine bestimmte Ressource zu beschränken.

Um die SourceAccount Bedingungsschlüssel aws: SourceArn und aws: zur Vertrauensrichtlinie hinzuzufügen **`aws-ec2-spot-fleet-tagging-role`**

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Rollen aus.
3. Suchen Sie die `aws-ec2-spot-fleet-tagging-role`, die Sie zuvor erstellt haben, und wählen Sie den Link (nicht das Kontrollkästchen) aus.
4. Wählen Sie unter Summary (Zusammenfassung) die Registerkarte Trust Relationships (Vertrauensstellungen) und dann Edit trust policy (Vertrauensrichtlinie bearbeiten) aus.
5. Fügen Sie in der JSON-Anweisung ein `Condition`-Element hinzu, das Ihre globalen `aws:SourceAccount`- und `aws:SourceArn`-Bedingungskontextschlüssel zur Verhinderung des Confused-Deputy-Problems folgendermaßen festlegt:

```
"Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
```

> **Note**
>
> Wenn der `aws:SourceArn`-Wert die Konto-ID enthält und Sie beide globalen Bedingungskontextschlüssel verwenden, müssen der `aws:SourceAccount`-Wert und das Konto im `aws:SourceArn`-Wert dieselbe Konto-ID verwenden, wenn sie in der gleichen Richtlinienanweisung verwendet wird.

Die endgültige Vertrauensrichtlinie wird folgendermaßen aussehen:

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "spotfleet.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:us-east-1:account_id:spot-fleet-request/sfr-
*"
      },
      "StringEquals": {
        "aws:SourceAccount": "account_id"
      }
    }
  }
}
```

6. Wählen Sie Richtlinie aktualisieren.

Die folgende Tabelle enthält potenzielle Werte für `aws:SourceArn`, um den Umfang Ihrer `aws-ec2-spot-fleet-tagging-role` in unterschiedlichem Grad an Spezifität einzuschränken.

API-Operation	Aufgerufener Service	Scope	**aws:SourceArn**
RequestSpotFlotte	AWS STS (AssumeRole)	Beschränken Sie die AssumeRole Funktion aws-ec2-spot-fleet-tagging-role spot-fleet-requests auf das angegebene Konto.	arn:aws:ec2:*: *123456789012* :spot-fleet-request/sfr-*
RequestSpotFlotte	AWS STS (AssumeRole)	Beschränken Sie die AssumeRole Funktion aws-ec2-spot-fleet-tagging-role spot-fleet-requests auf das angegebene Konto und die angegebene Region. Beachten Sie, dass diese Rolle in anderen Regionen nicht verwendbar ist.	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*
RequestSpotFlotte	AWS STS (AssumeRole)	Begrenzen Sie die AssumeRole -Funktion in aws-ec2-spot-fleet-tagging-role nur auf Maßnahmen, welche die Flotte sfr-11111111-1111-1111-1111-111111111111 betreffen. Beachten Sie, dass diese Rolle möglicher	arn:aws:ec2: *us-east-1* :*123456789012* :spot-fleet-request/sfr-*11111111-1111-1111-1111-111111111111*

API-Operation	Aufgerufener Service	Scope	`aws:SourceArn`
		weise nicht für andere Spot-Flotten verwendbar ist. Diese Rolle kann auch nicht verwendet werden, um neue Spot-Flot ten über RequestSp otFleet zu starten.	

Erstellen eine Spot-Flotten-Anforderung

Mithilfe von können Sie schnell eine Spot-Flotte-Anfrage erstellen AWS Management Console, indem Sie nur Ihren Anwendungs- oder Aufgabenbedarf und die Mindestanforderungen an die Rechenleistung auswählen. Amazon EC2 konfiguriert eine Flotte, die Ihren Bedürfnissen am besten entspricht und bewährten Methoden für Spot folgt. Weitere Informationen finden Sie unter Schnelle Erstellung einer Spot-Flotten-Anforderung (Konsole). Andernfalls können Sie jede der Standardeinstellungen ändern. Weitere Informationen finden Sie unter Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole) und Erstellen Sie eine Spot-Flotte mit dem AWS CLI.

Optionen zum Erstellen einer Spot-Flotte

- Schnelle Erstellung einer Spot-Flotten-Anforderung (Konsole)
- Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole)
- Erstellen Sie eine Spot-Flotte mit dem AWS CLI

Schnelle Erstellung einer Spot-Flotten-Anforderung (Konsole)

Führen Sie diese Schritte aus, um schnell eine Spot-Flotten-Anforderung zu erstellen.

So erstellen Sie eine Spot-Flotten-Anforderung mit den empfohlenen Einstellungen (Konsole):

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wenn Sie noch keine Erfahrung mit Spot haben, wird eine Willkommensseite angezeigt. Wählen Sie Get started aus. Andernfalls wählen Sie Request Spot-Instances (anfordern) aus.

4. Wählen Sie unter Startparameter die Option Startparameter manuell konfigurieren aus.
5. Wählen Sie für AMI ein AMI aus.
6. Geben Sie unter Zielkapazität für Gesamtzielkapazität die Anzahl der anzufordernden Einheiten an. Für den Typ der Einheit können Sie Instances, vCPUs oder Speicher (MiB) wählen.
7. Überprüfen Sie für Ihre Flottenanforderung auf einen Blick Ihre Flottenkonfiguration und wählen Sie Start aus.

Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole)

Sie können eine Spot-Flotte mit von Ihnen definierten Parametern erstellen.

So erstellen Sie eine Spot-Flotten-Anforderung mit definierten Parametern (Konsole):

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wenn Sie noch keine Erfahrung mit Spot haben, wird eine Willkommensseite angezeigt. Wählen Sie Get started aus. Andernfalls wählen Sie Request Spot-Instances (anfordern) aus.
4. Führen Sie für Startparameter die folgenden Schritte aus:

   a. Um die Startparameter in der Spot-Konsole zu definieren, wählen Sie Startparameter manuell konfigurieren aus.

   b. Wählen Sie für AMI eines der Basis-AMIs aus AWS, die von bereitgestellt werden, oder wählen Sie Search for AMI, um ein AMI aus unserer Benutzer-Community AWS Marketplace, das oder eines Ihrer eigenen zu verwenden.

   > **Note**
   >
   > Wenn ein in den Startparametern angegebenes AMI deregistriert oder deaktiviert ist, können keine neuen Instances über das AMI gestartet werden. Bei Flotten, die so eingestellt sind, dass sie die Zielkapazität beibehalten, wird die Zielkapazität nicht beibehalten.

   c. (Optional) Wählen Sie für Key pair name (Schlüsselpaarname= ein bestehendes Schlüsselpaar aus oder erstellen Sie ein neues.

      [Bestehendes Schlüsselpaar] Wählen Sie das Schlüsselpaar aus.

[Neues Schlüsselpaar] Wählen Sie Neues Schlüsselpaar erstellen aus, um zur Seite Schlüsselpaare zu gelangen. Wenn Sie fertig sind, kehren Sie zur Seite Spot-Anfragen zurück und aktualisieren Sie die Liste.

d. (Optional) Erweitern Sie Zusätzliche Startparameter und gehen Sie wie folgt vor:

   i. (Optional) Um die Amazon-EBS-Optimierung zu aktivieren, wählen Sie für EBS-optimiert die Option EBS-optimierte Instance starten aus.

   ii. (Optional) Um temporären Speicher auf Blockebene für Ihre Instances hinzuzufügen, wählen Sie für Instance store (Instance-Speicher) die Option Attach at launch (Beim Start anhängen) aus.

   iii. (Optional) Um Speicher hinzuzufügen, wählen Sie Neues Volume hinzufügen aus und geben Sie je nach Instance-Typ zusätzliche Instance-Speicher-Volumes oder Amazon-EBS-Volumes an.

   iv. (Optional) Die grundlegende Überwachung ist standardmäßig für Ihre Instances aktiviert. Um die detaillierte Überwachung zu aktivieren, wählen Sie unter Überwachung die Option CloudWatch Detaillierte Überwachung aktivieren aus.

   v. (Optional:) Wenn Sie für Tenancy eine Dedicated-Spot-Instance ausführen möchten, wählen Sie die Option Dedicated - run a dedicated instance (Dedicated – Dedicated-Instance ausführen) aus.

   vi. (Optional) Wählen Sie für Security groups (Sicherheitsgruppen) eine oder mehrere Sicherheitsgruppen aus oder erstellen Sie eine neue.

   [Bestehende Sicherheitsgruppe] Wählen Sie eine oder mehrere Sicherheitsgruppen aus.

   [Neue Sicherheitsgruppe] Wählen Sie Neue Sicherheitsgruppe erstellen aus, um zur Seite Sicherheitsgruppen zu gelangen. Wenn Sie fertig sind, kehren Sie zu den Spot-Anfragen zurück und aktualisieren Sie die Liste.

   vii. (Optional) Um Ihre Instances aus dem Internet erreichbar zu machen, wählen Sie für Auto-assign IPv4 Public IP (Automatisch öffentliche IPv4-IP zuweisen) die Option Enable (Aktivieren) aus.

   viii. (Optional) Um Ihre Spot-Instances mit einer IAM-Rolle zu starten, geben Sie für IAM instance profile (IAM-Instance-Profil) die Rolle an.

   ix. (Optional) Wenn Sie ein Start-Skript ausführen möchten, kopieren Sie dieses in User data.

x. (Optional) Um ein Tag hinzuzufügen, wählen Sie Tag erstellen aus, geben Sie den Schlüssel und Wert für das Tag ein und wählen Sie Erstellen aus. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

   Damit die Instances und die Spot-Flottenanforderung mit demselben Tag markiert werden, stellen Sie für jedes Tag sicher, dass sowohl Instance als auch Flotte ausgewählt ist. Um nur die von der Flotte gestarteten Instances zu markieren, löschen Sie Fleet. Um nur die Spot-Flottenanforderung zu markieren, löschen Sie Instances.

5. Gehen Sie für Additional request details (Zusätzliche Anforderungsdetails) wie folgt vor:

   a. Überprüfen Sie die zusätzlichen Details der Anfrage. Um Änderungen vorzunehmen, deaktivieren Sie Apply defaults (Standardeinstellungen anwenden).

   b. (Optional) Für IAM fleet role (IAM-Flottenrolle) können Sie die Standardrolle verwenden oder eine andere Rolle auswählen. Um nach dem Ändern der Rolle die Standardrolle zu verwenden, wählen Sie Use default role (Standardrolle verwenden).

   c. (Optional) Für Maximum price (Höchstpreis) können Sie den Standard-Höchstpreis (den On-Demand-Preis) verwenden oder den Höchstpreis angeben, den Sie zu zahlen bereit sind. Wenn Ihr Höchstpreis niedriger ist als der Spot-Preis für die von Ihnen ausgewählten Instance-Typen, werden Ihre Spot-Instances nicht gestartet.

   d. (Optional) Sie können eine Anfrage erstellen, die nur während eines bestimmten Zeitraums gültig ist, indem Sie Request valid from und Request valid until bearbeiten.

   e. (Optional) Ihre Spot-Instances werden standardmäßig beendet, wenn die Spot-Flottenanforderung abläuft. Um sie nach Ablauf Ihrer Anfrage am Laufen zu halten, deaktivieren Sie Terminate the instances when the request expires (Instances beenden, wenn die Anfrage abläuft).

   f. (Optional) Um Ihre Spot-Instances mit einem Load Balancer zu registrieren, wählen Sie die Option Receive traffic from one or more load balancers (Datenverkehr von einem oder mehreren Load Balancern entgegennehmen) und legen Sie einen oder mehrere Classic Load Balancer oder Zielgruppen fest.

6. Wählen Sie für Minimum compute unit (Minimale Recheneinheit) die minimalen Hardwarespezifikationen (vCPUs, Speicher und Arbeitsspeicher) aus, die Sie für Ihre Anwendung oder Aufgabe benötigen (entweder as specs (als Spezifikationen) oder as an instance type (als Instance-Typ).

   - Geben Sie für as specs (als Spezifikationen) die erforderliche Anzahl von vCPUs und die Speichergröße an.

- Übernehmen Sie für as an instance type (als Instance-Typ) den Standard-Instance-Typ oder wählen Sie Change instance type (Instance-Typ ändern) aus, um einen anderen Instance-Typ auszuwählen.

7. Führen Sie für die Zielkapazität die folgenden Schritte aus:

   a. Geben Sie für Gesamtzielkapazität die Anzahl der anzufordernden Einheiten an. Für den Typ der Einheit können Sie Instances, vCPUs oder Speicher (MiB) wählen. Um eine Zielkapazität von 0 anzugeben (damit Sie später Kapazität hinzufügen können), wählen Sie Maintain target capacity (Zielkapazität erhalten) aus.

   b. (Optional) Geben Sie für On-Demand-Basiskapazität einschließen die Anzahl der anzufordernden On-Demand-Einheiten an. Die Zahl muss unter der Total target capacity (Zielkapazität insgesamt) liegen. Amazon EC2 berechnet die Differenz und weist die Differenz Spot-Einheiten für die Anforderung zu.

      > **Important**
      >
      > Um optionale On-Demand-Kapazität anzugeben, müssen Sie zunächst eine Startvorlage auswählen.

   c. (Optional) Standardmäßig beendet Amazon EC2 Spot-Instances, wenn sie unterbrochen werden. Um die Zielkapazität aufrechtzuerhalten, wählen Sie Zielkapazität aufrechterhalten aus. Sie können dann angeben, dass Amazon EC2 Spot-Instances beendet, stoppt oder in den Ruhezustand versetzt, wenn sie unterbrochen werden. Hierzu wählen sie die entsprechende Option unter Interruption behavior aus.

      > **Note**
      >
      > Wenn ein in den Startparametern angegebenes AMI deregistriert oder deaktiviert ist, können keine neuen Instances über das AMI gestartet werden. Bei Flotten, die so eingestellt sind, dass sie die Zielkapazität beibehalten, wird die Zielkapazität nicht beibehalten.

   d. (Optional) Damit die Spot-Flotte eine Ersatz-Spot-Instance starten kann, wenn eine Benachrichtigung zum Instance-Neuausgleich für eine vorhandene Spot-Instance in der Flotte ausgegeben wird, wählen Sie Neuausgleich der Kapazität und dann eine Instance-Ersetzungsstrategie aus. Wenn Sie Vor Beendigung starten auswählen, geben Sie die

Verzögerung (in Sekunden) an, bevor die Spot-Flotte die alten Instances beendet. Weitere Informationen finden Sie unter Kapazitätsausgleich.

e. (Optional) Um den Betrag zu kontrollieren, den Sie pro Stunde für alle Spot-Instances in Ihrer Flotte zahlen, wählen Sie Maximalkosten für Spot-Instances einstellen und geben dann den maximalen Gesamtbetrag ein, den Sie pro Stunde zu zahlen bereit sind. Ist der maximale Gesamtbetrag erreicht, stoppt die Spot-Flotte das Starten von Spot-Instances auch dann, wenn die Zielkapazität noch nicht erreicht ist. Weitere Informationen finden Sie unter Kontrolle der Aufwendungen.

8. Gehen Sie unter Netzwerk wie folgt vor:

   a. Wählen Sie für Netzwerk eine vorhandene VPC aus oder erstellen Sie eine neue.

      [Vorhandene VPC] Wählen Sie die VPC aus.

      [Neue VPC] Wählen Sie Create new VPC (Neue VPC erstellen aus, um zur Amazon VPC-Konsole zu gelangen. Wenn Sie fertig sind, kehren Sie zum Assistenten zurück und aktualisieren Sie die Liste.

   b. (Optional:) Lassen Sie AWS für Availability Zone die Availability Zones für Ihre Spot-Instances auswählen oder geben Sie eine oder mehrere Availability Zones an.

      Wenn Sie mehr als ein Subnetz in einer Availability Zone haben, wählen Sie das geeignete Subnetz unter Subnet (Subnetz) aus. Um Subnetze hinzuzufügen, wählen Sie Create new subnet (Neues Subnetz) aus, um die Amazon VPC-Konsole aufzurufen. Wenn Sie fertig sind, kehren Sie zum Assistenten zurück und aktualisieren Sie die Liste.

9. Für Anforderungen an Instance-Typen können Sie entweder Instance-Attribute angeben und Amazon EC2 die optimalen Instance-Typen mit diesen Attributen identifizieren lassen oder Sie können eine Liste von Instances angeben. Weitere Informationen finden Sie unter Attributbasierte Auswahl von Instance-Typen für Spot-Flotte.

   a. Wenn Sie Specify instance attributes that match your compute requirements (Instance-Attribute angeben, die Ihren Computinganforderungen entsprechen) auswählen, geben Sie Ihre Instance-Attribute wie folgt an:

      i. Geben Sie für vCPUs die gewünschte minimale und maximale Anzahl der vCPUs ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beides.

ii. Geben Sie für Arbeitsspeicher (GiB) den gewünschten Mindest- und Höchstwert ein. Um kein Limit anzugeben, wählen Sie Kein Minimum, Kein Maximum oder beide Optionen aus.

iii. (Optional) Für Zusätzliche Instance-Attribute können Sie optional ein oder mehrere Attribute angeben, um Ihre Computinganforderungen genauer auszudrücken. Jedes zusätzliche Attribut fügt Ihrer Anforderung weitere Einschränkungen hinzu. Sie können die zusätzlichen Attribute weglassen. In diesem Fall werden die Standardwerte verwendet. Eine Beschreibung der einzelnen Attribute und ihrer Standardwerte finden Sie unter get-spot-placement-scores in der Amazon-EC2-Befehlszeilenreferenz.

iv. (Optional) Um die Instance-Typen mit Ihren angegebenen Attributen anzuzeigen, erweitern Sie Vorschau der übereinstimmenden Instance-Typen. Um Instance-Typen von der Verwendung in Ihrer Anfrage auszuschließen, wählen Sie die Instances und dann Ausgewählte Instance-Typen ausschließen aus.

b. Bei der Auswahl von Instance-Typen manuell auswählen wird von der Spot-Flotte eine Standardliste von Instance-Typen angegeben. Um weitere Instance-Typen auszuwählen, wählen Sie Add instance types (Instance-Typen hinzufügen) und die Instance-Typen aus, die in Ihrer Anfrage verwendet werden sollen, und wählen Sie Auswählen aus. Um Instance-Typen zu löschen, wählen Sie die Instance-Typen und dann Löschen aus.

10. Wählen Sie unter Zuweisungsstrategie die Strategie aus, die Ihre Anforderungen erfüllt. Weitere Informationen finden Sie unter Zuweisungsstrategien für Spot-Instances.
11. Überprüfen Sie für Ihre Flottenanfrage auf einen Blick Ihre Flottenkonfiguration und nehmen Sie gegebenenfalls Änderungen vor.
12. (Optional) Um eine Kopie der Startkonfiguration für die herunterzuladen AWS CLI, wählen Sie JSON-Konfiguration.
13. Wählen Sie Launch (Starten) aus.

    Der Spot-Flotten-Anforderungstyp lautet `fleet`. Wenn die Anforderung erfüllt wird, werden Anforderungen des Typs `instance` hinzugefügt, für die der Zustand `active` und der Status `fulfilled` lautet.

Erstellen Sie eine Spot-Flotte mit dem AWS CLI

Um eine Spot-Flotte-Anfrage mit dem zu erstellen AWS CLI

- Verwenden Sie den Befehl request-spot-fleet, um eine Spot-Flotten-Anforderung zu erstellen.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Beispiel-Konfigurationsdateien finden Sie unter Beispielkonfigurationen für Spot-Flotte.

Ausgabebeispiel:

```
{
    "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE"
}
```

Markieren einer Spot-Flotte

Um die Kategorisierung und Verwaltung Ihrer Spot-Flotten-Anforderungen zu vereinfachen, können Sie sie mit benutzerdefinierten Metadaten markieren. Sie können einer Spot-Flotten-Anforderung beim Erstellen oder danach eine Markierung zuweisen. Sie können Tags (Markierungen) über die Amazon EC2-Konsole oder ein Befehlszeilen-Tool zuweisen.

Wenn Sie eine Spot-Flotten-Anforderung markieren, werden die Instances und Volumes, die von der Spot-Flotte gestartet werden, nicht automatisch markiert. Sie müssen die von der Spot-Flotte gestarteten Instances und Volumes explizit markieren. Sie können festlegen, dass Tags (Markierungen) nur der Spot-Flotten-Anforderung, nur den Instances, die von der Flotte gestartet werden, nur den Volumes, die den von der Flotte gestarteten Instances zugeordnet sind oder allen dreien zugewiesen werden.

> **Note**
>
> Volume-Tags (Markierungen) werden nur für Volumes unterstützt, die an On-Demand-Instances angefügt sind. Sie können Volumes, die an Spot-Instances angehängt sind, nicht markieren.

Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

Inhalt

- Markieren bestehender Spot-Flotten
- Anzeigen der Tags (Markierungen) für Spot-Flotten-Anforderungen

Voraussetzung

Gewähren Sie dem Benutzer die Berechtigung zum Markieren von Ressourcen. Weitere Informationen finden Sie unter Beispiel: Markieren von Ressourcen.

So gewähren Sie einem Benutzer die Berechtigung zum Markieren von Ressourcen

Erstellen Sie eine IAM-Richtlinie, die Folgendes enthält:

- Die Aktion `ec2:CreateTags`. Dadurch erhält der Benutzer die Berechtigung zum Erstellen von Tags.
- Die Aktion `ec2:RequestSpotFleet`. Dadurch wird dem Benutzer die Berechtigung zum Erstellen einer Spot-Flotten-Anfrage gewährt.
- Für `Resource` müssen Sie `"*"` angeben. Dadurch können Benutzer alle Ressourcentypen markieren.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "TagSpotFleetRequest",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags",
                "ec2:RequestSpotFleet"
            ],
            "Resource": "*"
        }
    ]
}
```

Important

Derzeit unterstützen wir keine Berechtigungen auf Ressourcenebene für die `spot-fleet-request`-Ressource. Wenn Sie `spot-fleet-request` als Ressource angeben, erhalten

Sie eine nicht autorisierte Ausnahme, wenn Sie versuchen, die Flotte zu markieren. Das folgende Beispiel veranschaulicht, wie die Richtlinie nicht festgelegt wird.

```
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:RequestSpotFleet"
    ],
    "Resource": "arn:aws:ec2:us-east-1:111122223333:spot-fleet-request/*"
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.
- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Markieren einer neuen Spot-Flotte

So markieren Sie eine neue Spot-Flotten-Anforderung mithilfe der Konsole:

1. Folgen Sie dem Verfahren unter Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole).
2. Um ein Tag (Markierung) hinzuzufügen, erweitern Sie Additional configurations (Zusätzliche Konfigurationen), wählen Sie Add new Tag (Neuen Tag (Markierung) hinzufügen), und geben

Sie den Schlüssel und den Wert für den Tag (Markierung) ein. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).

Sie können die Spot-Flotten-Anforderung und die Instances jeweils mit demselben Tag (Markierung) markieren. Um beide zu markieren, stellen Sie sicher, dass sowohl Instance Tags (Instance-Tags (Markierungen)), als auch Fleet Tags (Flotten-Tags (Markierungen)) ausgewählt sind. Um nur die Spot-Flotten-Anforderung zu markieren, deaktivieren Sie Instance Tags (Instance-Tags (Markierungen)). Um nur die von der Flotte gestarteten Instances zu markieren, löschen Sie Fleet Tags (FlottenTags (Markierungen)).

3. Füllen Sie die erforderlichen Felder aus, um eine Spot-Flotten-Anforderung zu erstellen, und wählen Sie dann Launch (Starten) aus. Weitere Informationen finden Sie unter Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole).

Um eine neue Spot-Flotte-Anfrage mit dem zu taggen AWS CLI

Um eine Spot-Flotten-Anforderung bei ihrer Erstellung zu markieren, konfigurieren Sie die Spot-Flotten-Anforderung wie folgt:

- Legen Sie die Tags für die Spot-Flotten-Anforderung in `SpotFleetRequestConfig` fest.
- Legen Sie für `ResourceType` die Option `spot-fleet-request` fest. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

Im folgenden Beispiel wird die Spot-Flotten-Anforderung mit zwei Tags (Markierungen) markiert: Key=Environment und Value=Production sowie Key=Cost-Center und Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large"
            }
```

```
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Markieren einer neuen Spot-Flotte sowie der Instances und Volumes, die sie startet

Um eine neue Spot-Flotte-Anfrage und die damit gestarteten Instances und Volumes zu taggen, verwenden Sie AWS CLI

Um eine Spot-Flotten-Anforderung beim Erstellen zu markieren, und um die Instances und Volumes zu markieren, wenn sie von der Flotte gestartet werden, konfigurieren Sie die Spot-Flotten-Anforderung wie folgt:

Tags (Markierungen) für Spot-Flotten-Anforderungen:

- Legen Sie die Tags für die Spot-Flotten-Anforderung in `SpotFleetRequestConfig` fest.
- Legen Sie für `ResourceType` die Option `spot-fleet-request` fest. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

Instance-Tags (Markierungen):

- Geben Sie die Tags für die Instances in `LaunchSpecifications` an.
- Legen Sie für `ResourceType` die Option `instance` fest. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

  Alternativ können Sie die Markierungen für die Instance in der Startvorlage angeben, auf die in der Spot-Flotten-Anforderung verwiesen wird.

Volume-Tags (Markierungen):

- Geben Sie die Markierungen für die Volumes in der Startvorlage an, auf die in der Spot-Flotten-Anforderung verwiesen wird. Die Volume-Markierung in `LaunchSpecifications` wird nicht unterstützt.

Im folgenden Beispiel wird die Spot-Flotten-Anforderung mit zwei Tags (Markierungen) markiert: Key=Environment und Value=Production sowie Key=Cost-Center und Value=123. Die Instances, die von der Flotte gestartet werden, werden mit einer Markierung markiert (diese entspricht einer der Tags (Markierungen) für die Spot-Flotten-Anforderung): Key=Cost-Center und Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
```

```
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1,
        "TagSpecifications": [
            {
                "ResourceType": "spot-fleet-request",
                "Tags": [
                    {
                        "Key": "Environment",
                        "Value":"Production"
                    },
                    {
                        "Key": "Cost-Center",
                        "Value":"123"
                    }
                ]
            }
        ]
    }
}
```

Um Instances zu taggen, die von einer Spot-Flotte gestartet wurden, mit dem AWS CLI

Um Instances zu markieren, wenn sie von der Flotte gestartet werden, können Sie entweder die Markierungen in der Startvorlage angeben, auf die in der Spot-Flotten-Anforderung verwiesen wird oder die Markierungen in der Spot-Flotten-Anforderung wie folgt angeben:

- Geben Sie die Tags für die Instances in `LaunchSpecifications` an.
- Legen Sie für `ResourceType` die Option `instance` fest. Wenn Sie einen anderen Wert angeben, schlägt die Flottenanforderung fehl.
- Geben Sie für `Tags` das Schlüssel-Wert-Paar an. Sie können mehr als ein Schlüssel-Wert-Paar angeben.

Im folgenden Beispiel werden die Instances, die von der Flotte gestartet werden, mit einem Tags (Markierungen) gekennzeichnet: Key=Cost-Center und Value=123.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchSpecifications": [
            {
                "ImageId": "ami-0123456789EXAMPLE",
                "InstanceType": "c4.large",
                "TagSpecifications": [
                    {
                        "ResourceType": "instance",
                        "Tags": [
                            {
                                "Key": "Cost-Center",
                                "Value": "123"
                            }
                        ]
                    }
                ]
            }
        ],
        "SpotPrice": "5",
        "TargetCapacity": 2,
        "TerminateInstancesWithExpiration": true,
        "Type": "maintain",
        "ReplaceUnhealthyInstances": true,
        "InstanceInterruptionBehavior": "terminate",
        "InstancePoolsToUseCount": 1
    }
}
```

So markieren Sie Volumes, die an On-Demand-Instances angefügt sind, die von einer Spot-Flotte gestartet werden, mit der AWS CLI:

Um Volumes zu markieren, wenn sie von der Flotte erstellt werden, müssen Sie die Markierungen in der Startvorlage angeben, auf die in der Spot-Flotten-Anforderung verwiesen wird.

> **Note**
>
> Volume-Tags (Markierungen) werden nur für Volumes unterstützt, die an On-Demand-Instances angefügt sind. Sie können Volumes, die an Spot-Instances angehängt sind, nicht markieren.
> Die Volume-Markierung in `LaunchSpecifications` wird nicht unterstützt.

Markieren bestehender Spot-Flotten

So markieren Sie eine vorhandene Spot-Flotten-Anforderung mithilfe der Konsole:

Nachdem Sie eine Spot-Flotten-Anforderung erstellt haben, können Sie der Flottenanforderung mithilfe der Konsole Tags (Markierungen) hinzufügen.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie die Registerkarte Tags (Markierungen), und wählen Sie Create Tags (Tags (Markierungen) erstellen).

Um eine bestehende Spot-Flotte-Anfrage mit dem zu taggen AWS CLI

Sie können den Befehl create-Tags verwenden, um vorhandene Ressourcen zu markieren. Im folgenden Beispiel wird die vorhandene Spot-Flotten-Anforderung mit Key=purpose und Value=test markiert.

```
aws ec2 create-tags \
    --resources sfr-11112222-3333-4444-5555-66666EXAMPLE \
    --tags Key=purpose,Value=test
```

Anzeigen der Tags (Markierungen) für Spot-Flotten-Anforderungen

So zeigen Sie Tags (Markierungen) für Spot-Flotten-Anforderungen mithilfe der Konsole an:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.

3. Wählen Sie Ihre Spot-Flotten-Anforderung und dann die Registerkarte Tags (Tags (Markierungen)) aus.

So beschreiben Sie Tags (Markierungen) für Spot-Flotten-Anforderungen:

Verwenden Sie den Befehl describe-tags, um die Tags (Markierungen) für die angegebene Ressource anzuzeigen. Im folgenden Beispiel beschreiben Sie die Tags (Markierungen) für die angegebene Spot-Flotten-Anforderung.

```
aws ec2 describe-tags \
    --filters "Name=resource-id,Values=sfr-11112222-3333-4444-5555-66666EXAMPLE"
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Production"
        },
        {
            "Key": "Another key",
            "ResourceId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "ResourceType": "spot-fleet-request",
            "Value": "Another value"
        }
    ]
}
```

Sie können die Tags (Markierungen) einer Spot-Flotten-Anforderung auch anzeigen, indem Sie die Spot-Flotten-Anforderung beschreiben.

Verwenden Sie den Befehl describe-spot-fleet-requests, um die Konfiguration der angegebenen Spot-Flotten-Anforderung anzuzeigen, die alle Markierungen umfasst, die für die Flottenanforderung angegeben wurden.

```
aws ec2 describe-spot-fleet-requests \
    --spot-fleet-request-ids sfr-11112222-3333-4444-5555-66666EXAMPLE
```

```
{
```

```
    "SpotFleetRequestConfigs": [
        {
            "ActivityStatus": "fulfilled",
            "CreateTime": "2020-02-13T02:49:19.709Z",
            "SpotFleetRequestConfig": {
                "AllocationStrategy": "capacityOptimized",
                "OnDemandAllocationStrategy": "lowestPrice",
                "ExcessCapacityTerminationPolicy": "Default",
                "FulfilledCapacity": 2.0,
                "OnDemandFulfilledCapacity": 0.0,
                "IamFleetRole": "arn:aws:iam::111122223333:role/aws-ec2-spot-fleet-
tagging-role",
                "LaunchSpecifications": [
                    {
                        "ImageId": "ami-0123456789EXAMPLE",
                        "InstanceType": "c4.large"
                    }
                ],
                "TargetCapacity": 2,
                "OnDemandTargetCapacity": 0,
                "Type": "maintain",
                "ReplaceUnhealthyInstances": false,
                "InstanceInterruptionBehavior": "terminate"
            },
            "SpotFleetRequestId": "sfr-11112222-3333-4444-5555-66666EXAMPLE",
            "SpotFleetRequestState": "active",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                },
                {
                    "Key": "Another key",
                    "Value": "Another value"
                }
            ]
        }
    ]
}
```

Beschreiben der Spot-Flotte

Die Spot-Flotte startet Spot-Instances, wenn der Höchstpreis den Spot-Preis übersteigt und Kapazität verfügbar ist. Die Spot-Instances werden so lange ausgeführt, bis sie entweder unterbrochen oder von Ihnen beendet werden.

Spot-Flotte beschreiben (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus. Um die Konfigurationsdetails anzuzeigen, wählen Sie Description (Beschreibung) aus.
4. Um die Spot-Instances für die Spot-Flotte aufzulisten, wählen Sie Instances aus.
5. Zum Anzeigen des Verlaufs für die Spot-Flotte wählen Sie History (Verlauf) aus.

Spot-Flotte beschreiben (AWS CLI)

Verwenden Sie den Befehl describe-spot-fleet-requests, um Ihre Spot-Flotten-Anforderungen zu beschreiben.

```
aws ec2 describe-spot-fleet-requests
```

Verwenden Sie den Befehl describe-spot-fleet-instances, um die Spot-Instances für die angegebene Spot-Flotte zu beschreiben.

```
aws ec2 describe-spot-fleet-instances \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE
```

Verwenden Sie den Befehl describe-spot-fleet-request-history, um den Verlauf für die angegebene Spot-Flotten-Anforderung zu beschreiben.

```
aws ec2 describe-spot-fleet-request-history \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --start-time 2015-05-18T00:00:00Z
```

Ändern einer Spot-Flotten-Anforderung

Sie können eine aktive Spot-Flotten-Anforderung ändern, um die folgenden Aufgaben auszuführen:

- Erhöhen der Zielkapazität und des On-Demand-Anteils
- Verringern der Zielkapazität und des On-Demand-Anteils

> **Note**
>
> Sie können eine einmalige Spot-Flotten-Anforderung nicht ändern. Sie können eine Spot-Flotten-Anforderung nur ändern, wenn Sie beim Erstellen der Spot-Flotten-Anforderung Maintain target capacity (Zielkapazität erhalten) ausgewählt hatten.

Wenn Sie die Zielkapazität erhöhen, startet die Spot-Flotte zusätzliche Spot-Instances. Wenn Sie den On-Demand-Anteil erhöhen, startet die Spot-Flotte zusätzliche On-Demand-Instances.

Wenn Sie die Zielkapazität erhöhen, startet die Spot-Flotte die zusätzlichen Spot-Instances entsprechend der Zuweisungsstrategie für ihre Spot-Flotte-Anfrage.

Wenn Sie die Zielkapazität verringern, bricht die Spot-Flotte alle offenen Anforderungen ab, die die neue Zielkapazität überschreiten. Sie können anfordern, dass die Spot-Flotte Spot-Instances beendet, bis die Größe der Flotte die neue Zielkapazität erreicht hat. Wenn die Zuweisungsstrategie `diversified` lautet, beendet die Spot-Flotte Instances in allen Pools. Alternativ können Sie anfordern, dass die Spot-Flotte ihre aktuelle Größe beibehält, dabei jedoch keine Spot-Instances ersetzt, die unterbrochen werden oder die Sie manuell beenden.

Wenn eine Spot-Flotte eine Instance aufgrund einer Verringerung der Zielkapazität beendet, erhält die Instance eine Benachrichtigung über die Unterbrechung einer Spot-Instance.

So ändern Sie eine Spot-Flotten-Anforderung (Konsole):

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie Actions (Aktionen)und dann Modify target capacity (Zielkapazität bearbeiten) aus.
5. Führen Sie unter Modify target capacity die folgenden Schritte aus:

    a. Geben Sie die neue Zielkapazität und den neuen On-Demand-Anteil ein.

b. (Optional) Wenn Sie die Zielkapazität verringern, die aktuelle Größe der Flotte jedoch beibehalten möchten, heben Sie die Auswahl von Terminate instances (Instances beenden) auf.

c. Klicken Sie auf Submit (Absenden).

Um eine Spot-Flotte-Anfrage mit dem zu ändern AWS CLI

Verwenden Sie den Befehl modify-spot-fleet-request, um die Zielkapazität der angegebenen Spot-Flotten-Anforderung zu aktualisieren.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 20
```

Sie können den vorherigen Befehl folgendermaßen ändern, um die Zielkapazität der angegebenen Spot-Flotte zu verringern, ohne dadurch Spot-Instances zu beenden.

```
aws ec2 modify-spot-fleet-request \
    --spot-fleet-request-id sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --target-capacity 10 \
    --excess-capacity-termination-policy NoTermination
```

Abbrechen einer Spot-Flotten-Anforderung

Wenn Sie eine Spot-Flotte nicht mehr benötigen, können Sie die Spot-Flotten-Anfrage stornieren. Nachdem Sie eine Flotten-Anfrage storniert haben, werden auch alle der Flotte zugeordneten Spot-Anfragen storniert, sodass keine neuen Spot-Instances gestartet werden.

Wenn Sie eine Spot-Flotte-Anfrage stornieren, müssen Sie auch angeben, ob Sie alle zugehörige Instances beenden möchten. Dazu gehören sowohl On-Demand-Instances als auch Spot-Instances.

Wenn Sie festlegen, dass die Instances beendet werden müssen, wenn die Flotten-Anfrage abgebrochen wird, wechselt die Flotten-Anfrage in den `cancelled_terminating`-Status. Andernfalls wechselt die Flotten-Anfrage in den `cancelled_running`-Status, und die Instances werden so lange ausgeführt, bis sie unterbrochen werden oder Sie sie manuell beenden.

Einschränkungen

- Sie können bis zu 100 Flotten in einer einzigen Anfrage löschen. Wenn Sie die angegebene Anzahl überschreiten, werden keine Flotten gelöscht.

So brechen Sie eine Spot-Flotten-Anforderung ab (Konsole):

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus.
4. Wählen Sie Actions (Aktionen), Cancel request (Anforderungen abbrechen).
5. Gehen Sie im Dialogfeld Spot-Anfrage stornieren wie folgt vor:

    a. Um die zugeordneten Instances gleichzeitig mit dem Stornieren der Spot-Flotten-Anfrage zu beenden, belassen Sie das Kontrollkästchen Instances beenden aktiviert. Um die Spot-Flotten-Anfrage zu storinieren, ohne die zugehörigen Instances zu beenden, deaktivieren Sie das Kontrollkästchen Instances beenden.

    b. Wählen Sie Bestätigen aus.

Um eine Spot-Flottenanfrage zu stornieren und die zugehörigen Instances zu beenden, verwenden Sie AWS CLI

Verwenden Sie den cancel-spot-fleet-requests-Befehl, um die angegebene Spot-Flotten-Anfrage abzubrechen und ihre On-Demand-Instances und Spot-Instances zu beenden.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --terminate-instances
```

Beispielausgabe

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_terminating",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

So stornieren Sie eine Spot-Flotten-Anfrage mit der AWS CLI, ohne deren Instances zu beenden

Sie können den vorherigen Befehl mit dem `--no-terminate-instances`-Parameter ändern, um die angegebene Spot-Flotten-Anfrage zu stornieren, ohne deren On-Demand-Instances und Spot-Instances zu beenden.

```
aws ec2 cancel-spot-fleet-requests \
    --spot-fleet-request-ids sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE \
    --no-terminate-instances
```

Beispielausgabe

```
{
    "SuccessfulFleetRequests": [
        {
            "SpotFleetRequestId": "sfr-73fbd2ce-aa30-494c-8788-1cee4EXAMPLE",
            "CurrentSpotFleetRequestState": "cancelled_running",
            "PreviousSpotFleetRequestState": "active"
        }
    ],
    "UnsuccessfulFleetRequests": []
}
```

CloudWatch Metriken für Spot Fleet

Amazon EC2 bietet CloudWatch Amazon-Metriken, mit denen Sie Ihre Spot-Flotte überwachen können.

> **Important**
>
> Um die Genauigkeit zu gewährleisten, empfehlen wir, beim Verwenden dieser Metriken die detaillierte Überwachung zu aktivieren. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der detaillierten Überwachung für Ihre Instances.

Weitere Informationen zu den von Amazon EC2 bereitgestellten CloudWatch Metriken finden Sie unterÜberwachen Sie Ihre Instances mit CloudWatch.

Metriken für Spot-Flotten

Der `AWS/EC2Spot` Namespace umfasst die folgenden Metriken sowie die CloudWatch Metriken für die Spot-Instances in Ihrer Flotte. Weitere Informationen finden Sie unter Instance-Metriken.

Metrik	Beschreibung
`AvailableInstancePoolsCount`	Die Spot-Kapazitätspools, die in der Spot-Flotten-Anforderung angegeben wurden. Einheiten: Anzahl
`BidsSubmittedForCapacity`	Die Kapazität, für die Amazon EC2 Spot-Flotten-Anforderungen übermittelt hat. Einheiten: Anzahl
`EligibleInstancePoolCount`	Die Spot-Kapazitätspools, die in der Spot-Flotten-Anforderung angegeben sind, bei denen Amazon EC2 Anforderungen erfüllen kann. Amazon EC2 erfüllt keine Anforderungen in Pools, in denen Ihr Höchstpreis für Spot-Instances für Spot Instances unter dem Spot-Preis liegt oder der Spot-Preis über dem Preis für On-Demand-Instances liegt. Einheiten: Anzahl
`FulfilledCapacity`	Von Amazon EC2 erfüllte Kapazität. Einheiten: Anzahl
`MaxPercentCapacityAllocation`	Der Höchstwert von `PercentCapacityAllocation` über alle Spot-Flotten-Pools hinweg, die in der Spot-Flotten-Anforderung angegeben wurden. Einheiten: Prozent
`PendingCapacity`	Differenz zwischen `TargetCapacity` und `FulfilledCapacity`. Einheiten: Anzahl

Metrik	Beschreibung
`PercentCapacityAllocation`	Dem Spot-Kapazitätspool für die angegebenen Dimensionen zugeordnete Kapazität. Der höchste registriert Wert aller Spot-Kapazitätspools kann mit `MaxPercentCapacityAllocation` ermittelt werden. Einheiten: Prozent
`TargetCapacity`	Die Zielkapazität der Spot-Flotten-Anforderung. Einheiten: Anzahl
`TerminatingCapacity`	Die Kapazität, die beendet wird, da die bereitgestellte Kapazität größer als die Zielkapazität ist. Einheiten: Anzahl

Wenn die Maßeinheit einer Metrik `Count` ist, lautet die nützlichste Statistik `Average`.

Spot-Flotten-Dimensionen

Verwenden Sie die folgenden Dimensionen, um die Daten für Ihre Spot-Flotte zu filtern.

Dimensionen	Beschreibung
`AvailabilityZone`	Filtern Sie die Daten nach Availability Zone.
`FleetRequestId`	Filtern Sie die Daten nach Spot-Flottenanfrage.
`InstanceType`	Filtern Sie die Daten nach Instance-Typ.

Sehen Sie sich die CloudWatch Metriken für Ihre Spot-Flotte an

Sie können die CloudWatch Metriken für Ihre Spot-Flotte über die CloudWatch Amazon-Konsole einsehen. Diese Metriken werden in Überwachungsdiagrammen dargestellt. Diese Grafiken zeigen Datenpunkte, wenn die Spot-Flotte aktiv ist.

Metriken werden zuerst nach dem Namespace und dann nach den verschiedenen Kombinationen von Dimensionen in jedem Namespace gruppiert. Sie können beispielsweise alle Spot-Flotten-Metriken oder Gruppen von Spot-Flotten-Metriken nach Spot-Flotten-Anforderungs-ID, Instance-Typ oder Availability Zone anzeigen.

So zeigen Sie Spot-Flotten-Metriken an:

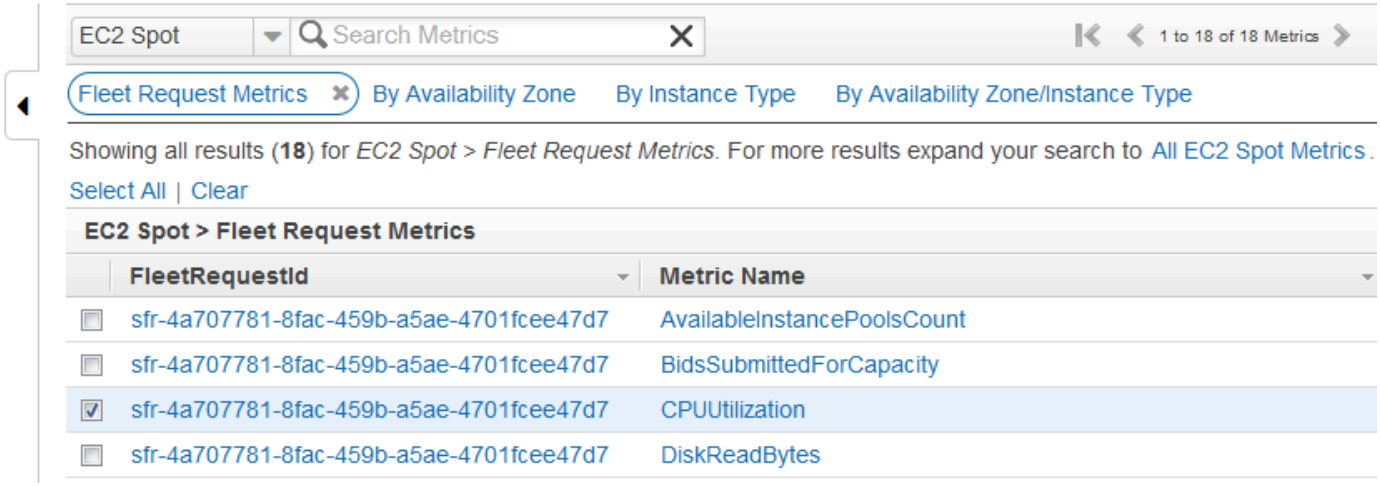
1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den EC2 Spot-Namespace aus.

   > **Note**
   >
   > Wenn der EC2 Spot-Namespace nicht angezeigt wird, gibt es dafür zwei Gründe. Entweder haben Sie Spot Fleet noch nicht verwendet — nur die AWS Dienste, die Sie verwenden, senden Messwerte an Amazon. CloudWatch Oder, falls Sie die Spot-Flotte in den letzten zwei Wochen nicht verwendet haben, wird der Namespace nicht angezeigt.

4. (Optional) Um die Metriken nach Dimensionen zu filtern, wählen Sie einen der folgenden Schritte aus:

   - Fleet Request Metrics (Flottenanforderungsmetriken) – Gruppieren nach Spot-Flotten-Anforderung
   - By Availability Zone (Nach Availability Zone) – Gruppieren nach Spot-Flotten-Anforderung und Availability Zone
   - By Instance Type (Nach Instance-Typ) – Gruppieren nach Spot-Flotten-Anforderung und Instance-Typ
   - By Availability Zone/Instance Type (Nach Availability Zone/Instance-Typ) – Gruppieren nach Spot-Flotten-Anforderung, Availability Zone und Instance-Typ

5. Um die Daten für eine Metrik anzuzeigen, aktivieren Sie das Kontrollkästchen neben der Metrik.



Automatische Skalierung für Spot-Flotten

Automatic Scaling (Automatische Skalierung) ist die Möglichkeit, die Zielkapazität Ihrer Spot-Flotte automatisch abhängig von der Nachfrage zu erhöhen oder zu verringern. Eine Spot-Flotte kann Instances als Reaktion auf eine oder mehrere Skalierungsrichtlinien innerhalb des gewählten Bereichs entweder starten (Scale out) oder beenden (Scale in).

Die Spot-Flotte unterstützt die folgenden Typen automatischer Skalierung:

- Target tracking scaling (Zielverfolgungsskalierung) – Erhöht oder verringert die aktuelle Kapazität der Flotte anhand eines Zielwerts für eine bestimmte Metrik. Dies ähnelt der Art und Weise, wie Ihr Thermostat die Temperatur in Ihrem Zuhause konstant hält – Sie wählen eine Temperatur aus und der Thermostat erledigt den Rest.
- Step scaling (Schrittweise Skalierung) – Erhöht oder verringert die aktuelle Kapazität der Flotte anhand einer Gruppe von Skalierungsanpassungen, die als Schrittanpassungen bezeichnet werden und je nach Umfang der Alarmüberschreitung variieren.
- Scheduled scaling (Geplante Skalierung) – Erhöht oder verringert die aktuellen Kapazität der Flotte anhand von Datum und Uhrzeit.

Wenn Sie Instance weighting (Instancegewichtung) verwenden, denken Sie daran, dass Spot-Flotten bei Bedarf die Zielkapazität überschreiten können. Die erfüllte Kapazität kann eine Gleitkommazahl sein, die Zielkapazität muss jedoch eine Ganzzahl sein, sodass die Spot-Flotte auf die nächste Ganzzahl aufgerundet wird. Sie müssen diese Verhalten berücksichtigen, wenn Sie sich das Ergebnis einer Skalierungsrichtlinie ansehen, wenn ein Alarm ausgelöst wird. Nehmen wir beispielsweise an, dass die Zielkapazität 30 und die erfüllte Kapazität 30,1 beträgt und die Skalierungsrichtlinie 1

abzieht. Wenn der Alarm ausgelöst wird, zieht der Auto Scaling-Prozess 1 von 30,1 ab und erhält 29,1. Dies wird auf 30 aufgerundet, sodass keine Skalierungsaktion erfolgt. Nehmen wir jetzt an, dass Sie Instance-Gewichtungen von 2, 4 und 8 sowie die Zielkapazität 10 ausgewählt haben, jedoch keine Instances mit der Gewichtung 2 verfügbar waren. Die Spot-Flotte hat so Instances mit den Gewichtungen 4 und 8 für eine erfüllte Kapazität von 12 bereitgestellt. Wenn die Skalierungsrichtlinie die Zielkapazität um 20 % verringert und ein Alarm ausgelöst wird, zieht der Auto Scaling-Prozess 12*0,2 von 12 ab und erhält 9,6. Dies wird auf 10 aufgerundet, sodass keine Skalierungsaktion erfolgt.

Die für die Spot-Flotte erstellten Skalierungsrichtlinien unterstützen eine Ruhephase. Dabei handelt es sich um die Anzahl an Sekunden, nachdem eine Skalierung abgeschlossen ist, bei der sich vorherige Skalierungen basierend auf Auslösern auf zukünftige Skalierungsereignisse auswirken können. Bei Richtlinien für die Erweiterung wird während Ruhephasen die Kapazität, die durch das vorherige Skalierungsereignis hinzugefügt wurde, welches die Ruhephase initiiert hat, als Teil der gewünschten Kapazität für die nächste Erweiterung berechnet. Der Zweck ist eine kontinuierliche (jedoch nicht exzessive) Erweiterung. Bei Richtlinien für die Verkleinerung wird die Ruhephase verwendet, um nachfolgende Anforderungen für die Erweiterung zu sperren, bis sie abgelaufen ist. Der Zweck ist eine vorsichtige Verkleinerung, um die Verfügbarkeit Ihrer Anwendung zu schützen. Wenn während der Ruhephase nach einer Erweiterung jedoch ein anderer Alarm eine Verkleinerung auslöst, skaliert das Auto Scaling Ihr skalierbares Ziel sofort.

Wir empfehlen, Instance-Metriken in einem Intervall von 1 Minute zu skalieren, da dadurch eine schnellere Reaktion auf Änderungen an der Auslastung sichergestellt wird. Werden Metriken in einem Intervall von 5 Minuten skaliert, kann dies zu einer verringerten Reaktionszeit und zu einer Skalierung von veralteten Metrikdaten führen. Um Metrikdaten für Ihre Instances innerhalb von 1 Minute CloudWatch an zu senden, müssen Sie speziell die detaillierte Überwachung aktivieren. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der detaillierten Überwachung für Ihre Instances und Erstellen einer Spot-Flotten-Anforderung mit definierten Parametern (Konsole).

Weitere Informationen zum Konfigurieren der Skalierung für eine Spot-Flotte finden Sie in den folgenden Ressourcen:

- Abschnitt application-autoscaling in der AWS CLI -Befehlsreferenz
- API-Referenz zu Application Auto Scaling
- Benutzerhandbuch zum Application Auto Scaling

IAM-Berechtigungen für automatische Skalierung von Spot-Flotten

Die automatische Skalierung für Spot Fleet wird durch eine Kombination der Amazon EC2-CloudWatch, Amazon- und Application Auto Scaling Scaling-APIs ermöglicht. Spot-Flottenanfragen werden mit Amazon EC2, Alarme mit CloudWatch und Skalierungsrichtlinien mit Application Auto Scaling erstellt.

Zusätzlich zu den IAM-Berechtigungen für Spot-Flotte und Amazon EC2 muss der Benutzer, der auf die Einstellungen für die Flottenskalierung zugreift, über die entsprechenden Berechtigungen für die Services verfügen, die dynamische Skalierung unterstützen. Benutzer müssen über die Berechtigungen verfügen, um die in der folgenden Beispielrichtlinie gezeigten Aktionen zu verwenden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "application-autoscaling:*",
                "ec2:DescribeSpotFleetRequests",
                "ec2:ModifySpotFleetRequest",
                "cloudwatch:DeleteAlarms",
                "cloudwatch:DescribeAlarmHistory",
                "cloudwatch:DescribeAlarms",
                "cloudwatch:DescribeAlarmsForMetric",
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:PutMetricAlarm",
                "cloudwatch:DisableAlarmActions",
                "cloudwatch:EnableAlarmActions",
                "iam:CreateServiceLinkedRole",
                "sns:CreateTopic",
                "sns:Subscribe",
                "sns:Get*",
                "sns:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

Sie können auch eigene IAM-Richtlinien erstellen, mit denen sich die Berechtigungen für Aufrufe der Application Auto Scaling-API präziser kontrollieren lassen. Weitere Informationen finden Sie unter Authentication and Access Control im Application Auto Scaling-Benutzerhandbuch.

Der Application Auto Scaling-Service benötigt außerdem die Erlaubnis, Ihre Spot-Flotte und CloudWatch Alarme zu beschreiben, sowie Berechtigungen, Ihre Spot-Flottenzielkapazität in Ihrem Namen zu ändern. Wenn Sie die automatische Skalierung für Ihre Spot-Flotte aktivieren, wird eine serviceverknüpfte Rolle namens `AWSServiceRoleForApplicationAutoScaling_EC2SpotFleetRequest` erstellt. Diese Service-verknüpfte Rolle gewährt Application Auto Scaling die Berechtigung zum Beschreiben der Alarme für die Richtlinien, zum Überwachen der aktuellen Kapazität der Flotte und zum Ändern der Kapazität der Flotte. Die ursprüngliche verwaltete Spot-Flotten-Rolle für Application Auto Scaling war `aws-ec2-spot-fleet-autoscale-role`, diese wird jedoch nicht mehr benötigt. Die Service-verknüpfte Rolle ist die Standardrolle für Application Auto Scaling. Weitere Informationen finden Sie unter Service-Linked Roles im Application Auto Scaling-Benutzerhandbuch.

Skalieren der Spot-Flotte anhand einer Zielverfolgungsrichtlinie

Mit Skalierungsrichtlinien für die Zielverfolgung wählen Sie eine Metrik aus und legen einen Zielwert fest. Spot Fleet erstellt und verwaltet die CloudWatch Alarme, die die Skalierungsrichtlinie auslösen, und berechnet die Skalierungsanpassung auf der Grundlage der Metrik und des Zielwerts. Durch die Skalierungsrichtlinie wird so viel Kapazität wie erforderlich hinzugefügt oder entfernt, damit die Metrik auf oder nahe an dem Zielwert gehalten wird. Abgesehen davon, dass eine Skalierungsrichtlinie für die Ziel-Nachverfolgung die Metrik nahe an dem Zielwert hält, passt sie sich auch an die Schwankungen in der Metrik aufgrund eines schwankenden Lastmusters an und verringert schnelle Schwankungen der Kapazität der Flotte.

Sie können für eine Spot-Flotte mehrere Skalierungsrichtlinien für die Zielverfolgung erstellen, sofern jede von ihnen eine andere Metrik verwendet. Die Flotte skaliert basierend auf der Richtlinie, welche die größte Kapazität in der Flotte bereitstellt. Dies ermöglicht Ihnen verschiedene Szenarien und stellt sicher, dass immer ausreichend Kapazität vorhanden ist, um Ihre Anwendungs-Workloads zu verarbeiten.

Um die Verfügbarkeit der Anwendung sicherzustellen, wird die Flotte schnellstmöglich proportional zur Metrik hochskaliert, jedoch etwas langsamer herunterskaliert.

Wenn eine Spot-Flotte eine Instance aufgrund einer Verringerung der Zielkapazität beendet, erhält die Instance eine Benachrichtigung über die Unterbrechung einer Spot-Instance.

Bearbeiten oder löschen Sie nicht die CloudWatch Alarme, die Spot Fleet für eine Skalierungsrichtlinie zur Zielverfolgung verwaltet. Die Spot-Flotte löscht die Alarme automatisch, wenn Sie die Skalierungsrichtlinie für die Zielverfolgung löschen.

Einschränkung

Die Spot-Flottenanforderung muss den Anforderungstyp `maintain` aufweisen. Die automatische Skalierung wird für Anfragen vom Typ `request` nicht unterstützt.

So konfigurieren Sie die Richtlinie für die Ziel-Nachverfolgung (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung und anschließend Auto Scaling (Automatische Skalierung) aus.
4. Wenn Auto Scaling nicht konfiguriert ist, wählen Sie Configure aus.
5. Legen Sie anhand von Scale capacity between die Mindest- und Höchstkapazität für Ihre Flotte fest. Ihre Flotte wird durch Auto Scaling nicht auf einen Wert unter der Mindest- bzw. über der Höchstkapazität skaliert.
6. Geben Sie unter Policy Name (Richtlinienname) einen Namen für diese Richtlinie ein.
7. Wählen Sie eine Target metric.
8. Geben Sie einen Target value (Zielwert) für die Metrik ein.
9. Geben Sie für die Abklingzeit einen neuen Wert (in Sekunden) ein oder behalten Sie den Standardwert bei.
10. (Optional) Aktivieren Sie Disable scale-in, um das Erstellen einer Richtlinie für die horizontale Skalierung basierend auf der aktuellen Konfiguration wegzulassen. Sie können eine Richtlinie für die horizontale Skalierung anhand einer anderen Konfiguration erstellen.
11. Wählen Sie Save aus.

Um eine Richtlinie für die Zielverfolgung mit dem zu konfigurieren AWS CLI

1. Registrieren Sie die Spot-Flotten-Anforderung mit dem Befehl register-scalable-target als skalierbares Ziel.
2. Erstellen Sie eine Skalierungsrichtlinie mit dem Befehl put-scaling-policy.

Skalieren der Spot-Flotte anhand von Richtlinien zur schrittweisen Skalierung

Bei Richtlinien zur schrittweisen Skalierung geben Sie CloudWatch Alarme an, um den Skalierungsprozess auszulösen. Wenn Sie die Zielkapazität beispielsweise erweitern möchten, wenn die CPU-Auslastung ein bestimmtes Level erreicht, erstellen Sie einen Alarm mit der von `CPUUtilization` bereitgestellten Metrik Amazon EC2.

Beim Erstellen einer Richtlinie zur schrittweisen Skalierung müssen Sie einen der folgenden Skalierungsanpassungstypen angeben:

- Add (Hinzufügen) – Erhöhen Sie die Zielkapazität der Flotte um eine angegebene Anzahl von Kapazitätseinheiten oder einen angegebenen Prozentsatz der aktuellen Kapazität.
- Remove (Entfernen) – Verringern Sie die Zielkapazität der Flotte um eine angegebene Anzahl von Kapazitätseinheiten oder einen angegebenen Prozentsatz der aktuellen Kapazität.
- Set to (Festlegen auf) – Legen Sie die Zielkapazität der Flotte auf die angegebene Anzahl an Kapazitätseinheiten fest.

Wenn ein Alarm ausgelöst wird, berechnet der Auto Scaling-Prozess die neue Zielkapazität anhand der erfüllten Kapazität und der Skalierungsrichtlinie und aktualisiert Sie Zielkapazität anschließend entsprechend. Nehmen wir beispielsweise an, dass die Zielkapazität und die erfüllte Kapazität 10 betragen und die Skalierungsrichtlinie 1 hinzufügt. Wenn der Alarm ausgelöst wird, fügt der Auto-Scaling-Prozess 1 bis 10 hinzu, um 11 zu erhalten. Die Spot-Flotte startet also 1 Instance.

Wenn eine Spot-Flotte eine Instance aufgrund einer Verringerung der Zielkapazität beendet, erhält die Instance eine Benachrichtigung über die Unterbrechung einer Spot-Instance.

Einschränkung

Die Spot-Flottenanforderung muss den Anforderungstyp `maintain` aufweisen. Auto Scaling wird für Anforderungen des Typs `request` oder Spot-Blöcke nicht unterstützt.

Voraussetzungen

- Überlegen Sie, welche CloudWatch Metriken für Ihre Anwendung wichtig sind. Sie können CloudWatch Alarme auf der Grundlage von Metriken AWS oder Ihrer eigenen benutzerdefinierten Metriken erstellen.
- Aktivieren Sie für die AWS Metriken, die Sie in Ihren Skalierungsrichtlinien verwenden werden, die Erfassung von CloudWatch Metriken, falls der Dienst, der die Metriken bereitstellt, sie nicht standardmäßig aktiviert.

Um einen CloudWatch Alarm zu erstellen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Klicken Sie im Navigationsbereich auf Alarms (Alarme).
3. Wählen Sie Create Alarm (Alarm erstellen) aus.
4. Wählen Sie auf der Seite Specify metric and conditions (Metrik und Bedingungen angeben) die Option Select metric (Metrik auswählen) aus:
5. Wählen Sie EC2 Spot, Fleet Request Metrics, wählen Sie eine Metrik aus (z. B. TargetCapacity) und wählen Sie dann Metrik auswählen aus.

   Die Seite Specify metric and conditions (Metrik und Bedingungen festlegen) mit einem Diagramm und weiteren Informationen über die von Ihnen ausgewählte Metrik werden anzeigt.
6. Wählen Sie unter Period (Zeitraum) den Auswertungszeitraum für den Alarm aus, z. B. 1 Minute. Beim Auswerten des Alarms wird jeder Zeitraum in einem Datenpunkt zusammengefasst.

   > **Note**
   >
   > Ein kürzerer Zeitraum erzeugt eine höhere Alarmempfindlichkeit.

7. Legen Sie unter Conditions (Bedingungen) den Schwellenwert des Alarms fest. Sie können beispielsweise einen Schwellenwert angeben, damit der Alarm jedes Mal ausgelöst wird, wenn der Wert für die Metrik bei 80 Prozent oder höher liegt.
8. Geben Sie unter Additional configuration (Zusätzliche Konfiguration) für Datapoints to alarm (Datenpunkte bis zum Alarm) an, wie viele Datenpunkte (Auswertungszeiträume) sich im Alarmzustand befinden müssen, damit der Alarm ausgelöst wird, z. B. 1 Bewertungszeitraum oder 2 von 3 Bewertungszeiträumen. Dies erzeugt einen Alarm, der in den ALARM-Zustand übergeht, wenn viele aufeinander folgende Zeiträume überschritten werden. Weitere Informationen finden Sie unter Auswertung eines Alarms im CloudWatch Amazon-Benutzerhandbuch.
9. Wählen Sie für Missing data treatment (Behandlung fehlender Daten) eine der Optionen aus (oder belassen Sie es bei der Standardoption Treat missing data as missing (Fehlende Daten als fehlend behandeln)). Weitere Informationen finden Sie unter Konfiguration der Behandlung fehlender Daten durch CloudWatch Alarme im CloudWatch Amazon-Benutzerhandbuch.
10. Wählen Sie Next.
11. (Optional) Um eine Benachrichtigung zu einem Skalierungsereignis zu empfangen, können Sie für Notification (Benachrichtigung) das Amazon SNS-Thema auswählen oder erstellen, das

zum Empfangen der Benachrichtigungen verwendet werden soll. Andernfalls können Sie die Benachrichtigung jetzt löschen und bei Bedarf später eine hinzufügen.

12. Wählen Sie Next.
13. Geben Sie unter Add a description (Hinzufügen einer Beschreibung) einen Namen und eine Beschreibung für den Alarm ein und klicken Sie auf Next (Weiter).
14. Wählen Sie Create Alarm (Alarm erstellen) aus.

So konfigurieren Sie die Richtlinie für schrittweise Skalierung für Ihre Spot-Flotte (Konsole):

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung und anschließend Auto Scaling (Automatische Skalierung) aus.
4. Wenn Auto Scaling nicht konfiguriert ist, wählen Sie Configure aus.
5. Legen Sie anhand von Scale capacity between die Mindest- und Höchstkapazität für Ihre Flotte fest. Die Skalierungsrichtlinien lassen Ihre Flotte nicht unter die Mindestkapazität oder über die maximale Kapazität hinaus skalieren.
6. Wählen Sie für Skalierungsrichtlinien, Richtlinientyp, Stufenskalierungsrichtlinie.
7. Zunächst enthalten Skalierungsrichtlinien Richtlinien namens ScaleUp und ScaleDown. Sie können diese Richtlinien abschließen oder sie mit Remove policy entfernen. Sie können außerdem Add policy (Richtlinie hinzufügen) auswählen.
8. Gehen Sie wie folgt vor, um eine Richtlinie zu definieren:

    a. Geben Sie unter Policy Name (Richtlinienname) einen Namen für diese Richtlinie ein.

    b. Wählen Sie für den Richtlinienauslöser einen vorhandenen Alarm aus oder wählen Sie Alarm erstellen, um die CloudWatch Amazon-Konsole zu öffnen und einen Alarm zu erstellen.

    c. Definieren Sie für Kapazität ändernden Betrag, um den skaliert werden soll, sowie die untere und obere Grenze der Schrittanpassung. Sie können eine bestimmte Anzahl von Instances oder einen Prozentsatz der bestehenden Flottengröße hinzufügen oder entfernen oder die Flotte auf eine exakte Größe festlegen.

    Um beispielsweise eine Richtlinie zur schrittweisen Skalierung zu erstellen, die die Kapazität der Flotte um 30 Prozent erhöht, wählen SieAdd, geben Sie `30` in das nächste Feld ein, und wählen Sie dann`percent`. Standardmäßig ist die untere Grenze für eine Hinzufügerichtlinie

die Alarmschwelle und die obere Grenze ist positiv (+) unendlich. Standardmäßig ist die obere Grenze für eine Entfernerichtlinie die Alarmschwelle und die untere Grenze ist negativ (-) unendlich.

d. (Optional) Um einen weiteren Schritt hinzuzufügen, wählen Sie Schritt hinzufügen.

e. Geben Sie für die Abklingzeit einen neuen Wert (in Sekunden) ein oder behalten Sie den Standardwert bei.

9. Wählen Sie Speichern.

Um Richtlinien für die schrittweise Skalierung für Ihre Spot-Flotte zu konfigurieren, verwenden Sie AWS CLI

1. Registrieren Sie die Spot-Flotten-Anforderung mit dem Befehl register-scalable-target als skalierbares Ziel.
2. Erstellen Sie eine Skalierungsrichtlinie mit dem Befehl put-scaling-policy.
3. Erstellen Sie mit dem Befehl put-metric-alarm einen Alarm, der die Skalierungsrichtlinie auslöst.

Skalieren der Spot-Flotte mit geplanter Skalierung

Eine Skalierung anhand eines Zeitplans ermöglicht es Ihnen, Ihre Anwendung entsprechend vorhersagbarer Anforderungsänderungen zu skalieren. Um die geplante Skalierung zu verwenden, erstellen Sie geplante Aktionen, die die Spot-Flotte anweisen, zu bestimmten Zeitpunkten Skalierungen durchzuführen. Wenn Sie eine geplante Aktion erstellen, geben Sie eine vorhandene Spot-Flotte und die minimale und maximale Kapazität an sowie, wann die Skalierung durchgeführt werden soll. Sie können geplante Aktionen erstellen, die nur einmal skalieren oder wiederholt geplant ausgeführt werden.

Sie können nur eine geplante Aktion für Spot-Flotten erstellen, die bereits vorhanden ist. Sie können eine geplante Aktion und eine Spot-Flotte nicht gleichzeitig erstellen.

Einschränkung

Die Spot-Flottenanforderung muss den Anforderungstyp `maintain` aufweisen. Auto Scaling wird für Anforderungen des Typs `request` oder Spot-Blöcke nicht unterstützt.

Erstellen Sie eine einmalige geplante Aktion wie folgt:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus und wählen Sie dann die Registerkarte Scheduled Scaling (Geplante Skalierung) im unteren Bildschirmbereich.
4. Klicken Sie auf Create Scheduled Action (Geplante Aktion erstellen).
5. Geben Sie unter Name einen neuen Namen für die geplante Aktion ein.
6. Geben Sie einen Wert für Minimum capacity (Minimale Kapazität), Maximum capacity (Maximale Kapazität) oder beides ein.
7. Wählen Sie für Recurrence (Wiederholung) Once (Einmal) aus.
8. (Optional) Wählen Sie ein Datum und eine Uhrzeit für Start time (Startzeit), End time (Endzeit) oder beides.
9. Klicken Sie auf Submit (Absenden).

Skalierung im Rahmen eines sich wiederholenden Zeitplans

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus und wählen Sie dann die Registerkarte Scheduled Scaling (Geplante Skalierung) im unteren Bildschirmbereich.
4. Wählen Sie für Recurrence (Wiederholung) einen der vordefinierten Zeitpläne (z. B. Every day (Jeden Tag)) oder wählen Sie Custom (Benutzerdefiniert) und geben Sie einen Cron-Ausdruck ein. Weitere Informationen zu den Cron-Ausdrücken, die von der geplanten Skalierung unterstützt werden, finden Sie unter Cron-Ausdrücke im Amazon CloudWatch Events-Benutzerhandbuch.
5. (Optional) Wählen Sie ein Datum und eine Uhrzeit für Start time (Startzeit), End time (Endzeit) oder beides.
6. Klicken Sie auf Submit (Absenden).

So bearbeiten Sie eine geplante Aktion

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus und wählen Sie dann die Registerkarte Scheduled Scaling (Geplante Skalierung) im unteren Bildschirmbereich.

4. Wählen Sie die geplante Aktion dann Actions (Aktionen) und anschließend Edit (Bearbeiten) aus.
5. Nehmen Sie die notwendigen Änderungen vor und klicken Sie auf Submit (Senden).

So löschen Sie eine geplante Aktion

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Spot Requests aus.
3. Wählen Sie Ihre Spot-Flotten-Anforderung aus und wählen Sie dann die Registerkarte Scheduled Scaling (Geplante Skalierung) im unteren Bildschirmbereich.
4. Wählen Sie die geplante Aktion dann Actions (Aktionen) und anschließend Delete (Löschen) aus.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Um die geplante Skalierung mit dem zu verwalten AWS CLI

Verwenden Sie die folgenden Befehle:

- put-scheduled-action
- describe-scheduled-actions
- delete-scheduled-action

Überwachen Sie Flottenereignisse mit Amazon EventBridge

Wenn sich der Zustand einer EC2-Flotte oder einer Spot-Flotte ändert, gibt die Flotte eine Benachrichtigung aus. Die Benachrichtigung wird als Ereignis zur Verfügung gestellt, das an Amazon gesendet wird EventBridge (früher bekannt als Amazon CloudWatch Events). Ereignisse werden auf bestmögliche Weise ausgegeben.

Mit Amazon EventBridge können Sie Regeln erstellen, die als Reaktion auf ein Ereignis programmatische Aktionen auslösen. Sie können beispielsweise zwei EventBridge Regeln erstellen: eine, die ausgelöst wird, wenn sich der Status einer Flotte ändert, und eine, die ausgelöst wird, wenn eine Instance in der Flotte beendet wird. Sie können die erste Regel so konfigurieren, dass bei einer Änderung des Flottenstatus die Regel ein SNS-Thema aufruft, um Ihnen eine E-Mail-Benachrichtigung zu senden. Sie können die zweite Regel so konfigurieren, dass beim Beenden einer Instance die Regel eine Lambda-Funktion aufruft, um eine neue Instance zu starten.

Themen

- EC2-Flotte-Ereignistypen
- Ereignistypen für Spot-Flotten
- EventBridge Amazon-Regeln erstellen

EC2-Flotte-Ereignistypen

> **Note**
>
> Nur Flotten vom Typ `maintain` und `request` emittieren Ereignisse. Flotten des Typs `instant` geben keine Ereignisse aus, da sie synchrone einmalige Anfragen senden und der Zustand der Flotte in der Antwort sofort bekannt ist.

Es gibt fünf EC2-Flotte-Ereignistypen. Für jeden Ereignistyp gibt es mehrere Sub-Typen.

Die Ereignisse werden EventBridge im JSON-Format gesendet. Die folgenden Felder des Ereignisses bilden das in der Regel definierte Ereignismuster, das eine Aktion auslöst:

`"source": "aws.ec2fleet"`

Gibt an, dass das Ereignis aus EC2-Flotte stammt.

`"detail-type": "EC2 Fleet State Change"`

Identifiziert den Ereignistyp.

`"detail": { "sub-type": "submitted" }`

Identifiziert den Ereignis-Sub-Typ.

Ereignistypen

- Verändern des EC2-Flottenzustand
- Ändern der Anforderung der EC2-Flotte-Spot-Instance
- Ändern der EC2-Flotten-Instance
- Informationen zur EC2-Flotte
- EC2-Flotten-Fehler

Verändern des EC2-Flottenzustand

EC2 Fleet sendet ein `EC2 Fleet State Change` Ereignis an Amazon, EventBridge wenn sich der Status einer EC2-Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "715ed6b3-b8fc-27fe-fad6-528c7b8bf8a2",
    "detail-type": "EC2 Fleet State Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:20Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "sub-type": "active"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`active`

Die EC2-Flotte-Anfrage wurde validiert und Amazon EC2 versucht, die Zielanzahl der laufenden Instances beizubehalten.

`deleted`

Die EC2-Flotte-Anforderung wird gelöscht und hat keine laufenden Instances. Die EC2-Flotte wird zwei Tage nach Beendigung der zugehörigen Instances gelöscht.

`deleted_running`

Die EC2-Flotte-Anforderung wird gelöscht und startet keine weiteren Instances. Die bestehenden Instances laufen weiter, bis sie unterbrochen oder beendet werden. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances unterbrochen oder beendet wurden.

`deleted_terminating`

Die EC2-Flotte-Anforderung wird gelöscht und die zugehörigen Instances werden beendet. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances beendet wurden.

`expired`

Die EC2-Flotte-Anforderung ist abgelaufen. Wenn die Anforderung mit `TerminateInstancesWithExpiration` erstellt wurde, zeigt ein nachfolgendes `terminated`-Ereignis an, dass die Instances beendet werden.

`modify_in_progress`

Die EC2-Flotte-Anforderung wird geändert. Die Anforderung bleibt in diesem Zustand, bis die Änderung vollständig verarbeitet wurde.

`modify_succeeded`

Die EC2-Flotte-Anforderung wurde geändert.

`submitted`

Die EC2-Flotte-Anforderung wird evaluiert und Amazon EC2 bereitet den Start der Zielanzahl von Instances vor.

`progress`

Die EC2-Flotte-Anfrage wird gerade erfüllt.

Ändern der Anforderung der EC2-Flotte-Spot-Instance

EC2 Fleet sendet ein `EC2 Fleet Spot Instance Request Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Spot-Instance-Anfrage in der Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "19331f74-bf4b-a3dd-0f1b-ddb1422032b9",
    "detail-type": "EC2 Fleet Spot Instance Request Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-11-09T09:00:05Z",
    "region": "us-east-1",
```

```
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/
fleet-83fd4e48-552a-40ef-9532-82a3acca5f10"
    ],
    "detail": {
        "spot-instance-request-id": "sir-rmqske6h",
        "description": "SpotInstanceRequestId sir-rmqske6h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`active`

Die Spot-Instance-Anforderung wurde erfüllt und ist mit einer Spot-Instance verknüpft.

`cancelled`

Sie haben die Spot-Instance-Anforderung storniert oder die Spot-Instance-Anforderung ist abgelaufen.

`disabled`

Sie haben die Spot-Instance angehalten.

`submitted`

Die Spot-Instance-Anforderung wird gesendet.

Ändern der EC2-Flotten-Instance

EC2 Fleet sendet ein `EC2 Fleet Instance Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Instance in der Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "542ce428-c8f1-0608-c015-e8ed6522c5bc",
    "detail-type": "EC2 Fleet Instance Change",
    "source": "aws.ec2fleet",
    "account": "123456789012",
```

```
    "time": "2020-11-09T09:00:23Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-598fb973-87b7-422d-
be4d-6b0809bfff0a"
    ],
    "detail": {
        "instance-id": "i-0c594155dd5ff1829",
        "description": "{\"instanceType\":\"c5.large\",\"image\":\"ami-6057e21a\",
\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":\"us-east-1d\"}",
        "sub-type": "launched"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`launched`

Eine neue Instance wurde gestartet.

`terminated`

Die Instance wurde beendet.

`termination_notified`

Eine Benachrichtigung über die Instance-Beendigung wurde gesendet, als eine Spot-Instance während der Herunterskalierung durch Amazon EC2 beendet wurde. Hierbei wurde die Zielkapazität der Flotte verkleinert, beispielsweise vom Kapazitätswert 4 auf 3.

Informationen zur EC2-Flotte

EC2 Fleet sendet ein `EC2 Fleet Information` Ereignis an Amazon EventBridge , wenn beim Versand ein Fehler auftritt. Das Informationsereignis hindert die Flotte nicht daran, ihre Zielkapazität zu erreichen.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "76529817-d605-4571-7224-d36cc1b2c0c4",
    "detail-type": "EC2 Fleet Information",
    "source": "aws.ec2fleet",
```

```
    "account": "123456789012",
    "time": "2020-11-09T08:17:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-8becf5fe-
bb9e-415d-8f54-3fa5a8628b91"
    ],
    "detail": {
        "description": "c4.xlarge, ami-0947d2ba12ee1ff75, Linux/UNIX, us-east-1a,
 Spot price in either SpotFleetRequestConfigData or SpotFleetLaunchSpecification or
 LaunchTemplate or LaunchTemplateOverrides is less than Spot market price $0.0619",
        "sub-type": "launchSpecUnusable"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`fleetProgressHalted`

Keiner der Preise in den Startspezifikationen ist gültig, da er unter dem Spot-Preis liegt (alle Startspezifikationen haben `launchSpecUnusable`-Ereignisse ausgelöst). Eine Startspezifikation könnte gültig werden, wenn sich der Spot-Preis ändert.

`launchSpecTemporarilyBlacklisted`

Die Konfiguration ist nicht gültig und mehrere Versuche, Instances zu starten, sind fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

`launchSpecUnusable`

Der Preis in einer Startspezifikation ist nicht gültig, da er unter dem Spot-Preis liegt.

`registerWithLoadBalancersFailed`

Der Versuch, Instances bei Load Balancern zu registrieren, ist fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

EC2-Flotten-Fehler

EC2 Fleet sendet ein `EC2 Fleet Error` Ereignis an Amazon EventBridge , wenn beim Versand ein Fehler auftritt. Das Fehlerereignis verhindert, dass die Flotte versucht, ihre Zielkapazität zu erfüllen.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "69849a22-6d0f-d4ce-602b-b47c1c98240e",
    "detail-type": "EC2 Fleet Error",
    "source": "aws.ec2fleet",
    "account": "123456789012",
    "time": "2020-10-07T01:44:24Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:fleet/fleet-9bb19bc6-60d3-4fd2-ae47-
d33e68eafa08"
    ],
    "detail": {
        "description": "m3.large, ami-00068cd7555f543d5, Linux/UNIX: IPv6 is not
 supported for the instance type 'm3.large'. ",
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`iamFleetRoleInvalid`

Die EC2-Flotte verfügt nicht über die erforderlichen Berechtigungen zum Starten oder Beenden einer Instance.

`allLaunchSpecsTemporarilyBlacklisted`

Keine der Konfigurationen ist gültig, und mehrere Versuche, Instances zu starten, sind fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

`spotInstanceCountLimitExceeded`

Sie haben das Limit für die Anzahl der Spot-Instances erreicht, die Sie starten können.

`spotFleetRequestConfigurationInvalid`

Die Konfiguration ist nicht gültig. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

Ereignistypen für Spot-Flotten

Es gibt fünf Spot-Flotten-Ereignistypen. Für jeden Ereignistyp gibt es mehrere Sub-Typen.

Die Ereignisse werden EventBridge im JSON-Format an gesendet. Die folgenden Felder des Ereignisses bilden das in der Regel definierte Ereignismuster, das eine Aktion auslöst:

`"source": "aws.ec2spotfleet"`

Gibt an, dass das Ereignis aus der Spot-Flotte stammt.

`"detail-type": "EC2 Spot Fleet State Change"`

Identifiziert den Ereignistyp.

`"detail": { "sub-type": "submitted" }`

Identifiziert den Ereignis-Sub-Typ.

Ereignistypen

- Verändern des EC2-Spot-Flottenzustands
- Ändern der Anforderung der EC2-Spot-Flotten-Spot-Instance
- Ändern der EC2-Spot-Flotten-Instance
- Informationen zur EC2-Spot-Flotte
- EC2-Spot-Flottenfehler

Verändern des EC2-Spot-Flottenzustands

Spot-Flotte sendet ein `EC2 Spot Fleet State Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Spot-Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "d1af1091-6cc3-2e24-203a-3b870e455d5b",
    "detail-type": "EC2 Spot Fleet State Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:57:06Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-4b6d274d-0cea-4b2c-
b3be-9dc627ad1f55"
    ],
```

```
    "detail": {
        "sub-type": "submitted"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`active`

Die Spot-Flotten-Anforderung wurde validiert und Amazon EC2 versucht, die gewünschte Anzahl von ausgeführten Instances beizubehalten.

`cancelled`

Die Spot-Flotten-Anforderung wird storniert und hat keine ausgeführten Instances. Die Spot-Flotte wird zwei Tage nach Beendigung der zugehörigen Instances gelöscht.

`cancelled_running`

Die Spot-Flotten-Anforderung wird storniert und startet keine weiteren Instances. Die bestehenden Instances laufen weiter, bis sie unterbrochen oder beendet werden. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances unterbrochen oder beendet wurden.

`cancelled_terminating`

Die Spot-Flotten-Anforderung wird storniert und die zugehörigen Instances werden beendet. Die Anforderung bleibt so lange in diesem Zustand, bis alle Instances beendet wurden.

`expired`

Die Spot-Flotten-Anforderung ist abgelaufen. Wenn die Anforderung mit `TerminateInstancesWithExpiration` erstellt wurde, zeigt ein nachfolgendes `terminated`-Ereignis an, dass die Instances beendet werden.

`modify_in_progress`

Die Spot-Flotten-Anforderung wird geändert. Die Anforderung bleibt in diesem Zustand, bis die Änderung vollständig verarbeitet wurde.

`modify_succeeded`

Die Spot-Flotten-Anforderung wurde geändert.

`submitted`

Die Spot-Flotten-Anforderung wird evaluiert und Amazon EC2 bereitet den Start der gewünschten Anzahl an Instances vor.

`progress`

Die Spot-Flotten-Anforderung wird gerade erfüllt.

Ändern der Anforderung der EC2-Spot-Flotten-Spot-Instance

Spot Fleet sendet ein `EC2 Spot Fleet Spot Instance Request Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Spot-Instance-Anfrage in der Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "cd141ef0-14af-d670-a71d-fe46e9971bd2",
    "detail-type": "EC2 Spot Fleet Spot Instance Request Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T08:53:21Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-
a98d2133-941a-47dc-8b03-0f94c6852ad1"
    ],
    "detail": {
        "spot-instance-request-id": "sir-a2w9gc5h",
        "description": "SpotInstanceRequestId sir-a2w9gc5h, PreviousState:
 cancelled_running",
        "sub-type": "cancelled"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`active`

Die Spot-Instance-Anforderung wurde erfüllt und ist mit einer Spot-Instance verknüpft.

`cancelled`

Sie haben die Spot-Instance-Anforderung storniert oder die Spot-Instance-Anforderung ist abgelaufen.

`disabled`

Sie haben die Spot-Instance angehalten.

`submitted`

Die Spot-Instance-Anforderung wird gesendet.

Ändern der EC2-Spot-Flotten-Instance

Spot Fleet sendet ein `EC2 Spot Fleet Instance Change` Ereignis an Amazon, EventBridge wenn sich der Status einer Instance in der Flotte ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "11591686-5bd7-bbaa-eb40-d46529c2710f",
    "detail-type": "EC2 Spot Fleet Instance Change",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T07:25:02Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-c8a764a4-bedc-4b62-
af9c-0095e6e3ba61"
    ],
    "detail": {
        "instance-id": "i-08b90df1e09c30c9b",
        "description": "{\"instanceType\":\"r4.2xlarge\",\"image\":
\"ami-032930428bf1abbff\",\"productDescription\":\"Linux/UNIX\",\"availabilityZone\":
\"us-east-1a\"}",
        "sub-type": "launched"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`launched`

Eine neue Instance wurde gestartet.

`terminated`

Die Instance wurde beendet.

`termination_notified`

Eine Benachrichtigung über die Instance-Beendigung wurde gesendet, als eine Spot-Instance während der Herunterskalierung durch Amazon EC2 beendet wurde. Hierbei wurde die Zielkapazität der Flotte verkleinert, beispielsweise vom Kapazitätswert 4 auf 3.

Informationen zur EC2-Spot-Flotte

Spot Fleet sendet ein `EC2 Spot Fleet Information` Ereignis an Amazon EventBridge , wenn beim Versand ein Fehler auftritt. Das Informationsereignis hindert die Flotte nicht daran, ihre Zielkapazität zu erreichen.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "73a60f70-3409-a66c-635c-7f66c5f5b669",
    "detail-type": "EC2 Spot Fleet Information",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-08T20:56:12Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/sfr-2531ea06-
af18-4647-8757-7d69c94971b1"
    ],
    "detail": {
        "description": "r3.8xlarge, ami-032930428bf1abbff, Linux/UNIX, us-east-1a, Spot
 bid price is less than Spot market price $0.5291",
        "sub-type": "launchSpecUnusable"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`fleetProgressHalted`

Keiner der Preise in den Startspezifikationen ist gültig, da er unter dem Spot-Preis liegt (alle Startspezifikationen haben `launchSpecUnusable`-Ereignisse ausgelöst). Eine Startspezifikation könnte gültig werden, wenn sich der Spot-Preis ändert.

`launchSpecTemporarilyBlacklisted`

Die Konfiguration ist nicht gültig und mehrere Versuche, Instances zu starten, sind fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

`launchSpecUnusable`

Der Preis in einer Startspezifikation ist nicht gültig, da er unter dem Spot-Preis liegt.

`registerWithLoadBalancersFailed`

Der Versuch, Instances bei Load Balancern zu registrieren, ist fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

EC2-Spot-Flottenfehler

Spot Fleet sendet ein `EC2 Spot Fleet Error` Ereignis an Amazon EventBridge , wenn beim Versand ein Fehler auftritt. Das Fehlerereignis verhindert, dass die Flotte versucht, ihre Zielkapazität zu erfüllen.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis.

```
{
    "version": "0",
    "id": "10adc4e7-675c-643e-125c-5bfa1b1ba5d2",
    "detail-type": "EC2 Spot Fleet Error",
    "source": "aws.ec2spotfleet",
    "account": "123456789012",
    "time": "2020-11-09T06:56:07Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ec2:us-east-1:123456789012:spot-fleet-request/
sfr-38725d30-25f1-4f30-83ce-2907c56dba17"
    ],
    "detail": {
        "description": "r4.2xlarge, ami-032930428bf1abbff, Linux/UNIX: The
 associatePublicIPAddress parameter can only be specified for the network interface
 with DeviceIndex 0. ",
```

```
        "sub-type": "spotFleetRequestConfigurationInvalid"
    }
}
```

Die möglichen Werte für `sub-type` sind:

`iamFleetRoleInvalid`

Die Spot-Flotte verfügt nicht über die erforderlichen Berechtigungen zum Starten oder Beenden einer Instance.

`allLaunchSpecsTemporarilyBlacklisted`

Keine der Konfigurationen ist gültig, und mehrere Versuche, Instances zu starten, sind fehlgeschlagen. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

`spotInstanceCountLimitExceeded`

Sie haben das Limit für die Anzahl der Spot-Instances erreicht, die Sie starten können.

`spotFleetRequestConfigurationInvalid`

Die Konfiguration ist nicht gültig. Weitere Informationen finden Sie in der Beschreibung des Ereignisses.

EventBridge Amazon-Regeln erstellen

Wenn eine Benachrichtigung über eine Statusänderung für eine EC2-Flotte oder Spot-Flotte ausgegeben wird, wird das Ereignis für die Benachrichtigung an Amazon EventBridge gesendet. Wenn ein Ereignismuster EventBridge erkannt wird, das einem in einer Regel definierten Muster entspricht, EventBridge ruft es ein oder mehrere Ziele auf, die in der Regel angegeben sind.

Sie können eine EventBridge Regel schreiben und automatisieren, welche Aktionen ausgeführt werden, wenn das Ereignismuster der Regel entspricht.

Themen

- Erstellen Sie EventBridge Amazon-Regeln zur Überwachung von EC2-Flottenereignissen
- Erstellen Sie EventBridge Amazon-Regeln zur Überwachung von Spot-Flottenereignissen

Erstellen Sie EventBridge Amazon-Regeln zur Überwachung von EC2-Flottenereignissen

Wenn eine Benachrichtigung über eine Statusänderung für eine EC2-Flotte ausgegeben wird, wird das Ereignis für die Benachrichtigung EventBridge in Form einer JSON-Datei an Amazon gesendet. Sie können eine EventBridge Regel schreiben, um zu automatisieren, welche Aktionen ergriffen werden, wenn ein Ereignismuster mit der Regel übereinstimmt. Wenn ein Ereignismuster EventBridge erkannt wird, das einem in einer Regel definierten Muster entspricht, EventBridge ruft es das in der Regel angegebene Ziel (oder die Ziele) auf.

Die folgenden Felder bilden das in der Regel definierte Ereignismuster:

`"source": "aws.ec2fleet"`

Gibt an, dass das Ereignis aus EC2-Flotte stammt.

`"detail-type": "EC2 Fleet State Change"`

Identifiziert den Ereignistyp.

`"detail": { "sub-type": "submitted" }`

Identifiziert den Ereignis-Sub-Typ.

Eine Liste der EC2-Flotten-Ereignisse und Beispielereignisdaten finden Sie unter the section called “EC2-Flotte-Ereignistypen”.

Beispiele

- Erstellen Sie eine EventBridge Regel, um eine Benachrichtigung zu senden
- Erstellen Sie eine EventBridge Regel zum Auslösen einer Lambda-Funktion

Erstellen Sie eine EventBridge Regel, um eine Benachrichtigung zu senden

Im folgenden Beispiel wird eine EventBridge Regel erstellt, die jedes Mal, wenn Amazon EC2 eine Benachrichtigung über eine Änderung des EC2-Flottenstatus ausgibt, eine E-Mail, eine Textnachricht oder eine mobile Push-Benachrichtigung sendet. Das Signal in diesem Beispiel wird als `EC2 Fleet State Change`-Ereignis ausgegeben, das die durch die Regel definierte Aktion auslöst.

Bevor Sie die EventBridge Regel erstellen, müssen Sie das Amazon SNS SNS-Thema für die E-Mail, Textnachricht oder mobile Push-Benachrichtigung erstellen.

Um eine EventBridge Regel zum Senden einer Benachrichtigung zu erstellen, wenn sich der Status einer EC2-Flotte ändert

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:

   a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

      Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.

   b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird dieses stets an den standardmäßigen Event Bus Ihres Kontos weitergeleitet.

   c. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.

   d. Wählen Sie Weiter aus.
4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:

   a. Wählen Sie als Quelle für Ereignisse die Option AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.

   b. Bei Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, um mit dem `EC2 Fleet Instance Change`-Ereignis übereinzustimmen.

      ```
      {
       "source": ["aws.ec2fleet"],
       "detail-type": ["EC2 Fleet Instance Change"]
      }
      ```

      Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

      i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

C. Wählen Sie für AWS Service name (Servicename) EC2 Fleet (EC2-Flotte) aus.

D. Wählen Sie für Event type (Ereignistyp) EC2 Fleet Instance Change (Änderung der EC2-Flotten-Instance) aus.

E. Um die Vorlage anzupassen, wählen Sie Edit pattern (Muster bearbeiten) und nehmen Sie Ihre Änderungen vor, damit sie dem Beispiel-Ereignismuster entsprechen.

ii. (Alternativ) So geben Sie ein benutzerdefiniertes Ereignismuster an:

A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.

b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.

c. Wählen Sie für Topic (Thema) ein vorhandenes Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).

e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.

7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.

b. Wählen Sie Regel erstellen aus.

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

Erstellen Sie eine EventBridge Regel zum Auslösen einer Lambda-Funktion

Im folgenden Beispiel wird eine EventBridge Regel erstellt, die jedes Mal eine Lambda-Funktion auslöst, wenn Amazon EC2 beim Start einer Instance eine EC2 Fleet-Instance-Änderungsbenachrichtigung ausgibt. Das Signal in diesem Beispiel wird als `EC2 Fleet Instance Change`-Ereignis, Sub-Typ `launched`, ausgegeben, das die durch die Regel definierte Aktion auslöst.

Bevor Sie die EventBridge Regel erstellen, müssen Sie die Lambda-Funktion erstellen.

Um die Lambda-Funktion zu erstellen, die in der EventBridge Regel verwendet werden soll

1. Öffnen Sie die AWS Lambda Konsole unter https://console.aws.amazon.com/lambda/.
2. Wählen Sie Create function (Funktion erstellen).
3. Geben Sie einen Namen für Ihre Funktion ein, konfigurieren Sie den Code und wählen Sie dann Create function (Funktion erstellen).

   Weitere Informationen zur Verwendung von Lambda finden Sie unter Erstellen einer Lambda-Funktion mit der Konsole im Entwicklerhandbuch für AWS Lambda .

Um eine EventBridge Regel zum Auslösen einer Lambda-Funktion zu erstellen, wenn sich der Status einer Instance in einer EC2-Flotte ändert

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:

   a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

      Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.

b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird dieses stets an den standardmäßigen Event Bus Ihres Kontos weitergeleitet.

c. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.

d. Wählen Sie Weiter aus.

4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:

a. Wählen Sie als Quelle für Ereignisse die Option AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.

b. Für Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, das dem `EC2 Fleet Instance Change`-Ereignis und `launched`-Subtyp übereinstimmt.

```
{
 "source": ["aws.ec2fleet"],
 "detail-type": ["EC2 Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

C. Wählen Sie für AWS Service name (Servicename) EC2 Fleet (EC2-Flotte) aus.

D. Wählen Sie für Event type (Ereignistyp) EC2 Fleet Instance Change (Änderung der EC2-Flotten-Instance) aus.

E. Wählen Sie Edit pattern (Muster bearbeiten) aus und fügen Sie `"detail": {"sub-type": ["launched"]` hinzu, um dem Beispiel-Ereignismuster zu

entsprechen. Fügen Sie für das richtige JSON-Format ein Komma (`,`) nach der vorhergehenden eckigen Klammer (`]`) ein.

ii. (Alternativ) So geben Sie ein benutzerdefiniertes Ereignismuster an:

A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.

b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.

c. Wählen Sie für Topic (Thema) Lambda function (Lambda-Funktion) und für Function (Funktion) die Funktion, die Sie erstellt haben, um beim Auftreten des Ereignisses zu reagieren.

d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).

e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.

7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.

b. Wählen Sie Regel erstellen aus.

Ein Tutorial zum Erstellen einer Lambda-Funktion und einer EventBridge Regel, die die Lambda-Funktion ausführt, finden Sie unter Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge im AWS Lambda Developer Guide.

Erstellen Sie EventBridge Amazon-Regeln zur Überwachung von Spot-Flottenereignissen

Wenn eine Benachrichtigung über eine Statusänderung für eine Spot-Flotte ausgegeben wird, wird das Ereignis für die Benachrichtigung EventBridge in Form einer JSON-Datei an Amazon gesendet. Sie können eine EventBridge Regel schreiben, um zu automatisieren, welche Aktionen ergriffen werden, wenn ein Ereignismuster mit der Regel übereinstimmt. Wenn ein Ereignismuster EventBridge erkannt wird, das einem in einer Regel definierten Muster entspricht, EventBridge ruft es das in der Regel angegebene Ziel (oder die Ziele) auf.

Die folgenden Felder bilden das in der Regel definierte Ereignismuster:

`"source": "aws.ec2spotfleet"`

Gibt an, dass das Ereignis aus der Spot-Flotte stammt.

`"detail-type": "EC2 Spot Fleet State Change"`

Identifiziert den Ereignistyp.

`"detail": { "sub-type": "submitted" }`

Identifiziert den Ereignis-Sub-Typ.

Eine Liste der Spot-Flotten-Ereignisse und Beispielereignisdaten finden Sie unter the section called “Ereignistypen für Spot-Flotten”.

Beispiele

- Erstellen Sie eine EventBridge Regel, um eine Benachrichtigung zu senden
- Erstellen Sie eine EventBridge Regel zum Auslösen einer Lambda-Funktion

Erstellen Sie eine EventBridge Regel, um eine Benachrichtigung zu senden

Im folgenden Beispiel wird eine EventBridge Regel erstellt, mit der jedes Mal, wenn Amazon EC2 eine Benachrichtigung über eine Änderung des Status der Spot-Flotte ausgibt, eine E-Mail, eine Textnachricht oder eine mobile Push-Benachrichtigung sendet. Das Signal in diesem Beispiel wird als `EC2 Spot Fleet State Change`-Ereignis ausgegeben, das die durch die Regel definierte Aktion auslöst. Bevor Sie die EventBridge Regel erstellen, müssen Sie das Amazon SNS SNS-Thema für die E-Mail, Textnachricht oder mobile Push-Benachrichtigung erstellen.

Um eine EventBridge Regel zum Senden einer Benachrichtigung zu erstellen, wenn sich der Status einer Spot-Flotte ändert

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:

   a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

      Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.

   b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird dieses stets an den standardmäßigen Event Bus Ihres Kontos weitergeleitet.

   c. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.

   d. Wählen Sie Weiter aus.
4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:

   a. Wählen Sie als Quelle für Ereignisse die Option AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.

   b. Bei Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, um mit dem `EC2 Spot Fleet Instance Change`-Ereignis übereinzustimmen.

      ```
      {
       "source": ["aws.ec2spotfleet"],
       "detail-type": ["EC2 Spot Fleet Instance Change"]
      }
      ```

      Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

      i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

C. Wählen Sie für AWS Service EC2 Spot Fleet (EC2-Spot-Flotte) aus.

D. Wählen Sie für Event type (Ereignistyp) EC2 Spot Fleet Instance Change (Änderung der EC2-Spot-Flotten-Instance) aus.

E. Um die Vorlage anzupassen, wählen Sie Edit pattern (Muster bearbeiten) und nehmen Sie Ihre Änderungen vor, damit sie dem Beispiel-Ereignismuster entsprechen.

ii. (Alternativ) So geben Sie ein benutzerdefiniertes Ereignismuster an:

A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.

b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.

c. Wählen Sie für Topic (Thema) ein vorhandenes Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).

e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.

7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.

b. Wählen Sie Regel erstellen aus.

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

Erstellen Sie eine EventBridge Regel zum Auslösen einer Lambda-Funktion

Im folgenden Beispiel wird eine EventBridge Regel erstellt, die jedes Mal eine Lambda-Funktion auslöst, wenn Amazon EC2 beim Start einer Instance eine Spot-Fleet-Instance-Änderungsbenachrichtigung ausgibt. Das Signal in diesem Beispiel wird als `EC2 Spot Fleet Instance Change`-Ereignis, Sub-Typ `launched`, ausgegeben, das die durch die Regel definierte Aktion auslöst.

Bevor Sie die EventBridge Regel erstellen, müssen Sie die Lambda-Funktion erstellen.

Um die Lambda-Funktion zu erstellen, die in der EventBridge Regel verwendet werden soll

1. Öffnen Sie die AWS Lambda Konsole unter https://console.aws.amazon.com/lambda/.
2. Wählen Sie Create function (Funktion erstellen).
3. Geben Sie einen Namen für Ihre Funktion ein, konfigurieren Sie den Code und wählen Sie dann Create function (Funktion erstellen).

   Weitere Informationen zur Verwendung von Lambda finden Sie unter Erstellen einer Lambda-Funktion mit der Konsole im Entwicklerhandbuch für AWS Lambda .

Um eine EventBridge Regel zum Auslösen einer Lambda-Funktion zu erstellen, wenn sich der Status einer Instance in einer Spot-Flotte ändert

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Zum Define rule detail (Festlegen der Regeldetails) gehen Sie folgendermaßen vor:

   a. Geben Sie für die Regel einen Name (Namen) und optional eine Beschreibung ein.

      Eine Regel darf nicht denselben Namen wie eine andere Regel in derselben Region und auf demselben Event Bus haben.

b. Bei Event bus (Ereignisbus) wählen Sie default (Standard) aus. Wenn ein AWS -Service in Ihrem Konto ein Ereignis ausgibt, wird dieses stets an den standardmäßigen Event Bus Ihres Kontos weitergeleitet.

c. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.

d. Wählen Sie Weiter aus.

4. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:

a. Wählen Sie als Quelle für Ereignisse die Option AWS Veranstaltungen oder EventBridge Partnerveranstaltungen aus.

b. Für Event pattern (Ereignismuster) in diesem Beispiel geben Sie das folgende Ereignismuster an, das dem `EC2 Spot Fleet Instance Change`-Ereignis und `launched`-Subtyp übereinstimmt.

```
{
 "source": ["aws.ec2spotfleet"],
 "detail-type": ["EC2 Spot Fleet Instance Change"],
 "detail": {
   "sub-type": ["launched"]
}
```

Um das Ereignismuster hinzuzufügen, können Sie entweder eine Vorlage verwenden, indem Sie Event pattern form (Ereignismusterformular) auswählen oder Sie spezifizieren Ihr eigenes Muster, indem Sie Custom pattern (JSON-Editor) (Benutzerdefiniertes Muster (JSON-Editor)) auswählen, siehe nachfolgend:

i. Gehen Sie wie folgt vor, um eine Vorlage zum Erstellen des Ereignismusters zu erstellen:

A. Wählen Sie Event pattern form (Ereignismusterformular) aus.

B. Als Event source (Ereignisquelle) wählen Sie AWS -Services aus.

C. Wählen Sie für AWS Service EC2 Spot Fleet (EC2-Spot-Flotte) aus.

D. Wählen Sie für Event type (Ereignistyp) EC2 Spot Fleet Instance Change (Änderung der EC2-Spot-Flotten-Instance) aus.

E. Wählen Sie Edit pattern (Muster bearbeiten) aus und fügen Sie `"detail": {"sub-type": ["launched"]` hinzu, um dem Beispiel-Ereignismuster zu

entsprechen. Fügen Sie für das richtige JSON-Format ein Komma (`,`) nach der vorhergehenden eckigen Klammer (`]`) ein.

ii. (Alternativ) So geben Sie ein benutzerdefiniertes Ereignismuster an:

A. Wählen Sie Custom pattern (JSON editor) (Benutzerdefiniertes Muster (JSON-Editor)) aus.

B. In dem Feld Event pattern (Ereignismuster) fügen Sie das Ereignismuster für dieses Beispiel hinzu.

c. Wählen Sie Weiter aus.

5. Bei Select target(s) (Ziel(e) auswählen) gehen Sie wie folgt vor:

a. Bei Target types (Zieltypen) wählen Sie AWS -Service aus.

b. Bei Select a target (Ziel auswählen) wählen Sie SNS topic (SNS-Thema) aus, um eine E-Mail, eine SMS oder eine mobile Push-Benachrichtigung zu senden, wenn das Ereignis eintritt.

c. Wählen Sie für Topic (Thema) Lambda function (Lambda-Funktion) und für Function (Funktion) die Funktion, die Sie erstellt haben, um beim Auftreten des Ereignisses zu reagieren.

d. (Optional) Unter Additional settings (Zusätzliche Einstellungen) können Sie optional zusätzliche Einstellungen konfigurieren. Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren (Schritt 16).

e. Wählen Sie Weiter aus.

6. (Optional) Bei Tags können Sie Ihrer Regel optional einen Tag oder mehrere Tags hinzufügen und dann Next (Weiter) auswählen.

7. Bei Review and create (Überprüfen und erstellen) gehen Sie wie folgt vor:

a. Überprüfen Sie die Details der Regel und ändern Sie sie nach Bedarf.

b. Wählen Sie Regel erstellen aus.

Ein Tutorial zum Erstellen einer Lambda-Funktion und einer EventBridge Regel, die die Lambda-Funktion ausführt, finden Sie unter Tutorial: Log the State of an Amazon EC2 Instance Using EventBridge im AWS Lambda Developer Guide.

Tutorials für EC2-Flotte und Spot-Flotte

Die folgenden Tutorials führen Sie durch die gängigen Prozesse zum Erstellen von EC2-Flotten und Spot-Flotten.

Tutorials

- Praktische Anleitung: Verwenden von EC2-Flotte mit Instance-Gewichtung
- Praktische Anleitung: Verwenden von EC2-Flotte mit On-Demand als Primärkapazität
- Tutorial: Starten von On-Demand-Instances mithilfe von Kapazitätsreservierungen
- Tutorial: Starten von Instances in Kapazitätsblöcken
- Praktische Anleitung: Verwenden von Spot-Flotte mit Instance-Gewichtung

Praktische Anleitung: Verwenden von EC2-Flotte mit Instance-Gewichtung

In dieser Anleitung wird ein fiktives Unternehmen mit dem Namen Example Corp verwendet, um das Anfordern einer EC2-Flotte mit Instance-Gewichtung zu veranschaulichen.

Ziel

Example Corp, ein Pharmaunternehmen, möchte die Rechenleistung von Amazon EC2 zum Prüfen chemischer Verbindungen nutzen, die im Kampf gegen Krebs eingesetzt werden könnten.

Planung

Example Corp macht sich zunächst mit den Bewährten Methoden für Spot vertraut. Als Nächstes ermittelt Example Corp die Anforderungen für die eigene EC2-Flotte.

Instance-Typen

Example Corp verfügt über eine rechen- und speicherintensive Anwendung, welche die beste Leistung bei mindestens 60 GB Speicher und mit mindestens acht virtuellen CPUs (vCPUs) aufweist. Das Unternehmen möchte diese Ressourcen für die Anwendung zum geringstmöglichen Preis maximieren. Example Corp entscheidet, dass die folgenden EC2-Instance-Typen die Anforderungen erfüllen würden:

Instance-Typ	Arbeitsspeicher (GiB)	vCPUs

Instance-Typ	Arbeitsspeicher (GiB)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Zielkapazität in Einheiten

Bei der Gewichtung von Instanzen kann die Zielkapazität einer Anzahl von Instanzen (Standard) oder einer Kombination von Faktoren wie Kernen (vCPUs), Arbeitsspeicher () und Speicher (GBGiBs) entsprechen. Example Corp betrachtet die Basis für ihre Anwendung (60 GB RAM und acht vCPUs) als eine Einheit und entscheidet, dass ein 20-Faches dieser Menge ihre Anforderungen erfüllen würde. Deshalb legt das Unternehmen für seine EC2-Flotte-Anfrage eine Zielkapazität von 20 fest.

Instance-Gewichtungen

Nach dem Festlegen der Zielkapazität berechnet Example Corp die Instance-Gewichtungen. Zum Berechnen der Instance-Gewichtungen der einzelnen Instance-Typen ermitteln sie die folgenden Einheiten der einzelnen Instance-Typen, die zum Erreichen der Zielkapazität erforderlich sind:

- r3.2xlarge (61,0 GB, 8 vCPUs) = 1 Einheit von 20
- r3.4xlarge (122,0 GB, 16 vCPUs) = 2 Einheiten von 20
- r3.8xlarge (244,0 GB, 32 vCPUs) = 4 Einheiten von 20

Aus diesem Grund weist Example Corp die Instance-Gewichtungen 1, 2 und 4 den entsprechenden Startkonfigurationen in ihrer EC2-Flotte-Anfrage zu.

Preis pro Einheitsstunde

Example Corp verwendet den On-Demand-Preis pro Instance-Stunde als Startpunkt für den Preis. Es wäre auch möglich, frühere Spot-Preise oder eine Kombination aus beidem zu verwenden. Zum Berechnen des Preises pro Einheitsstunde teilen sie den Startpreis pro Instance-Stunde durch die Gewichtung. Beispiel:

Instance-Typ	On-Demand-Preis	Instance-Gewichtung	Preis pro Einheitsstunde
r3.2xlarge	0,7 USD	1	0,7 USD
r3.4xLarge	$1.4	2	0,7 USD
r3.8xLarge	$2,8	4	0,7 USD

Example Corp könnte einen globalen Preis pro Einheitsstunde in Höhe von 0,7 USD angeben und für alle drei Instance-Typen wettbewerbsfähig sein. Sie könnten auch einen globalen Preis pro Einheitsstunde in Höhe von 0,7 USD und einen spezifischen Preis pro Einheitsstunde in Höhe von 0,9 USD in der `r3.8xlarge`-Startspezifikation verwenden.

Überprüfen der Berechtigungen

Vor dem Erstellen einer EC2-Flotte überprüft Example Corp, ob eine IAM-Rolle mit den erforderlichen Berechtigungen verfügbar ist. Weitere Informationen finden Sie unter EC2-Flotte-Voraussetzungen.

Erstellen einer Startvorlage

Als Nächstes erstellt Example Corp eine Startvorlage. Die Startvorlagen-ID wird im folgenden Schritt verwendet. Weitere Informationen finden Sie unter Erstellen einer Startvorlage.

Erstellen der EC2-Flotte

Example Corp erstellt eine Datei mit dem Namen `config.json` und der folgenden Konfiguration für die EC2-Flotte: Ersetzen Sie im folgenden Beispiel die Ressourcenbezeichner durch Ihre eigenen Ressourcenbezeichner.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "1"
            },
```

```
            "Overrides": [
                {
                    "InstanceType": "r3.2xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 1
                },
                {
                    "InstanceType": "r3.4xlarge",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 2
                },
                {
                    "InstanceType": "r3.8xlarge",
                    "MaxPrice": "0.90",
                    "SubnetId": "subnet-482e4972",
                    "WeightedCapacity": 4
                }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Example Corp erstellt die EC2-Flotte mit dem folgenden create-fleet-Befehl:

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Weitere Informationen finden Sie unter Erstellen einer EC2-Flotte.

Bereitstellung

Die Zuweisungsstrategie legt fest, aus welchen Spot-Kapazitätspools Ihre Spot-Instances stammen.

Bei der `lowest-price`-Strategie (der Standardstrategie) stammen die Spot-Instances aus dem Pool mit dem niedrigsten Preis pro Einheit zum Zeitpunkt der Bereitstellung. Zum Bereitstellen von 20 Kapazitätseinheiten startet die EC2-Flotte entweder 20 `r3.2xlarge`-Instances (20 geteilt durch 1), 10 `r3.4xlarge`-Instances (20 geteilt durch 2) oder 5 `r3.8xlarge`-Instances (20 geteilt durch 4).

Würde Example Corp die `diversified`-Strategie verwenden, dann würden die Spot-Instances aus allen drei Pools stammen. Die EC2-Flotte würde 6 `r3.2xlarge`-Instances (die 6 Einheiten bereitstellen), 3 `r3.4xlarge`-Instances (die 6 Einheiten bereitstellen) und 2 `r3.8xlarge`-Instances (die 8 Einheiten bereitstellen) mit insgesamt 20 Einheiten starten.

Praktische Anleitung: Verwenden von EC2-Flotte mit On-Demand als Primärkapazität

In dieser Anleitung wird ein fiktives Unternehmen mit dem Namen ABC Online verwendet, um das Anfordern einer EC2-Flotte mit On-Demand als Primärkapazität und Spot-Kapazität, wenn verfügbar, zu veranschaulichen.

Ziel

ABC Online, ein Restaurantbetreiber, möchte in der Lage sein, Amazon EC2-Kapazität für alle EC2-Instance-Typen und Kaufoptionen bereitzustellen, um die gewünschte Größe, Leistung und Kosten zu erreichen.

Plan

ABC Online benötigt eine feste Kapazität, um in Spitzenzeiten arbeiten zu können, möchte aber von einer erhöhten Kapazität zu einem niedrigeren Preis profitieren. ABC Online ermittelt die folgenden Anforderungen für die eigene EC2-Flotte:

- On-Demand-Instance-Kapazität – ABC Online benötigt 15 On-Demand-Instances, um sicherzustellen, dass der Datenverkehr in Spitzenzeiten verarbeitet werden kann.
- Spot-Instance-Kapazität – ABC Online möchte die Leistung verbessern, aber zu einem niedrigeren Preis, durch die Bereitstellung von 5 Spot-Instances.

Überprüfen der Berechtigungen

Vor dem Erstellen einer EC2-Flotte prüft ABC Online, ob eine IAM-Rolle mit den erforderlichen Berechtigungen verfügbar ist. Weitere Informationen finden Sie unter EC2-Flotte-Voraussetzungen.

Erstellen einer Startvorlage

Als Nächstes erstellt ABC Online eine Startvorlage. Die Startvorlagen-ID wird im folgenden Schritt verwendet. Weitere Informationen finden Sie unter Erstellen einer Startvorlage.

Erstellen der EC2-Flotte

ABC Online erstellt eine Datei mit dem Namen `config.json` und der folgenden Konfiguration für die EC2-Flotte: Ersetzen Sie im folgenden Beispiel die Ressourcenbezeichner durch Ihre eigenen Ressourcenbezeichner.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-07b3bc7625cdab851",
                "Version": "2"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 20,
        "OnDemandTargetCapacity":15,
        "DefaultTargetCapacityType": "spot"
    }
}
```

ABC Online erstellt die EC2-Flotte mit dem folgenden create-fleet-Befehl:

```
aws ec2 create-fleet \
    --cli-input-json file://config.json
```

Weitere Informationen finden Sie unter Erstellen einer EC2-Flotte.

Bereitstellung

Die Zuweisungsstrategie legt fest, dass die On-Demand-Kapazität immer erfüllt ist, während der Saldo der Zielkapazität als Spot erfüllt ist, wenn Kapazität und Verfügbarkeit vorhanden sind.

Tutorial: Starten von On-Demand-Instances mithilfe von Kapazitätsreservierungen

Dieses Tutorial führt Sie durch alle Schritte, die Sie ausführen müssen, damit Ihre EC2-Flotte On-Demand-Instances in `targeted` Kapazitätsreservierungen startet.

Sie erfahren, wie Sie eine Flotte so konfigurieren, dass `targeted`-On-Demand-Kapazitätsreservierungen zuerst beim Starten von On-Demand-Instances verwendet werden. Außerdem erfahren Sie, wie Sie die Flotte so konfigurieren, dass die Flotte, wenn die gesamte On-Demand-Zielkapazität die Anzahl der verfügbaren ungenutzten Kapazitätsreservierungen überschreitet, die angegebene Zuordnungsstrategie verwendet, um die Instance-Pools auszuwählen, in denen die verbleibende Zielkapazität gestartet werden soll.

EC2-Flotte-Konfiguration

In diesem Tutorial sieht die Flottenkonfiguration wie folgt aus:

- Zielkapazität: 10 On-Demand-Instances
- Nicht verwendete `targeted`-Kapazitätsreservierungen: 6 (geringer als die On-Demand-Zielkapazität der Flotte von 10 On-Demand-Instances)
- Anzahl der Kapazitätsreservierungspools: 2 (`us-east-1a` und `us-east-1b`)
- Anzahl der Kapazitätsreservierungen pro Pool: 3
- On-Demand-Zuordnungsstrategie: `lowest-price` (Wenn die Anzahl der nicht genutzten Kapazitätsreservierungen kleiner als die On-Demand-Zielkapazität ist, bestimmt die Flotte die Pools, in denen die verbleibende On-Demand-Kapazität basierend auf der On-Demand-Zuordnungsstrategie gestartet werden soll.)

  Beachten Sie, dass Sie auch die `prioritized`-Zuordnungsstrategie anstelle der `lowest-price`-Zuordnungsstrategie verwenden können.

Starten von On-Demand-Instances in targeted-Kapazitätsreservierungen müssen Sie eine Reihe von Schritten wie folgt ausführen:

- Schritt 1: Erstellen von Kapazitätsreservierungen
- Schritt 2: Erstellen einer Ressourcengruppe für Kapazitätsreservierung
- Schritt 3: Hinzufügen der Kapazitätsreservierungen zur Ressourcengruppe der Kapazitätsreservierung
- (Optional) Schritt 4: Anzeigen der Kapazitätsreservierungen in der Ressourcengruppe
- Schritt 5: Erstellen einer Startvorlage, die angibt, dass die Kapazitätsreservierung auf eine bestimmte Ressourcengruppe abzielt
- (Optional) Schritt 6: Beschreiben der Startvorlage
- Schritt 7: Erstellen einer EC2-Flotte

- (Optional) Schritt 8: Anzeigen der Anzahl der verbleibenden ungenutzten Kapazitätsreservierungen

Schritt 1: Erstellen von Kapazitätsreservierungen

Verwenden Sie den Befehl create-capacity-reservation (Kapazitätsreservierung erstellen), um die Kapazitätsreservierungen zu erstellen, drei für `us-east-1a` und weitere drei für `us-east-1b`. Mit Ausnahme der Availability Zone sind die anderen Attribute der Kapazitätsreservierungen identisch.

3 Kapazitätsreservierungen in **`us-east-1a`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1a\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Beispiel für die resultierende ID der Kapazitätsreservierung

```
cr-1234567890abcdef1
```

3 Kapazitätsreservierungen in **`us-east-1b`**

```
aws ec2 create-capacity-reservation \
    --availability-zone us-east-1b\
    --instance-type c5.xlarge\
    --instance-platform Linux/UNIX \
    --instance-count 3 \
    --instance-match-criteria targeted
```

Beispiel für die resultierende ID der Kapazitätsreservierung

```
cr-54321abcdef567890
```

Schritt 2: Erstellen einer Ressourcengruppe für Kapazitätsreservierung

Verwenden des `resource-groups`-Dienstes und des Befehls create-group (Erstellen einer Gruppe), um eine Ressourcengruppe für Kapazitätsreservierung zu erstellen In diesem Beispiel

hat die Ressourcengruppe den Namen `my-cr-group`. Informationen dazu, warum Sie eine Ressourcengruppe erstellen müssen, finden Sie unter Verwenden von Kapazitätsreservierungen für On-Demand-Instances.

```
aws resource-groups create-group \
    --name my-cr-group \
    --configuration '{"Type":"AWS::EC2::CapacityReservationPool"}'
 '{"Type":"AWS::ResourceGroups::Generic", "Parameters": [{"Name": "allowed-resource-
types", "Values": ["AWS::EC2::CapacityReservation"]}]}'
```

Schritt 3: Hinzufügen der Kapazitätsreservierungen zur Ressourcengruppe der Kapazitätsreservierung

Verwenden des `resource-groups`-Dienstes und des Befehls group-resources (Gruppenressourcen), um die Kapazitätsreservierungen, die Sie in Schritt 1 erstellt haben, der Ressourcengruppe Kapazitätsreservierungen hinzuzufügen. Beachten Sie, dass Sie die On-Demand-Kapazitätsreservierungen anhand ihrer ARNs referenzieren müssen.

```
aws resource-groups group-resources \
    --group my-cr-group \
    --resource-arns \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1 \
      arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890
```

Beispielausgabe

```
{
   "Failed": [],
   "Succeeded": [
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-1234567890abcdef1",
   "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/cr-54321abcdef567890"
   ]
}
```

(Optional) Schritt 4: Anzeigen der Kapazitätsreservierungen in der Ressourcengruppe

Verwenden des `resource-groups`-Dienstes und des Befehls list-group-resources (Gruppenressourcen auflisten), um optional die Ressourcengruppe zu beschreiben, um ihre Kapazitätsreservierungen anzuzeigen.

```
aws resource-groups list-group-resources --group my-cr-group
```

Beispielausgabe

```
{
    "ResourceIdentifiers": [
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-1234567890abcdef1"
        },
        {
            "ResourceType": "AWS::EC2::CapacityReservation",
            "ResourceArn": "arn:aws:ec2:us-east-1:123456789012:capacity-reservation/
cr-54321abcdef567890"
        }
    ]
}
```

Schritt 5: Erstellen einer Startvorlage, die angibt, dass die Kapazitätsreservierung auf eine bestimmte Ressourcengruppe abzielt

Verwenden des Befehls create-launch-template (Startvorlage erstellen), um eine Startvorlage zu erstellen, in der Sie die zu verwendenden Kapazitätsreservierungen angeben können. In diesem Beispiel wird die Flotte `targeted`-Kapazitätsreservierungen verwenden, die einer Ressourcengruppe hinzugefügt wurden. Daher geben die Startvorlagendaten an, dass die Kapazitätsreservierung auf eine bestimmte Ressourcengruppe ausgerichtet ist. In diesem Beispiel hat die Startvorlage den Namen `my-launch-template`.

```
aws ec2 create-launch-template \
    --launch-template-name my-launch-template \
    --launch-template-data \
        '{"ImageId": "ami-0123456789example",
          "CapacityReservationSpecification":
            {"CapacityReservationTarget":
                { "CapacityReservationResourceGroupArn": "arn:aws:resource-groups:us-
east-1:123456789012:group/my-cr-group" }
            }
        }'
```

(Optional) Schritt 6: Beschreiben der Startvorlage

Verwenden des Befehls describe-launch-template (Startvorlage beschreiben), um optional die Startvorlage zu beschreiben, um ihre Konfiguration anzuzeigen.

```
aws ec2 describe-launch-template-versions --launch-template-name my-launch-template
```

Beispielausgabe

```
{
    "LaunchTemplateVersions": [
        {
            "LaunchTemplateId": "lt-01234567890example",
            "LaunchTemplateName": "my-launch-template",
            "VersionNumber": 1,
            "CreateTime": "2021-01-19T20:50:19.000Z",
            "CreatedBy": "arn:aws:iam::123456789012:user/Admin",
            "DefaultVersion": true,
            "LaunchTemplateData": {
                "ImageId": "ami-0947d2ba12ee1ff75",
                "CapacityReservationSpecification": {
                    "CapacityReservationTarget": {
                        "CapacityReservationResourceGroupArn": "arn:aws:resource-
groups:us-east-1:123456789012:group/my-cr-group"
                    }
                }
            }
        }
    ]
}
```

Schritt 7: Erstellen einer EC2-Flotte

Erstellen Sie eine EC2-Flotte, die die Konfigurationsinformationen für die Instances angibt, die sie starten soll. Die folgende EC2-Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die Startvorlage `my-launch-template` ist die Startvorlage, die Sie in Schritt 5 erstellt haben. Es gibt zwei Instance-Pools mit jeweils demselben Instance-Typ (`c5.xlarge`), aber mit unterschiedlichen Availability Zones (`us-east-1a` und `us-east-1b`). Der Preis der Instance-Pools ist derselbe, da die Preise für die Region und nicht für die Availability Zone definiert sind. Die gesamte Zielkapazität beträgt 10 und der Standardzielkapazitätstyp ist `on-demand`. Die On-Demand-

Zuordnungsstrategie ist `lowest-price`. Die Nutzungsstrategie für Kapazitätsreservierungen ist `use-capacity-reservations-first`.

> **Note**
>
> Der Flottentyp muss `instant` sein. Andere Flotten-Typen unterstützen `use-capacity-reservations-first` nicht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Nachdem Sie die `instant`-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 10 Instances gestartet, um die Zielkapazität zu erreichen:

- Die Kapazitätsreservierungen werden zuerst verwendet, um 6 On-Demand-Instances wie folgt zu starten:
  - 3 On-Demand-Instances werden in die 3 `c5.xlarge` `targeted`Kapazitätsreservierungen in `us-east-1a` gestartet
  - 3 On-Demand-Instances werden in die 3 `c5.xlarge` `targeted`Kapazitätsreservierungen in `us-east-1b` gestartet
- Um die Zielkapazität zu erreichen, werden 4 zusätzliche On-Demand-Instances gemäß der On-Demand-Zuordnungsstrategie in die reguläre On-Demand-Strategie gestartet, die in diesem Beispiel `lowest-price` ist. Da die Pools jedoch denselben Preis haben (da der Preis pro Region und nicht pro Availability Zone ist), startet die Flotte die restlichen 4 On-Demand-Instances in einem der Pools.

(Optional) Schritt 8: Anzeigen der Anzahl der verbleibenden ungenutzten Kapazitätsreservierungen

Nachdem die Flotte gestartet wurde, können Sie optional describe-capacity-reservations (Kapazitätsreservierungen beschreiben) ausführen, um zu sehen, wie viele nicht verwendete Kapazitätsreservierungen noch übrig sind. In diesem Beispiel sollte die folgende Antwort angezeigt werden, die zeigt, dass alle Kapazitätsreservierungen in allen Pools verwendet wurden.

```
{ "CapacityReservationId":  "cr-111",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}

 { "CapacityReservationId":  "cr-222",
     "InstanceType":  "c5.xlarge",
     "AvailableInstanceCount":  0
}
```

Tutorial: Starten von Instances in Kapazitätsblöcken

Dieses Tutorial führt Sie durch die Schritte, die Sie durchführen müssen, damit Ihre EC2-Flotte Instances in Kapazitätsblöcken startet. Weitere Informationen zu Kapazitätsblöcken finden Sie unter. Kapazitätsblöcke für ML

Sie können eine EC2-Flotte vom Typ instant verwenden, um Instances in Kapazitätsblöcken zu starten. Weitere Informationen finden Sie unter Verwenden einer EC2-Flotte des Typs „Instant“.

In den meisten Fällen sollte die Zielkapazität der Anfrage für die EC2-Flotte kleiner oder gleich der verfügbaren Kapazität der von Ihnen angestrebten Kapazitätsblock-Reservierung sein. Zielkapazitätsanfragen, die die Grenzen der Kapazitätsblock-Reservierung überschreiten, werden nicht erfüllt. Wenn die Anfrage für die Zielkapazität die Grenzen Ihrer Kapazitätsblock-Reservierung überschreitet, erhalten Sie eine Ausnahme wegen unzureichender Kapazität für die Kapazität, die die Grenzen Ihrer Kapazitätsblock-Reservierung überschreitet.

> **Note**
>
> Bei Kapazitätsblöcken wird die EC2-Flotte für den Rest der gewünschten Zielkapazität nicht auf den Start von On-Demand-Instances zurückgreifen.

Wenn die EC2-Flotte nicht in der Lage ist, die angeforderte Zielkapazität in einer verfügbaren Kapazitätsblock-Reservierung zu erfüllen, wird die EC2-Flotte so viel Kapazität wie möglich bereitstellen und die Instances zurückgeben, die gestartet werden konnten. Sie können den Aufruf der EC2-Flotte wiederholen, bis alle Instances bereitgestellt sind.

Nachdem Sie die EC2-Flotten-Anfrage konfiguriert haben, müssen Sie bis zum Startdatum Ihrer Kapazitätsblock-Reservierung warten. Wenn Sie Anfragen an die EC2-Flotte stellen, um in einen Kapazitätsblock zu starten, der noch nicht begonnen hat, erhalten Sie eine Fehlermeldung wegen unzureichender Kapazität.

Nachdem Ihre Kapazitätsblock-Reservierung aktiv wird, können Sie EC2-Flotten-API-Aufrufe durchführen und die Instances basierend auf den von Ihnen ausgewählten Parametern in Ihrem Kapazitätsblock bereitstellen. Im Kapazitätsblock ausgeführte Instances werden so lange ausgeführt, bis Sie sie über einen separaten Amazon-EC2-API-Aufruf anhalten oder beenden oder bis Amazon EC2 die Instances beendet, wenn die Kapazitätsblock-Reservierung endet.

Überlegungen

- Mehrere Kapazitätsblöcke in derselben `CreateFleet`-Anfrage werden nicht unterstützt.
- Die Verwendung von `OnDemandTargetCapacity` oder `SpotTargetCapacity` bei gleichzeitiger Einstellung von `capacity-block` als `DefaultTargetCapacity` wird nicht unterstützt.

- Wenn `DefaultTargetCapacityType` auf `capacity-block` gesetzt ist, können Sie `OnDemandOptions::CapacityReservationOptions` nicht angeben. Es kommt zu einer Ausnahme.

Erstellen einer Startvorlage

Die Startvorlagen-ID wird im folgenden Schritt verwendet. Weitere Informationen finden Sie unter Erstellen einer Startvorlage.

Um die Startvorlage zu konfigurieren, setzen Sie für `InstanceMarketOptionsRequest MarketType` auf `capacity-block`. Geben Sie die ID der Kapazitätsblock-Reservierung an, die Sie als Ziel verwenden möchten, indem Sie den `CapacityReservationID`-Parameter festlegen.

Erstellen der EC2-Flotte

Erstellen Sie eine Datei mit dem Namen `config.json` und der folgenden Konfiguration für die EC2-Flotte. Ersetzen Sie im folgenden Beispiel die Ressourcenbezeichner durch Ihre eigenen Ressourcenbezeichner.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "CBR-launch-template",
                "Version": "1"
            },
            "Overrides": [
                {
                    "InstanceType": "p5.48xlarge",
                    "AvailabilityZone": "us-east-1a"
                },
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "capacity-block"
    },
    "Type": "instant"
}
```

Verwenden Sie den folgenden create-fleet-Befehl.

```
aws ec2 create-fleet \
     --cli-input-json file://config.json
```

Weitere Informationen finden Sie unter Erstellen einer EC2-Flotte.

Praktische Anleitung: Verwenden von Spot-Flotte mit Instance-Gewichtung

In dieser Anleitung wird ein fiktives Unternehmen mit dem Namen Example Corp verwendet, um das Anfordern einer Spot-Flotte mit Instance-Gewichtung zu veranschaulichen.

Ziel

Example Corp, ein Pharmaunternehmen, möchte die Rechenleistung von Amazon EC2 zum Prüfen chemischer Verbindungen verwenden, die im Kampf gegen Krebs eingesetzt werden könnten.

Planung

Example Corp macht sich zunächst mit den Bewährten Methoden für Spot vertraut. Als Nächstes ermittelt Example Corp die folgenden Anforderungen für ihre Spot-Flotte.

Instance-Typen

Example Corp verfügt über eine rechen- und speicherintensive Anwendung, welche die beste Leistung bei mindestens 60 GB Speicher und mit mindestens acht virtuellen CPUs (vCPUs) aufweist. Das Unternehmen möchte diese Ressourcen für die Anwendung zum geringstmöglichen Preis maximieren. Example Corp entscheidet, dass die folgenden EC2-Instance-Typen die Anforderungen erfüllen würden:

Instance-Typ	Arbeitsspeicher (GiB)	vCPUs
r3.2xlarge	61	8
r3.4xlarge	122	16
r3.8xlarge	244	32

Zielkapazität in Einheiten

Bei der Gewichtung von Instanzen kann die Zielkapazität einer Anzahl von Instanzen (Standard) oder einer Kombination von Faktoren wie Kernen (vCPUs), Arbeitsspeicher () und Speicher (GBGiBs)

entsprechen. Example Corp betrachtet die Basis für ihre Anwendung (60 GB RAM und acht vCPUs) als 1 Einheit und entscheidet, dass ein 20-Faches dieser Menge ihre Anforderungen erfüllen würde. Das Unternehmen legt die Zielkapazität ihrer Spot-Flotten-Anforderung also auf 20 fest.

Instance-Gewichtungen

Nach dem Festlegen der Zielkapazität berechnet Example Corp die Instance-Gewichtungen. Zum Berechnen der Instance-Gewichtungen der einzelnen Instance-Typen ermitteln sie die folgenden Einheiten der einzelnen Instance-Typen, die zum Erreichen der Zielkapazität erforderlich sind:

- r3.2xlarge (61,0 GB, 8 vCPUs) = 1 Einheit von 20
- r3.4xlarge (122,0 GB, 16 vCPUs) = 2 Einheiten von 20
- r3.8xlarge (244,0 GB, 32 vCPUs) = 4 Einheiten von 20

Aus diesem Grund weist Example Corp den entsprechenden Startkonfigurationen in ihrer Spot-Flotten-Anforderung die Instance-Gewichtungen 1, 2 und 4 zu.

Preis pro Einheitsstunde

Example Corp verwendet den On-Demand-Preis pro Instance-Stunde als Startpunkt für den Preis. Es wäre auch möglich, frühere Spot-Preise oder eine Kombination aus beidem zu verwenden. Zum Berechnen des Preises pro Einheitsstunde teilen sie den Startpreis pro Instance-Stunde durch die Gewichtung. Beispiel:

Instance-Typ	On-Demand-Preis	Instance-Gewichtung	Preis pro Einheitsstunde
r3.2xlarge	0,7 USD	1	0,7 USD
r3.4xLarge	$1.4	2	0,7 USD
r3.8xLarge	$2,8	4	0,7 USD

Example Corp könnte einen globalen Preis pro Einheitsstunde in Höhe von 0,7 USD angeben und für alle drei Instance-Typen wettbewerbsfähig sein. Sie könnten auch einen globalen Preis pro Einheitsstunde in Höhe von 0,7 USD und einen spezifischen Preis pro Einheitsstunde in Höhe von 0,9 USD in der `r3.8xlarge`-Startspezifikation verwenden.

Überprüfen der Berechtigungen

Vor dem Erstellen einer Spot-Flotten-Anforderung vergewissert sich Example Corp, dass eine IAM-Rolle mit den erforderlichen Berechtigungen vorhanden ist. Weitere Informationen finden Sie unter Spot-Flotten-Berechtigungen.

Erstellen Sie die Anforderung

Example Corp erstellt eine Datei `config.json` mit der folgenden Konfiguration für die Spot-Flotten-Anforderung:

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.2xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 1
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.4xlarge",
      "SubnetId": "subnet-482e4972",
      "WeightedCapacity": 2
    },
    {
      "ImageId": "ami-1a2b3c4d",
      "InstanceType": "r3.8xlarge",
      "SubnetId": "subnet-482e4972",
      "SpotPrice": "0.90",
      "WeightedCapacity": 4
    }
  ]
}
```

Example Corp erstellt die Spot-Flotten-Anforderung mit dem Befehl request-spot-fleet.

```
aws ec2 request-spot-fleet --spot-fleet-request-config file://config.json
```

Weitere Informationen finden Sie unter Spot-Flotte-Anforderungstypen.

Bereitstellung

Die Zuweisungsstrategie legt fest, aus welchen Spot-Kapazitätspools Ihre Spot-Instances stammen.

Bei der `lowestPrice`-Strategie (der Standardstrategie) stammen die Spot-Instances aus dem Pool mit dem niedrigsten Preis pro Einheit zum Zeitpunkt der Bereitstellung. Zum Bereitstellen von 20 Kapazitätseinheiten öauncht die Spot-Flotte entweder 20 `r3.2xlarge`-Instances (20 geteilt durch 1), 10 `r3.4xlarge`-Instances (20 geteilt durch 2) oder 5 `r3.8xlarge`-Instances (20 geteilt durch 4).

Würde Example Corp die `diversified`-Strategie verwenden, dann würden die Spot-Instances aus allen drei Pools stammen. Die Spot-Flotte würde 6 `r3.2xlarge`-Instances (die 6 Einheiten bereitstellen), 3 `r3.4xlarge`-Instances (die 6 Einheiten bereitstellen) und 2 `r3.8xlarge`-Instances (die 8 Einheiten bereitstellen) mit insgesamt 20 Einheiten starten.

Beispielkonfigurationen für EC2-Flotte und Spot-Flotte

Die folgenden Beispiele zeigen Startkonfigurationen, die Sie zum Erstellen von EC2-Flotten und Spot-Fleets verwenden können.

Themen

- EC2-Flotte-Beispielkonfigurationen
- Beispielkonfigurationen für Spot-Flotte

EC2-Flotte-Beispielkonfigurationen

Die folgenden Beispiele zeigen Startkonfigurationen, die Sie mit dem create-fleet-Befehl zum Erstellen einer EC2-Flotte verwenden können. Weitere Informationen zu den Parametern finden Sie unter create-fleet in der AWS CLI -Befehlsreferenz.

Beispiele

- Beispiel 1: Starten von Spot-Instances als Standard-Kaufoption
- Beispiel 2: Starten von On-Demand-Instances als Standard-Kaufoption
- Beispiel 3: Starten von On-Demand-Instances als primäre Kapazität

- Beispiel 4: Starten Sie On-Demand-Instances mit mehreren Kapazitätsreservierungen
- Beispiel 5: Starten Sie On-Demand-Instances mithilfe von Kapazitätsreservierungen, wenn die gesamte Zielkapazität die Anzahl der ungenutzten Kapazitätsreservierungen übersteigt
- Beispiel 6: Starten Sie On-Demand-Instances mithilfe gezielter Kapazitätsreservierungen
- Beispiel 7: Konfigurieren Sie den Kapazitätsausgleich, um Ersatz-Spot-Instances zu starten
- Beispiel 8: Starten Sie Spot-Instances in einer kapazitätsoptimierten Flotte
- Beispiel 9: Starten Sie Spot-Instances in einer kapazitätsoptimierten Flotte mit Prioritäten
- Beispiel 10: Starten Sie Spot-Instances in einer Flotte price-capacity-optimized
- Beispiel 11: Konfigurieren Sie die attributbasierte Auswahl des Instance-Typs

Beispiel 1: Starten von Spot-Instances als Standard-Kaufoption

Das folgende Beispiel gibt die minimalen Parameter an, die in einer EC2-Flotte benötigt werden: eine Startvorlage, eine Zielkapazität und eine Standard-Kaufoption. Die Startvorlage wird durch ihre Startvorlagen-ID und Versionsnummer identifiziert. Die Zielkapazität für die Flotte beträgt 2 Instances, die Standard-Kaufoption ist `spot`, was dazu führt, dass die Flotte 2 Spot-Instances startet.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "spot"
    }
}
```

Beispiel 2: Starten von On-Demand-Instances als Standard-Kaufoption

Das folgende Beispiel gibt die minimalen Parameter an, die in einer EC2-Flotte benötigt werden: eine Startvorlage, eine Zielkapazität und eine Standard-Kaufoption. Die Startvorlage wird durch ihre Startvorlagen-ID und Versionsnummer identifiziert. Die Zielkapazität für die Flotte beträgt 2 Instances,

die Standard-Kaufoption ist `on-demand`, was dazu führt, dass die Flotte 2 On-Demand-Instances startet.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "DefaultTargetCapacityType": "on-demand"
    }
}
```

Beispiel 3: Starten von On-Demand-Instances als primäre Kapazität

Das folgende Beispiel gibt die Gesamtzielkapazität von 2 Instances für die Flotte und eine Zielkapazität von 1 On-Demand-Instance an. Die Standard-Kaufoption ist `spot`. Die Flotte startet 1 On-Demand-Instance wie angegeben, muss aber noch eine weitere Instance starten, um die gesamte Zielkapazität zu erreichen. Die Kaufoption für die Differenz wird berechnet als `TotalTargetCapacity` – `OnDemandTargetCapacity` = `DefaultTargetCapacityType`, was dazu führt, dass die Flotte 1 Spot Instance launcht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 2,
        "OnDemandTargetCapacity": 1,
        "DefaultTargetCapacityType": "spot"
```

```
    }
}
```

Beispiel 4: Starten Sie On-Demand-Instances mit mehreren Kapazitätsreservierungen

Sie können eine Flotte so konfigurieren, dass sie On-Demand-Kapazitätsreservierungen zuerst beim Start von On-Demand-Instances verwendet, indem Sie die Nutzungsstrategie für Kapazitätsreservierungen auf `use-capacity-reservations-first` festlegen. Dieses Beispiel zeigt, wie die Flotte die Kapazitätsreservierungen auswählt, die verwendet werden sollen, wenn mehr Kapazitätsreservierungen vorhanden sind, als für die Erreichung der Zielkapazität erforderlich sind.

In diesem Beispiel sieht die Flottenkonfiguration wie folgt aus:

- Zielkapazität: 12 On-Demand-Instances
- Gesamt nicht verwendete Kapazitätsreservierungen: 15 (mehr als die On-Demand-Zielkapazität der Flotte von 12 On-Demand-Instances)
- Anzahl der Kapazitätsreservierungspools: 3 (`m5.large`, `m4.xlarge`, und `m4.2xlarge`)
- Anzahl der Kapazitätsreservierungen pro Pool: 5
- On-Demand-Zuordnungsstrategie `lowest-price` (Wenn mehrere ungenutzte Kapazitätsreservierungen in mehreren Instance-Pools vorhanden sind, bestimmt die Flotte anhand der On-Demand-Zuordnungsstrategie die Pools, in denen die On-Demand-Instances gestartet werden sollen.)

  Beachten Sie, dass Sie auch die `prioritized`-Zuordnungsstrategie anstelle der `lowest-price`-Zuordnungsstrategie verwenden können.

Kapazitätsreservierungen

Das Konto hat die folgenden 15 nicht verwendeten Kapazitätsreservierungen in 3 verschiedenen Pools. Die Anzahl der Kapazitätsreservierungen in jedem Pool wird durch `AvailableInstanceCount` angezeigt.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
```

```
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Flottenkonfiguration

Die folgende Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die gesamte Zielkapazität beträgt 12 und der Standardzielkapazitätstyp ist `on-demand`. Die On-Demand-Zuordnungsstrategie ist `lowest-price`. Die Nutzungsstrategie für Kapazitätsreservierungen ist `use-capacity-reservations-first`.

In diesem Beispiel ist der On-Demand-Instance-Preis:

- `m5.large` - 0,096 USD pro Stunde
- `m4.xlarge` - 0,20 USD pro Stunde
- `m4.2xlarge` - 0,40 USD pro Stunde

> **Note**
>
> Der Flottentyp muss vom Typ `instant` sein. Andere Flotten-Typen unterstützen `use-capacity-reservations-first` nicht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateId": "lt-abc1234567example",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 12,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Nachdem Sie die `instant`-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 12 Instances gestartet, um die Zielkapazität zu erreichen:

- 5 `m5.large` On-Demand-Instances in `us-east-1a` – `m5.large` in `us-east-1a` ist der niedrigste Preis, und es gibt fünf verfügbare ungenutzte `m5.large`-Kapazitätsreservierungen
- 5 `m4.xlarge`-On-Demand-Instances in us-east-1a – `m4.xlarge` in `us-east-1a` ist der niedrigste Preis und es gibt fünf verfügbare ungenutzte `m4.xlarge`-Kapazitätsreservierungen.
- 2 `m4.2xlarge`-On-Demand-Instances in us-east-1a – `m4.2xlarge` in `us-east-1a` ist der drittniedrigste Preis und es gibt fünf verfügbare, nicht verwendete `m4.2xlarge`-Kapazitätsreservierungen, von denen nur zwei benötigt werden, um die Zielkapazität zu erfüllen

Nachdem die Flotte gestartet wurde, können Sie describe-capacity-reservations ausführen, um zu sehen, wie viele nicht verwendete Kapazitätsreservierungen noch übrig sind. In diesem Beispiel sollten Sie die folgende Antwort sehen, die zeigt, dass alle `m5.large`- und `m4.xlarge`-Kapazitätsreservierungen verwendet wurden, wobei 3 `m4.2xlarge`-Kapazitätsreservierungen nicht verwendet wurden.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 3
}
```

Beispiel 5: Starten Sie On-Demand-Instances mithilfe von Kapazitätsreservierungen, wenn die gesamte Zielkapazität die Anzahl der ungenutzten Kapazitätsreservierungen übersteigt

Sie können eine Flotte so konfigurieren, dass sie On-Demand-Kapazitätsreservierungen zuerst beim Start von On-Demand-Instances verwendet, indem Sie die Nutzungsstrategie für Kapazitätsreservierungen auf `use-capacity-reservations-first` festlegen. Dieses

Beispiel zeigt, wie die Flotte die Instance-Pools auswählt, in denen On-Demand-Instances gestartet werden sollen, wenn die gesamte Zielkapazität die Anzahl der verfügbaren ungenutzten Kapazitätsreservierungen überschreitet.

In diesem Beispiel sieht die Flottenkonfiguration wie folgt aus:

- Zielkapazität: 16 On-Demand-Instances
- Gesamt nicht verwendete Kapazitätsreservierungen: 15 (weniger als die On-Demand-Zielkapazität der Flotte von 16 On-Demand-Instances)
- Anzahl der Kapazitätsreservierungspools: 3 (`m5.large`, `m4.xlarge`, und `m4.2xlarge`)
- Anzahl der Kapazitätsreservierungen pro Pool: 5
- On-Demand-Zuordnungsstrategie: `lowest-price` (Wenn die Anzahl der nicht genutzten Kapazitätsreservierungen kleiner als die On-Demand-Zielkapazität ist, bestimmt die Flotte die Pools, in denen die verbleibende On-Demand-Kapazität basierend auf der On-Demand-Zuordnungsstrategie gestartet werden soll.)

  Beachten Sie, dass Sie auch die `prioritized`-Zuordnungsstrategie anstelle der `lowest-price`-Zuordnungsstrategie verwenden können.

Kapazitätsreservierungen

Das Konto hat die folgenden 15 nicht verwendeten Kapazitätsreservierungen in 3 verschiedenen Pools. Die Anzahl der Kapazitätsreservierungen in jedem Pool wird durch `AvailableInstanceCount` angezeigt.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "InstancePlatform": "Linux/UNIX",
```

```
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount":5,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Flottenkonfiguration

Die folgende Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die gesamte Zielkapazität beträgt 16 und der Standardzielkapazitätstyp ist `on-demand`. Die On-Demand-Zuordnungsstrategie ist `lowest-price`. Die Nutzungsstrategie für Kapazitätsreservierungen ist `use-capacity-reservations-first`.

In diesem Beispiel ist der On-Demand-Instance-Preis:

- m5.large – 0,096 USD pro Stunde
- m4.xlarge – 0,20 USD pro Stunde
- m4.2xlarge – 0,40 USD pro Stunde

> **Note**
>
> Der Flottentyp muss `instant` sein. Andere Flotten-Typen unterstützen `use-capacity-reservations-first` nicht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
```

```
                "LaunchTemplateId": "lt-0e8c754449b27161c",
                "Version": "1"
            }
            "Overrides": [
                {
                  "InstanceType": "m5.large",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                },
                {
                  "InstanceType": "m4.2xlarge",
                  "AvailabilityZone": "us-east-1a",
                  "WeightedCapacity": 1
                }
              ]

        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 16,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
        "CapacityReservationOptions": {
            "UsageStrategy": "use-capacity-reservations-first"
        }
    },
    "Type": "instant",
}
```

Nachdem Sie die `instant`-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 16 Instances gestartet, um die Zielkapazität zu erreichen:

- 6 `m5.large`-On-Demand-Instances in `us-east-1a` – `m5.large` in `us-east-1a` ist der niedrigste Preis, und es gibt fünf verfügbare ungenutzte `m5.large`-Kapazitätsreservierungen. Die Kapazitätsreservierungen werden zuerst verwendet, um 5 On-Demand-Instances zu starten. Nachdem die verbleibenden `m4.xlarge`- und `m4.2xlarge`-Kapazitätsreservierungen genutzt

werden, um die Zielkapazität zu erreichen, wird eine zusätzliche On-Demand-Instance gemäß der On-Demand-Zuordnungsstrategie gestartet, die in diesem Beispiel `lowest-price` ist.

- 5 `m4.xlarge` On-Demand-Instances in `us-east-1a` – `m4.xlarge` in `us-east-1a` ist der zweitniedrigste Preis, und es gibt fünf verfügbare ungenutzte `m4.xlarge`-Kapazitätsreservierungen
- 5 `m4.2xlarge` On-Demand-Instances in `us-east-1a` – `m4.2xlarge` in `us-east-1a` ist der drittniedrigste Preis, und es gibt fünf verfügbare ungenutzte `m4.2xlarge`-Kapazitätsreservierungen

Nachdem die Flotte gestartet wurde, können Sie describe-capacity-reservations ausführen, um zu sehen, wie viele nicht verwendete Kapazitätsreservierungen noch übrig sind. In diesem Beispiel sollte die folgende Antwort angezeigt werden, die zeigt, dass alle Kapazitätsreservierungen in allen Pools verwendet wurden.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "m5.large",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "m4.xlarge",
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-333",
    "InstanceType": "m4.2xlarge",
    "AvailableInstanceCount": 0
}
```

Beispiel 6: Starten Sie On-Demand-Instances mithilfe gezielter Kapazitätsreservierungen

Sie können eine Flotte so konfigurieren, dass sie `targeted`-On-Demand-Kapazitätsreservierungen zuerst beim Start von On-Demand-Instances verwendet, indem Sie die Nutzungsstrategie für Kapazitätsreservierungen auf `use-capacity-reservations-first` festlegen. In diesem Beispiel wird gezeigt, wie On-Demand-Instances in `targeted`-Kapazitätsreservierungen, bei denen die

Attribute der Kapazitätsreservierungen mit Ausnahme ihrer Availability Zones (`us-east-1a` und `us-east-1b`) gleich sind. Außerdem wird veranschaulicht, wie die Flotte die Instance-Pools auswählt, in denen On-Demand-Instances gestartet werden sollen, wenn die gesamte Zielkapazität die Anzahl der verfügbaren ungenutzten Kapazitätsreservierungen überschreitet.

In diesem Beispiel sieht die Flottenkonfiguration wie folgt aus:

- Zielkapazität: 10 On-Demand-Instances
- Nicht verwendete `targeted`-Kapazitätsreservierungen: 6 (geringer als die On-Demand-Zielkapazität der Flotte von 10 On-Demand-Instances)
- Anzahl der Kapazitätsreservierungspools: 2 (`us-east-1a` und `us-east-1b`)
- Anzahl der Kapazitätsreservierungen pro Pool: 3
- On-Demand-Zuordnungsstrategie: `lowest-price` (Wenn die Anzahl der nicht genutzten Kapazitätsreservierungen kleiner als die On-Demand-Zielkapazität ist, bestimmt die Flotte die Pools, in denen die verbleibende On-Demand-Kapazität basierend auf der On-Demand-Zuordnungsstrategie gestartet werden soll.)

  Beachten Sie, dass Sie auch die `prioritized`-Zuordnungsstrategie anstelle der `lowest-price`-Zuordnungsstrategie verwenden können.

Einen Walkthrough zu den Verfahren, die Sie ausführen müssen, um dieses Beispiel zu erreichen, finden Sie unter Tutorial: Starten von On-Demand-Instances mithilfe von Kapazitätsreservierungen.

Kapazitätsreservierungen

Das Konto hat die folgenden 6 nicht verwendeten Kapazitätsreservierungen in 2 verschiedenen Pools. In diesem Beispiel unterscheiden sich die Pools durch ihre Availability Zones. Die Anzahl der Kapazitätsreservierungen in jedem Pool wird durch `AvailableInstanceCount` angezeigt.


```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1a",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

```
{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "InstancePlatform": "Linux/UNIX",
    "AvailabilityZone": "us-east-1b",
    "AvailableInstanceCount": 3,
    "InstanceMatchCriteria": "open",
    "State": "active"
}
```

Flottenkonfiguration

Die folgende Flottenkonfiguration zeigt nur die relevanten Konfigurationen für dieses Beispiel. Die gesamte Zielkapazität beträgt 10 und der Standardzielkapazitätstyp ist `on-demand`. Die On-Demand-Zuordnungsstrategie ist `lowest-price`. Die Nutzungsstrategie für Kapazitätsreservierungen ist `use-capacity-reservations-first`.

In diesem Beispiel ist der On-Demand-Instance-Preis für `c5.xlarge` in `us-east-1` 0,17 USD pro Stunde.

> **Note**
>
> Der Flottentyp muss `instant` sein. Andere Flotten-Typen unterstützen `use-capacity-reservations-first` nicht.

```
{
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
            "Overrides": [
               {
                   "InstanceType": "c5.xlarge",
                   "AvailabilityZone": "us-east-1a"
               },
               {
                    "InstanceType": "c5.xlarge",
                    "AvailabilityZone": "us-east-1b"
               }
```

```
            ]
        }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 10,
        "DefaultTargetCapacityType": "on-demand"
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price",
        "CapacityReservationOptions": {
             "UsageStrategy": "use-capacity-reservations-first"
         }
    },
    "Type": "instant"
}
```

Nachdem Sie die `instant`-Flotte mit der vorherigen Konfiguration erstellt haben, werden die folgenden 10 Instances gestartet, um die Zielkapazität zu erreichen:

- Die Kapazitätsreservierungen werden zuerst verwendet, um 6 On-Demand-Instances wie folgt zu starten:
  - 3 On-Demand-Instances werden in die 3 `c5.xlarge` `targeted`Kapazitätsreservierungen in `us-east-1a` gestartet
  - 3 On-Demand-Instances werden in die 3 `c5.xlarge` `targeted`Kapazitätsreservierungen in `us-east-1b` gestartet
- Um die Zielkapazität zu erreichen, werden 4 zusätzliche On-Demand-Instances gemäß der On-Demand-Zuordnungsstrategie in die reguläre On-Demand-Strategie gestartet, die in diesem Beispiel `lowest-price` ist. Da die Pools jedoch denselben Preis haben (da der Preis pro Region und nicht pro Availability Zone ist), startet die Flotte die restlichen 4 On-Demand-Instances in einem der Pools.

Nachdem die Flotte gestartet wurde, können Sie describe-capacity-reservations ausführen, um zu sehen, wie viele nicht verwendete Kapazitätsreservierungen noch übrig sind. In diesem Beispiel sollte die folgende Antwort angezeigt werden, die zeigt, dass alle Kapazitätsreservierungen in allen Pools verwendet wurden.

```
{
    "CapacityReservationId": "cr-111",
    "InstanceType": "c5.xlarge",
```

```
    "AvailableInstanceCount": 0
}

{
    "CapacityReservationId": "cr-222",
    "InstanceType": "c5.xlarge",
    "AvailableInstanceCount": 0
}
```

Beispiel 7: Konfigurieren Sie den Kapazitätsausgleich, um Ersatz-Spot-Instances zu starten

Im folgenden Beispiel wird die EC2-Flotte so konfiguriert, dass eine Ersatz-Spot-Instance gestartet wird, wenn Amazon EC2 eine Neuausgleichsempfehlung für eine Spot-Instance in der Flotte ausgibt. Um die automatische Ersetzung von Spot-Instances zu konfigurieren, geben Sie für `ReplacementStrategy` `launch-before-terminate` an. Um die Zeitverzögerung vom Start der neuen Ersatz-Spot-Instances bis zum automatischen Löschen der alten Spot-Instances zu konfigurieren, geben Sie für `termination-delay` einen Wert in Sekunden an. Weitere Informationen finden Sie unter Konfigurationsoptionen.

> **Note**
>
> Wir empfehlen die Verwendung von `launch-before-terminate` nur wenn Sie vorhersagen können, wie lange Ihre Verfahren zum Herunterfahren der Instances dauern werden, damit die alten Instances erst beendet werden, nachdem diese Verfahren abgeschlossen sind. Ihnen werden alle Instances in Rechnung gestellt, während sie ausgeführt werden.

Die Wirksamkeit der Kapazitätsausgleichsstrategie hängt von der Anzahl der in der EC2-Flotte-Anforderung angegebenen Spot-Kapazitätspools ab. Wir empfehlen, dass Sie die Flotte mit einem diversifizierten Satz von Instance-Typen und Availability Zones konfigurieren und für `AllocationStrategy` `capacity-optimized` angeben. Weitere Informationen darüber, was Sie bei der Konfiguration eines EC2-Flotte für einen Kapazitätsausgleich beachten sollten, finden Sie unter Kapazitätsausgleich.

```
{
    "ExcessCapacityTerminationPolicy": "termination",
    "LaunchTemplateConfigs": [
```

```
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "LaunchTemplate",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "c3.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c4.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       },
                       {
                           "InstanceType": "c5.large",
                           "WeightedCapacity": 1,
                            "Placement": {
                               "AvailabilityZone": "us-east-1a"
                           }
                       }
                ]
          }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 5,
        "DefaultTargetCapacityType": "spot"
    },
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        "MaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
```

```
}
```

Beispiel 8: Starten Sie Spot-Instances in einer kapazitätsoptimierten Flotte

Im folgenden Beispiel wird veranschaulicht, wie eine EC2-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die die Kapazität optimiert. Um die Kapazität zu optimieren, müssen Sie `AllocationStrategy` auf `capacity-optimized` festlegen.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Die Zielkapazität beträgt 50 Spot-Instances. Die EC2-Flotte versucht, 50 Spot-Instances in dem Spot-Kapazitätspool zu starten, der über die optimale Kapazität für die Anzahl der zu startenden Instances verfügt.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized",
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
```

```
                ]
            }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"

    }
}
```

Beispiel 9: Starten Sie Spot-Instances in einer kapazitätsoptimierten Flotte mit Prioritäten

Im folgenden Beispiel wird veranschaulicht, wie eine EC2-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die die Kapazität optimiert und dabei die Priorität so weit wie möglich berücksichtigt.

Bei Verwendung der `capacity-optimized-prioritized`-Zuweisungsstrategie können Sie den `Priority`-Parameter verwenden, um die Prioritäten der Spot-Kapazitätspools anzugeben. Je niedriger die Zahl ist, desto höher ist die Priorität. Sie können die gleiche Priorität auch für mehrere Spot-Kapazitätspools festlegen, wenn sie für Sie die gleiche Priorität haben. Wenn Sie keine Priorität für einen Pool festlegen, wird für den Pool die niedrigste Priorität angenommen.

Um Spot-Kapazitätspools zu priorisieren, müssen Sie `AllocationStrategy` auf `capacity-optimized-prioritized` festlegen. Die EC2-Flotte wird zuerst für die Kapazität optimiert, berücksichtigt jedoch so gut wie möglich die Prioritäten (wenn z. B. die Berücksichtigung der Prioritäten keinen wesentlichen Einfluss auf die Fähigkeit der EC2-Flotte zur Bereitstellung optimaler Kapazität hat). Dies ist eine gute Option für Workloads, bei denen die Möglichkeit von Unterbrechungen minimiert werden muss und die Präferenz für bestimmte Instance-Typen wichtig ist.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Jeder Pool wird priorisiert. Je niedriger die Zahl ist, desto höher ist die Priorität. Die Zielkapazität beträgt 50 Spot-Instances. Die EC2-Flotte versucht nach Möglichkeit, 50 Spot-Instances in dem Spot-Kapazitätspool mit der höchsten Priorität zu starten. Zuerst optimiert sie jedoch die Kapazität.

```
{
    "SpotOptions": {
        "AllocationStrategy": "capacity-optimized-prioritized"
        },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
```

```
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "Placement": {
                                "AvailabilityZone": "us-west-2a"
                            },
                        },
                         {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            },
                         },
                         {
                            "InstanceType": "c5.2xlarge",
                            "Priority": 3,
                            "Placement": {
                                "AvailabilityZone": "us-west-2b"
                            }
                         }
                    ]
             }
    ],
    "TargetCapacitySpecification": {
            "TotalTargetCapacity": 50,
            "DefaultTargetCapacityType": "spot"
}
```

Beispiel 10: Starten Sie Spot-Instances in einer Flotte price-capacity-optimized

Im folgenden Beispiel wird veranschaulicht, wie eine EC2-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die sowohl die Kapazität als auch den Preis optimiert. Um die Kapazität zu optimieren und gleichzeitig den Preis zu berücksichtigen, müssen Sie den Spot `AllocationStrategy` auf `price-capacity-optimized` setzen.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Die Zielkapazität beträgt 50 Spot-Instances. Die EC2-Flotte versucht, 50 Spot Instances in dem Spot-

Kapazitätspool zu starten, der über die optimale Kapazität für die Anzahl der zu startenden Instances verfügt, und gleichzeitig den günstigsten Pool auszuwählen.

```
{
    "SpotOptions": {
        "AllocationStrategy": "price-capacity-optimized",
        "MinTargetCapacity": 2,
        "SingleInstanceType": true
    },
    "OnDemandOptions": {
        "AllocationStrategy": "lowest-price"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2a"
                           },
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           },
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "Placement": {
                               "AvailabilityZone": "us-west-2b"
                           }
                       }
                  ]
           }
    ],
    "TargetCapacitySpecification": {
        "TotalTargetCapacity": 50,
        "OnDemandTargetCapacity":0,
```

```
        "SpotTargetCapacity":50,
        "DefaultTargetCapacityType": "spot"
    },
    "Type": "instant"
}
```

Beispiel 11: Konfigurieren Sie die attributbasierte Auswahl des Instance-Typs

Im folgenden Beispiel wird veranschaulicht, wie eine EC2-Flotte so konfiguriert wird, dass sie die attributbasierte Instance-Typauswahl zur Identifizierung von Instance-Typen verwendet. Um die erforderlichen Instance-Attribute anzugeben, geben Sie die Attribute in der `InstanceRequirements`-Struktur an.

Im folgenden Beispiel werden zwei Instance-Attribute angegeben:

- `VCpuCount` – Es sind mindestens 2 vCPUs angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.
- `MemoryMiB` – Es werden mindestens 4 MiB Arbeitsspeicher angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.

Alle Instance-Typen mit 2 oder mehr vCPUs und 4 MiB oder mehr Arbeitsspeicher werden identifiziert. Der Preisschutz und die Zuweisungsstrategie könnten jedoch einige Instance-Typen ausschließen, wenn die EC2-Flotte die Flotte bereitstellt.

Eine Liste und Beschreibungen aller möglichen Attribute, die Sie angeben können, finden Sie InstanceRequirementsin der Amazon EC2 API-Referenz.

```
{
 "SpotOptions": {
  "AllocationStrategy": "price-capacity-optimized"
 },
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
```

```
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }],
 "TargetCapacitySpecification": {
  "TotalTargetCapacity": 20,
  "DefaultTargetCapacityType": "spot"
 },
 "Type": "instant"
}
```

Beispielkonfigurationen für Spot-Flotte

Die folgenden Beispiele zeigen Startkonfigurationen, die Sie mit dem Befehl request-spot-fleet zum Erstellen einer Spot-Flotten-Anforderung verwenden können. Weitere Informationen finden Sie unter Erstellen eine Spot-Flotten-Anforderung.

> **Note**
>
> Für eine Spot-Flotte können Sie in einer Startvorlage oder Startspezifikation keine Netzwerkschnittstellen-ID angeben. Achten Sie darauf, dass Sie den `NetworkInterfaceID`-Parameter in Ihrer Startvorlage oder -spezifikation weglassen.

Beispiele

- Beispiel 1: Starten von Spot-Instances mit der kostengünstigsten Availability Zone oder dem kostengünstigsten Subnetz in der Region
- Beispiel 2: Starten von Spot-Instances mit der kostengünstigsten Availability Zone oder dem kostengünstigsten Subnetz in einer angegebenen Liste
- Beispiel 3: Starten von Spot-Instances mit dem kostengünstigsten Instance-Typ in einer angegebenen Liste
- Beispiel 4. Außerkraftsetzen des Preises für die Anforderung
- Beispiel 5: Starten einer Spot-Flotte mit der diversifizierten Zuweisungsstrategie
- Beispiel 6: Starten einer Spot-Flotte mit Instance-Gewichtung
- Beispiel 7: Starten einer Spot-Flotte mit On-Demand-Kapazität

Beispiel 1: Starten von Spot-Instances mit der kostengünstigsten Availability Zone oder dem kostengünstigsten Subnetz in der Region

Das folgende Beispiel gibt eine einzelne Startspezifikation ohne eine Availability Zone oder ein Subnetz an. Die Spot-Flotte startet die Instances in der kostengünstigsten Availability Zone mit einem Standard-Subnetz. Der Preis, den Sie zahlen, wird den On-Demand-Preis nicht überschreiten.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Beispiel 2: Starten von Spot-Instances mit der kostengünstigsten Availability Zone oder dem kostengünstigsten Subnetz in einer angegebenen Liste

Die folgenden Beispiele geben zwei Startspezifikationen mit verschiedenen Availability Zones oder Subnetzen, aber demselben Instance-Typ und AMI an.

Availability Zones

Die Spot-Flotte startet die Instances in dem Standard-Subnetz der kostengünstigsten Availability Zone, die Sie angegeben haben.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "KeyName": "my-key-pair",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "m3.medium",
          "Placement": {
              "AvailabilityZone": "us-west-2a, us-west-2b"
          },
          "IamInstanceProfile": {
              "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
          }
      }
  ]
}
```

Subnets

Sie können Standardsubnetze oder nicht standardmäßige Subnetze angeben. Die nicht standardmäßigen Subnetze können zu einer Standard-VPC oder einer nicht standardmäßigen VPC gehören. Der Spot-Service startet die Instances in dem Subnetz in der kostengünstigsten Availability Zone.

Sie können in einer Spot-Flotten-Anforderung nicht verschiedene Subnetze in derselben Availability Zone angeben.

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
```

```
            "ImageId": "ami-1a2b3c4d",
            "KeyName": "my-key-pair",
            "SecurityGroups": [
                {
                    "GroupId": "sg-1a2b3c4d"
                }
            ],
            "InstanceType": "m3.medium",
            "SubnetId": "subnet-a61dafcf, subnet-65ea5f08",
            "IamInstanceProfile": {
                "Arn": "arn:aws:iam::123456789012:instance-profile/my-iam-role"
            }
        }
    ]
}
```

Wenn die Instances in einer Standard-VPC gestartet werden, erhalten sie standardmäßig eine öffentliche IPv4-Adresse. Wenn die Instances in einer nicht standardmäßigen VPC gestartet werden, erhalten sie standardmäßig keine öffentliche IPv4-Adresse. Verwenden Sie eine Netzwerkschnittstelle in der Startspezifikation, um Instances, die in einer nicht standardmäßigen VPC gestartet wurden, eine öffentliche IPv4-Adresse zuzuweisen. Wenn Sie eine Netzwerkschnittstelle angeben, müssen Sie die Subnetz-ID und die Sicherheitsgruppen-ID mithilfe der Netzwerkschnittstelle angeben.

```
    ...
        {
            "ImageId": "ami-1a2b3c4d",
            "KeyName": "my-key-pair",
            "InstanceType": "m3.medium",
            "NetworkInterfaces": [
                {
                    "DeviceIndex": 0,
                    "SubnetId": "subnet-1a2b3c4d",
                    "Groups": [ "sg-1a2b3c4d" ],
                    "AssociatePublicIpAddress": true
                }
            ],
            "IamInstanceProfile": {
                "Arn": "arn:aws:iam::880185128111:instance-profile/my-iam-role"
            }
        }
    ...
```

Beispiel 3: Starten von Spot-Instances mit dem kostengünstigsten Instance-Typ in einer angegebenen Liste

Die folgenden Beispiele geben zwei Startkonfigurationen mit verschiedenen Instance-Typen, aber demselben AMI sowie derselben Availability Zone bzw. demselben Subnetz an. Die Spot-Flotte startet die Instances mit dem angegebenen Instance-Typ mit dem niedrigsten Preis.

Availability Zone

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "Placement": {
            "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Subnetz

```
{
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "c5.4xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "SecurityGroups": [
              {
                  "GroupId": "sg-1a2b3c4d"
              }
          ],
          "InstanceType": "r3.8xlarge",
          "SubnetId": "subnet-1a2b3c4d"
      }
  ]
}
```

Beispiel 4. Außerkraftsetzen des Preises für die Anforderung

Es wird empfohlen, den Standard-Höchstpreis zu verwenden, bei dem es sich um den On-Demand-Preis handelt. Wenn Sie es vorziehen, können Sie einen Höchstpreis für die Flottenanforderung und Höchstpreise für einzelne Startspezifikationen angeben.

Die folgenden Beispiele geben einen Höchstpreis für die Flottenanforderung und Höchstpreise für zwei oder drei Startspezifikationen an. Der Höchstpreis für die Flottenanforderung wird für alle Startspezifikationen verwendet, die keinen Höchstpreis angeben. Die Spot-Flotte startet die Instances mit dem Instance-Typ mit dem niedrigsten Preis.

Availability Zone

```
{
  "SpotPrice": "1.00",
```

```
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.10"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.4xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          },
          "SpotPrice": "0.20"
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.8xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
    ]
}
```

Subnetz

```
{
  "SpotPrice": "1.00",
  "TargetCapacity": 30,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "SpotPrice": "0.10"
      },
      {
```

```
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.4xlarge",
            "SubnetId": "subnet-1a2b3c4d",
            "SpotPrice": "0.20"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.8xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Beispiel 5: Starten einer Spot-Flotte mit der diversifizierten Zuweisungsstrategie

Im folgenden Beispiel wird die Zuweisungsstrategie `diversified` verwendet. Die Startspezifikationen weisen verschiedene Instance-Typen, aber dasselbe AMI sowie dieselbe Availability Zone bzw. dasselbe Subnetz auf. Die Spot-Flotte verteilt die 30 Instances auf die drei Startspezifikationen, sodass 10 Instances von jedem Typ vorhanden sind. Weitere Informationen finden Sie unter Zuweisungsstrategien für Spot-Instances.

Availability Zone

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
```

```
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      }
  ]
}
```

Subnetz

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-1a2b3c4d"
        }
    ]
}
```

Eine bewährte Methode, um die Wahrscheinlichkeit zu erhöhen, dass eine Spot-Anforderung bei einem Stromausfall in einer der Availability Zones (AZ) von der EC2-Kapazität erfüllt werden kann, ist die Verteilung auf verschiedene Zonen. Für dieses Szenario müssen Sie jede verfügbare Availability Zone in die Startspezifikation einfügen. Und anstatt jedes Mal dasselbe Subnetz zu verwenden, sollten Sie drei eindeutige Subnetze verwenden (die jeweils einer anderen Zone zugeordnet sind).

Availability Zone

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 30,
  "AllocationStrategy": "diversified",
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c4.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2a"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "m3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2b"
          }
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "Placement": {
              "AvailabilityZone": "us-west-2c"
          }
      }
  ]
}
```

Subnetz

```
{
    "SpotPrice": "0.70",
    "TargetCapacity": 30,
    "AllocationStrategy": "diversified",
    "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
    "LaunchSpecifications": [
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c4.2xlarge",
```

```
            "SubnetId": "subnet-1a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "m3.2xlarge",
            "SubnetId": "subnet-2a2b3c4d"
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "r3.2xlarge",
            "SubnetId": "subnet-3a2b3c4d"
        }
    ]
}
```

Beispiel 6: Starten einer Spot-Flotte mit Instance-Gewichtung

Die folgenden Beispiele verwenden die Instance-Gewichtung, d. h. der Preis versteht sich pro Einheitsstunde anstatt pro Instance-Stunde. Jede Startkonfigurationen listet einen anderen Instance-Typ und eine andere Gewichtung auf. Die Spot-Flotte wählt den Instance-Typ mit dem niedrigsten Preis pro Einheitsstunde aus. Die Spot-Flotte berechnet die Anzahl der zu startenden Spot-Instances, indem die Zielkapazität durch die Instance-Gewichtung dividiert wird. Wenn es sich beim Ergebnis nicht um eine Ganzzahl handelt, rundet die Spot-Flotte es auf die nächste Ganzzahl auf, damit die Größe Ihrer Flotte nicht unter der Zielkapazität liegt.

Wenn die `r3.2xlarge`-Anforderung erfolgreich ist, stellt Spot 4 dieser Instances bereit. 20 geteilt durch 6 ergibt insgesamt 3,33 Instances; dies wird auf 4 Instances aufgerundet.

Wenn die `c3.xlarge`-Anforderung erfolgreich ist, stellt Spot 7 dieser Instances bereit. 20 geteilt durch 3 ergibt insgesamt 6,66 Instances; dies wird auf 7 Instances aufgerundet.

Weitere Informationen finden Sie unter Instance-Gewichtung für Spot-Flotten.

Availability Zone

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
```

```
            "InstanceType": "r3.2xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
            "WeightedCapacity": 6
        },
        {
            "ImageId": "ami-1a2b3c4d",
            "InstanceType": "c3.xlarge",
            "Placement": {
                "AvailabilityZone": "us-west-2b"
            },
            "WeightedCapacity": 3
        }
    ]
}
```

Subnetz

```
{
  "SpotPrice": "0.70",
  "TargetCapacity": 20,
  "IamFleetRole": "arn:aws:iam::123456789012:role/aws-ec2-spot-fleet-tagging-role",
  "LaunchSpecifications": [
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "r3.2xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 6
      },
      {
          "ImageId": "ami-1a2b3c4d",
          "InstanceType": "c3.xlarge",
          "SubnetId": "subnet-1a2b3c4d",
          "WeightedCapacity": 3
      }
  ]
}
```

Beispiel 7: Starten einer Spot-Flotte mit On-Demand-Kapazität

Um sicherzustellen, dass Sie immer über Instance-Kapazität verfügen, können Sie eine Anforderung nach On-Demand-Kapazität in Ihre Spot-Flotten-Anforderung aufnehmen. Wenn Kapazität vorhanden

ist, ist die On-Demand-Anfrage immer erfüllt. Der Saldo der Zielkapazität wird als Spot erfüllt, wenn Kapazität und Verfügbarkeit vorhanden sind.

Das folgende Beispiel gibt die gewünschte Zielkapazität als 10 an, von denen 5 On-Demand-Kapazität sein müssen. Die Spot-Kapazität wird nicht angegeben; sie ergibt sich aus dem Betrag der Zielkapazität abzüglich der On-Demand-Kapazität. Amazon EC2 startet 5 Kapazitätseinheiten als On-Demand und 5 Kapazitätseinheiten (10–5=5) als Spot, wenn Amazon EC2-Kapazität und Verfügbarkeit vorhanden sind.

Weitere Informationen finden Sie unter On-Demand-Kapazität in Spot-Flotten.

```
{
  "IamFleetRole": "arn:aws:iam::781603563322:role/aws-ec2-spot-fleet-tagging-role",
  "AllocationStrategy": "lowestPrice",
  "TargetCapacity": 10,
  "SpotPrice": null,
  "ValidFrom": "2018-04-04T15:58:13Z",
  "ValidUntil": "2019-04-04T15:58:13Z",
  "TerminateInstancesWithExpiration": true,
  "LaunchSpecifications": [],
  "Type": "maintain",
  "OnDemandTargetCapacity": 5,
  "LaunchTemplateConfigs": [
    {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "lt-0dbb04d4a6cca5ad1",
        "Version": "2"
      },
      "Overrides": [
        {
          "InstanceType": "t2.medium",
          "WeightedCapacity": 1,
          "SubnetId": "subnet-d0dc51fb"
        }
      ]
    }
  ]
}
```

Beispiel 8: Konfigurieren des Kapazitätsneuausgleichs, um den Ersatz Spot-Instances zu starten

Im folgenden Beispiel wird die Spot-Flotte so konfiguriert, dass eine Ersatz-Spot-Instance gestartet wird, wenn Amazon EC2 eine Neuausgleichsempfehlung für eine Spot-Instance in der Flotte ausgibt. Um die automatische Ersetzung von Spot-Instances zu konfigurieren, geben Sie für `ReplacementStrategy` `launch-before-terminate` an. Um die Zeitverzögerung vom Start der neuen Ersatz-Spot-Instances bis zum automatischen Löschen der alten Spot-Instances zu konfigurieren, geben Sie für `termination-delay` einen Wert in Sekunden an. Weitere Informationen finden Sie unter Konfigurationsoptionen.

> **Note**
>
> Wir empfehlen die Verwendung von `launch-before-terminate` nur, wenn Sie vorhersagen können, wie lange Ihre Verfahren zum Herunterfahren der Instances dauern werden. Dadurch wird sichergestellt, dass die alten Instances erst beendet werden, wenn die Verfahren zum Herunterfahren abgeschlossen sind. Ihnen werden alle Instances in Rechnung gestellt, während sie ausgeführt werden.

Die Wirksamkeit der Kapazitätsneuausgleichsstrategie hängt von der Anzahl der in der Spot-Flotten-Anforderung angegebenen Spot-Kapazitätspools ab. Wir empfehlen, dass Sie die Flotte mit einem diversifizierten Satz von Instance-Typen und Availability Zones konfigurieren und für `AllocationStrategy` `capacityOptimized` angeben. Weitere Informationen darüber, was Sie bei der Konfiguration einer Spot-Flotte für einen Kapazitätsneuausgleich beachten sollten, finden Sie unter Kapazitätsausgleich.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
        "IamFleetRole": "arn:aws:iam::000000000000:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateName": "LaunchTemplate",
                    "Version": "1"
                },
                 "Overrides": [
```

```
                        {
                            "InstanceType": "c3.large",
                            "WeightedCapacity": 1,
                            "Placement": {
                                "AvailabilityZone": "us-east-1a"
                            }
                        },
                        {
                            "InstanceType": "c4.large",
                            "WeightedCapacity": 1,
                            "Placement": {
                                "AvailabilityZone": "us-east-1a"
                            }
                        },
                        {
                            "InstanceType": "c5.large",
                            "WeightedCapacity": 1,
                            "Placement": {
                                "AvailabilityZone": "us-east-1a"
                            }
                        }
                ]
          }
    ],
        "TargetCapacity": 5,
        "SpotMaintenanceStrategies": {
            "CapacityRebalance": {
                "ReplacementStrategy": "launch-before-terminate",
                "TerminationDelay": "720"
            }
        }
    }
}
```

Beispiel 9: Starten von Spot-Instances in einer kapazitätsoptimierten Flotte

Im folgenden Beispiel wird veranschaulicht, wie eine Spot-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die die Kapazität optimiert. Um die Kapazität zu optimieren, müssen Sie `AllocationStrategy` auf `capacityOptimized` festlegen.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Die Zielkapazität beträgt 50 Spot-Instances. Die Spot-Flotte versucht, 50 Spot-Instances in dem Spot-

Kapazitätspool zu starten, der über die optimale Kapazität für die Anzahl der zu startenden Instances verfügt.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimized",
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                       {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                       {
                           "InstanceType": "m4.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                       },
                       {
                           "InstanceType": "c5.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                       }
                ]
           }
      ]
}
```

Beispiel 10: Starten von Spot-Instances in einer kapazitätsoptimierten Flotte mit Prioritäten

Im folgenden Beispiel wird veranschaulicht, wie eine Spot-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die die Kapazität optimiert und dabei die Priorität so weit wie möglich berücksichtigt.

Bei Verwendung der `capacityOptimizedPrioritized`-Zuweisungsstrategie können Sie den `Priority`-Parameter verwenden, um die Prioritäten der Spot-Kapazitätspools anzugeben. Je niedriger die Zahl ist, desto höher ist die Priorität. Sie können die gleiche Priorität auch für mehrere

Spot-Kapazitätspools festlegen, wenn sie für Sie die gleiche Priorität haben. Wenn Sie keine Priorität für einen Pool festlegen, wird für den Pool die niedrigste Priorität angenommen.

Um Spot-Kapazitätspools zu priorisieren, müssen Sie `AllocationStrategy` auf `capacityOptimizedPrioritized` festlegen. Die Spot-Flotte wird zuerst für die Kapazität optimiert, berücksichtigt jedoch so gut wie möglich die Prioritäten (wenn z. B. die Berücksichtigung der Prioritäten keinen wesentlichen Einfluss auf die Fähigkeit der Spot-Flotte zur Bereitstellung optimaler Kapazität hat). Dies ist eine gute Option für Workloads, bei denen die Möglichkeit von Unterbrechungen minimiert werden muss und die Präferenz für bestimmte Instance-Typen wichtig ist.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Jeder Pool wird priorisiert. Je niedriger die Zahl ist, desto höher ist die Priorität. Die Zielkapazität beträgt 50 Spot-Instances. Die Spot-Flotte versucht nach Möglichkeit, 50 Spot-Instances in dem Spot-Kapazitätspool mit der höchsten Priorität zu starten. Zuerst optimiert sie jedoch die Kapazität.

```
{
    "TargetCapacity": "50",
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "capacityOptimizedPrioritized"
    },
    "LaunchTemplateConfigs": [
        {
            "LaunchTemplateSpecification": {
                "LaunchTemplateName": "my-launch-template",
                "Version": "1"
            },
                 "Overrides": [
                        {
                            "InstanceType": "r4.2xlarge",
                            "Priority": 1,
                            "AvailabilityZone": "us-west-2a"
                       },
                        {
                            "InstanceType": "m4.2xlarge",
                            "Priority": 2,
                            "AvailabilityZone": "us-west-2b"
                        },
                        {
                            "InstanceType": "c5.2xlarge",
                            "Priority": 3,
                            "AvailabilityZone": "us-west-2b"
                        }
```

```
                ]
            }
        ]
}
```

Beispiel 11: Spot-Instances in einer priceCapacityOptimized Flotte starten

Im folgenden Beispiel wird veranschaulicht, wie eine Spot-Flotte mit einer Spot-Zuweisungsstrategie konfiguriert wird, die sowohl die Kapazität als auch den Preis optimiert. Um die Kapazität zu optimieren und gleichzeitig den Preis zu berücksichtigen, müssen Sie den Spot `AllocationStrategy` auf `priceCapacityOptimized` setzen.

Im folgenden Beispiel geben die drei Startspezifikationen drei Spot-Kapazitätspools an. Die Zielkapazität beträgt 50 Spot-Instances. Die Spot-Flotte versucht, 50 Spot Instances in dem Spot-Kapazitätspool zu starten, der über die optimale Kapazität für die Anzahl der zu startenden Instances verfügt und gleichzeitig den günstigsten Pool auszuwählen.

```
{
    "SpotFleetRequestConfig": {
        "AllocationStrategy": "priceCapacityOptimized",
        "OnDemandAllocationStrategy": "lowestPrice",
        "ExcessCapacityTerminationPolicy": "default",
        "IamFleetRole": "arn:aws:iam::111111111111:role/aws-ec2-spot-fleet-tagging-
role",
        "LaunchTemplateConfigs": [
            {
                "LaunchTemplateSpecification": {
                    "LaunchTemplateId": "lt-0123456789example",
                    "Version": "1"
                },
                "Overrides": [
                     {
                           "InstanceType": "r4.2xlarge",
                           "AvailabilityZone": "us-west-2a"
                      },
                      {
                           "InstanceType": "m4.2xlarge",
                           "AvailabilityZone": "us-west-2b"
                      },
                      {
                           "InstanceType": "c5.2xlarge",
                           "AvailabilityZone": "us-west-2b"
```

```
                    }
                ]
            }
        ],
        "TargetCapacity": 50,
        "Type": "request"
    }
}
```

Beispiel 12: Konfigurieren von attributbasierter Auswahl von Instance-Typen

Im folgenden Beispiel wird veranschaulicht, wie eine Spot-Flotte so konfiguriert wird, dass sie die attributbasierte Instance-Typauswahl zur Identifizierung von Instance-Typen verwendet. Um die erforderlichen Instance-Attribute anzugeben, geben Sie die Attribute in der `InstanceRequirements`-Struktur an.

Im folgenden Beispiel werden zwei Instance-Attribute angegeben:

- `VCpuCount` – Es sind mindestens 2 vCPUs angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.
- `MemoryMiB` – Es werden mindestens 4 MiB Arbeitsspeicher angegeben. Da kein Maximum angegeben ist, gibt es keine Höchstgrenze.

Alle Instance-Typen mit 2 oder mehr vCPUs und 4 MiB oder mehr Arbeitsspeicher werden identifiziert. Der Preisschutz und die Zuweisungsstrategie könnten jedoch einige Instance-Typen ausschließen, wenn die Spot-Flotte die Flotte bereitstellt.

Eine Liste und Beschreibungen aller möglichen Attribute, die Sie angeben können, finden Sie InstanceRequirementsin der Amazon EC2 API-Referenz.

```
{
 "AllocationStrategy": "priceCapacityOptimized",
 "TargetCapacity": 20,
 "Type": "request",
 "LaunchTemplateConfigs": [{
  "LaunchTemplateSpecification": {
   "LaunchTemplateName": "my-launch-template",
   "Version": "1"
  },
  "Overrides": [{
```

```
   "InstanceRequirements": {
    "VCpuCount": {
     "Min": 2
    },
    "MemoryMiB": {
     "Min": 4
    }
   }
  }]
 }]
}
```

Flottenkontingente

Die üblichen Amazon-EC2-Quotas (zuvor als Limits bezeichnet) gelten für Instances, die von einer EC2-Flotte oder einer Spot-Flotte gestartet werden, z. B. Spot-Instance-Limits und Volumen-Limits.

Darüber hinaus gelten die folgenden Quotas:

Quota-Beschreibung	Kontingent
Die Anzahl der EC2-Flotten und Spot-Flotten pro Typregion `maintain` und `request` in den `active` Bundesstaaten, und `deleted_running` `cancelled_running`	1 000 [1] [2] [3]
Die Anzahl der EC2-Flotten des Typs `instant`	Unbegrenzt
Die Anzahl der Spot-Kapazitätspools (eindeutige Kombination aus Instance-Typ und Subnetz) für EC2-Flotten und Spot-Flotten des Typs und `maintain` `request`	300 [1]
Die Anzahl der Spot-Kapazitätspools (eindeutige Kombination aus Instance-Typ und Subnetz) für EC2-Flotten des Typs `instant`	Unbegrenzt
Größe der Benutzerdaten in einer Startspezifikation	16 KB [2]

Quota-Beschreibung	Kontingent
Zielkapazität pro EC2-Flotte oder Spot-Flotte	10.000
Die Zielkapazität in allen EC2-Flotten und Spot-Flotten in einer Region	100 000 [1]
Eine EC2-Flotten- oder Spot-Flotten-Anforderung kann sich nicht über mehrere Regionen erstrecken.	
Eine EC2-Flotten- oder Spot-Flotten-Anforderung kann sich nicht über verschiedene Subnetze in derselben Availability Zone erstrecken.	

[1] Diese Quotas gelten sowohl für EC2-Flotten als auch für Spot-Flotten.

[2] Dabei handelt es sich um feste Quotas. Sie können keine Erhöhung einiger dieser Quotas beantragen.

[3] Nachdem Sie eine EC2-Flotte gelöscht oder eine Spot-Flotte-Anforderung storniert haben und wenn Sie angegeben haben, dass die Flotte ihre Spot-Instances nicht beenden soll, wenn Sie die Anforderung gelöscht oder storniert haben, tritt die Flottenanfrage in den Status `deleted_running` (EC2-Flotte) oder `cancelled_running` (Spot-Flotten-Zustand) und die Instances werden weiter ausgeführt, bis sie unterbrochen oder manuell beendet werden. Wenn Sie die Instances beenden, tritt die Flottenanforderung in den Status `deleted_terminating` (EC2-Flotte) oder `cancelled_terminating` (Spot-Flotte) und wird auf diese Quota angerechnet. Weitere Informationen finden Sie unter Löschen einer EC2-Flotte und Abbrechen einer Spot-Flotten-Anforderung.

Anfordern einer Quota-Erhöhung für die Zielkapazität

Wenn Sie mehr als diese Standard-Quota für die Zielkapazität benötigen, können Sie eine Quota-Erhöhung anfordern.

So fordern Sie eine Quota-Erhöhung für die Zielkapazität an

1. Öffnen Sie das Fallformular AWS Support Center Create.

2. Wählen Sie Service Limit increase (Erhöhung des Servicelimits).
3. Bei Limit type (Limit-Typ) wählen Sie EC2 fleet (EC2-Flotte) aus.
4. Wählen Sie unter Region die AWS Region aus, für die Sie die Erhöhung des Kontingents beantragen möchten.
5. Bei Limit (Limit) wählen Sie Target Fleet Capacity per Fleet (in units) (Zielflottenkapazität pro Flotte (in Einheiten)) oder Target Fleet Capacity per Region (in units) (Zielflottenkapazität pro Region (in Einheiten)) aus, abhängig davon, welche Quota Sie erhöhen möchten.
6. Geben Sie unter New limit value (Neuer Limit-Wert) den neuen Wert ein.
7. Um eine Erhöhung für eine andere Quota anzufordern, wählen Sie Add another request (Weitere Anforderung hinzufügen) aus und wiederholen Sie die Schritte 4 bis 6.
8. Bei Use case description (Beschreibung des Anwendungsfalls) geben Sie Ihren Grund für die Anforderung einer Quota-Erhöhung an.
9. Unter Contact options (Kontakt-Optionen) geben Sie Ihre bevorzugte Kontaktsprache und Kontaktmethode an.
10. Wählen Sie Absenden aus.

Überwachen von Amazon EC2

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer Amazon Elastic Compute Cloud (Amazon EC2) -Instances und Ihrer AWS Lösungen. Sie sollten Überwachungsdaten aus allen Teilen Ihrer AWS Lösungen sammeln, damit Sie einen Fehler an mehreren Stellen leichter debuggen können, falls einer auftritt. Bevor Sie jedoch mit der Überwachung von Amazon EC2 beginnen, sollten Sie einen Überwachungsplan erstellen, der Folgendes enthalten sollte:

- Was sind Ihre Ziele bei der Überwachung?
- Welche Ressourcen werden überwacht?
- Wie oft werden diese Ressourcen überwacht?
- Welche Überwachungstools werden verwendet?
- Wer soll die Überwachungsaufgaben ausführen?
- Wer soll benachrichtigt werden, wenn Fehler auftreten?

Nachdem Sie Ihre Überwachungsziele festgelegt und Ihren Überwachungsplan erstellt haben, legen Sie im nächsten Schritt einen Ausgangswert für normale Amazon EC2-Leistung in Ihrer Umgebung fest. Sie sollten die Amazon EC2-Leistung zu verschiedenen Zeiten und unter verschiedenen Belastungsbedingungen messen. Wenn Sie Amazon EC2 überwachen, sollten Sie einen Verlauf der von Ihnen gesammelten Überwachungsdaten speichern. Sie können die aktuelle Amazon EC2-Leistung mit diesen historischen Daten zur Identifikation normaler Leistungsmuster und Leistungsanomalien sowie zur Entwicklung von Verfahren für deren Handhabung vergleichen. Sie können zum Beispiel die CPU-Verwendung, den Festplatten-I/O-Vorgang und die Netzwerkauslastung für Ihre EC2-Instances überwachen. Wenn die Leistung außerhalb der festgelegten Grundwerte liegt, müssen Sie die Instance neu konfigurieren oder optimieren, um die CPU-Nutzung zu verringern, die Festplatten-I/O zu verbessern oder den Netzwerkverkehr zu reduzieren.

Zur Festlegung eines Grundwertes sollten Sie mindestens die folgenden Elemente überwachen:

Zu überwachendes Element	Amazon EC2-Metrik	Agent/Protokolle überwachen CloudWatch
CPU-Auslastung	CPUUtilization	

Zu überwachendes Element	Amazon EC2-Metrik	Agent/Protokolle überwachen CloudWatch
Netzwerkauslastung	NetworkIn NetworkOut	
Festplattenleistung	DiskReadOperationen DiskWriteOps	
Schreib-/Lesevorgänge	DiskReadByte DiskWriteByte	
Speichernutzung, Festplatten-Swap-Auslastung, Speicherplatzauslastung, Auslastung der Auslagerungsdatei, Protokollerfassung		[Linux- und Windows Server-Instances] Erfassen Sie mit dem Agenten Metriken und Protokolle von Amazon EC2 EC2-Instances und lokalen Servern CloudWatch [Migration von einem vorherigen CloudWatch Logs-Agent auf Windows Server-Instances] Migrieren Sie die Protokollerfassung der Windows Server-Instance auf den Agenten CloudWatch

Automatisierte und manuelle Überwachung

AWS bietet verschiedene Tools, mit denen Sie Amazon EC2 überwachen können. Sie können einige dieser Tools so konfigurieren, dass diese die Überwachung für Sie übernehmen, während bei anderen Tools ein manuelles Eingreifen nötig ist.

Überwachungstools

- Automatisierte Überwachungstools

- Manuelle Überwachungstools

Automatisierte Überwachungstools

Sie können die folgenden automatisierten Tools zur Überwachung von Amazon EC2 verwenden und möglicherweise auftretende Probleme melden:

- Systemstatusprüfungen — Überwachen Sie die AWS Systeme, die für die Nutzung Ihrer Instance erforderlich sind, um sicherzustellen, dass sie ordnungsgemäß funktionieren. Bei diesen Prüfungen werden Probleme mit Ihrer Instance erkannt, bei deren Behebung ein AWS Eingreifen erforderlich ist. Wenn eine System-Statusprüfung fehlschlägt, können Sie wählen, bis AWS das Problem behebt oder Sie können es selbst lösen (zum Beispiel per Anhalten und Neustarten einer Instance oder deren Beendigung und Ersetzung). Beispiele für Probleme, die dazu führen, dass Systemstatusprüfungen fehlschlagen, sind:
  - Verlust der Netzwerkverbindung
  - Systemstromausfall
  - Softwareprobleme auf dem physischen Host
  - Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen

  Weitere Informationen finden Sie unter Statusprüfungen für Ihre Instances.
- Instance Status Checks (Instance-Statusprüfungen) – Überwachen Sie die Software- und Netzwerkkonfiguration Ihrer individuellen Instance. Bei diesen Überprüfungen werden Probleme Ihrer Instance erkannt, für die zur Reparatur Ihre Beteiligung erforderlich ist. Wenn eine Instance-Statusprüfung nicht bestanden wird, müssen Sie das Problem normalerweise selbst lösen (z. B. per Neustart der Instance oder durch das Vornehmen von Änderungen an Ihrem Betriebssystem). Beispiele für Probleme, die dazu führen, dass Instance-Statusprüfungen fehlschlagen, sind unter anderem:
  - Fehlgeschlagene System-Statusprüfungen
  - Falsch konfigurierte Netzwerk- oder Startup-Konfiguration
  - Unzureichender Speicher
  - Beschädigtes Dateisystem
  - Inkompatibler Kernel

  Weitere Informationen finden Sie unter Statusprüfungen für Ihre Instances.

- CloudWatch Amazon-Alarme — beobachten Sie eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum und führen Sie eine oder mehrere Aktionen aus, die auf dem Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über mehrere Zeiträume basieren. Bei der Aktion handelt es sich um eine Benachrichtigung, die an ein Amazon-Simple-Notification-Service (Amazon-SNS)-Thema oder eine Amazon-EC2-Auto-Scaling-Richtlinie gesendet wird. Bei Alarmen werden nur Aktionen für anhaltende Statusänderungen ausgelöst. CloudWatch Alarme lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Zustand befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.
- Amazon EventBridge — Automatisieren Sie Ihre AWS Services und reagieren Sie automatisch auf Systemereignisse. Ereignisse von AWS Services werden nahezu EventBridge in Echtzeit übermittelt, und Sie können automatische Aktionen festlegen, die ergriffen werden, wenn ein Ereignis mit einer von Ihnen erstellten Regel übereinstimmt. Weitere Informationen finden Sie unter Was ist Amazon EventBridge? .
- Amazon CloudWatch Logs — überwachen, speichern und greifen Sie auf Ihre Protokolldateien von Amazon EC2 EC2-Instances oder anderen Quellen zu. AWS CloudTrail Weitere Informationen finden Sie im Amazon CloudWatch Logs-Benutzerhandbuch.
- CloudWatch Agent — sammelt Protokolle und Metriken auf Systemebene von Hosts und Gästen auf Ihren EC2-Instances und lokalen Servern. Weitere Informationen finden Sie unter Erfassung von Metriken und Protokollen von Amazon EC2 EC2-Instances und lokalen Servern mit dem CloudWatch Agenten im CloudWatch Amazon-Benutzerhandbuch.

Manuelle Überwachungstools

Ein weiterer wichtiger Teil der Überwachung von Amazon EC2 ist die manuelle Überwachung der Elemente, die von den Überwachungsskripts, Statusprüfungen und CloudWatch Alarmen nicht abgedeckt werden. Die Amazon EC2- und CloudWatch Konsolen-Dashboards bieten einen at-a-glance Überblick über den Status Ihrer Amazon EC2 EC2-Umgebung.

- Das Amazon EC2-Dashboard zeigt:
  - Zustand des Services und geplante Ereignisse nach Region
  - Instance-Status
  - Statusüberprüfungen
  - Alarmstatus

  - Instance-Metrik-Details (klicken Sie im Navigationsbereich auf Instances, wählen Sie eine Instance und klicken Sie dann auf die Registerkarte Monitoring (Überwachung))
  - Volumetrische Details (klicken Sie im Navigationsbereich auf Volumes, wählen Sie ein Volume und klicken Sie dann auf die Registerkarte Monitoring (Überwachung))
- Amazon CloudWatch Dashboard zeigt:
  - Aktuelle Alarme und Status
  - Diagramme mit Alarmen und Ressourcen
  - Servicestatus

  Darüber hinaus können CloudWatch Sie Folgendes verwenden:
  - Aufzeichnen von Amazon EC2-Überwachungsdaten, um Probleme zu beheben und Trends zu erkennen.
  - Suchen und durchsuchen Sie alle Ihre AWS Ressourcenmetriken
  - Erstellen und Bearbeiten von Alarmen, um über Probleme benachrichtigt zu werden
  - Sehen Sie sich at-a-glance Übersichten über Ihre Alarme und AWS Ressourcen an

Bewährte Methoden für Überwachung

Verwenden Sie die folgenden bewährten Überwachungsmethoden, die Sie bei Ihren Amazon EC2-Überwachungsaufgaben unterstützen.

- Machen Sie Überwachung zur Priorität, um kleine Probleme zu lösen, bevor Sie sich zu größeren entwickeln.
- Erstellen und implementieren Sie einen Überwachungsplan, der Überwachungsdaten aus allen Teilen Ihrer AWS Lösung sammelt, sodass Sie einen etwaigen Ausfall an mehreren Stellen leichter debuggen können. In Ihrem Überwachungsplan sollten zumindest die folgenden Fragen beantwortet sein:
  - Was sind Ihre Ziele bei der Überwachung?
  - Welche Ressourcen werden überwacht?
  - Wie oft werden diese Ressourcen überwacht?
  - Welche Überwachungstools werden verwendet?
  - Wer soll die Überwachungsaufgaben ausführen?
  - Wer soll benachrichtigt werden, wenn Fehler auftreten?

- Automatisieren Sie Überwachungsaufgaben so weit wie möglich.
- Überprüfen Sie die Logdateien auf Ihren EC2-Instances

Überwachen des Status Ihrer Instances

Sie können den Status Ihrer Instances überwachen, indem Sie Statusüberprüfungen und geplante Ereignisse für Ihre Instances anzeigen.

Bei einer Statusprüfung erhalten Sie die Informationen, die sich aus den automatisierten Überprüfungen von Amazon EC2 ergeben. Mit diesen automatisierten Überprüfungen wird ermittelt, ob bestimmte Probleme Ihre Instances beeinflussen. Die Informationen zur Statusprüfung bieten Ihnen zusammen mit den von Amazon CloudWatch bereitgestellten Daten einen detaillierten Einblick in den Betrieb jeder Ihrer Instanzen.

Sie können außerdem den Status bestimmter Ereignisse anzeigen, die für Ihre Instances geplant sind. Der Status von Ereignissen gibt Auskunft über anstehende Aktivitäten, die für Ihre Instances geplant sind (z. B. Neustart oder Ruhestand). Sie liefern außerdem die geplante Start- und Endzeit jedes Ereignisses.

Inhalt

Statusprüfungen für Ihre Instances

Mithilfe der Statusüberwachung für Instances können Sie schnell ermitteln, ob Amazon EC2 Probleme erkannt hat, die Ihre Instances möglicherweise daran hindern, Anwendungen auszuführen. Amazon EC2 führt automatisierte Prüfungen bei jeder laufenden EC2-Instance durch, um Hardware- und Softwareprobleme zu identifizieren. Sie können die Ergebnisse dieser Statusprüfungen anzeigen, um bestimmte bzw. erkennbare Probleme zu ermitteln. Die Daten zum Ereignisstatus ergänzen die Informationen, die Amazon EC2 bereits über den Status der einzelnen Instances (wie`pending`,`running`,`stopping`) und die von Amazon CloudWatch überwachten Nutzungsmetriken (CPU-Auslastung, Netzwerkverkehr und Festplattenaktivität) bereitstellt.

Statusprüfungen werden minütlich durchgeführt und geben als Status "Bestanden" oder "Fehler" zurück. Wenn alle Überprüfungen bestanden wurden, lautet der Gesamtstatus der Instance

OK. Falls mindestens eine Überprüfung nicht bestanden wird, lautet der Gesamtstatus impaired (beeinträchtigt). Statusprüfungen sind in Amazon EC2 integriert und können daher nicht deaktiviert oder gelöscht werden.

Wenn eine Statusüberprüfung fehlschlägt, wird die entsprechende CloudWatch Metrik für Statusprüfungen inkrementiert. Weitere Informationen finden Sie unter Statusprüfungsmetriken. Sie können diese Metriken verwenden, um CloudWatch Alarme zu erstellen, die auf der Grundlage des Ergebnisses der Statusprüfungen ausgelöst werden. Beispielsweise können Sie einen Alarm erstellen, mit dem Sie gewarnt werden, wenn Statusprüfungen für eine bestimmte Instance fehlschlagen. Weitere Informationen finden Sie unter Erstellen und Bearbeiten von Statusprüfungsalarmen.

Sie können auch einen CloudWatch Amazon-Alarm erstellen, der eine Amazon EC2-Instance überwacht und die Instance automatisch wiederherstellt, wenn sie aufgrund eines zugrunde liegenden Problems beeinträchtigt wird. Weitere Informationen finden Sie unter Resilienz der Instanz.

Inhalt

Arten von Statusprüfungen

Es gibt drei Arten von Statusprüfungen.

System-Statusprüfungen

Systemstatusprüfungen überwachen die AWS Systeme, auf denen Ihre Instance ausgeführt wird. Bei diesen Überprüfungen werden die zugrunde liegenden Probleme Ihrer Instance erkannt, für die zur Reparatur die Beteiligung von AWS erforderlich ist. Wenn eine Systemstatusprüfung fehlschlägt, können Sie wählen, ob Sie warten AWS möchten, bis das Problem behoben ist, oder Sie können es selbst lösen. Für von Amazon EBS unterstützte Instances können Sie die Instance selbst stoppen und starten, was in den meisten Fällen dazu führt, dass die Instance auf einen neuen Host migriert wird. Für Linux-Instances mit Unterstützung durch Instance-Speicher können Sie die Instance

beenden und ersetzen. Bei Windows-Instances muss das Stamm-Volume ein Amazon EBS-Volume sein. Der Instance-Speicher wird für das Stamm-Volume nicht unterstützt. Beachten Sie, dass Instance-Speicher-Volumes kurzlebig sind und alle Daten verloren gehen, wenn die Instance gestoppt wird.

Hier sind Beispiele für Probleme aufgeführt, die dazu führen können, dass System-Statusprüfungen fehlschlagen:

- Verlust der Netzwerkverbindung
- Systemstromausfall
- Softwareprobleme auf dem physischen Host
- Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen

Wenn eine Systemstatusprüfung fehlschlägt, erhöhen wir die Metrik StatusCheckFailed_System.

Bare Metal-Instances

Wenn Sie einen Neustart vom Betriebssystem auf einer Bare-Metal-Instance durchführen, gibt die Systemstatusprüfung möglicherweise vorübergehend einen Fehlerstatus zurück. Wenn die Instance verfügbar ist, sollte die Systemstatusprüfung einen Passstatus zurückgeben.

Instance-Statusprüfungen

Instance Status Checks (Instance-Statusprüfungen) Überwachen Sie die Software- und Netzwerkkonfiguration Ihrer individuellen Instance. Amazon EC2 überprüft den Zustand der Instance, indem es eine ARP-Anfrage (Address Resolution Protocol) an die Netzwerkschnittstelle (NIC) sendet. Bei diesen Überprüfungen werden Probleme Ihrer Instance erkannt, für die zur Reparatur Ihre Beteiligung erforderlich ist. Wenn eine Instance-Statusprüfung nicht bestanden wird, müssen Sie das Problem normalerweise selbst lösen (z. B. per Neustart der Instance oder durch das Vornehmen von Konfigurationsänderungen für die Instance).

> **Note**
>
> Neuere Linux-Distributionen, die die Netzwerkkonfiguration verwenden`systemd-networkd`, berichten möglicherweise anders über Integritätsprüfungen als frühere Distributionen. Während des Startvorgangs kann dieser Netzwerktyp früher gestartet und möglicherweise vor anderen Startaufgaben beendet werden, die sich ebenfalls auf den Zustand der Instance

auswirken können. Statusprüfungen, die von der Netzwerkverfügbarkeit abhängen, können einen fehlerfreien Status melden, bevor andere Aufgaben abgeschlossen sind.

Hier sind Beispiele für Probleme aufgeführt, die dazu führen können, dass Instance-Statusprüfungen fehlschlagen:

- Fehlgeschlagene System-Statusprüfungen
- Fehlerhafte Netzwerk- oder Startup-Konfiguration
- Unzureichender Speicher
- Beschädigtes Dateisystem
- Inkompatibler Kernel
- [Windows-Instanzen] Während des Neustarts einer Instanz oder während der Bündelung einer durch den Windows-Instanzspeicher gestützten Instanz wird bei einer Instanzstatusprüfung ein Fehler gemeldet, bis die Instanz wieder verfügbar ist.

Wenn eine Überprüfung des Instance-Status fehlschlägt, erhöhen wir die Metrik Failed_Instance.StatusCheck

Bare Metal-Instances

Wenn Sie einen Neustart des Betriebssystems auf einer Bare-Metal-Instance durchführen, gibt die Instance-Statusprüfung möglicherweise vorübergehend einen Fehlerstatus zurück. Wenn die Instance verfügbar wird, sollte die Instance-Statusprüfung einen Passstatus zurückgeben.

Verknüpfte EBS-Statusprüfungen

Verknüpfte EBS-Statusprüfungen überwachen, ob die an eine Instance angehängten Amazon EBS-Volumes erreichbar sind und I/O-Operationen abschließen können. Die `StatusCheckFailed_AttachedEBS`-Metrik ist ein binärer Wert, der auf eine Beeinträchtigung hinweist, wenn eines oder mehrere der an die Instance angehängten EBS-Volumes I/O-Operationen nicht abschließen können. Diese Statusprüfungen erkennen grundlegende Probleme mit der Datenverarbeitungs- oder Amazon EBS-Infrastruktur. Wenn die angehängte EBS-Statusprüf-Metrik fehlschlägt, können Sie entweder warten, AWS bis das Problem behoben ist, oder Sie können Maßnahmen ergreifen, z. B. die betroffenen Volumes austauschen oder die Instance beenden und neu starten.

Hier sind Beispiele für Probleme aufgeführt, die dazu führen können, dass angehängte EBS-Statusprüfungen fehlschlagen:

- Hardware- oder Softwareprobleme auf den Speichersubsystemen, die den EBS-Volumes zugrunde liegen
- Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit der EBS-Volumes beeinträchtigen
- Verbindungsprobleme zwischen der Instance und den EBS-Volumes

Sie können die `StatusCheckFailed_AttachedEBS`-Metrik verwenden, um die Stabilität Ihres Workloads zu verbessern. Sie können diese Metrik verwenden, um CloudWatch Amazon-Alarme zu erstellen, die auf der Grundlage des Ergebnisses der Statusprüfung ausgelöst werden. Sie könnten beispielsweise ein Failover auf eine sekundäre Instance oder Availability Zone durchführen, wenn Sie eine anhaltende Auswirkung feststellen. Alternativ können Sie die I/O-Leistung jedes angeschlossenen Volumes mithilfe von CloudWatch EBS-Metriken überwachen, um das beschädigte Volume zu erkennen und zu ersetzen. Wenn Ihre Workload die I/O zu keinem der mit Ihrer Instance verknüpften EBS-Volumes steuert und die verknüpfte EBS-Statusprüfung auf eine Beeinträchtigung hinweist, können Sie die Instance beenden und neu starten, um Probleme mit dem physischen Host zu beheben, die sich auf die Erreichbarkeit der EBS-Volumes auswirken. Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken für Amazon EBS

> **Note**
>
> - Die verknüpfte EBS-Statusprüfungsmetrik ist nur für Nitro-Instances verfügbar.
> - Sie können die angehängte Metrik zur EBS-Statusprüfung überwachen, indem Sie auf der Grundlage der `StatusCheckFailed_AttachedEBS` Metrik einen CloudWatch Alarm erstellen. Sie können diese Statusprüfung nicht mit dem Befehl AWS CLI describe-instance-status anzeigen.

Mit Statusprüfungen arbeiten

Sie können mit Statusprüfungen arbeiten, indem Sie die Konsole und Befehlszeilentools verwenden, wie z. B. die AWS CLI.

Themen

- Anzeigen der Statusprüfungen
- Erstellen und Bearbeiten von Statusprüfungsalarmen

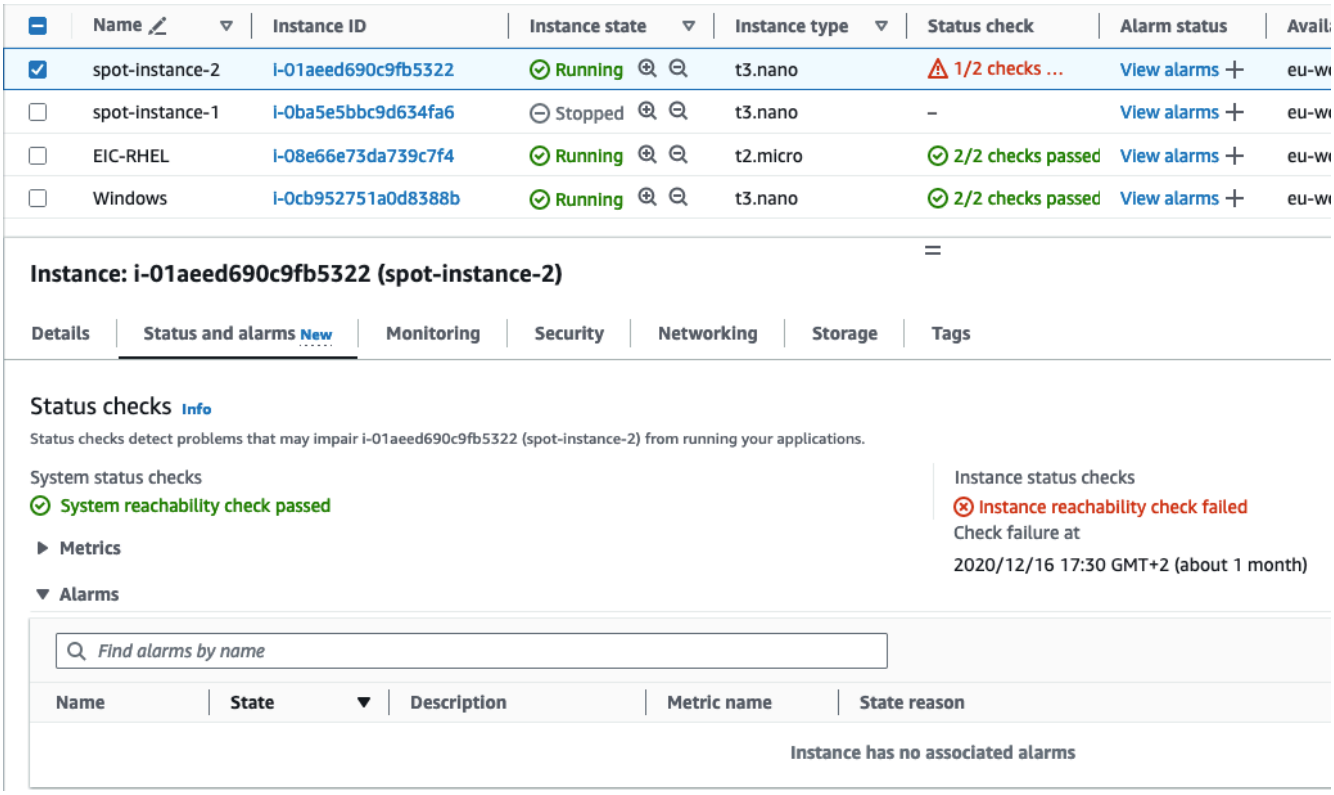
Anzeigen der Statusprüfungen

Verwenden Sie eine der folgenden Methoden, um Statusprüfungen anzuzeigen.

Console

Anzeigen der Statusprüfungen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Auf der Seite Instances ist in der Spalte Statusprüfungen jeweils der Betriebszustand einer Instance angegeben.
4. Wählen Sie die Instance aus, um ihren Status anzuzeigen, und wählen Sie anschließend die Registerkarte Status und Alarme.



Wenn Ihre Instance eine nicht bestandene Statusprüfung aufweist, müssen Sie das Problem normalerweise selbst lösen (z. B. per Neustart der Instance oder durch das Vornehmen von

Konfigurationsänderungen für die Instance). Informationen zur Behebung von Fehlern bei der System- oder Instanzstatusprüfung auf Linux-Instances finden Sie unter. Beheben Sie Linux-Instances mit fehlgeschlagenen Statusprüfungen

5. Um die CloudWatch Metriken für Statuschecks zu überprüfen, erweitern Sie auf der Registerkarte Status und Alarme die Option Metriken, um die Grafiken für die folgenden Metriken anzuzeigen:

   - Statusprüfung für System fehlgeschlagen
   - Statusprüfung für Instance fehlgeschlagen

   Weitere Informationen finden Sie unter the section called “Statusprüfungsmetriken”.

Command line

Sie können Statusprüfungen für ausgeführte Instances anzeigen, indem Sie den Befehl describe-instance-status (AWS CLI) verwenden.

Verwenden Sie den folgenden Befehl, um den Status aller Instances anzuzeigen.

```
aws ec2 describe-instance-status
```

Führen Sie den folgenden Befehl aus, um den Status aller Instances mit dem Instance-Status `impaired` anzufordern.

```
aws ec2 describe-instance-status \
    --filters Name=instance-status.status,Values=impaired
```

Verwenden Sie den folgenden Befehl, um den Status einer einzelnen Instance abzurufen.

```
aws ec2 describe-instance-status \
    --instance-ids i-1234567890abcdef0
```

Alternativ können Sie die folgenden -Befehle verwenden:

- Get-EC2InstanceStatus (AWS Tools for Windows PowerShell)
- DescribeInstanceStatus (Amazon EC2 EC2-Abfrage-API)

Wenn Sie über eine Linux-Instance verfügen, bei der die Statusprüfung fehlgeschlagen ist, finden Sie weitere Informationen unterBeheben Sie Linux-Instances mit fehlgeschlagenen Statusprüfungen.

Erstellen und Bearbeiten von Statusprüfungsalarmen

Sie können die Metriken für die Statusprüfung verwenden, um CloudWatch Alarme zu erstellen, die Sie benachrichtigen, wenn bei einer Instance eine Statusprüfung nicht bestanden hat.

> **Important**
>
> Bei Statusprüfungen und Alarmen für Statusprüfungen kann es vorübergehend zu einem unzureichenden Datenstatus kommen, wenn Metrikdatenpunkte fehlen. Das ist zwar selten, kann aber passieren, wenn es zu einer Unterbrechung der metrischen Berichtssysteme kommt, selbst wenn eine Instanz fehlerfrei ist. Wir empfehlen, diesen Status als fehlende Daten zu behandeln und nicht als Fehlschlag bei der Statusüberprüfung oder als Alarmverletzung. Dies gilt insbesondere dann, wenn als Reaktion Aktionen zum Stoppen, Beenden, Neustarten oder Wiederherstellen der Instance ergriffen werden.

Verwenden Sie eine der folgenden Methoden, um einen Alarm für die Statusprüfung zu erstellen:

Console

Gehen Sie wie folgt vor, um einen Alarm zu konfigurieren, der Ihnen eine Benachrichtigung per E-Mail sendet oder eine Instance bei nicht bestandener Statusprüfung anhält, beendet oder wiederherstellt.

So erstellen Sie einen Statusprüfungsalarm

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance, dann die Registerkarte Statusprüfungen und Aktionen, Statusprüfalarm erstellen aus.
4. Wählen Sie auf der Seite CloudWatch Alarme verwalten unter Alarm hinzufügen oder bearbeiten die Option Alarm erstellen aus.
5. Aktivieren Sie für Alarmbenachrichtigung den Schalter, um Amazon Simple Notification Service (Amazon SNS) -Benachrichtigungen zu konfigurieren. Wählen Sie ein vorhandenes

Amazon SNS-Thema aus oder geben Sie einen Namen ein, um ein neues Thema zu erstellen.

Wenn Sie der Liste mit den Empfängern eine E-Mail-Adresse hinzugefügt oder ein neues Thema erstellt haben, sendet Amazon SNS an jede neue Adresse eine Bestätigungs-E-Mail, um die Abonnierung zu bestätigen. Jeder Empfänger muss die Abonnierung bestätigen, indem er in dieser Nachricht auf den Link klickt. Warnungsbenachrichtigungen werden nur an bestätigte Adressen gesendet.

6. Aktivieren Sie für Alarmaktion den Schalter, um eine Aktion anzugeben, die ausgeführt werden soll, wenn der Alarm ausgelöst wird. Wählen Sie die Aktion aus.
7. Wählen Sie unter larm thresholds (Alarmschwellenwerte) die Metrik und Kriterien für den Alarm aus.

   Sie können die Standardeinstellungen für Group samples by (Beispiele gruppieren nach) (Average (Durchschnitt)) und für Type of data to sample (Datentypen für die Probenahme) (Status check failed:either) (Statusprüfung ist fehlgeschlagen:beide) übernehmen oder an Ihre Anforderungen anpassen.

   Legen Sie unter Consecutive period (Kontinuierlicher Zeitraum) die Anzahl von Zeiträumen fest, die ausgewertet werden sollen, und wählen Sie unter Period (Zeitraum) die Dauer des Auswertungszeitraums aus, nach dem der Alarm ausgelöst und eine E-Mail gesendet wird.
8. (Optional) Wählen Sie für Beispiel-Metrikdaten die Option Zu Dashboard hinzufügen aus.
9. Wählen Sie Create (Erstellen) aus.

Falls Sie Änderungen an einem Alarm zum Instance-Status vornehmen möchten, können Sie ihn bearbeiten.

Erstellen eines Ereignisfensters

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instanz aus und wählen Sie Aktionen, Überwachung, CloudWatch Alarme verwalten aus.
4. Wählen Sie auf der Seite CloudWatch Alarme verwalten unter Alarm hinzufügen oder bearbeiten die Option Alarm bearbeiten aus.
5. Wählen Sie unter Search for alarm (Alarmsuche) den Alarm aus.

6. Wenn Sie die Änderungen vorgenommen haben, wählen Sie Update (Aktualisieren) aus.

Command line

Im folgenden Beispiel veröffentlicht der Alarm eine Benachrichtigung für das SNS-Thema `arn:aws:sns:us-west-2:111122223333:my-sns-topic`, wenn die Instance die Instance- oder System-Statusprüfung in mindestens zwei aufeinanderfolgenden Zeiträumen nicht besteht. Die verwendete CloudWatch Metrik ist`StatusCheckFailed`.

Um einen Alarm für die Statusprüfung mit dem zu erstellen AWS CLI

1. Wählen Sie ein vorhandenes SNS-Thema aus oder erstellen Sie ein neues Thema. Weitere Informationen finden Sie unter Using AWS CLI the with Amazon SNS im AWS Command Line Interface Benutzerhandbuch.
2. Verwenden Sie den folgenden Befehl list-metrics, um die verfügbaren CloudWatch Amazon-Metriken für Amazon EC2 anzuzeigen.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

3. Verwenden Sie den folgenden put-metric-alarm-Befehl, um den Alarm zu erstellen.

```
aws cloudwatch put-metric-alarm \
    --alarm-name StatusCheckFailed-Alarm-for-i-1234567890abcdef0 \
    --metric-name StatusCheckFailed \
    --namespace AWS/EC2 \
    --statistic Maximum \
    --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
    --unit Count \
    --period 300 \
    --evaluation-periods 2 \
    --threshold 1 \
    --comparison-operator GreaterThanOrEqualToThreshold \
    --alarm-actions arn:aws:sns:us-west-2:111122223333:my-sns-topic
```

Der Zeitraum ist der Zeitraum in Sekunden, in dem CloudWatch Amazon-Metriken erfasst werden. Im Beispiel wird der Wert 300 verwendet, also 60 Sekunden multipliziert mit 5 Minuten. Die Bewertungsperiode ist die Anzahl von aufeinanderfolgenden Zeiträumen, für die der Wert der Metrik mit dem Schwellenwert verglichen werden muss. In diesem Beispiel wird der Wert 2 verwendet. Die Alarmaktionen sind die Aktionen, die durchgeführt werden

sollen, wenn dieser Alarm ausgelöst wird. In diesem Beispiel wird der Alarm so konfiguriert, dass mit Amazon SNS eine E-Mail gesendet wird.

Statusänderungsereignisse für Ihre Instances

Amazon EC2 sendet ein `EC2 Instance State-change Notification` Ereignis an Amazon, EventBridge wenn sich der Status einer Instance ändert.

Im Folgenden finden Sie Beispieldaten für dieses Ereignis. In diesem Beispiel ist die Instance in den `pending`-Status übergegangen.

```
{
   "id":"7bf73129-1428-4cd3-a780-95db273d1602",
   "detail-type":"EC2 Instance State-change Notification",
   "source":"aws.ec2",
   "account":"123456789012",
   "time":"2021-11-11T21:29:54Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1111"
   ],
   "detail":{
      "instance-id":"i-abcd1111",
      "state":"pending"
   }
}
```

Die möglichen Werte für `state` sind:

- `pending`
- `running`
- `stopping`
- `stopped`
- `shutting-down`
- `terminated`

Wenn Sie eine Instance starten, geht sie zunächst in den `pending`-Status und dann in den `running`-Status über. Wenn Sie eine Instance stoppen, geht sie in den `stopping`-Status und dann

in den `stopped`-Status über. Wenn Sie eine Instance beenden, geht sie in den `shutting-down`-Status und dann in den `terminated`-Status über.

Erhalt einer E-Mail-Benachrichtigung, wenn eine Instance ihren Status ändert

Um E-Mail-Benachrichtigungen zu erhalten, wenn sich der Status Ihrer Instance ändert, erstellen Sie ein Amazon SNS SNS-Thema und dann eine EventBridge Regel für das `EC2 Instance State-change Notification` Ereignis.

So erstellen Sie ein SNS-Thema

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Themen aus.
3. Wählen Sie Thema erstellen aus.
4. Wählen Sie unter Type (Typ) die Option Standard aus.
5. Geben Sie unter Name einen Namen für Ihr Thema ein.
6. Wählen Sie Thema erstellen aus.
7. Wählen Sie Create subscription (Abonnement erstellen) aus.
8. Wählen Sie unter Protocol (Protokoll) die Option Email (E-Mail) aus.
9. Geben Sie unter Endpoint (Endpunkt) die E-Mail-Adresse ein, an die die Benachrichtigungen gesendet werden sollen.
10. Wählen Sie Create subscription (Abonnement erstellen) aus.
11. Sie erhalten eine E-Mail-Nachricht mit der folgenden Betreffzeile: AWS Notification - Subscription Confirmation. Befolgen Sie die Anweisungen, um Ihr Abonnement zu bestätigen.

Um eine Regel zu erstellen EventBridge

1. Öffnen Sie die EventBridge Amazon-Konsole unter https://console.aws.amazon.com/events/.
2. Wählen Sie Regel erstellen aus.
3. Geben Sie unter Name einen Namen für Ihre Regel ein.
4. Bei Rule type (Regeltyp) wählen Sie Rule with an event pattern (Regel mit einem Ereignismuster) aus.
5. Wählen Sie Weiter aus.
6. Bei Build event pattern (Ereignis-Muster erstellen) gehen Sie wie folgt vor:

a. Wählen Sie für Ereignisquelle die Option AWS-Services aus.

b. Wählen Sie für AWS-Service EC2.

c. Wählen Sie in Event Type (Ereignistyp) EC2 Instance State-change Notification (Benachrichtigung über die Statusänderung der EC2-Instance) aus

d. Standardmäßig senden wir Benachrichtigungen für jede Statusänderung für jede Instance. Wenn Sie möchten, können Sie bestimmte Status oder bestimmte Instances auswählen.

7. Wählen Sie Weiter aus.
8. Geben Sie ein Ziel wie folgt an:

   a. Für Target types (Zieltypen), wählen Sie AWS-Service aus.

   b. Für Select a target (Wählen Sie ein Ziel aus), wählen Sie SNS-Thema aus.

   c. Wählen Sie für Topic (Thema) das SNS-Thema aus, das Sie im vorherigen Verfahren erstellt haben.

9. Wählen Sie Weiter aus.
10. (Optional) Fügen Sie Ihrer Regel Tags hinzu.
11. Wählen Sie Weiter aus.
12. Wählen Sie Regel erstellen aus.
13. Um Ihre Regel zu testen, initiieren Sie eine Statusänderung. Starten Sie beispielsweise eine gestoppte Instance, beenden Sie eine laufende Instance oder starten Sie eine Instance. Sie erhalten E-Mail-Nachrichten mit der folgenden Betreffzeile: AWS Notification Message. Der Text der E-Mail enthält die Ereignisdaten.

Geplante Ereignisse für Ihre Instances

AWS kann Ereignisse für Ihre Instances planen, z. B. einen Neustart, Stop/Start oder Außerbetriebnahme. Diese Ereignisse treten nicht häufig auf. Wenn eine Ihrer Instances von einem geplanten Ereignis betroffen sein wird, AWS sendet er vor dem geplanten Ereignis eine E-Mail an die E-Mail-Adresse, die mit Ihrem AWS Konto verknüpft war. Die E-Mail enthält Details zum Ereignis, z. B. das Start- und Enddatum. Je nach Ereignis können Sie möglicherweise Maßnahmen ergreifen, um den Zeitpunkt des Ereignisses zu steuern. AWS sendet auch ein AWS Health Ereignis, das Sie mithilfe von Amazon CloudWatch Events überwachen und verwalten können. Weitere Informationen zur Überwachung von AWS Health Ereignissen mit CloudWatch finden Sie unter AWS Health Ereignisse mit CloudWatch Ereignissen überwachen.

Geplante Ereignisse werden von verwaltet AWS; Sie können keine Ereignisse für Ihre Instances planen. Sie können die von geplanten Ereignisse anzeigen AWS, Benachrichtigungen über geplante Ereignisse so anpassen, dass sie Tags in die E-Mail-Benachrichtigung aufnehmen oder daraus entfernen, und Aktionen ausführen, wenn ein Neustart, Stillstand oder Stopp einer Instance geplant ist.

Auf der Seite Kontoeinstellungen können Sie die Kontaktinformationen für Ihr Konto aktualisieren, um sicherzustellen, dass Sie über geplante Ereignisse benachrichtigt werden.

> **Note**
>
> Wenn eine Instance von einem geplanten Ereignis betroffen ist und Teil einer Auto-Scaling-Gruppe ist, ersetzt Amazon EC2 Auto Scaling sie schließlich im Rahmen ihrer Integritätsprüfungen, ohne dass weitere Maßnahmen von Ihrer Seite erforderlich sind. Weitere Informationen über von Amazon EC2 Auto Scaling ausgeführte Zustandsprüfungen finden Sie unter Zustandsprüfungen für Auto-Scaling-Instances im Amazon-EC2-Auto-Scaling-Benutzerhandbuch.

Inhalt

Arten von geplanten Ereignissen

Amazon EC2 kann die folgenden Ereignistypen für Ihre Instances erstellen, bei denen das Ereignis zu einem geplanten Zeitpunkt auftritt:

- Instance stop (Instance-Stopp): Zur geplanten Zeit wird die Instance gestoppt. Wenn Sie sie wieder starten, wird sie zu einem neuen Host migriert. Dies gilt nur für Amazon EBS-gestützte Instances.

- Instance retirement(Instance-Außerbetriebnahme): Zur geplanten Zeit wird die Instance gestoppt, wenn sie durch Amazon EBS gesichert wird oder beendet, wenn sie durch den Instance-Speicher gesichert wird.
- Instance reboot (Instance-Neustart): Zur geplanten Zeit wird die Instance neu gestartet.
- System reboot (Systemneustart): Zur geplanten Zeit wird der Host der Instance neu gestartet.
- System maintenance (Systemwartung): Zur geplanten Zeit kann die Instance vorübergehend von der Netzwerk- oder Stromversorgungswartung betroffen sein.

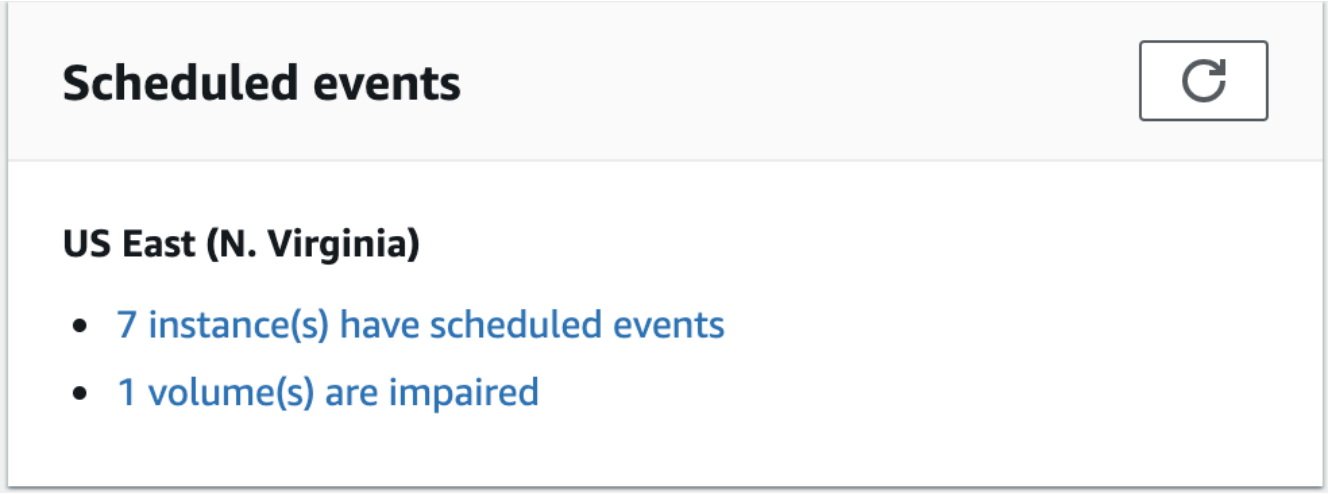
Anzeigen geplanter Ereignisse

Zusätzlich zum Erhalt von Benachrichtigungen über geplante Ereignisse per E-Mail können Sie auch mit einer der folgenden Methoden eine Prüfung auf geplante Ereignisse durchführen.

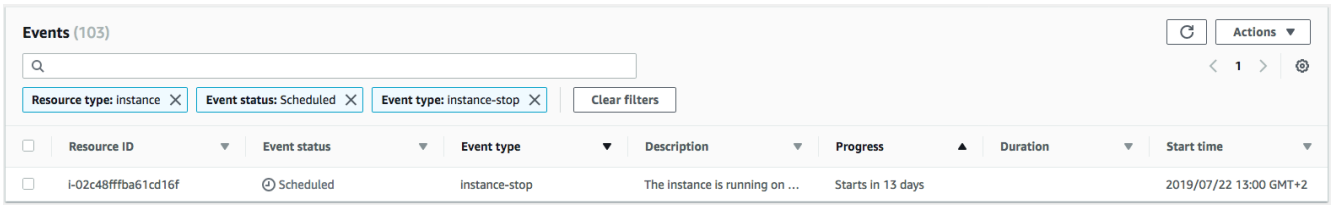
Console

Um geplante Ereignisse für Ihre Instances anzuzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Alle Ressourcen mit einem zugeordneten Ereignis werden unter Geplante Ereignisse angezeigt.



3. Für weitere Einzelheiten, wählen Sie im Navigationsbereich die Option Ereignisse aus. Alle Ressourcen mit einem zugeordneten Ereignis werden angezeigt. Sie können nach Merkmalen wie Ereignistyp, Ressourcentyp und Availability Zone filtern.



AWS CLI

Um geplante Ereignisse für Ihre Instances anzuzeigen

Verwenden Sie den Befehl describe-instance-status .

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0 \
    --query "InstanceStatuses[].Events"
```

Die folgende Beispielausgabe zeigt ein Neustartereignis.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0d59937288b749b32",
            "Code": "system-reboot",
            "Description": "The instance is scheduled for a reboot",
            "NotAfter": "2019-03-15T22:00:00.000Z",
            "NotBefore": "2019-03-14T20:00:00.000Z",
            "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
         }

    ]
]
```

Hier ist eine Beispielausgabe mit einem Ereignis zur Ausmusterung einer Instance angegeben.

```
[
    "Events": [
        {
            "InstanceEventId": "instance-event-0e439355b779n26",

            "Code": "instance-stop",
            "Description": "The instance is running on degraded hardware",
```

```
            "NotBefore": "2015-05-23T00:00:00.000Z"
        }
    ]
]
```

PowerShell

So zeigen Sie geplante Ereignisse für Ihre Instances mit der a AWS Tools for Windows PowerShell

Verwenden Sie den folgenden Get-EC2InstanceStatus-Befehl.

```
PS C:\> (Get-EC2InstanceStatus -InstanceId i-1234567890abcdef0).Events
```

Hier ist eine Beispielausgabe mit einem Ereignis zur Ausmusterung einer Instance angegeben.

```
Code         : instance-stop
Description  : The instance is running on degraded hardware
NotBefore    : 5/23/2015 12:00:00 AM
```

Instance metadata

So zeigen Sie geplante Ereignisse für Ihre Instances mithilfe von Instance-Metadaten an

Sie können Informationen zu aktiven Wartungsereignissen für Ihre Instances mithilfe von Instance-Metadatenservice Version 2 oder Instance-Metadatenservice Version 1 aus den Instance-Metadaten abrufen.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-
aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-
data/events/maintenance/scheduled
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/
scheduled
```

Es folgt eine Beispielausgabe mit Informationen zu einem geplanten Systemneustartereignis im JSON-Format.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "active"
  }
]
```

So zeigen Sie den Ereignisverlauf für abgeschlossene oder abgebrochene Ereignisse für Ihre Instances mit Instance-Metadaten an.

Sie können Informationen zu abgeschlossenen oder abgebrochenen Ereignissen für Ihre Instances mithilfe von Instance-Metadatenservice Version 2 oder Instance-Metadatenservice Version 1 aus den Instance-Metadaten abrufen.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/events/maintenance/history
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/events/maintenance/history
```

Es folgt eine Beispielausgabe mit Informationen zu einem abgebrochenen und zu einem abgeschlossenen Systemneustartereignis im JSON-Format.

```
[
  {
    "NotBefore" : "21 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
```

```
    "Description" : "[Canceled] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "21 Jan 2019 09:17:23 GMT",
    "State" : "canceled"
  },
  {
    "NotBefore" : "29 Jan 2019 09:00:43 GMT",
    "Code" : "system-reboot",
    "Description" : "[Completed] scheduled reboot",
    "EventId" : "instance-event-0d59937288b749b32",
    "NotAfter" : "29 Jan 2019 09:17:23 GMT",
    "State" : "completed"
  }
]
```

AWS Health

Sie können den verwenden AWS Health Dashboard , um mehr über Ereignisse zu erfahren, die sich auf Ihre Instance auswirken können. Die AWS Health Dashboard unterteilt Probleme in drei Gruppen: offene Probleme, geplante Änderungen und andere Benachrichtigungen. In der Gruppe der geplanten Änderungen werden laufende oder anstehende Elemente angegeben.

Weitere Informationen finden Sie unter Erste Schritte mit dem AWS Health Dashboard im AWS Health -Benutzerhandbuch.

Anpassen geplanter Ereignisbenachrichtigungen

Sie können geplante Ereignisbenachrichtigungen so anpassen, dass Tags (Markierungen) in die E-Mail-Benachrichtigung aufgenommen werden. Dies erleichtert die Identifizierung der betroffenen Ressource (Instances oder Dedicated Hosts) und die Priorisierung von Aktionen für das bevorstehende Ereignis.

Wenn Sie Ereignisbenachrichtigungen so anpassen, dass sie Tags (Markierungen) einschließen, können Sie sich für das Einschließen der folgenden Elemente entscheiden:

- Alle Tags (Markierungen), die mit der betroffenen Ressource verknüpft sind
- Nur bestimmte Tags (Markierungen), die mit der betroffenen Ressource verknüpft sind

Angenommen, Sie weisen beispielsweise allen Ihren Instances `application`-, `costcenter`-, `project`- und `owner`-Tags (Markierungen) zu. Sie können sich dafür entscheiden,

alle Tags (Markierungen) in Ereignisbenachrichtigungen aufzunehmen. Wenn Sie in Ereignisbenachrichtigungen nur die Tags (Markierungen) `owner` und `project` sehen möchten, können Sie alternativ auch nur diese Tags (Markierungen) einbeziehen.

Nachdem Sie die einzubeziehenden Tags (Markierungen) ausgewählt haben, enthalten die Ereignisbenachrichtigungen die Ressourcen-ID (Instance-ID oder Dedicated Host-ID) und die Schlüssel-Wert-Paare des Tags (Markierungen), die mit der betroffenen Ressource verknüpft sind.

Aufgaben

- Einschließen der Tags (Markierungen) in Ereignisbenachrichtigungen
- Entfernen der Tags (Markierungen) aus Ereignisbenachrichtigungen
- Anzeigen der Tags (Markierungen), die in Ereignisbenachrichtigungen einzubeziehen sind

Einschließen der Tags (Markierungen) in Ereignisbenachrichtigungen

Die Tags (Markierungen), die Sie einbeziehen möchten, gelten für alle Ressourcen (Instances und Dedicated Hosts) in der ausgewählten Region. Um Ereignisbenachrichtigungen in anderen Regionen anzupassen, wählen Sie zunächst die gewünschte Region aus und führen Sie dann die folgenden Schritte aus.

Sie können Tags mit einer der folgenden Methoden in die Ereignisbenachrichtigungen aufnehmen.

Console

So schließen Sie Tags (Markierungen) in Ereignisbenachrichtigungen ein:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie Actions (Aktionen), Manage event notifications (Ereignisbenachrichtigungen verwalten).
4. Aktivieren Sie Tags in Ereignisbenachrichtigungen einbeziehen.
5. Führen Sie je nach den Tags (Markierungen), die Sie in die Ereignisbenachrichtigungen aufnehmen möchten, eine der folgenden Aktionen aus:
   - Um alle der betroffenen Instance oder dem Dedicated Host zugeordneten Tags einzuschließen, wählen Sie Alle Tags einschließen aus.
   - Um die einzuschließenden Tags auszuwählen, wählen Sie Einzuschließende Tags auswählen und wählen Sie dann die Tag-Schlüssel aus oder geben Sie sie ein.

6. Wählen Sie Save (Speichern) aus.

AWS CLI

So schließen Sie alle Tags (Markierungen) in Ereignisbenachrichtigungen ein:

Verwenden Sie den AWS CLI -Befehl register-instance-event-notification-attributes und setzen Sie den Parameter `IncludeAllTagsOfInstance` auf `true`.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=true"
```

So schließen Sie bestimmte Tags (Markierungen) in Ereignisbenachrichtigungen ein:

Verwenden Sie den AWS CLI -Befehl register-instance-event-notification-attributes und geben Sie die einzufügenden Tags mit dem `InstanceTagKeys` Parameter an.

```
aws ec2 register-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Entfernen der Tags (Markierungen) aus Ereignisbenachrichtigungen

Sie können Tags aus Ereignisbenachrichtigungen mit einer der folgenden Methoden entfernen.

Console

So entfernen Sie Tags (Markierungen) aus Ereignisbenachrichtigungen:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie Actions (Aktionen), Manage event notifications (Ereignisbenachrichtigungen verwalten).
4. Um alle Tags aus Ereignisbenachrichtigungen zu entfernen, deaktivieren Sie Tags in Ereignisbenachrichtigungen einbeziehen.
5. Um bestimmte Tags aus Ereignisbenachrichtigungen zu entfernen, wählen Sie das X) für die entsprechenden Tag-Schlüssel aus.
6. Wählen Sie Save (Speichern) aus.

AWS CLI

So entfernen Sie alle Tags (Markierungen) aus Ereignisbenachrichtigungen:

Verwenden Sie den AWS CLI -Befehl deregister-instance-event-notification-attributes und setzen Sie den Parameter `IncludeAllTagsOfInstance` auf `false`.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute "IncludeAllTagsOfInstance=false"
```

So entfernen Sie bestimmte Tags (Markierungen) aus Ereignisbenachrichtigungen:

Verwenden Sie den AWS CLI Befehl deregister-instance-event-notification-attributes und geben Sie die zu entfernenden Tags mithilfe des `InstanceTagKeys` Parameters an.

```
aws ec2 deregister-instance-event-notification-attributes \
    --instance-tag-attribute 'InstanceTagKeys=["tag_key_1", "tag_key_2",
 "tag_key_3"]'
```

Anzeigen der Tags (Markierungen), die in Ereignisbenachrichtigungen einzubeziehen sind

Sie können die Tags anzeigen, die in Ereignisbenachrichtigungen enthalten sein sollen, indem Sie eine der folgenden Methoden verwenden.

Console

So zeigen Sie die in Ereignisbenachrichtigungen einzuschließende Tags (Markierungen) an:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie Actions (Aktionen), Manage event notifications (Ereignisbenachrichtigungen verwalten).

AWS CLI

So zeigen Sie die in Ereignisbenachrichtigungen einzuschließende Tags (Markierungen) an:

Verwenden Sie den Befehl describe-instance-event-notification-attributes AWS CLI .

```
aws ec2 describe-instance-event-notification-attributes
```

Verwenden von Instances, für die das Anhalten oder Aussondern geplant ist

Wenn ein irreparabler Ausfall des zugrunde liegenden Hosts für Ihre Instance AWS erkannt wird, plant es, dass die Instance je nach Art des Root-Geräts für die Instance gestoppt oder beendet wird. Wenn das Root-Gerät ein EBS-Volume ist, wird für die Instance das Anhalten geplant. Wenn das Root-Gerät ein Instance-Speicher-Volume ist, wird für die Instance das Beenden geplant. Weitere Informationen finden Sie unter Ausmusterung einer Instance.

> **Important**
>
> Alle Daten, die auf Instance-Speicher-Volumes gespeichert sind, gehen verloren, wenn eine Instance angehalten, in den Ruhezustand versetzt oder beendet wird. Dies gilt auch für Instance-Speicher-Volumes, die an eine Instance mit einem EBS-Volume als Root-Gerät angefügt sind. Achten Sie darauf, dass Sie Daten von Ihren Instance-Speicher-Volumes speichern, die Sie später möglicherweise noch benötigen, bevor die Instance angehalten, in den Ruhezustand versetzt oder beendet wird.

Aktionen für Amazon EBS-gestützte Instances

Sie können warten, bis die Instance wie geplant angehalten wird. Alternativ hierzu können Sie die Instance auch selbst beenden und starten. Sie wird dann zu einem neuen Host migriert. Weitere Informationen zum Anhalten Ihrer Instance zusätzlich zu Informationen zu den Änderungen an Ihrer Instance-Konfiguration nach dem Anhalten finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.

Sie können ein sofortiges Beenden und Starten in Reaktion auf ein geplantes Instance-Stopp-Ereignis automatisieren. Weitere Informationen finden Sie unter Automatisieren von Aktionen für Amazon-EC2-Instances im AWS Health -Benutzerhandbuch.

Aktionen für Instances mit Instance-Speicher

Wir empfehlen Ihnen, über Ihr neuestes AMI eine Ersatz-Instance zu starten und alle erforderlichen Daten zur Ersatz-Instance zu migrieren, bevor für die Instance die geplante Beendigung eintritt. Anschließend können Sie die ursprüngliche Instance beenden oder warten, bis sie wie geplant beendet wird.

Verwenden von Instances, für die der Neustart geplant ist

Wenn Aufgaben wie die Installation von Updates oder die Wartung des zugrunde liegenden Hosts ausgeführt werden AWS müssen, kann die Instanz oder der zugrunde liegende Host für einen Neustart geplant werden. Sie können den Zeitplan für die meisten Neustartereignisse ändern, so dass Ihre Instance ganz nach Wunsch an einem bestimmten Datum um eine bestimmte Uhrzeit neu gestartet wird.

Anzeigen des Neustartereignistyps

Sie können anzeigen, ob es sich bei einem Neustartereignis um einen Instance-Neustart oder einen Systemneustart handelt.

Console

So zeigen Sie die Art des geplanten Neustart-Ereignisses an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie Resource type: instance (Ressourcentyp: Instance) aus der Filterliste aus.
4. Zeigen Sie für jede Instance den Wert in der Spalte Event Type (Ereignistyp) an. Der Wert lautet entweder system-reboot (System-Neustart) oder instance-reboot (Instance-Neustart).

AWS CLI

So zeigen Sie die Art des geplanten Neustart-Ereignisses an

Verwenden Sie den Befehl describe-instance-status .

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0
```

Für geplante Neustartereignisse ist der Wert für `Code` entweder `system-reboot` oder `instance-reboot`. Die folgende Beispielausgabe zeigt ein `system-reboot`-Ereignis:

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
```

```
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

Aktionen für den Instance-Neustart

Sie können warten, bis der Neustart der Instance innerhalb des geplanten Wartungsfensters stattfindet, den Neustart der Instance für ein passendes Datum und eine passende Uhrzeit neu planen oder die Instance zu einem für Sie günstigen Zeitpunkt selbst neu starten.

Nachdem Ihre Instance neu gestartet wurde, wird das geplante Ereignis gelöscht und die Beschreibung des Ereignisses wird aktualisiert. Die ausstehende Wartung für den zugrunde liegenden Host ist dann abgeschlossen, und Sie können Ihre Instance wieder verwenden, nachdem sie vollständig gestartet wurde.

Aktionen für den Systemneustart

Sie können das System nicht selbst neu starten. Sie können warten, bis der System-Neustart während seines geplanten Wartungsfensters auftritt oder eine Änderung des Zeitplans des System-Neustarts auf ein geeignetes Datum um eine geeignete Uhrzeit vornehmen. Ein System-Neustart dauert in der Regel nur wenige Minuten. Nachdem der System-Neustart durchgeführt wurde, behält die Instance ihre IP-Adresse und ihren DNS-Namen bei. Auch werden alle Daten auf den lokalen Instance-Speicher-Volumes beibehalten. Nachdem der System-Neustart abgeschlossen wurde, wird das geplante Ereignis für die Instance gelöscht. Sie können nun überprüfen, ob die Software auf der Instance erwartungsgemäß funktioniert.

Falls die Instance zu einem anderen Zeitpunkt gewartet werden muss und Sie den Zeitplan des System-Neustarts nicht ändern können, können Sie eine Amazon EBS-gestützte Instance auch anhalten und wieder starten. Sie wird dadurch zu einem neuen Host migriert. Die Daten auf den lokalen Instance-Speicher-Volumes werden aber nicht beibehalten. Sie können auch ein sofortiges Beenden und Starten von Instances in Reaktion auf ein geplantes System-Neustart-Ereignis automatisieren. Weitere Informationen finden Sie unter Automatisieren von Aktionen für EC2-Instances im AWS Health -Benutzerhandbuch. Im Fall einer Instance-Speicher-gestützten Instance können Sie (falls der Zeitplan des System-Neustarts nicht geändert werden kann) über Ihr aktuelles

AMI auch eine Ersatz-Instance starten, alle erforderlichen Daten vor dem Eintreten des geplanten Wartungsfensters zur Ersatz-Instance migrieren und die ursprüngliche Instance dann beenden.

Verwenden von Instances, für die die Wartung geplant ist

Wenn der zugrundeliegende Host für eine Instance gewartet werden AWS muss, plant es die Wartung der Instance. Es gibt zwei Arten von Wartungsereignissen: Netzwerkwartung und Stromversorgungswartung.

Bei der Netzwerkwartung wird die Netzwerkverbindung von geplanten Instances kurz unterbrochen. Die normale Netzwerkverbindung wird für Ihre Instance wiederhergestellt, nachdem die Wartung abgeschlossen ist.

Bei der Stromversorgungswartung werden geplante Instances kurz in den Offlinezustand versetzt und dann neu gestartet. Wenn ein Neustart durchgeführt wird, werden alle Konfigurationseinstellungen Ihrer Instance beibehalten.

Überprüfen Sie nach dem Neustart Ihrer Instance (normalerweise nach nur wenigen Minuten), ob Ihre Anwendung wie erwartet funktioniert. An diesem Punkt sollte der Instance kein geplantes Ereignis mehr zugeordnet sein oder falls doch, sollte die Beschreibung des geplanten Ereignisses mit [Completed] ([Abgeschlossen]) beginnen. Es kann manchmal bis zu einer Stunde dauern, bis die Beschreibung des Instance-Status aktualisiert wird. Abgeschlossene Wartungsereignisse werden bis zu eine Woche lang im Dashboard der Amazon EC2-Konsole angezeigt.

Aktionen für Amazon EBS-gestützte Instances

Sie können warten, bis die Wartung wie geplant durchgeführt wird. Alternativ hierzu können Sie die Instance auch beenden und starten. Sie wird dann zu einem neuen Host migriert. Weitere Informationen zum Anhalten Ihrer Instance zusätzlich zu Informationen zu den Änderungen an Ihrer Instance-Konfiguration nach dem Anhalten finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.

Sie können das sofortige Beenden und Starten in Reaktion auf ein geplantes Wartungsereignis automatisieren. Weitere Informationen finden Sie unter Automatisieren von Aktionen für EC2-Instances im AWS Health -Benutzerhandbuch.

Aktionen für Instances mit Instance-Speicher

Sie können warten, bis die Wartung wie geplant durchgeführt wird. Falls Sie während eines geplanten Wartungsfensters den normalen Betrieb aufrechterhalten möchten, können Sie über Ihr aktuelles

AMI auch eine Ersatz-Instance starten, alle erforderlichen Daten vor dem Eintreten des geplanten Wartungsfensters zur Ersatz-Instance migrieren und die ursprüngliche Instance dann beenden.

Erneutes Planen eines geplanten Ereignisses

Sie können ein Ereignis so neu planen, dass es zu einem bestimmten Datum und einer Uhrzeit Ihrer Wahl erfolgt. Nur Ereignisse mit einem Stictag können verschoben werden. Es gibt weitere Einschränkungen für die Neuplanung eines Ereignisses.

Sie können ein Ereignis mit einer der folgenden Methoden neu planen.

Console

So planen Sie ein Ereignis neu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Wählen Sie Resource type: instance (Ressourcentyp: Instance) aus der Filterliste aus.
4. Wählen Sie eine oder mehrere Instances aus. Wählen Sie dann Actions (Aktionen), Schedule event (Ereignis planen).

   Der Zeitplan kann nur für zeitlich befristete Ereignisse mit einem Wert für Deadline (Frist) geändert werden. Wenn eines der ausgewählten Ereignisse keinen Stichtag hat, ist Actions (Aktionen), Schedule event (Ereignis planen) deaktiviert.
5. Geben Sie für New start time (Neue Startzeit) ein neues Datum und eine neue Uhrzeit für das Ereignis ein. Das neue Datum und die neue Uhrzeit müssen vor dem Zeitpunkt von Event Deadline (Ereignisfrist) liegen.
6. Wählen Sie Save (Speichern) aus.

   Es kann ein oder zwei Minuten dauern, bis die aktualisierte Startzeit des Ereignisses in der Konsole angezeigt wird.

AWS CLI

So planen Sie ein Ereignis neu

1. Der Zeitplan kann nur für zeitlich befristete Ereignisse mit einem Wert für `NotBeforeDeadline` geändert werden. Verwenden Sie den describe-instance-status-Befehl zur Ansicht des `NotBeforeDeadline`-Parameterwertes:

```
aws ec2 describe-instance-status \
    --instance-id i-1234567890abcdef0
```

Die folgende Beispielausgabe zeigt ein `system-reboot`-Ereignis, dessen Zeitplan geändert werden kann, da `NotBeforeDeadline` einen Wert enthält:

```
[
    "Events": [
                {
                    "InstanceEventId": "instance-event-0d59937288b749b32",
                    "Code": "system-reboot",
                    "Description": "The instance is scheduled for a reboot",
                    "NotAfter": "2019-03-14T22:00:00.000Z",
                    "NotBefore": "2019-03-14T20:00:00.000Z",
                    "NotBeforeDeadline": "2019-04-05T11:00:00.000Z"
                }
            ]
]
```

2. Um den Zeitplan des Ereignisses zu ändern, verwenden Sie den Befehl modify-instance-event-start-time. Geben Sie die neue Ereignis-Startzeit mit dem `not-before`-Parameter an. Die neue Ereignis-Startzeit muss vor dem Zeitpunkt von liege `NotBeforeDeadline`.

```
aws ec2 modify-instance-event-start-time \
    --instance-id i-1234567890abcdef0 \
    --instance-event-id instance-event-0d59937288b749b32 \
    --not-before 2019-03-25T10:00:00.000
```

Es kann ein oder zwei Minuten dauern, bis der Befehl describe-instance-status den aktualisierten `not-before` Parameterwert zurückgibt.

Einschränkungen

- Nur Ereignisse mit einem Ereignistermin können neu geplant werden. Der Zeitplan des Ereignisses kann bis hin zum Ablaufdatum der Ereignisfrist geändert werden. Die Spalte Frist in der Konsole und das `NotBeforeDeadline` Feld in der AWS CLI geben an, ob das Ereignis einen Stichtag hat.
- Nur Ereignisse, die noch nicht gestartet wurden, können neu geplant werden. Die Spalte Startzeit in der Konsole und das `NotBefore` Feld in der AWS CLI geben die Startzeit des Ereignisses

an. Ereignisse, die zum Start in den nächsten 5 Minuten geplant sind, können nicht neu geplant werden.

- Die neue Startzeit muss mindestes 60 Minuten nach der aktuellen Uhrzeit liegen.
- Wenn Sie den Zeitplan mehrerer Ereignisse über die Konsole ändern, wird das Ablaufdatum der Ereignisfrist anhand des Ereignisses mit dem frühesten Ablaufdatum der Ereignisfrist bestimmt.

Definieren Sie Ereignisfenster für geplante Ereignisse

Sie können benutzerdefinierte, wöchentlich wiederkehrende Ereignisfenster für geplante Ereignisse definieren, die Ihre Amazon-EC2-Instances neu starten, anhalten oder beenden. Sie können einem Ereignisfenster eine oder mehrere Instances zuweisen. Wenn ein geplantes Ereignis für diese Instances geplant ist, plant AWS die Ereignisse innerhalb des zugehörigen Ereignisfensters.

Sie können Ereignisfenster verwenden, um die Verfügbarkeit von Workloads zu maximieren, indem Sie Ereignisfenster angeben, die in Zeiten mit geringer Auslastung für Ihre Workload auftreten. Sie können die Ereignisfenster auch an Ihren internen Wartungsplänen ausrichten.

Sie definieren ein Ereignisfenster, indem Sie einen Satz von Zeitbereichen angeben. Der minimale Zeitbereich beträgt 2 Stunden. Die kombinierten Zeitbereiche müssen mindestens 4 Stunden betragen.

Sie können einem Ereignisfenster eine oder mehrere Instances zuordnen, indem Sie entweder Instance-IDs oder Instance-Tags (Markierungen) verwenden. Sie können Dedicated Hosts auch einem Ereignisfenster zuordnen, indem Sie die Host-ID verwenden.

> **Warning**
>
> Ereignisfenster gelten nur für geplante Ereignisse, die Instances anhalten, neu starten oder beenden.
> Ereignisfenster sind nicht anwendbar für:
>
> - Beschleunigte geplante Ereignisse und Netzwerkwartungsereignisse.
> - Ungeplante Wartungsarbeiten wie AutoRecovery ungeplante Neustarts.

Arbeiten mit Ereignisfenstern

- Überlegungen
- Ereignisfenster anzeigen

- Erstellen von Ereignisfenstern
- Ändern von Ereignisfenstern
- Löschen von Ereignisfenstern
- Ereignisfenster markieren

Überlegungen

- Alle Zeiträume des Ereignisfensters sind in UTC angegeben.
- Die Mindestdauer des wöchentlichen Ereignisfensters beträgt 4 Stunden.
- Die Zeitbereiche innerhalb eines Ereignisfensters müssen jeweils mindestens 2 Stunden betragen.
- Einem Ereignisfenster kann nur ein Zieltyp (Instance-ID, Dedicated-Host-ID oder Instance-Tags (Markierungen)) zugeordnet werden.
- Ein Ziel (Instance-ID, Dedicated Host oder Instance-Tags (Markierungen)) kann nur einem Ereignisfenster zugeordnet werden.
- Einem Ereignisfenster können maximal 100 Instance-IDs oder 50 Dedicated-Host-IDs oder 50 Instance-Tags (Markierungen) zugeordnet werden. Die Instance-Tags (Markierungen) können beliebig vielen Instances zugeordnet werden.
- Pro Region können maximal 200 Ereignisfenster erstellt werden. AWS
- Bei mehreren Instances, die Ereignisfenstern zugeordnet sind, können möglicherweise gleichzeitig geplante Ereignisse auftreten.
- Wenn AWS bereits eine Veranstaltung geplant wurde, wirkt sich die Änderung eines Veranstaltungsfensters nicht auf die Uhrzeit der geplanten Veranstaltung aus. Wenn das Ereignis einen StichTags (Markierungen) hat, können Sie das Ereignis neu planen.
- Sie können eine Instance vor dem geplanten Ereignis stoppen und starten, wodurch die Instance auf einen neuen Host migriert wird und das geplante Ereignis nicht mehr stattfindet.

Ereignisfenster anzeigen

Sie können Ereignisfenster mit einer der folgenden Methoden anzeigen.

Console

So zeigen Sie Ereignisfenster an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich die Option Events.
3. Klicken Sie auf Aktionen, Verwalten von Ereignisfenstern.
4. Wählen Sie ein Ereignisfenster aus, um dessen Details anzuzeigen.

AWS CLI

So beschreiben Sie alle Ereignisfenster

Verwenden Sie den Befehl describe-instance-event-windows.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1
```

Erwartete Ausgabe

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0abcdef1234567890",
            "Name": "myEventWindowName",
            "CronExpression": "* 21-23 * * 2,3",
            "AssociationTarget": {
                "InstanceIds": [
                    "i-1234567890abcdef0",
                    "i-0598c7d356eba48d7"
                ],
                "Tags": [],
                "DedicatedHostIds": []
            },
            "State": "active",
            "Tags": []
        }

        ...

    ],
    "NextToken": "9d624e0c-388b-4862-a31e-a85c64fc1d4a"
}
```

So beschreiben Sie ein bestimmtes Ereignisfenster

Verwenden Sie den Befehl describe-instance-event-windows mit dem `--instance-event-window-id`-Parameter, um ein bestimmtes Ereignisfenster zu beschreiben.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

So beschreiben Sie Ereignisfenster, die einem oder mehreren Filtern entsprechen

Verwenden Sie den Befehl describe-instance-event-windows mit dem `--filters`-Parameter. Im folgenden Beispiel wird der `instance-id`-Filter verwendet, um alle der Ereignisfenster zu beschreiben, die der angegebenen Instance zugeordnet sind.

Wenn ein Filter verwendet wird, führt er eine direkte Übereinstimmung durch. Der `instance-id`-Filter ist jedoch anders. Wenn es keine direkte Übereinstimmung mit der Instance-ID gibt, wird auf indirekte Verknüpfungen mit dem Ereignisfenster zurückgegriffen, wie z. B. die Tags der Instance oder die Dedicated-Host-ID (wenn sich die Instance auf einem Dedicated Host befindet).

Eine Liste der unterstützten Filter finden Sie unter describe-instance-event-windows in der AWS CLI -Referenz.

```
aws ec2 describe-instance-event-windows \
    --region us-east-1 \
    --filters Name=instance-id,Values=i-1234567890abcdef0 \
    --max-results 100 \
    --next-token <next-token-value>
```

Erwartete Ausgabe

Im folgenden Beispiel befindet sich die Instance auf einem Dedicated Host, der dem Ereignisfenster zugeordnet ist.

```
{
    "InstanceEventWindows": [
        {
            "InstanceEventWindowId": "iew-0dbc0adb66f235982",
            "TimeRanges": [
                {
                    "StartWeekDay": "sunday",
                    "StartHour": 2,
                    "EndWeekDay": "sunday",
```

```
                    "EndHour": 8
                }
            ],
            "Name": "myEventWindowName",
            "AssociationTarget": {
                "InstanceIds": [],
                "Tags": [],
                "DedicatedHostIds": [
                    "h-0140d9a7ecbd102dd"
                ]
            },
            "State": "active",
            "Tags": []
        }
    ]
}
```

Erstellen von Ereignisfenstern

Sie können ein oder mehrere Ereignisfenster erstellen. Für jedes Ereignisfenster geben Sie einen oder mehrere Zeitblöcke an. Sie können beispielsweise ein Ereignisfenster mit Zeitblöcken erstellen, die jeden Tag um 4 Uhr morgens für 2 Stunden auftreten. Oder Sie erstellen ein Ereignisfenster mit Zeitblöcken, die sonntags von 2.00–4.00 Uhr und mittwochs von 3.00–5.00 Uhr stattfinden.

Informationen zu den Ereignisfenstereinschränkungen finden Sie unter Überlegungen weiter oben in diesem Thema.

So lange werden die Ereignisfenster wöchentlich wiederholt, bis Sie sie löschen.

Verwenden Sie eine der folgenden Methoden, um ein Ereignisfenster zu erstellen.

Console

So erstellen Sie ein Ereignisfenster

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Klicken Sie auf Aktionen, Verwalten von Ereignisfenstern.
4. Wählen Sie Instance-Ereignisfenster erstellen.
5. Geben Sie für Ereignisfenstername einen beschreibenden Namen für das Ereignisfenster ein.

6. Wählen Sie für Ereignisfensterzeitplan die Zeitblöcke im Ereignisfenster aus, indem Sie den Cron-Zeitplanersteller verwenden oder Zeitbereiche angeben.

   - Wenn Sie den Cron-Zeitplanersteller auswählen, geben Sie Folgendes an:
     1. Geben Sie für Tage (UTC) die Wochentage an, an denen das Ereignisfenster auftritt.
     2. Geben Sie für Startzeit (UTC) die Zeit an, zu der das Ereignisfenster beginnt.
     3. Geben Sie für Dauer die Dauer der Zeitblöcke im Ereignisfenster an. Die Mindestdauer pro Zeitblock beträgt 2 Stunden. Die Mindestdauer des Ereignisfensters muss insgesamt 4 Stunden betragen oder überschreiten. Alle Uhrzeiten sind in UTC angegeben.
   - Wenn Sie Zeitbereiche auswählen, wählen Sie Neuen Zeitbereich hinzufügen und geben Sie den Starttag und die Startzeit sowie den Endtag und die Endzeit an. Wiederholen Sie diesen Schritt für jeden Zeitraum. Die Mindestdauer pro Zeitbereich beträgt 2 Stunden. Die Mindestdauer für alle Zeitbereiche zusammen muss insgesamt 4 Stunden betragen oder überschreiten.
7. (Optional) Ordnen Sie für Zieldetails eine oder mehrere Instances dem Ereignisfenster zu, sodass das geplante Ereignis während des zugeordneten Ereignisfensters auftritt, wenn die Instances zur Wartung geplant sind. Sie können einem Ereignisfenster eine oder mehrere Instances zuordnen, indem Sie Instance-IDs oder Instance-Tags verwenden. So verknüpfen Sie einen Dedicated Host mit einem Ereignisfenster mithilfe einer Host-ID.

   Beachten Sie, dass Sie das Ereignisfenster erstellen können, ohne dem Fenster ein Ziel zuzuordnen. Später können Sie das Fenster ändern, um ein oder mehrere Ziele zu verknüpfen.
8. (Optional) Wählen Sie für Ereignisfenster-Tags (Markierungen) die Option Tags (Markierungen) hinzufügen und geben Sie den Schlüssel und den Wert für den Tag (Markierung) ein. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).
9. Wählen Sie Ereignisfenster erstellen.

AWS CLI

Um mit dem ein Ereignisfenster zu erstellen AWS CLI, erstellen Sie zunächst das Ereignisfenster und ordnen dann dem Ereignisfenster ein oder mehrere Ziele zu.

Erstellen eines Ereignisfensters

Sie können beim Ändern des Ereignisfensters entweder einen Zeitbereich oder einen Cron-Ausdruck definieren, aber nicht beides.

So erstellen Sie ein Ereignisfenster mit einem Zeitbereich

Verwenden Sie den Befehl create-instance-event-window und geben Sie den `--time-range`-Parameter an. Sie können außerdem den Parameter `--cron-expression` nicht angeben.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8 \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

So erstellen Sie ein Ereignisfenster mit einem Cron-Ausdruck

Verwenden Sie den Befehl create-instance-event-window und geben Sie den `--cron-expression`-Parameter an. Sie können außerdem den Parameter `--time-range` nicht angeben.

```
aws ec2 create-instance-event-window \
    --region us-east-1 \
    --cron-expression "* 21-23 * * 2,3" \
    --tag-specifications "ResourceType=instance-event-
window,Tags=[{Key=K1,Value=V1}]" \
    --name myEventWindowName
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Zuordnen eines Ziels mit einem Ereignisfenster

Sie können einem Ereignisfenster nur einen Zieltyp (Instance-IDs, Dedicated-Host-IDs oder Instance-Tags (Markierungen)) zuordnen.

So verknüpfen Sie Instance-Tags mit einem Ereignisfenster

Verwenden Sie den Befehl Associate-instance-event-window und geben Sie den `instance-event-window-id`-Parameter an, um das Ereignisfenster anzugeben. Um Instance-Tags (Markierungen) zuzuordnen, geben Sie den `--association-target`-Parameter und für die Parameterwerte ein oder mehrere Tags (Markierungen) an.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [
                {
                    "Key": "k2",
                    "Value": "v2"
                },
                {
                    "Key": "k1",
                    "Value": "v1"
                }
            ],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

So verknüpfen Sie eine oder mehrere Instances mit einem Ereignisfenster

Verwenden Sie den Befehl Associate-instance-event-window und geben Sie den `instance-event-window-id`-Parameter an, um das Ereignisfenster anzugeben. Um Instances zuzuordnen, geben Sie den `--association-target`-Parameter und für die Parameterwerte eine oder mehrere Instance-IDs an.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
```

```
        "AssociationTarget": {
            "InstanceIds": [
                "i-1234567890abcdef0",
                "i-0598c7d356eba48d7"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

So verknüpfen Sie einen Dedicated Host mit einem Ereignisfenster

Verwenden Sie den Befehl Associate-instance-event-window und geben Sie den `instance-event-window-id`-Parameter an, um das Ereignisfenster anzugeben. Um einen Dedicated Host zuzuordnen, geben Sie den `--association-target`-Parameter und für die Parameterwerte eine oder mehrere Dedicated-Host-IDs an.

```
aws ec2 associate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "DedicatedHostIds=h-029fa35a02b99801d"
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": [
                "h-029fa35a02b99801d"
            ]
        },
        "State": "creating"
    }
}
```

Ändern von Ereignisfenstern

Sie können alle der Felder eines Ereignisfensters mit Ausnahme der ID ändern. Wenn beispielsweise die Sommerzeit beginnt, möchten Sie möglicherweise den Zeitplan für das Ereignisfenster ändern. Bei vorhandenen Ereignisfenstern empfiehlt es sich möglicherweise, Ziele hinzuzufügen oder zu entfernen.

Verwenden Sie eine der folgenden Methoden, um ein Ereignisfenster zu ändern.

Console

So ändern Sie ein Ereignisfenster

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Klicken Sie auf Aktionen, Verwalten von Ereignisfenstern.
4. Wählen Sie das zu ändernde Ereignisfenster aus und wählen Sie dann Aktionen, Instance-Ereignisfenster ändern.
5. Ändern Sie die Felder im Ereignisfenster und wählen Sie dann Ereignisfenster ändern.

AWS CLI

Um ein Ereignisfenster mithilfe von zu ändern AWS CLI, können Sie den Zeitraum oder den Cron-Ausdruck ändern und dem Ereignisfenster ein oder mehrere Ziele zuordnen oder die Verknüpfung aufheben.

Ändern der Zeit des Ereignisfensters

Sie können beim Ändern des Ereignisfensters entweder einen Zeitbereich oder einen Cron-Ausdruck ändern, aber nicht beides.

So ändern Sie den Zeitbereich eines Ereignisfensters

Verwenden Sie den Befehl modify-instance-event-window und geben Sie das zu ändernde Ereignisfenster an. Geben Sie den `--time-range`-Parameter an, um den Zeitbereich zu ändern. Sie können außerdem den Parameter `--cron-expression` nicht angeben.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
```

```
    --time-range StartWeekDay=monday,StartHour=2,EndWeekDay=wednesday,EndHour=8
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

So ändern Sie eine Reihe von Zeitbereichen für ein Ereignisfenster

Verwenden Sie den Befehl modify-instance-event-window und geben Sie das zu ändernde Ereignisfenster an. Geben Sie den `--time-range`-Parameter an, um den Zeitbereich zu ändern. Sie können den `--cron-expression`-Parameter nicht auch im selben Aufruf angeben.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
```

```
    --instance-event-window-id iew-0abcdef1234567890 \
    --time-range '[{"StartWeekDay": "monday", "StartHour": 2, "EndWeekDay":
 "wednesday", "EndHour": 8},
   {"StartWeekDay": "thursday", "StartHour": 2, "EndWeekDay": "friday",
 "EndHour": 8}]'
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "TimeRanges": [
            {
                "StartWeekDay": "monday",
                "StartHour": 2,
                "EndWeekDay": "wednesday",
                "EndHour": 8
            },
            {
                "StartWeekDay": "thursday",
                "StartHour": 2,
                "EndWeekDay": "friday",
                "EndHour": 8
            }
        ],
        "Name": "myEventWindowName",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

So ändern Sie den Cron-Ausdruck eines Ereignisfensters

Verwenden Sie den Befehl modify-instance-event-window und geben Sie das zu ändernde Ereignisfenster an. Geben Sie den `--cron-expression`-Parameter an, um den Cron-Ausdruck zu ändern. Sie können außerdem den Parameter `--time-range` nicht angeben.

```
aws ec2 modify-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --cron-expression "* 21-23 * * 2,3"
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [
                "i-0abcdef1234567890",
                "i-0be35f9acb8ba01f0"
            ],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating",
        "Tags": [
            {
                "Key": "K1",
                "Value": "V1"
            }
        ]
    }
}
```

Ändern der Ziele, die einem Ereignisfenster zugeordnet sind

Sie können einem Ereignisfenster zusätzliche Ziele zuordnen. Sie können auch die Zuordnung vorhandener Ziele von einem Ereignisfenster aufheben. Sie können jedoch einem Ereignisfenster nur einen Zieltyp (Instance-IDs, Dedicated-Host-IDs oder Instance-Tags (Markierungen)) zuordnen.

So ordnen Sie einem Ereignisfenster zusätzliche Ziele zu

Anweisungen zum Verknüpfen von Zielen mit einem Ereignisfenster finden Sie unter Associate a target with an event window.

So trennen Sie die Instance-Tags von einem Ereignisfenster

Verwenden Sie den Befehl disassociate-instance-event-window und geben Sie den `instance-event-window-id`-Parameter an, um das Ereignisfenster anzugeben. Um die Zuordnung der Instance-Tags (Markierungen) aufzuheben, geben Sie den `--association-target`-Parameter und für die Parameterwerte ein oder mehrere Tags (Markierungen) an.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceTags=[{Key=k2,Value=v2},{Key=k1,Value=v1}]"
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

So trennen Sie eine oder mehrere Instances von einem Ereignisfenster

Verwenden Sie den Befehl disassociate-instance-event-window und geben Sie den `instance-event-window-id`-Parameter an, um das Ereignisfenster anzugeben. Um die Zuordnung von Instances aufzuheben, geben Sie den `--association-target`-Parameter und für die Parameterwerte eine oder mehrere Instance-IDs an.

```
aws ec2 disassociate-instance-event-window \
```

```
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target "InstanceIds=i-1234567890abcdef0,i-0598c7d356eba48d7"
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

So trennen Sie einen Dedicated Host von einem Ereignisfenster

Verwenden Sie den Befehl disassociate-instance-event-window und geben Sie den `instance-event-window-id`-Parameter an, um das Ereignisfenster anzugeben. Um die Zuordnung zu einem Dedicated Host aufzuheben, geben Sie den `--association-target`-Parameter und für die Parameterwerte eine oder mehrere Dedicated-Host-IDs an.

```
aws ec2 disassociate-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890 \
    --association-target DedicatedHostIds=h-029fa35a02b99801d
```

Erwartete Ausgabe

```
{
    "InstanceEventWindow": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "Name": "myEventWindowName",
        "CronExpression": "* 21-23 * * 2,3",
        "AssociationTarget": {
            "InstanceIds": [],
            "Tags": [],
```

```
            "DedicatedHostIds": []
        },
        "State": "creating"
    }
}
```

Löschen von Ereignisfenstern

Sie können mit einer der folgenden Methoden jeweils ein Ereignisfenster löschen.

Console

So löschen Sie ein Ereignisfenster

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Klicken Sie auf Aktionen, Verwalten von Ereignisfenstern.
4. Wählen Sie das zu löschende Ereignisfenster aus, und wählen Sie dann Aktionen, Instance-Ereignisfenster löschen.
5. Geben Sie bei der Aufforderung **`delete`** ein und klicken Sie dann auf Delete (Löschen).

AWS CLI

So löschen Sie ein Ereignisfenster

Verwenden Sie den Befehl delete-instance-event-window und geben Sie das zu ändernde Ereignisfenster an.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
    --instance-event-window-id iew-0abcdef1234567890
```

So erzwingen Sie das Löschen eines Ereignisfensters

Verwenden Sie den `--force-delete`-Parameter, wenn das Ereignisfenster derzeit mit Zielen verknüpft ist.

```
aws ec2 delete-instance-event-window \
    --region us-east-1 \
```

```
    --instance-event-window-id iew-0abcdef1234567890 \
    --force-delete
```

Erwartete Ausgabe

```
{
    "InstanceEventWindowState": {
        "InstanceEventWindowId": "iew-0abcdef1234567890",
        "State": "deleting"
    }
}
```

Ereignisfenster markieren

Sie können ein Ereignisfenster beim Erstellen oder danach markieren.

Informationen zum Markieren eines Ereignisfensters beim Erstellen finden Sie unter Erstellen von Ereignisfenstern.

Verwenden Sie eine der folgenden Methoden, um ein Ereignisfenster mit Tags (Markierungen) zu versehen.

Console

So markieren Sie ein vorhandenes Ereignisfenster

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Events.
3. Klicken Sie auf Aktionen, Verwalten von Ereignisfenstern.
4. Wählen Sie das zu markierende Ereignisfenster aus, und wählen Sie dann Aktionen, Ereignisfenster-Tags der Instance verwalten aus.
5. Um einen Tag (Markierung) hinzuzufügen, wählen Sie Tag (Markierung) hinzufügen. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).
6. Wählen Sie Save (Speichern) aus.

AWS CLI

So markieren Sie ein vorhandenes Ereignisfenster

Verwenden Sie den Befehl create-tags, um vorhandene Ressourcen zu markieren. Im folgenden Beispiel wird das vorhandene Ereignisfenster mit key=purpose und value=test markiert.

```
aws ec2 create-tags \
    --resources iew-0abcdef1234567890 \
    --tags Key=purpose,Value=test
```

Überwachen Sie Ihre Instances mit CloudWatch

Sie können Ihre Instances mithilfe von Amazon überwachen CloudWatch, das Rohdaten aus Amazon EC2 sammelt und zu lesbaren Metriken nahezu in Echtzeit verarbeitet. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufgezeichnet, damit Sie auf Verlaufsinformationen zugreifen können und einen besseren Überblick darüber erhalten, wie Ihre Webanwendung oder der Service ausgeführt werden.

Standardmäßig sendet Amazon EC2 Metrikdaten innerhalb von 5 Minuten CloudWatch an. Um Metrikdaten für Ihre Instance innerhalb von 1 Minute CloudWatch an zu senden, können Sie die detaillierte Überwachung der Instance aktivieren. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der detaillierten Überwachung für Ihre Instances.

Die Amazon EC2 EC2-Konsole zeigt eine Reihe von Diagrammen an, die auf den Rohdaten von Amazon CloudWatch basieren. Je nach Ihren Anforderungen ziehen Sie es möglicherweise vor, Daten für Ihre Instances von Amazon als von CloudWatch den Diagrammen in der Konsole zu beziehen.

CloudWatch Abrechnungs- und Kosteninformationen von Amazon finden Sie unter CloudWatch Abrechnung und Kosten im CloudWatch Amazon-Benutzerhandbuch.

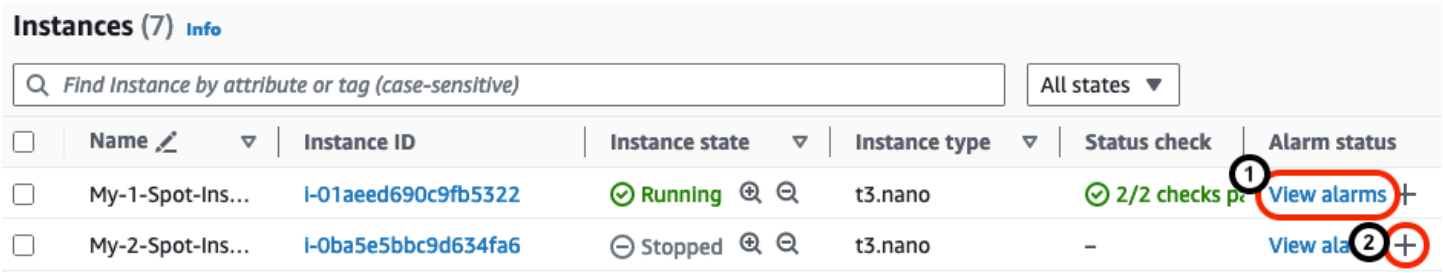
Inhalt

- Erstellen Sie einen CloudWatch Alarm für eine Instance
- Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird

Amazon EC2 EC2-Instance-Alarme

Sie können CloudWatch Amazon-Alarme für Ihre Instances auf dem Instance-Bildschirm in der Amazon EC2-Konsole anzeigen und erstellen.

Der folgende Screenshot zeigt die Konsolensteuerungen mit den Nummern 1 und 2 zum Anzeigen und Erstellen von Alarmen auf dem Instance-Bildschirm.



Alarme auf dem Instanzen-Bildschirm anzeigen

Sie können die Alarme jeder Instanz auf dem Instanzen-Bildschirm einsehen.

Um den Alarm einer Instanz vom Instanzen-Bildschirm aus einzusehen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie in der Instanzentabelle für die von Ihnen gewählte Instanz die Option Alarme anzeigen aus (im vorherigen Screenshot mit 1 nummeriert).
4. Wählen Sie im ***Beispielfenster Alarm-Details für i-0123456789*** den Namen des Alarms aus, um den Alarm in der Konsole anzuzeigen. CloudWatch

Erstellen Sie Alarme auf dem Bildschirm „Instanzen“

Auf dem Bildschirm „Instanzen“ können Sie für jede Instanz einen Alarm erstellen.

Um vom Instanzen-Bildschirm aus einen Alarm für eine Instanz zu erstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie in der Instanzentabelle für die von Ihnen gewählte Instanz das Pluszeichen (im vorherigen Screenshot mit 2 nummeriert).
4. Erstellen Sie auf dem Bildschirm „ CloudWatch Alarme verwalten“ Ihren Alarm. Weitere Informationen finden Sie unter Erstellen Sie einen CloudWatch Alarm für eine Instance.

Aktivieren oder Deaktivieren der detaillierten Überwachung für Ihre Instances

Standardmäßig ist für Ihre Instance die grundlegende Überwachung aktiviert. Optional können Sie auch die detaillierte Überwachung aktivieren.

In der folgenden Tabelle werden die Unterschiede zwischen der grundlegenden Überwachung und der detaillierten Überwachung von Instances beschrieben.

Überwachungstyp	Beschreibung	Gebühren
Grundlegende Überwachung	Nur Metriken für die Statusprüfung sind in Zeitabständen von 1 Minute verfügbar. Alle anderen Metriken sind in 5-Minuten-Intervallen verfügbar.	Keine Gebühren.
Detaillierte Überwachung	Alle Metriken, einschließlich der Metriken für die Statusprüfung, sind in Zeitintervallen von 1 Minute verfügbar. Um Daten auf diese Weise zu erhalten, müssen Sie dies für die Instance gesondert aktivieren. Bei Instances, für die Sie die detaillierte Überwachung aktiviert haben, können Sie aggregierte Daten auch aus Gruppen mit ähnlichen Instances erhalten.	Ihnen wird pro Metrik berechnet, an die gesendet wird CloudWatch. Die Datenspeicherung wird Ihnen nicht berechnet. Weitere Informationen finden Sie unter Kostenpflichtiges Kontingent und Beispiel 1 — EC2 Detailed Monitoring auf der CloudWatch Amazon-Preisseite.

Themen

Erforderliche IAM-Berechtigungen

Um die detaillierte Überwachung für eine Instance zu aktivieren, muss Ihr Benutzer über die Berechtigung zur Verwendung der MonitorInstances-API-Aktion verfügen. Um die detaillierte Überwachung für eine Instances zu deaktivieren, muss Ihr Benutzer über die Berechtigung zur Verwendung der UnmonitorInstances-API-Aktion verfügen.

Aktivieren der detaillierten Überwachung

Sie können die detaillierte Überwachung auf einer Instance aktivieren, während Sie sie starten bzw. während sie ausgeführt oder angehalten wird. Das Aktivieren der detaillierten Überwachung für eine Instance wirkt sich nicht auf die Überwachung der EBS-Volumes aus, die mit der Instance verknüpft sind. Weitere Informationen finden Sie unter CloudWatch Amazon-Metriken für Amazon EBS.

Console

Aktivieren der detaillierten Überwachung für eine vorhandene Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und klicken Sie auf Aktionen, Überwachung und Fehlerbehebung, Detaillierte Überwachung verwalten.
4. Wählen Sie auf der Detailseite Detaillierte Überwachung für Detaillierte Überwachung das Kontrollkästchen Aktivieren ais.
5. Wählen Sie Save (Speichern) aus.

Aktivieren der detaillierten Überwachung beim Starten einer Instance

Wenn Sie eine Instance über die Amazon EC2 EC2-Konsole starten, aktivieren Sie unter Erweiterte Details das Kontrollkästchen Detailed CloudWatch monitoring.

AWS CLI

Aktivieren der detaillierten Überwachung für eine vorhandene Instance

Verwenden Sie den Befehl monitor-instances, um die detaillierte Überwachung für die angegebenen Instances zu aktivieren.

```
aws ec2 monitor-instances --instance-ids i-1234567890abcdef0
```

Aktivieren der detaillierten Überwachung beim Starten einer Instance

Verwenden Sie den Befehl run-instances mit dem Flag `--monitoring`, um die detaillierte Überwachung zu aktivieren.

```
aws ec2 run-instances --image-id ami-09092360 --monitoring Enabled=true...
```

Deaktivieren der detaillierten Überwachung

Sie können die detaillierte Überwachung auf einer Instance ausschalten, während Sie sie starten bzw. während sie ausgeführt oder angehalten wird.

Console

Deaktivieren der detaillierten Überwachung

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, Detaillierte Überwachung verwalten aus.
4. Deaktivieren Sie auf der Detailseite Detaillierte Überwachung für Detaillierte Überwachung das Kontrollkästchen Aktivieren.
5. Wählen Sie Save (Speichern) aus.

AWS CLI

Deaktivieren der detaillierten Überwachung

Verwenden Sie den Befehl unmonitor-instances, um die detaillierte Überwachung für die angegebenen Instances zu deaktivieren.

```
aws ec2 unmonitor-instances --instance-ids i-1234567890abcdef0
```

Listet die verfügbaren CloudWatch Metriken für Ihre Instances auf

Amazon EC2 sendet Metriken an Amazon CloudWatch. Sie können die AWS Management Console, oder eine API verwenden AWS CLI, um die Metriken aufzulisten, an CloudWatch die Amazon EC2 sendet. Standardmäßig deckt jeder Datenpunkt die sich an die Startzeit anschließenden 5 Minuten an Aktivität für die Instance ab. Wenn Sie die detaillierte Überwachung aktiviert haben, deckt jeder Datenpunkt die nächste Minute an Aktivität ab der Startzeit ab. Beachten Sie, dass für die Statistiken Minimum, Maximum und Durchschnitt die minimale Granularität für die Metriken, die EC2 bereitstellt, 1 Minute beträgt.

Weitere Informationen zum Abrufen der Statistiken für diese Metriken erhalten Sie unter Abrufen der Statistiken von Metriken für Ihre Instances.

Inhalt

Instance-Metriken

Der `AWS/EC2`-Namespace enthält die folgenden Instance-Metriken.

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`CPUUtilization`	Der Prozentsatz der physischen CPU-Zeit, die Amazon EC2 für die Ausführung der EC2-Instance verwendet, einschließlich der Zeit, die für die Ausführung sowohl des Benutzercodes als auch des Amazon-EC2-Codes aufgewendet wird. Auf einer sehr hohen Ebene ist `CPUUtilization` die Summe aus Gast `CPUUtilization` und Hypervisor `CPUUtilization` . Tools in Ihrem Betriebssystem können CloudWatch aufgrund von Faktoren wie der Simulation älterer Geräte, der Konfiguration von Geräten anderer Hersteller, interrupter Arbeitslasten, Live-Migration und Live-Update einen anderen Prozentsatz anzeigen.	Prozent	• Durchschnitt • Minimum • Maximum
`DiskReadOps`	Abgeschlossene Lesevorgänge von allen der Instance zu Verfügung stehenden Instance-Speicher-Volumes in einem angegebenen Zeitraum. Zum Berechnen der durchschnittlichen I/O-Operationen pro Sekunde (IOPS) für einen Zeitraum dividieren Sie die Gesamtvorgänge im Zeitraum durch die Anzahl der Sekunden in dem Zeitraum. Wenn es keine Instance-Speicher-Volumes gibt, ist der Wert 0 oder die Metrik wird nicht angezeigt.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`DiskWriteOps`	Abgeschlossene Schreibvorgänge von allen der Instance zu Verfügung stehenden Instance-Speicher-Volumes in einem angegebenen Zeitraum. Zum Berechnen der durchschnittlichen I/O operationen pro Sekunde (IOPS) für einen Zeitraum dividieren Sie die Gesamtvorgänge im Zeitraum durch die Anzahl der Sekunden in dem Zeitraum. Wenn es keine Instance-Speicher-Volumes gibt, ist der Wert 0 oder die Metrik wird nicht angezeigt.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`DiskReadBytes`	Von allen der Instance zu Verfügung stehenden Instance-Speicher-Volumes gelesene Byte. Diese Metrik wird verwendet, um das von der Festplatte der Instance gelesene Datenvolumen der Anwendung zu ermitteln. Damit kann die Geschwindigkeit der Anwendung bestimmt werden. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Byte/Sekunden zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die mathematische CloudWatch Metrikfunktion verwenden, um die Byte `DIFF_TIME` pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `DiskReadBytes` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch. Wenn es keine Instance-Speicher-Volumes gibt, ist der Wert 0 oder die Metrik wird nicht angezeigt.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`DiskWriteBytes`	In alle der Instance zu Verfügung stehenden Instance-Speicher-Volumes geschriebene Byte. Diese Metrik wird verwendet, um das auf die Festplatte der Instance geschriebene Datenvolumen der Anwendung zu ermitteln. Damit kann die Geschwindigkeit der Anwendung bestimmt werden. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Byte/Sekunden zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME`, um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `DiskWriteBytes` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch. Wenn es keine Instance-Speicher-Volumes gibt, ist der Wert 0 oder die Metrik wird nicht angezeigt.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`MetadataNoToken`	Die Anzahl der erfolgreichen Zugriffe auf den Instance Metadata Service (IMDS) mithilfe einer Methode, die kein Token verwendet. Diese Metrik wird verwendet, um festzustellen, ob Prozesse auf Instanzmetadaten zugreifen, die den Instanzmetadatendienst Version 1 (IMDSv1) verwenden, der kein Token verwendet. Wenn alle Anfragen tokengestützte Sitzungen verwenden, d. h. Instance Metadata Service Version 2 (IMDSv2), ist der Wert 0. Weitere Informationen finden Sie unter Übergang zur Verwendung von Instance-Metadatenservice Version 2.	Anzahl	• Summe • Perzentile
`MetadataNoTokenRejected`	Gibt an, wie oft ein IMDSv1-Aufruf versucht wurde, nachdem IMDSv1 deaktiviert wurde. Wenn diese Metrik angezeigt wird, bedeutet dies, dass ein IMDSv1-Anruf versucht und abgelehnt wurde. Sie können entweder IMDSv1 erneut aktivieren oder sicherstellen, dass alle Ihre Anrufe IMDSv2 verwenden. Weitere Informationen finden Sie unter Übergang zur Verwendung von Instance-Metadatenservice Version 2.	Anzahl	• Summe • Perzentile

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`NetworkIn`	Anzahl der von der Instance auf allen Netzwerkschnittstellen empfangenen Byte. Diese Metrik gibt das an eine einzelne Instance eingehende Netzwerkdatenvolumen an. Der ermittelte Wert ist die Anzahl der während des Zeitraums empfangenen Byte. Wenn Sie eine grundlegene Überwachung (fünf Minuten) verwenden und die Statistik eine Summe ist, können Sie diese Zahl durch 300 teilen, um Bytes/Sekunde zu ermitteln. Wenn Sie eine detaillierte (einminütige) Überwachung haben und die Statistik eine Summe ist, teilen Sie sie durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden , um die Byte pro Sekunde `DIFF_TIME` zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `NetworkIn` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`NetworkOut`	Anzahl der von der Instance auf allen Netzwerkschnittstellen gesendeten Byte. Diese Metrik gibt das an eine einzelne Instance ausgehende Netzwerkdatenvolumen an. Der ermittelte Wert ist die Anzahl der während des Zeitraums gesendeten Bytes. Wenn Sie eine grundlegene Überwachung (fünf Minuten) verwenden und die Statistik eine Summe ist, können Sie diese Zahl durch 300 teilen, um Bytes/Sekunde zu ermitteln. Wenn Sie eine detaillierte (einminütige) Überwachung haben und die Statistik eine Summe ist, teilen Sie sie durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME` , um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `NetworkOut` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`NetworkPacketsIn`	Anzahl der von der Instance auf allen Netzwerkschnittstellen empfangenen Pakete. Diese Metrik gibt das an eine einzelne Instance eingehende Netzwerkdatenvolumen an, ausgedrückt in Anzahl an Paketen. Diese Metrik ist nur für die grundlegende Überwachung verfügbar (Fünf-Minuten-Intervalle). Um die Anzahl der Pakete pro Sekunde (PPS) zu berechnen, die Ihre Instance für die fünf Minuten erhalten hat, teilen Sie die Summe des Statistikwertes durch 300. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME` , um die Pakete pro Sekunde zu finden. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `NetworkPacketsIn` haben`m1`, gibt die mathematische Formel die Metrik in Paketen pro Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`NetworkPackets0ut`	Anzahl der von der Instance auf allen Netzwerkschnittstellen gesendeten Pakete. Diese Metrik gibt das von einer einzelnen Instance ausgehende Netzwerkdatenvolumen an, ausgedrückt in Anzahl an Paketen. Diese Metrik ist nur für die grundlegende Überwachung verfügbar (Fünf-Minuten-Intervalle). Um die Anzahl der Pakete pro Sekunde (PPS) zu berechnen, die Ihre Instance die fünf Minuten lang gesendet hat, teilen Sie die Summe des Statistikwertes durch 300. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME` , um die Pakete pro Sekunde zu finden. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `NetworkPackets0ut` haben`m1`, gibt die mathematische Formel die Metrik in Paketen pro Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

CPU-Guthaben-Metriken

Der `AWS/EC2`-Namespace enthält die folgenden CPU-Gutschriftmetriken für Ihre Instances mit Spitzenleistung.

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`CPUCreditUsage`	Die Anzahl der von der Instance für die CPU-Nutzung verbrauchten CPU-Guthaben. Ein CPU-Guthaben entspricht einer vCPU mit einer Auslastung von 100 % und einer Nutzungsdauer von einer Minute oder einer äquivalenten Kombination von vCPUs, Auslastung und Nutzungsdauer (z. B. eine vCPU mit einer Auslastung von 50 % mit einer Nutzungsdauer von zwei Minuten oder zwei vCPUs mit einer Auslastung von 25 % und einer Nutzungsdauer von zwei Minuten). Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar. Wenn Sie ein größeres Intervall als 5 Minuten angeben, verwenden Sie die Statistik `Sum` anstelle der Statistik `Average`.	Guthaben (vCPU-Minuten)	• Summe • Durchschnitt • Minimum • Maximum
`CPUCreditBalance`	Die Anzahl verdienter CPU-Guthaben, die eine Instance angesammelt hat, seit sie gestartet wurde. Für T2 Standard beinhaltet `CPUCreditBalance` auch die Anzahl der angesammelten Startguthaben. Guthaben werden auf dem Guthaben-Konto angesammelt, nachdem sie verdient wurden, und davon entfernt, wenn sie verbraucht werden. Der Guthaben-Kontostand hat ein maximales Limit, das anhand der Instance-Größe bestimmt wird. Nachdem das Limit erreicht ist, verfallen alle neu verdienten Guthabenpunkte. Für T2 Standard zählen Startguthaben nicht zum Limit.	Guthaben (vCPU-Minuten)	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
	Die Guthaben in `CPUCreditBalance` sind verfügbar, um die Leistung der Instance über die Baseline ihrer CPU-Nutzung hinaus zu steigern. Wenn eine Instance ausgeführt wird, verfallen Guthaben im `CPUCreditBalance` nicht. Wenn eine T3- oder T3a-Instance angehalten wird, bleibt der `CPUCreditBalance` -Wert sieben Tage lang erhalten. Danach verfallen alle angesammelten Guthaben. Wenn eine T2-Instance beendet wird, bleibt der `CPUCreditBalance` -Wert nicht erhalten, und alle angesammelten Guthaben gehen verloren. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar.		
`CPUSurplusCreditBalance`	Die Anzahl überzähliger Guthaben, die von einer `unlimited` -Instance verbraucht wurden, wenn ihr `CPUCreditBalance` -Wert null ist. Der `CPUSurplusCreditBalance` -Wert wird durch erworbene CPU-Guthaben abgezahlt. Wenn die Anzahl überzähliger Guthaben die Höchstzahl der Guthaben überschreitet, die die Instance in einem 24-Stunden-Zeitraum verdienen kann, fallen für die verbrauchten überzähligen Guthaben zusätzliche Gebühren an. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar.	Guthaben (vCPU-Minuten)	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`CPUSurplusCreditsCharged`	Die Anzahl verbrauchter überzähliger Guthaben, die nicht durch verdiente CPU-Guthaben zurückgezahlt wurden, und für die deshalb eine zusätzliche Gebühr anfällt. Verbrauchte überzählige Guthaben werden in Rechnung gestellt, wenn einer der folgenden Fälle auftritt: • Die ausgegebenen überzähligen Guthaben überschreiten die maximale Anzahl an Guthaben, die die Instance in einem 24-Stunden-Zeitraum verdienen kann. Über das Maximum hinaus ausgegebene überzählige Guthaben werden am Ende der Stunde abgerechnet. • Die Instance wird angehalten oder beendet. • Die Instance wird von `unlimited` in `standard` geändert. Die Metriken für CPU-Guthaben sind nur mit einer fünfminütigen Frequenz verfügbar.	Guthaben (vCPU-Minuten)	• Summe • Durchschnitt • Minimum • Maximum

Dedicated-Host-Metriken

Der `AWS/EC2`-Namespace enthält die folgenden Metriken für T3-Dedicated-Hosts.

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`DedicatedHostCPUUtilization`	Der Prozentsatz der zugewiesenen Rechenkapazität, die derzeit von den Instances verwendet wird, die auf dem Dedicated Host ausgeführt werden.	Prozent	• Summe • Durchschnitt • Minimum • Maximum

Amazon EBS-Metriken für Nitro-basierte Instances

Der `AWS/EC2`-Namespace beinhaltet zusätzliche Amazon EBS-Metriken für Volumes, die Nitro-basierten Instances angefügt sind, die keine Bare-Metal-Instances sind.

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`EBSReadOps`	Abgeschlossene Lesevorgänge von allen an die Instance angefügten Amazon EBS-Volumes in einem angegebenen Zeitraum. Zum Berechnen der durchschnittlichen Lese-I/O Operations per Second (Lese-IOPS, Ein- und Ausgabe-Befehle pro Sekunde) für einen Zeitraum dividieren Sie die Gesamtvorgänge im Zeitraum durch die Anzahl der Sekunden im Zeitraum. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Lese-IOPS zu ermitteln . Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
	`DIFF_TIME` , um die Operationen pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als `m1` grafisch darstellt `EBSReadOps` haben, gibt die metrische mathematische Formel die Metrik in Operationen/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.		

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`EBSWriteOps`	Abgeschlossene Schreibvorgänge in alle an die Instance angehängten EBS-Volumes in einem angegebenen Zeitraum. Zum Berechnen der durchschnittlichen Schreib-I/O Operations per Second (Schreib-IOPS, Ein- und Ausgabe-Befehle pro Sekunde) für einen Zeitraum dividieren Sie die Gesamtvorgänge im Zeitraum durch die Anzahl der Sekunden im Zeitraum. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Schreib-IOPS zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME`, um die Operationen pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als `m1` grafisch dargestellt `EBSWriteOps` haben, gibt die metrische mathematische Formel die Metrik in Operationen/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`EBSReadBytes`	Die aus allen an die Instance angefügten EBS-Volumes gelesenen Bytes in einem angegebenen Zeitraum. Der ermittelte Wert ist die Anzahl der während des Zeitraums gelesenen Bytes. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Lese-Bytes/Sekunden zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden `DIFF_TIME` , um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `EBSReadBytes` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`EBSWriteBytes`	Die in alle an die Instance angefügten EBS-Volumes geschriebenen Bytes in einem angegebenen Zeitraum. Der ermittelte Wert ist die Anzahl der während des Zeitraums geschriebenen Bytes. Wenn Sie die grundlegende Überwachung (alle 5 Minuten) verwenden, können Sie diesen Wert durch 300 teilen, um die Schreib-Bytes/Sekunden zu ermitteln. Wenn Sie die detaillierte Überwachung (einminütig) verwenden, teilen Sie den Wert durch 60. Sie können auch die CloudWatch metrische mathematische Funktion verwenden`DIFF_TIME`, um die Byte pro Sekunde zu ermitteln. Wenn Sie beispielsweise CloudWatch als grafisch dargestellt `EBSWriteBytes` haben`m1`, gibt die mathematische Formel die Metrik in Byte/Sekunde `m1/(DIFF_TIME(m1))` zurück. Weitere Informationen zu `DIFF_TIME` und anderen metrischen mathematischen Funktionen finden Sie unter Verwenden von metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.	Bytes	• Summe • Durchschnitt • Minimum • Maximum

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`EBSIOBalance%`	Bietet Informationen über den Prozentanteil der verbleibenden I/O-Guthaben im Burst-Bucket. Diese Metrik ist nur für die grundlegende Überwachung verfügbar. Diese Metrik ist nur für einige `*.4xlarge` -Instance-Größen und kleiner verfügbar, die mindestens einmal alle 24 Stunden für nur 30 Minuten ihre maximale Leistung erreichen. Die `Sum`-Statistik ist für diese Metrik nicht anwendbar.	Prozent	• Minimum • Maximum
`EBSByteBalance%`	Bietet Informationen über den Prozentanteil der verbleibenden Durchsatz-Guthaben im Burst-Bucket. Diese Metrik ist nur für die grundlegende Überwachung verfügbar. Diese Metrik ist nur für einige `*.4xlarge` -Instance-Größen und kleiner verfügbar, die mindestens einmal alle 24 Stunden für nur 30 Minuten ihre maximale Leistung erreichen. Die `Sum`-Statistik ist für diese Metrik nicht anwendbar.	Prozent	• Minimum • Maximum

Informationen zu den für Ihre EBS-Volumes bereitgestellten Metriken finden Sie unter Metriken für Amazon EBS-Volumes im Amazon EBS-Benutzerhandbuch. Weitere Informationen zu den für Ihre Spot-Flotten verfügbaren Metriken erhalten Sie unter CloudWatch Metriken für Spot Fleet.

Statusprüfungsmetriken

Standardmäßig sind die Metriken für Statusprüfungen mit einer einminütigen Frequenz kostenlos verfügbar. Für eine erneut gestartete Instance stehen Metrikdaten zu Statusprüfungen erst dann

zur Verfügung, wenn die Instance den Initialisierungszustand abgeschlossen hat (innerhalb weniger Minuten wechselt die Instance in den Zustand „`running`“). Weitere Informationen zu EC2-Statusprüfungen finden Sie unter Statusprüfungen für Ihre Instances.

Der `AWS/EC2`-Namespace enthält die folgenden Metriken zu Statusprüfungen.

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`StatusCheckFailed`	Berichtet, ob die Instance in der letzten Minute sowohl die Instance-Statusprüfung als auch die System-Statusprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an. Standardmäßig ist diese Metrik mit einer einminütigen Frequenz kostenlos verfügbar.	Anzahl	• Summe • Durchschnitt
`StatusCheckFailed_Instance`	Berichtet, ob die Instance in der letzten Minute die Instance-Statusprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an. Standardmäßig ist diese Metrik mit einer einminütigen Frequenz kostenlos verfügbar.	Anzahl	• Summe • Durchschnitt
`StatusCheckFailed_System`	Berichtet, ob die Instance in der letzten Minute die System-Statusprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an. Standardmäßig ist diese Metrik mit einer einminütigen Frequenz kostenlos verfügbar.	Anzahl	• Summe • Durchschnitt

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`StatusCheckFailed_AttachedEBS`	Berichtet, ob die Instance in der letzten Minute die verknüpfte EBS-Statusprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an. Standardmäßig ist diese Metrik mit einer einminütigen Frequenz kostenlos verfügbar.	Anzahl	• Summe • Durchschnitt

Der `AWS/EBS` Namespace umfasst die folgende Metrik zur Statusprüfung.

Metrik	Beschreibung	Einheit	Aussagekräftige Statistiken
`VolumeStalledIOCheck`	Hinweis: Nur für Nitro-Instances. Nicht veröffentlicht für an Amazon ECS angehängte Bände und AWS Fargate Aufgaben. Meldet, ob ein Volume in der letzten Minute eine unterbrochene E/A-Überprüfung bestanden hat. Diese Metrik nimmt den Wert `0` (bestanden) oder 1 (fehlgeschlagen) an.	Anzahl	• Summe • Durchschnitt • Minimum • Maximum

Metriken zur Spiegelung des Datenverkehrs

Der `AWS/EC2`-Namespace enthält Metriken für gespiegelten Datenverkehr. Weitere Informationen finden Sie unter Überwachen von gespiegeltem Datenverkehr mithilfe von Amazon CloudWatch im Amazon VPC Traffic Mirroring Guide.

Metriken zu Auto-Scaling-Gruppen

Der Namespace `AWS/AutoScaling` enthält Metriken für Auto-Scaling-Gruppen. Weitere Informationen finden Sie unter Überwachen von CloudWatch Metriken für Ihre Auto Scaling Scaling-Gruppen und -Instances im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

Amazon EC2-Metrikdimensionen

Sie können die folgenden Dimensionen verwenden, um die in den vorherigen Tabellen aufgeführten Metriken zu verfeinern.

Dimension	Beschreibung
`AutoScalingGroupName`	Diese Dimension filtert die angeforderten Daten für alle Instances einer angegebenen Kapazitätsgruppe. Eine Auto Scaling-Gruppe ist eine Sammlung von Instances, die Sie definieren, wenn Sie Auto Scaling verwenden. Diese Dimension ist nur für Amazon EC2-Metriken verfügbar, wenn sich die Instances in einer solchen Auto Scaling-Gruppe befinden. Verfügbar für Instances, für die die detaillierte oder die grundlegende Überwachung aktiviert ist.
`ImageId`	Diese Dimension filtert die angeforderten Daten für alle Instances, auf denen dieses Amazon EC2 Amazon Machine Image (AMI) ausgeführt wird. Verfügbar für Instances, für die die detaillierte Überwachung aktiviert ist.
`InstanceId`	Diese Dimension filtert die angeforderten Daten nur für die identifizierte Instance. So können Sie eine exakte Instance festlegen, von der aus die Daten überwacht werden sollen.
`InstanceType`	Diese Dimension filtert die angeforderten Daten für alle Instances, die mit diesem angegebenen Instance-Typ ausgeführt werden. So können Sie Ihre Daten nach dem Typ der ausgeführten Instance kategorisieren. Sie können beispielsweise Daten aus einer m1.small-Instance und einer m1.large-Instance vergleichen, um zu ermitteln, welche für Ihre Anwendung den größeren geschäftlichen Nutzen bietet.

Dimension	Beschreibung
	Verfügbar für Instances, für die die detaillierte Überwachung aktiviert ist.

Amazon EC2-Nutzungsmetriken

Sie können CloudWatch Nutzungsmetriken verwenden, um einen Überblick über die Ressourcennutzung Ihres Kontos zu erhalten. Verwenden Sie diese Kennzahlen, um Ihre aktuelle Servicenutzung in CloudWatch Diagrammen und Dashboards zu visualisieren.

Die Nutzungsmetriken von Amazon EC2 entsprechen den AWS Servicekontingenten. Sie können Alarme konfigurieren, mit denen Sie benachrichtigt werden, wenn sich Ihre Nutzung einem Servicekontingent nähert. Weitere Informationen zur CloudWatch Integration mit Servicekontingenten finden Sie unter AWS Nutzungsmetriken im CloudWatch Amazon-Benutzerhandbuch.

Amazon EC2 veröffentlicht die folgenden Metriken im `AWS/Usage`-Namespace.

Metrik	Beschreibung
`ResourceCount`	Die Anzahl der angegebenen Ressourcen, die in Ihrem Konto ausgeführt werden. Die Ressourcen werden durch die Dimensionen definiert, die der Metrik zugeordnet sind. Die nützlichste Statistik für diese Metrik ist `MAXIMUM`, die die maximale Anzahl der Ressourcen darstellt, die während des 1-Minuten-Zeitraums verwendet werden.

Die folgenden Dimensionen werden verwendet, um die Nutzungsmetriken zu verfeinern, die von Amazon EC2 veröffentlicht werden.

Dimension	Beschreibung
`Service`	Der Name des AWS Dienstes, der die Ressource enthält. Für Amazon EC2-Nutzungsmetriken lautet der Wert für diese Dimension `EC2`.

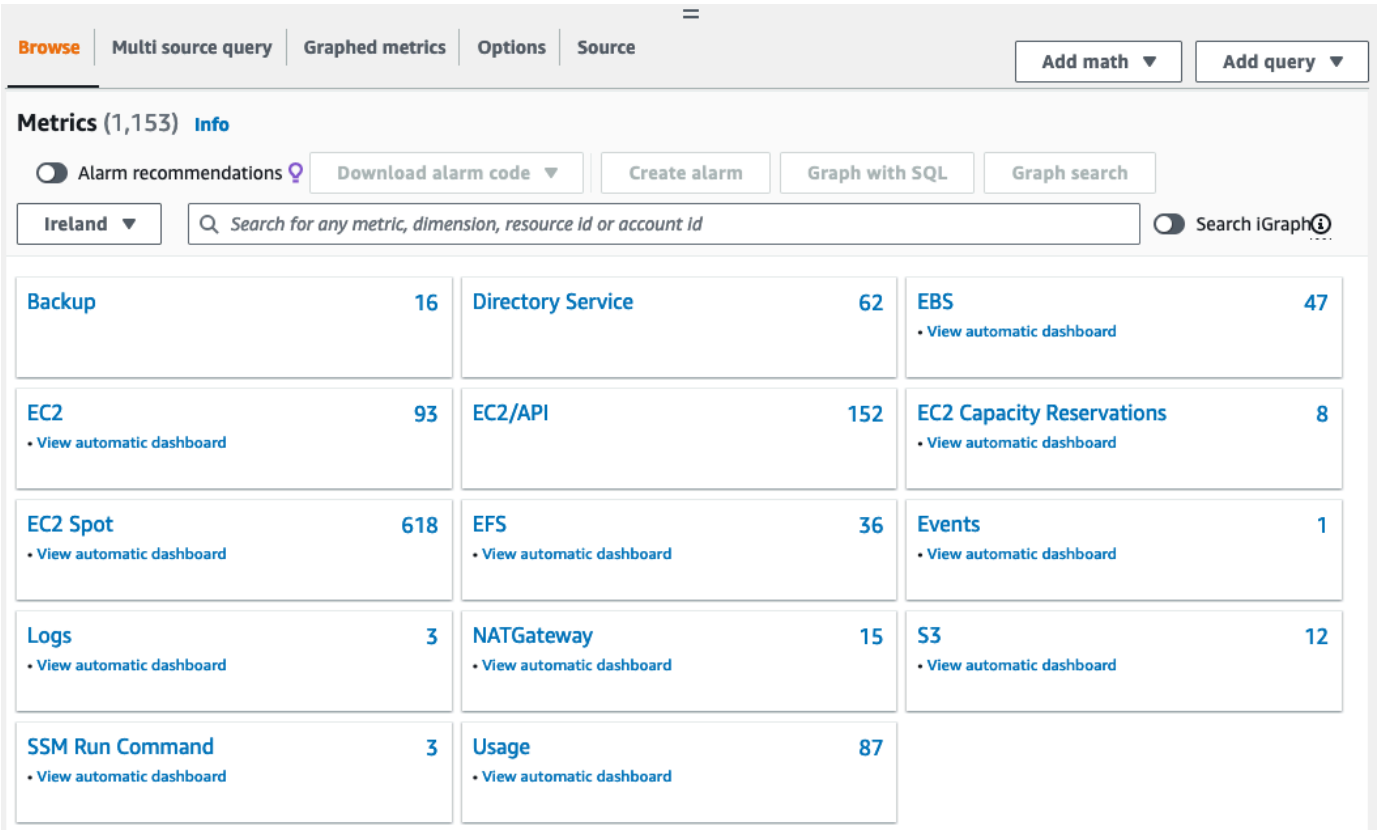
Dimension	Beschreibung
`Type`	Der Typ von Entität, die gemeldet wird. Derzeit ist der einzige gültige Wert für Amazon EC2-Nutzungsmetriken `Resource`.
`Resource`	Der Typ der Ressource, die ausgeführt wird. Derzeit ist der einzige gültige Wert für Amazon EC2-Nutzungsmetriken `vCPU`, der Informationen über ausgeführte Instance zurückgibt.
`Class`	Die Klasse der nachverfolgten Ressource. Für Amazon EC2-Nutzungsmetriken mit `vCPU` als Wert der `Resource`-Dimension sind die gültigen Werte `Standard/OnDemand` , `F/OnDemand` , `G/OnDemand` , `Inf/OnDemand` , `P/OnDemand` und `X/OnDemand` . Die Werte für diese Dimension definieren den ersten Buchstaben der Instance-Typen, die von der Metrik gemeldet werden. `Standard/OnDemand` gibt beispielsweise Informationen über alle laufenden Instances mit Typen zurück, die mit A, C, D, H, I, M, R, T und Z beginnen, und `G/OnDemand` gibt Informationen über alle laufenden Instances mit Typen zurück, die mit G beginnen.

Auflisten von Metriken mit der Konsole

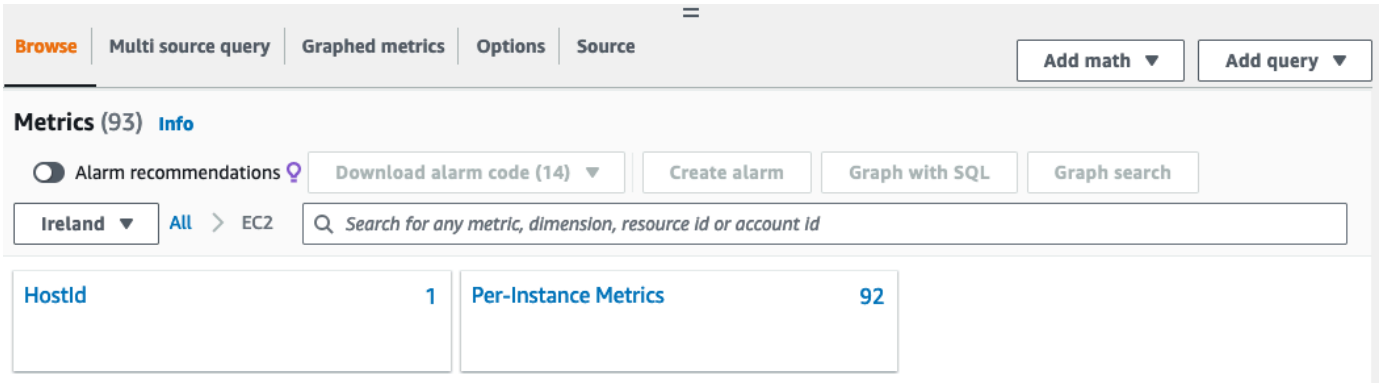
Metriken werden zuerst nach dem Namespace und dann nach verschiedenen Dimensionskombinationen in jedem Namespace gruppiert. Beispiel: Sie können alle von Amazon EC2 bereitgestellten Metriken oder die nach Instance-ID, Instance-Typ, Image-ID (AMI) oder Auto Scaling-Gruppe gruppierten Metriken anzeigen.

So zeigen Sie verfügbare Metriken nach Kategorie an (Konsole)

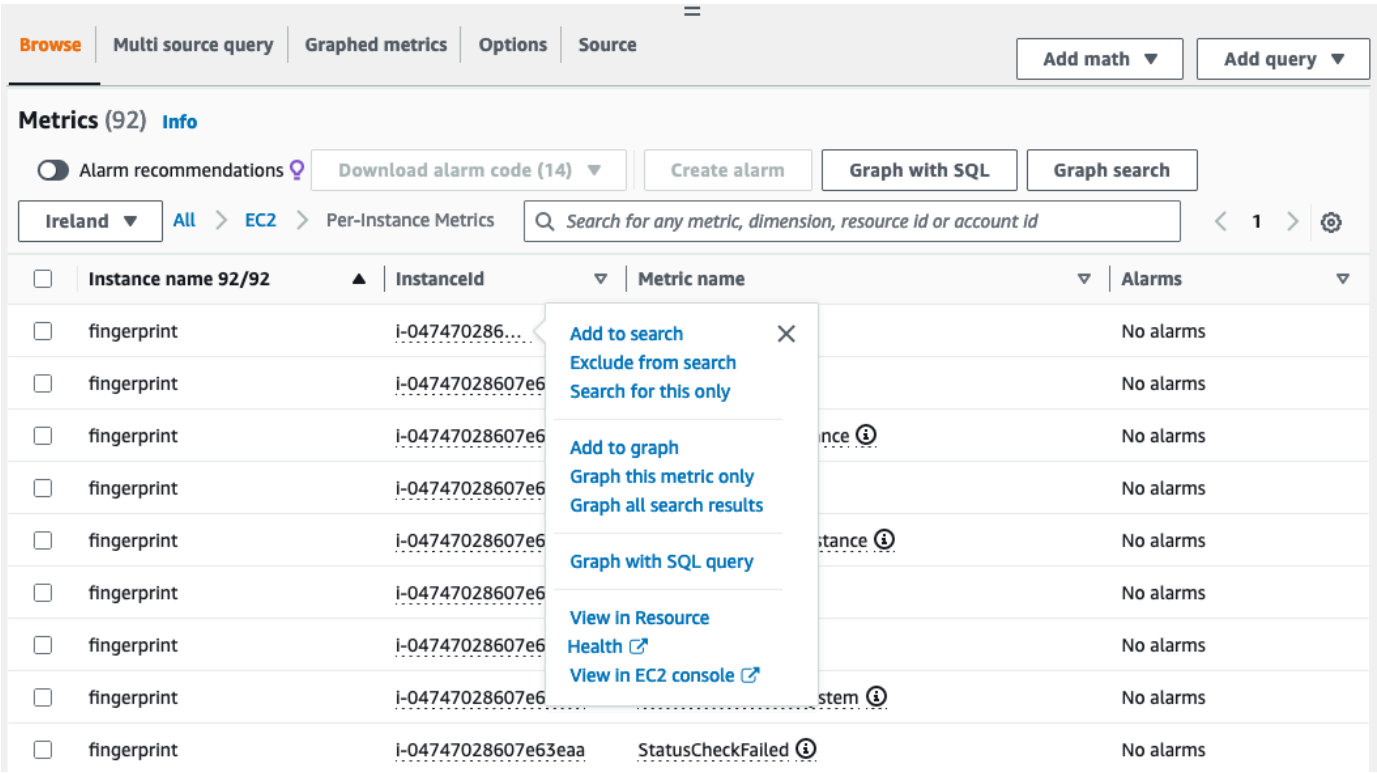
1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Erweitern Sie im Navigationsbereich Metriken und wählen Sie dann Alle Metriken aus.
3. Wählen Sie den Metrik-Namespace EC2.



4. Wählen Sie eine Metrikdimension aus (z. B. Per-Instance Metrics (Metriken pro Instance)).



5. Verwenden Sie die Spaltenüberschrift, um die Metriken zu sortieren. Um eine Metrik grafisch darzustellen, müssen Sie das Kontrollkästchen neben der Metrik aktivieren. Um nach Ressource zu filtern, müssen Sie zunächst die Ressourcen-ID und dann die Option Zu Suche hinzufügen auswählen. Um nach Metrik zu filtern, müssen Sie den Metriknamen und anschließend Add to search (Zur Suche hinzufügen) auswählen.



Listen Sie Metriken auf, indem Sie AWS CLI

Verwenden Sie den Befehl list-metrics, um die CloudWatch Metriken für Ihre Instances aufzulisten.

Auflisten aller verfügbaren Metriken für Amazon EC2 (AWS CLI)

Im folgenden Beispiel wird der `AWS/EC2`-Namespace angegeben, um alle Metriken für Amazon EC2 anzuzeigen.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

Ausgabebeispiel:

```
{
  "Metrics": [
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
```

```
            }
        ],
        "MetricName": "NetworkOut"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "CPUUtilization"
    },
    {
        "Namespace": "AWS/EC2",
        "Dimensions": [
            {
                "Name": "InstanceId",
                "Value": "i-1234567890abcdef0"
            }
        ],
        "MetricName": "NetworkIn"
    },
    ...
  ]
}
```

So listen Sie alle verfügbaren Metriken für eine Instance auf (AWS CLI)

Im folgenden Beispiel werden der `AWS/EC2`-Namespace und die `InstanceId`-Dimension angegeben, um die Ergebnisse nur für die angegebene Instance anzuzeigen.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --dimensions
 Name=InstanceId,Value=i-1234567890abcdef0
```

So listen Sie eine Metrik für alle Instances auf (AWS CLI)

Im folgenden Beispiel werden der `AWS/EC2`-Namespace und ein Metrikname angegeben, um die Ergebnisse nur für die angegebene Metrik anzuzeigen.

```
aws cloudwatch list-metrics --namespace AWS/EC2 --metric-name CPUUtilization
```

Installieren und konfigurieren Sie den CloudWatch Agenten mithilfe der Amazon EC2 EC2-Konsole, um zusätzliche Metriken hinzuzufügen

Die Installation und Konfiguration des CloudWatch Agenten mithilfe der Amazon EC2-Konsole befindet sich in der Beta-Phase für Amazon EC2 und kann sich ändern.

Standardmäßig CloudWatch stellt Amazon grundlegende Metriken wie `CPUUtilization` und `NetworkIn` für die Überwachung Ihrer Amazon EC2 EC2-Instances bereit. Um zusätzliche Metriken zu sammeln, können Sie den CloudWatch Agenten auf Ihren EC2-Instances installieren und den Agenten dann so konfigurieren, dass er ausgewählte Metriken ausgibt. Anstatt den CloudWatch Agenten auf jeder EC2-Instance manuell zu installieren und zu konfigurieren, können Sie die Amazon EC2 EC2-Konsole verwenden, um dies für Sie zu erledigen.

In diesem Thema wird erklärt, wie Sie die Amazon EC2 EC2-Konsole verwenden können, um den CloudWatch Agenten auf Ihren Instances zu installieren und den Agenten so zu konfigurieren, dass er ausgewählte Metriken ausgibt.

Die manuellen Schritte für diesen Vorgang finden Sie unter Installation des CloudWatch Agenten mithilfe AWS Systems Manager im CloudWatch Amazon-Benutzerhandbuch. Weitere Informationen über den CloudWatch Agenten finden Sie unter Erfassung von Metriken, Protokollen und Traces mit dem CloudWatch Agenten.

Themen

Voraussetzungen

Um Amazon EC2 zur Installation und Konfiguration des CloudWatch Agenten verwenden zu können, müssen Sie die in diesem Abschnitt beschriebenen Benutzer- und Instance-Voraussetzungen erfüllen.

Voraussetzungen für Benutzer

Um diese Funktion nutzen zu können, muss Ihr IAM-Konsolenbenutzer oder Ihre IAM-Rolle über die für die Verwendung von Amazon EC2 erforderlichen Berechtigungen und die folgenden IAM-Berechtigungen verfügen:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:PutParameter"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/EC2-Custom-Metrics-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:ListCommandInvocations",
                "ssm:DescribeInstanceInformation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetInstanceProfile",
                "iam:SimulatePrincipalPolicy"
            ],
            "Resource": "*"
        }
    ]
}
```

Voraussetzungen für die Instanz

- Status der Instanz: `running`
- Unterstütztes Betriebssystem: Linux
- AWS Systems Manager Agent (SSM-Agent): Installiert. Zwei Hinweise zum SSM-Agenten:

  - Der SSM-Agent ist auf einigen Amazon Machine Images (AMIs) vorinstalliert, die von vertrauenswürdigen Drittanbietern AWS bereitgestellt werden. Informationen zu den unterstützten AMIs und Anweisungen zur Installation des SSM-Agenten finden Sie im Benutzerhandbuch unter Amazon Machine Images (AMIs) with SSM Agent preinstalled.AWS Systems Manager
  - Wenn Sie Probleme mit dem SSM-Agenten haben, finden Sie weitere Informationen unter Problembehandlung beim SSM-Agenten im Benutzerhandbuch.AWS Systems Manager
- IAM-Berechtigungen für die Instanz: Die folgenden AWS verwalteten Richtlinien müssen einer IAM-Rolle hinzugefügt werden, die der Instanz zugeordnet ist:
  - AmazonSSM ManagedInstance Core — Ermöglicht einer Instance, Systems Manager zur Installation und Konfiguration des CloudWatch Agenten zu verwenden.
  - CloudWatchAgentServerRichtlinie — Ermöglicht einer Instance, den CloudWatch Agenten zum Schreiben von Daten zu verwenden. CloudWatch

  Informationen zum Hinzufügen von IAM-Berechtigungen zu Ihrer Instance finden Sie unter Verwenden von Instanzprofilen im IAM-Benutzerhandbuch.

Funktionsweise

Bevor Sie die Amazon EC2 EC2-Konsole zur Installation und Konfiguration des CloudWatch Agenten verwenden können, müssen Sie sicherstellen, dass Ihr IAM-Benutzer oder Ihre IAM-Rolle und die Instances, auf denen Sie Metriken hinzufügen möchten, bestimmte Voraussetzungen erfüllen. Anschließend können Sie die Amazon EC2 EC2-Konsole verwenden, um den CloudWatch Agenten auf Ihren ausgewählten Instances zu installieren und zu konfigurieren.

Erfüllen Sie zunächst die Voraussetzungen

- Sie benötigen die erforderlichen IAM-Berechtigungen — Bevor Sie beginnen, stellen Sie sicher, dass Ihr Konsolenbenutzer oder Ihre Rolle über die erforderlichen IAM-Berechtigungen verfügt, um diese Funktion nutzen zu können.
- Instanzen — Um die Funktion nutzen zu können, müssen Ihre EC2-Instances Linux-Instances sein, auf denen der SSM-Agent installiert ist, über die erforderlichen IAM-Berechtigungen verfügen und ausgeführt werden.

Dann können Sie die Funktion verwenden

1. Wählen Sie Ihre Instances aus — In der Amazon EC2 EC2-Konsole wählen Sie die Instances aus, auf denen der CloudWatch Agent installiert und konfiguriert werden soll. Anschließend starten Sie den Vorgang, indem Sie „ CloudWatch Agent konfigurieren“ wählen.
2. SSM-Agent validieren — Amazon EC2 überprüft, ob der SSM-Agent auf jeder Instance installiert und gestartet ist. Alle Instances, die diese Prüfung nicht bestehen, werden vom Prozess ausgeschlossen. Der SSM-Agent wird verwendet, um während dieses Prozesses Aktionen auf der Instance auszuführen.
3. IAM-Berechtigungen validieren — Amazon EC2 überprüft, ob jede Instance über die erforderlichen IAM-Berechtigungen für diesen Prozess verfügt. Alle Instances, die diese Prüfung nicht bestehen, werden vom Prozess ausgeschlossen. Die IAM-Berechtigungen ermöglichen es dem CloudWatch Agenten, Metriken von der Instance zu sammeln und ihn in den SSM-Agenten AWS Systems Manager zu integrieren, um ihn zu verwenden.
4. CloudWatch Agent validieren — Amazon EC2 überprüft, ob der CloudWatch Agent auf jeder Instance installiert ist und ausgeführt wird. Falls Instances diese Prüfung nicht bestehen, bietet Amazon EC2 an, den CloudWatch Agenten für Sie zu installieren und zu starten. Sobald dieser Vorgang abgeschlossen ist, erfasst der CloudWatch Agent die ausgewählten Metriken für jede Instance.
5. Metrikkonfiguration auswählen — Sie wählen die Metriken aus, die der CloudWatch Agent von Ihren Instances ausgeben soll. Nach der Auswahl speichert Amazon EC2 eine Konfigurationsdatei im Parameter Store, wo sie verbleibt, bis der Vorgang abgeschlossen ist. Amazon EC2 löscht die Konfigurationsdatei aus dem Parameter Store, sofern der Vorgang nicht unterbrochen wird. Beachten Sie, dass, wenn Sie keine Metrik auswählen, sie aber zuvor zu Ihrer Instance hinzugefügt haben, diese nach Abschluss dieses Vorgangs aus Ihrer Instance entfernt wird.
6. CloudWatch Agentenkonfiguration aktualisieren — Amazon EC2 sendet die Metrikkonfiguration an den CloudWatch Agenten. Dies ist der letzte Schritt in diesem Prozess. Wenn dies erfolgreich ist, können Ihre Instances Daten für die ausgewählten Metriken ausgeben und Amazon EC2 löscht die Konfigurationsdatei aus dem Parameter Store.

Kosten

Zusätzliche Metriken, die Sie während dieses Vorgangs hinzufügen, werden als benutzerdefinierte Metriken in Rechnung gestellt. Weitere Informationen zu den Preisen von CloudWatch Metriken finden Sie unter CloudWatch Amazon-Preise.

Installieren und konfigurieren Sie den CloudWatch Agenten

Sie können die Amazon EC2 EC2-Konsole verwenden, um den CloudWatch Agenten zu installieren und zu konfigurieren, um zusätzliche Metriken hinzuzufügen.

> **Note**
>
> Jedes Mal, wenn Sie dieses Verfahren ausführen, überschreiben Sie die bestehende CloudWatch Agentenkonfiguration. Wenn Sie keine Metrik auswählen, die zuvor ausgewählt wurde, wird sie aus der Instanz entfernt.

Um den CloudWatch Agenten mit der Amazon EC2 EC2-Konsole zu installieren und zu konfigurieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instances aus, auf denen der CloudWatch Agent installiert und konfiguriert werden soll.
4. Wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Agent konfigurieren.

   > **Tip**
   >
   > Diese Funktion ist nicht in allen verfügbar AWS-Regionen. Wenn Configure CloudWatch Agent nicht verfügbar ist, versuchen Sie es mit einer anderen Region.

5. Lesen Sie für jeden Schritt des Vorgangs den Konsolentext und wählen Sie dann Weiter.
6. Um den Vorgang abzuschließen, wählen Sie im letzten Schritt Vollständig aus.

Abrufen der Statistiken von Metriken für Ihre Instances

Sie können Statistiken zu den CloudWatch Metriken für Ihre Instances abrufen.

Inhalt

- Aggregieren von Statistiken nach Auto Scaling-Gruppe
- Aggregieren von Statistiken nach AMI

Statistik-Übersicht

Statistiken sind Aggregationen von Metrikdaten über bestimmte Zeiträume. CloudWatch stellt Statistiken bereit, die auf den metrischen Datenpunkten basieren, die durch Ihre benutzerdefinierten Daten oder durch andere Dienste bereitgestellt werden. AWS CloudWatch Für die Aggregationen werden der Namespace, der Metrikname, die Dimensionen und die Datenpunkt-Maßeinheit innerhalb des von Ihnen angegebenen Zeitraums verwendet. Die folgende Tabelle beschreibt die verfügbaren Statistiken.

Statistik	Beschreibung
`Minimum`	Der niedrigste beobachtete Wert während eines angegebenen Zeitraums. Sie können diesen Wert verwenden, um für Ihre Anwendung Aktivitäten geringen Umfangs zu bestimmen.
`Maximum`	Der höchste beobachtete Wert während eines angegebenen Zeitraums. Sie können diesen Wert verwenden, um für Ihre Anwendung Aktivitäten hohen Umfangs zu bestimmen.
`Sum`	Alle für die passende Metrik übermittelten Werte werden addiert. Diese Statistik kann nützlich sein, um das Gesamtvolumen einer Metrik zu ermitteln.
`Average`	Der Wert von `Sum`/`SampleCount` während eines angegebenen Zeitraums. Wenn Sie diese Statistik mit dem `Minimum` und dem `Maximum` vergleichen, können Sie den vollen Umfang einer Metrik bestimmen und feststellen, wie nahe die durchschnittliche Nutzung an das `Minimum` und `Maximum` heranreicht. Dank dieses Vergleichs wissen Sie dann, wann Sie Ihre Ressourcen je nach Bedarf erhöhen oder verringern sollten.
`SampleCount`	Die Anzahl der für die statistische Berechnung verwendeten Datenpunkte.
`pNN.NN`	Der Wert des angegebenen Perzentils. Sie können ein beliebiges Perzentil mit bis zu zwei Dezimalstellen (z. B. p95,45) angeben.

Abrufen von Statistiken für eine bestimmte Instance

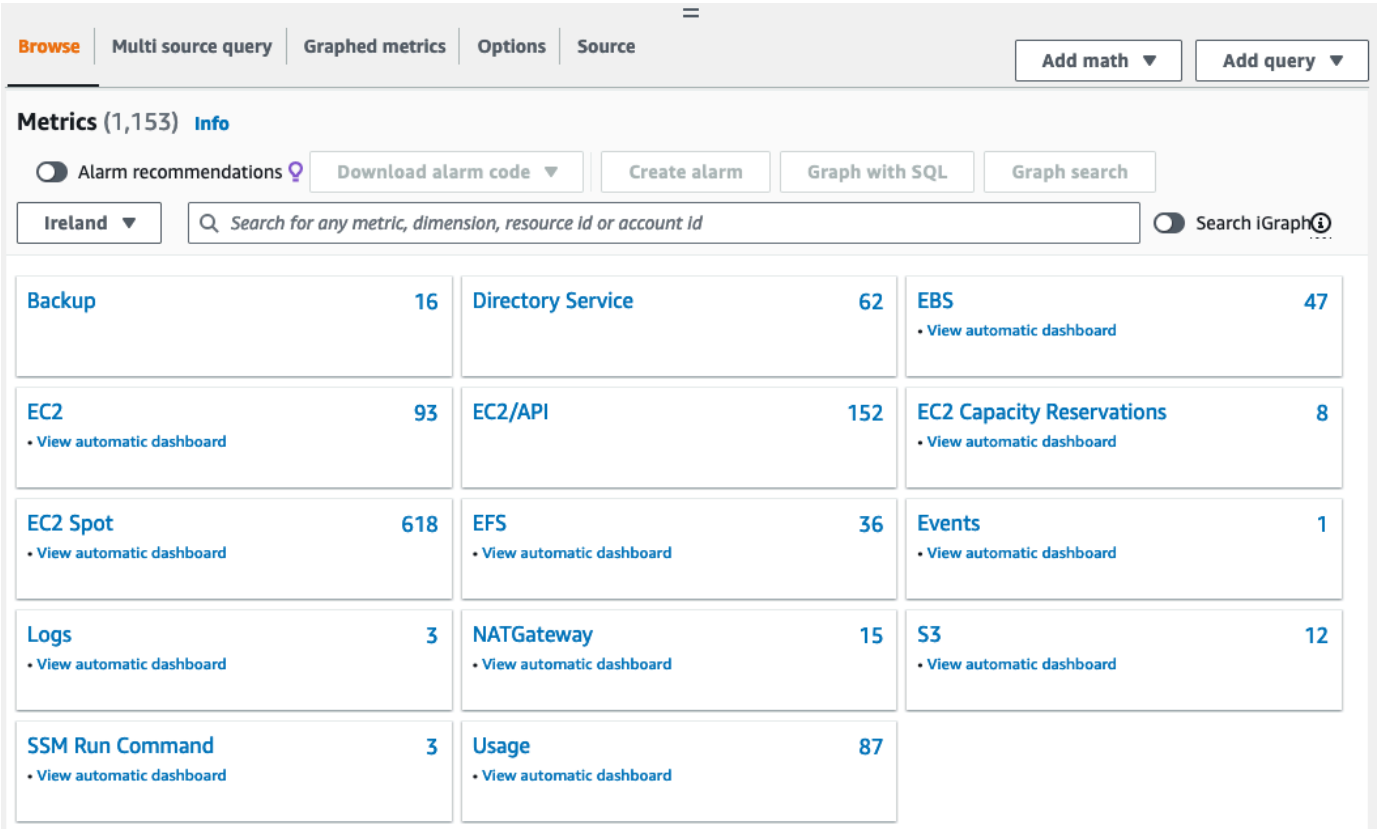
Die folgenden Beispiele zeigen Ihnen, wie Sie mit AWS Management Console oder die AWS CLI die maximale CPU-Auslastung einer bestimmten EC2-Instance ermitteln können.

Voraussetzungen

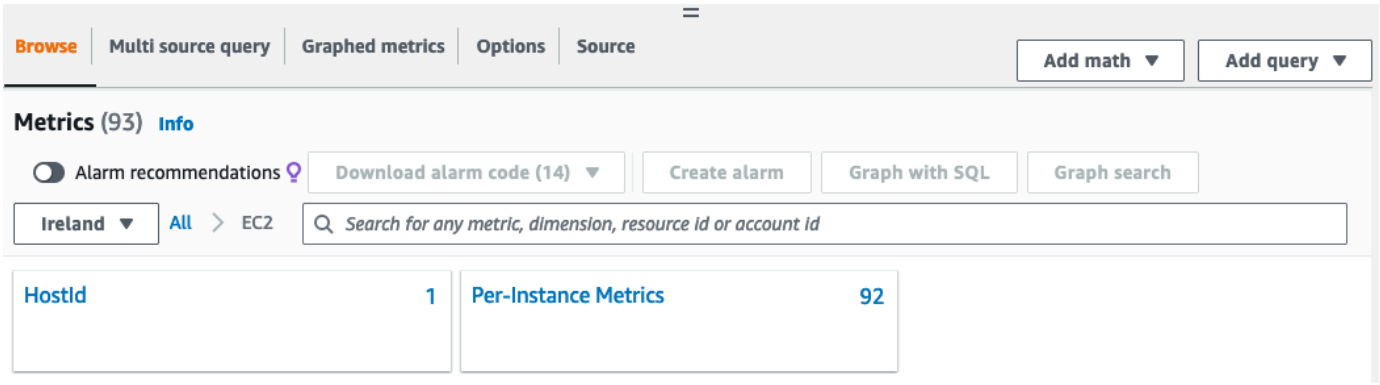
- Sie müssen die ID der Instance kennen. Sie können die Instance-ID mit der AWS Management Console oder mit dem Befehl describe-instances abrufen.
- Standardmäßig ist die grundlegende Überwachung aktiviert. Sie können aber auch eine detaillierte Überwachung aktivieren. Weitere Informationen finden Sie unter Aktivieren oder Deaktivieren der detaillierten Überwachung für Ihre Instances.

So zeigen Sie die CPU-Auslastung für eine bestimmte Instance an (Konsole)

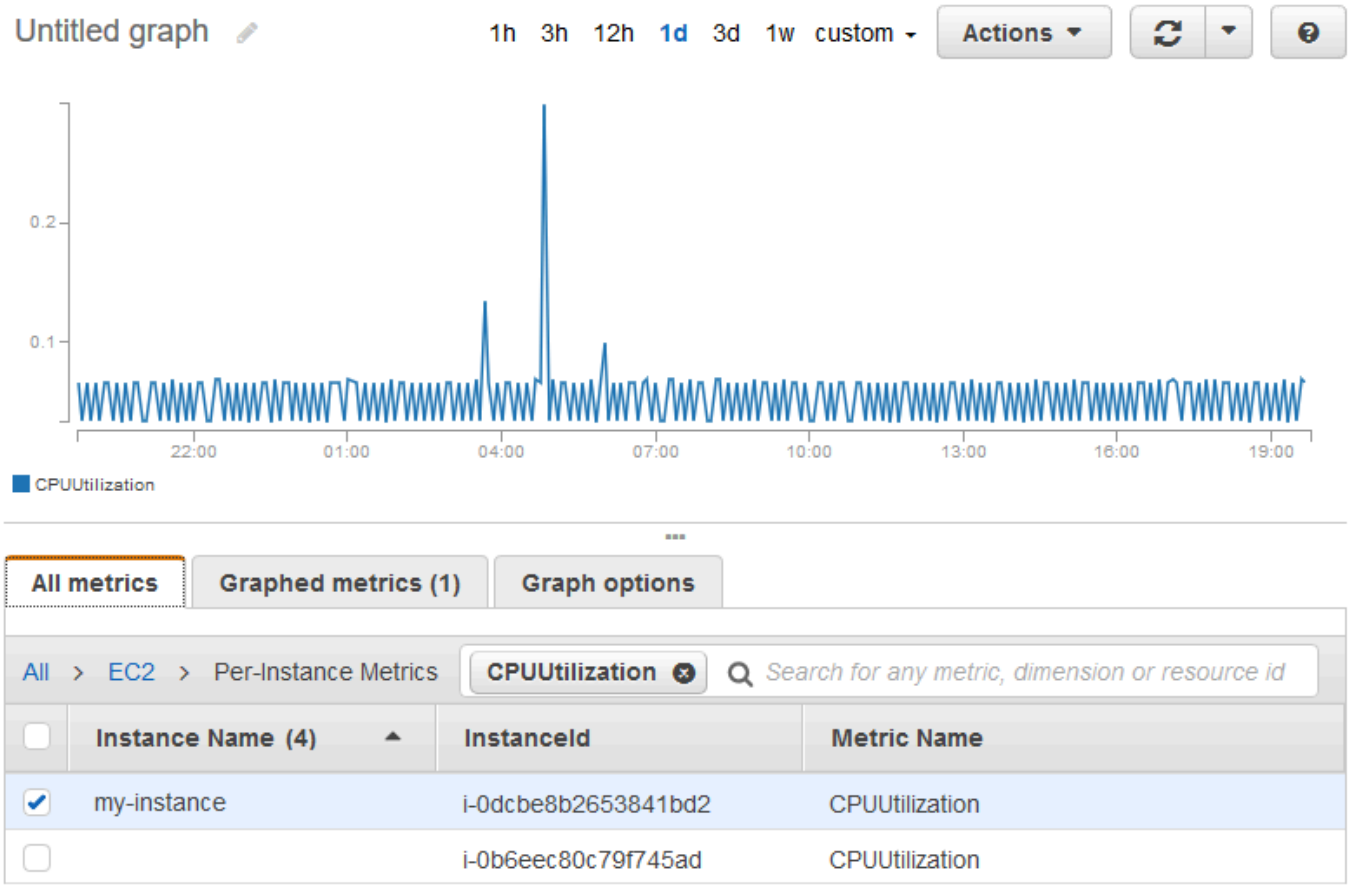
1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den Metrik-Namespace EC2.



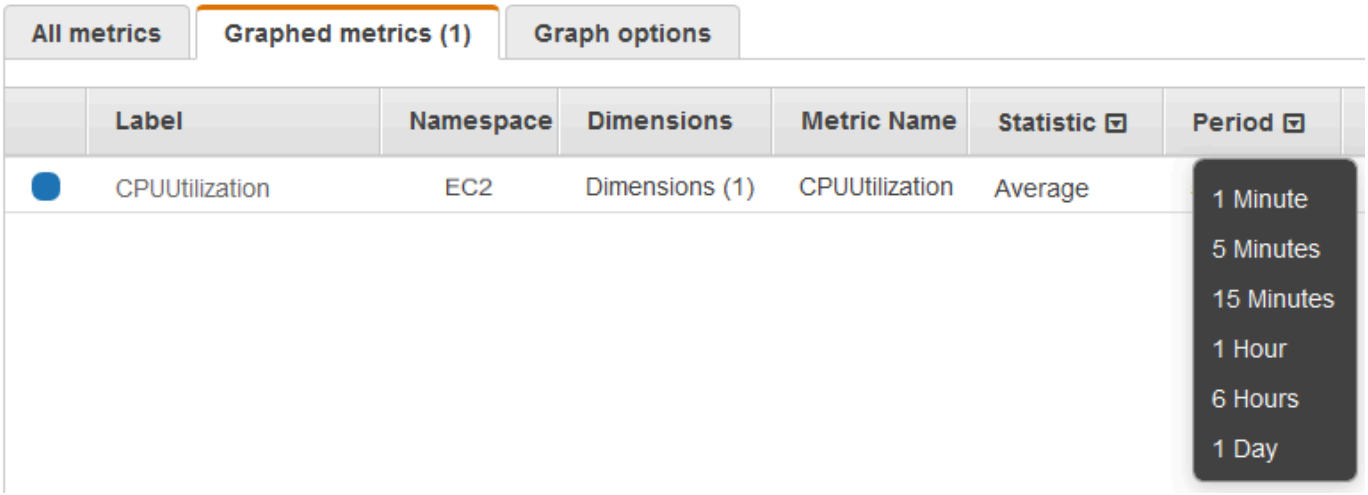
4. Wählen Sie die Dimension Per-Instance Metrics (Metriken pro Instance) aus.



5. Geben Sie **`CPUUtilization`** in das Suchfeld ein und drücken Sie die Eingabetaste. Wählen Sie die Zeile für eine konkrete Instance aus, in der ein Diagramm mit der CPUUtilization-Metrik für die Instance angezeigt wird. Wählen Sie das Stiftsymbol aus, um das Diagramm zu benennen. Wenn Sie den Zeitraum ändern möchten, müssen Sie einen der vordefinierten Werte oder custom (benutzerdefiniert) auswählen.



6. Um die Statistik oder den Zeitraum der Metrik zu ändern, müssen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) auswählen. Wählen Sie die Spaltenüberschrift oder einen einzelnen Wert und anschließend einen anderen Wert aus.



So rufen Sie die CPU-Auslastung für eine bestimmte Instance ab (AWS CLI)

Verwenden Sie den Befehl get-metric-statistics, um die CPUUtilization-Metrik für die angegebene Instance mithilfe des angegebenen Zeitraums und Zeitintervalls abzurufen:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
--statistics Maximum --dimensions Name=InstanceId,Value=i-1234567890abcdef0 \
--start-time 2022-10-18T23:18:00 --end-time 2022-10-19T23:18:00
```

Es folgt eine Beispielausgabe. Jeder Wert repräsentiert die maximale CPU-Auslastung in Prozent für eine einzelne EC2 Instance.

```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-19T00:18:00Z",
            "Maximum": 0.33000000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T03:18:00Z",
            "Maximum": 99.670000000000002,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T07:18:00Z",
            "Maximum": 0.34000000000000002,
```

```
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-19T12:18:00Z",
            "Maximum": 0.34000000000000002,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Aggregieren von Statistiken auf allen Instances

Sie können verfügbare Statistiken für die Instances aggregieren, für die die detaillierte Überwachung aktiviert ist. Instances, die die grundlegende Überwachung verwenden, sind nicht in den Zusammenfassungen enthalten. Bevor Sie die Statistiken abrufen können, die für alle Instances aggregiert wurden, müssen Sie die detaillierte Überwachung (gegen Aufpreis) aktivieren, bei der Daten in 1-Minuten-Intervallen bereitgestellt werden.

Beachten Sie, dass Amazon CloudWatch keine Daten regionsübergreifend AWS aggregieren kann. Die Metriken sind zwischen Regionen vollständig voneinander getrennt.

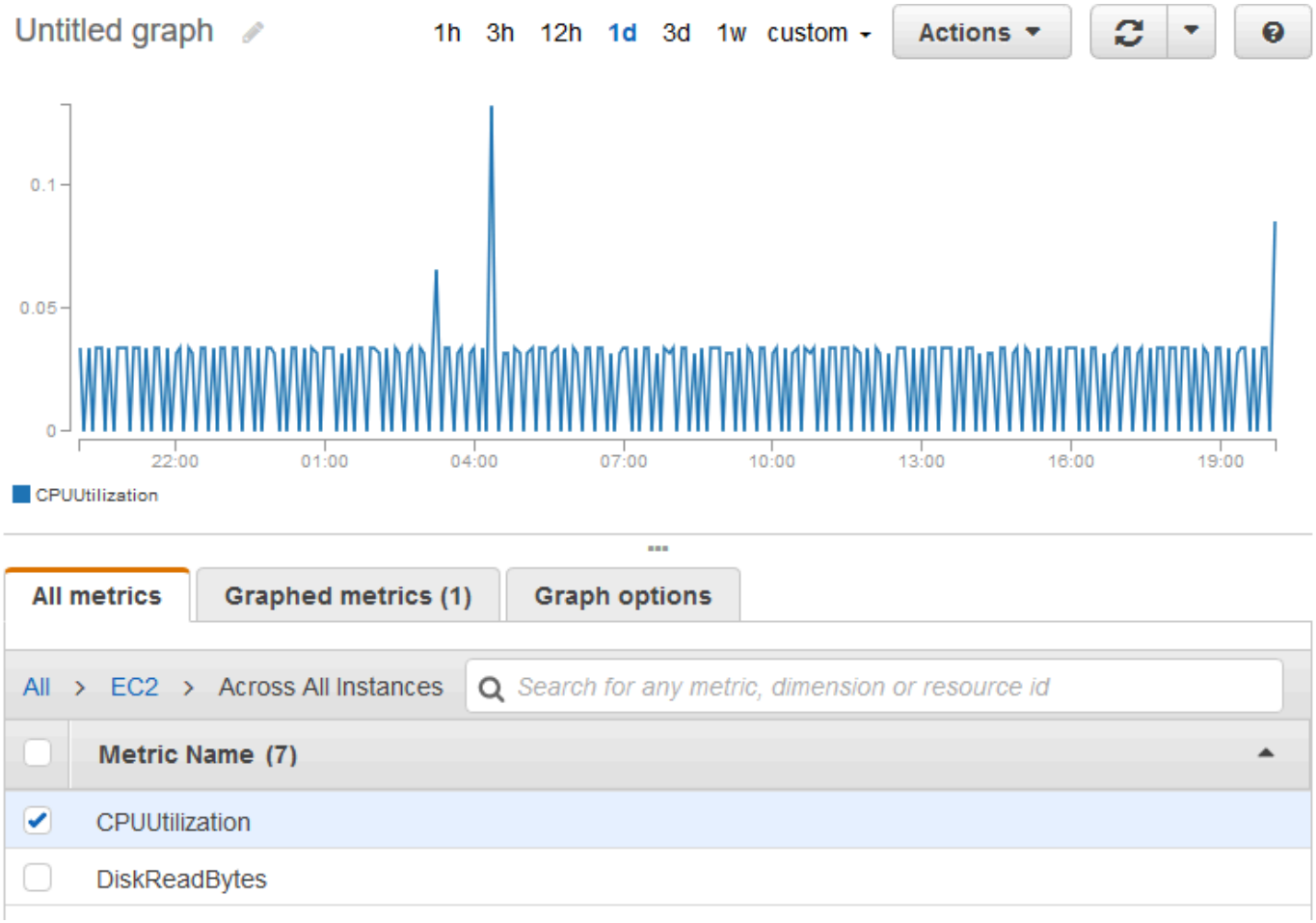
Dieses Beispiel zeigt, wie Sie die detaillierte Überwachung verwenden können, um die durchschnittliche CPU-Auslastung für Ihre EC2 Instances abzurufen. Da keine Dimension angegeben ist, werden Statistiken für alle Dimensionen im `AWS/EC2` Namespace CloudWatch zurückgegeben.

> **Important**
>
> Diese Technik zum Abrufen aller Dimensionen in einem AWS Namespace funktioniert nicht für benutzerdefinierte Namespaces, die Sie auf Amazon veröffentlichen. CloudWatch Bei benutzerdefinierten Namespaces müssen Sie die vollständige Palette von Dimensionen angeben, die im Zusammenhang mit einem bestimmten Datenpunkt stehen, um Statistiken zu diesem Datenpunkt abzurufen.

So zeigen Sie die durchschnittliche CPU-Auslastung für Ihre gesamten Instances an (Konsole)

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/cloudwatch/. CloudWatch
2. Wählen Sie im Navigationsbereich Metriken aus.

3. Wählen Sie den Namespace EC2 und Across All Instances (Über alle Instances) aus.
4. Wählen Sie die Zeile mit CPUUtilization aus, in der ein Diagramm für die Metrik Ihrer gesamten EC2 Instances angezeigt wird. Wählen Sie das Stiftsymbol aus, um das Diagramm zu benennen. Wenn Sie den Zeitraum ändern möchten, müssen Sie einen der vordefinierten Werte oder custom (benutzerdefiniert) auswählen.



5. Um die Statistik oder den Zeitraum der Metrik zu ändern, müssen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) auswählen. Wählen Sie die Spaltenüberschrift oder einen einzelnen Wert und anschließend einen anderen Wert aus.

So rufen Sie die durchschnittliche CPU-Auslastung für Ihre gesamten Instances ab (AWS CLI)

Verwenden Sie den Befehl get-metric-statistics wie folgt, um den Durchschnittswert der CPUUtilization-Metrik für Ihre gesamten Instances abzurufen.

```
aws cloudwatch get-metric-statistics \
    --namespace AWS/EC2 \
    --metric-name CPUUtilization \
```

```
    --period 3600  --statistics "Average" "SampleCount" \
    --start-time 2022-10-11T23:18:00 \
    --end-time 2022-10-12T23:18:00
```

Ausgabebeispiel:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2022-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2022-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```

Aggregieren von Statistiken nach Auto Scaling-Gruppe

Sie können Statistiken für die EC2 Instances in einer Auto Scaling-Gruppe aggregieren. Beachten Sie, dass Amazon CloudWatch keine Daten regionsübergreifend AWS aggregieren kann. Die Metriken sind zwischen Regionen vollständig voneinander getrennt.

Dieses Beispiel zeigt, wie Sie die Gesamtzahl der Bytes abrufen, die für eine einzelne Auto Scaling-Gruppe auf den Datenträger geschrieben werden. Der Gesamtzahl wird für einminütige Zeiträume eines 24-Stunden-Intervalls für alle EC2 Instances in der angegebenen Auto Scaling-Gruppe berechnet.

Zur Anzeige DiskWriteBytes für die Instances in einer Auto Scaling Scaling-Gruppe (Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den Namespace EC2 und anschließend By Auto Scaling Group (Nach Auto Scaling-Gruppe) aus.
4. Wählen Sie die Zeile für die DiskWriteByte-Metrik und die spezifische Auto Scaling Scaling-Gruppe aus, in der ein Diagramm für die Metrik für die Instances in der Auto Scaling Scaling-Gruppe angezeigt wird. Wählen Sie das Stiftsymbol aus, um das Diagramm zu benennen. Wenn Sie den Zeitraum ändern möchten, müssen Sie einen der vordefinierten Werte oder custom (benutzerdefiniert) auswählen.
5. Um die Statistik oder den Zeitraum der Metrik zu ändern, müssen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) auswählen. Wählen Sie die Spaltenüberschrift oder einen einzelnen Wert und anschließend einen anderen Wert aus.

Zur Anzeige DiskWriteBytes für die Instances in einer Auto Scaling Scaling-Gruppe (AWS CLI)

Verwenden Sie den Befehl get-metric-statistics wie folgt:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name DiskWriteBytes
 --period 360 \
--statistics "Sum" "SampleCount" --dimensions Name=AutoScalingGroupName,Value=my-asg --
start-time 2022-10-16T23:18:00 --end-time 2022-10-18T23:18:00
```

Ausgabebeispiel:

```
{
    "Datapoints": [
        {
            "SampleCount": 18.0,
            "Timestamp": "2022-10-19T21:36:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
        },
        {
            "SampleCount": 5.0,
            "Timestamp": "2022-10-19T21:42:00Z",
            "Sum": 0.0,
            "Unit": "Bytes"
```

```
        }
    ],
    "Label": "DiskWriteBytes"
}
```

Aggregieren von Statistiken nach AMI

Sie können Statistiken für Ihre Instances aggregieren, für die die detaillierte Überwachung aktiviert ist. Instances, die die grundlegende Überwachung verwenden, sind nicht in den Zusammenfassungen enthalten. Bevor Sie die Statistiken abrufen können, die für alle Instances aggregiert wurden, müssen Sie die detaillierte Überwachung (gegen Aufpreis) aktivieren, bei der Daten in 1-Minuten-Intervallen bereitgestellt werden.

Beachten Sie, dass Amazon CloudWatch keine Daten regionsübergreifend AWS aggregieren kann. Die Metriken sind zwischen Regionen vollständig voneinander getrennt.

Dieses Beispiel zeigt, wie Sie die durchschnittliche CPU-Auslastung für alle Instances abrufen, die ein bestimmtes Amazon Machine Image (AMI) verwenden. Der Durchschnitt wird über 60-Sekunden-Intervalle für einen Zeitraum von einem Tag berechnet.

So zeigen Sie die durchschnittliche CPU-Auslastung nach AMI an (Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den Namespace EC2 aus und dann By Image (AMI) Id (Nach Image-ID (AMI)).
4. Wählen Sie die Zeile für die Metrik CPUUtilization und das spezifische AMI aus, das für ein bestimmtes AMI ein Diagramm für die Metrik anzeigt. Wählen Sie das Stiftsymbol aus, um das Diagramm zu benennen. Wenn Sie den Zeitraum ändern möchten, müssen Sie einen der vordefinierten Werte oder custom (benutzerdefiniert) auswählen.
5. Um die Statistik oder den Zeitraum der Metrik zu ändern, müssen Sie die Registerkarte Graphed metrics (Grafisch dargestellte Metriken) auswählen. Wählen Sie die Spaltenüberschrift oder einen einzelnen Wert und anschließend einen anderen Wert aus.

So rufen Sie die durchschnittliche CPU-Auslastung für eine Image-ID ab (AWS CLI)

Verwenden Sie den Befehl get-metric-statistics wie folgt:

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization
 --period 3600 \
```

```
--statistics Average --dimensions Name=ImageId,Value=ami-3c47a355 --start-
time 2022-10-10T00:00:00 --end-time 2022-10-11T00:00:00
```

Es folgt eine Beispielausgabe. Jeder Wert stellt die durchschnittliche CPU-Auslastung in Prozent für die EC2 Instances mit dem angegebenen AMI dar.


```
{
    "Datapoints": [
        {
            "Timestamp": "2022-10-10T07:00:00Z",
            "Average": 0.041000000000000009,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T14:00:00Z",
            "Average": 0.079579831932773085,
            "Unit": "Percent"
        },
        {
            "Timestamp": "2022-10-10T06:00:00Z",
            "Average": 0.036000000000000011,
            "Unit": "Percent"
        },
        ...
    ],
    "Label": "CPUUtilization"
}
```


Grafisches Darstellen von Metriken für Ihre Instances

Nachdem Sie die Instance gestartet haben, können Sie die Amazon EC2-Konsole öffnen und auf der Registerkarte Monitoring (Überwachung) die Überwachungsdiagramme für eine Instance anzeigen. Jedes Diagramm basiert auf einer der verfügbaren Amazon EC2-Metriken.

Folgende Diagramme sind verfügbar:

- Durchschnittliche CPU-Auslastung (in Prozent)
- Durchschnittliche Lesevorgänge (in Byte)
- Durchschnittliche Schreibvorgänge (in Byte)
- Maximaler Netzwerkeingang (in Byte)
- Maximaler Netzwerkausgang (in Byte)

- Zusammenfassung der Datenträger-Lesevorgänge (Anzahl)
- Zusammenfassung der Datenträger-Schreibvorgänge (Anzahl)
- Statuszusammenfassung (Beliebig)
- Statuszusammenfassung Instance (Anzahl)
- Statuszusammenfassung System (Anzahl)

Weitere Informationen zu den für die Diagramme bereitgestellten Metriken und Daten erhalten Sie unter Listet die verfügbaren CloudWatch Metriken für Ihre Instances auf.

Stellen Sie Metriken mithilfe der CloudWatch Konsole grafisch dar

Sie können die CloudWatch Konsole auch verwenden, um von Amazon EC2 und anderen AWS Services generierte Metrikdaten grafisch darzustellen. Weitere Informationen finden Sie unter Metriken grafisch darstellen im CloudWatch Amazon-Benutzerhandbuch.

Erstellen Sie einen CloudWatch Alarm für eine Instance

Sie können einen CloudWatch Alarm erstellen, der die CloudWatch Metriken für eine Ihrer Instances überwacht. CloudWatchsendet Ihnen automatisch eine Benachrichtigung, wenn die Metrik einen von Ihnen angegebenen Schwellenwert erreicht. Sie können einen CloudWatch Alarm mit der Amazon EC2 EC2-Konsole oder mit den erweiterten Optionen der CloudWatch Konsole erstellen.

Um einen Alarm mit der CloudWatch Konsole zu erstellen

Beispiele finden Sie unter CloudWatchAmazon-Alarme erstellen im CloudWatch Amazon-Benutzerhandbuch.

So erstellen Sie einen Alarm mit der Amazon EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.
4. Wählen Sie auf der Detailseite CloudWatch Alarme verwalten unter Alarm hinzufügen oder bearbeiten die Option Alarm erstellen aus.
5. Wählen Sie unter Alarmbenachrichtigung, ob Sie Amazon Simple Notification Service (Amazon SNS)-Benachrichtigungen konfigurieren möchten. Geben Sie ein vorhandenes Amazon SNS-Thema ein oder geben Sie einen Namen ein, um ein neues Thema zu erstellen.

6. Wählen Sie unter Alarmaktion, ob Sie eine Aktion angeben möchten, die beim Auslösen des Alarms ausgeführt werden soll. Wählen Sie eine Aktion aus der Liste aus.
7. Wählen Sie unter Alarmschwellenwerte die Metrik und Kriterien für den Alarm aus. Wenn Sie beispielsweise einen Alarm erstellen möchten, der ausgelöst wird, wenn die CPU-Auslastung für einen Zeitraum von fünf Minuten 80 % erreicht, gehen Sie wie folgt vor:
   a. Behalten Sie die Standardeinstellung für Stichproben gruppieren nach (Durchschnitt) und Art der abzufragenden Daten (CPU-Auslastung) bei.
   b. Wählen Sie für Alarm bei die Option **>=** aus und geben Sie unter Prozent den Wert **`0.80`** ein.
   c. Geben unter Aufeinanderfolgender Zeitraum den Wert **1** ein und wählen Sie unter Zeitraum die Option 5 Minuten.
8. (Optional) Wählen Sie für Beispiel-Metrikdaten die Option Zu Dashboard hinzufügen aus.
9. Wählen Sie Create (Erstellen) aus.

Sie können Ihre CloudWatch Alarmeinstellungen von der Amazon EC2 EC2-Konsole oder der CloudWatch Konsole aus bearbeiten. Wenn Sie Ihren Alarm löschen möchten, können Sie dies von der CloudWatch Konsole aus tun. Weitere Informationen finden Sie unter Bearbeiten oder Löschen eines CloudWatch Alarms im CloudWatch Amazon-Benutzerhandbuch.

Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird

Mithilfe von CloudWatch Amazon-Alarmaktionen können Sie Alarme erstellen, die Ihre Instances automatisch stoppen, beenden, neu starten oder wiederherstellen. Sie können die Aktionen zum Anhalten oder Beenden nutzen, um Geld zu sparen, wenn eine Instance über einen längeren Zeitraum nicht ausgeführt werden muss. Sie können die Aktionen zum Neustarten oder Wiederherstellen verwenden, um diese Instances automatisch neu zu starten oder um sie – für den Fall, dass eine Systembeeinträchtigung eintritt – auf einer neuen Hardware wiederherzustellen.

> **Note**
>
> Abrechnungs- und Preisinformationen für Amazon CloudWatch Alarms finden Sie unter CloudWatch Abrechnung und Kosten im CloudWatch Amazon-Benutzerhandbuch.

Die `AWSServiceRoleForCloudWatchEvents` dienstbezogene Rolle ermöglicht es AWS , Alarmaktionen in Ihrem Namen durchzuführen. Wenn Sie zum ersten Mal einen Alarm in der AWS Management Console, der oder der AWS CLI IAM-API erstellen, CloudWatch wird die dienstbezogene Rolle für Sie erstellt.

Es gibt eine Reihe von Szenarien, bei denen Sie Ihre Instance möglicherweise automatisch anhalten oder beenden möchten. Beispielsweise verwenden Sie Instances für die Stapelverarbeitung von Gehaltsabrechnungen oder wissenschaftliche Datenverarbeitungsaufgaben, die für einen bestimmten Zeitraum ausgeführt werden und ihre Arbeit anschließend abschließen. Anstatt diese Instances im Leerlauf beizubehalten (und damit Kosten anfallen zu lassen), können Sie sie auch anhalten oder beenden und so Geld sparen. Der Hauptunterschied zwischen der Verwendung einer Alarmaktion zum Anhalten und einer Alarmaktion zum Beenden besteht darin, dass Sie eine angehaltene Instance problemlos wieder neu starten können, wenn sie später wieder ausgeführt werden soll, und Sie dieselbe Instance-ID und dasselbe Stamm-Volume beibehalten können. Eine beendete Instance können Sie dagegen nicht neu starten. Stattdessen müssen Sie eine neue Instance starten. Wenn eine Instance angehalten oder beendet wird, gehen Daten auf Instance-Speicher-Volumes verloren.

Sie können die Aktionen Beenden, Beenden, Neustarten oder Wiederherstellen zu jedem Alarm hinzufügen, der für eine Amazon EC2-Metrik pro Instance festgelegt ist, einschließlich grundlegender und detaillierter Überwachungsmetriken, die von Amazon CloudWatch (im `AWS/EC2` Namespace) bereitgestellt werden, sowie zu allen benutzerdefinierten Metriken, die die `InstanceId` Dimension enthalten, sofern sich ihr Wert auf eine gültige laufende Amazon EC2 EC2-Instance bezieht.

> **Important**
>
> Alarme zur Statusprüfung können vorübergehend in den `INSUFFICIENT_DATA` Status wechseln, wenn metrische Datenpunkte fehlen. Dies ist zwar selten, kann aber passieren, wenn es zu einer Unterbrechung der metrischen Berichtssysteme kommt, selbst wenn eine Instanz fehlerfrei ist. Wir empfehlen, den `INSUFFICIENT_DATA` Status als fehlende Daten und nicht als Alarmverletzung zu behandeln, insbesondere wenn der Alarm so konfiguriert wird, dass eine Instance gestoppt, beendet, neu gestartet oder wiederhergestellt wird.

Konsolenunterstützung

Sie können Alarme mit der Amazon EC2 EC2-Konsole oder der CloudWatch Konsole erstellen. Für die Vorgehensweisen in dieser Dokumentation wird die Amazon EC2-Konsole verwendet. Verfahren,

die die CloudWatch Konsole verwenden, finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Erstellen von Alarmen, die eine Instance stoppen, beenden, neu starten oder wiederherstellen.

Berechtigungen

Sie müssen über das `iam:CreateServiceLinkedRole` verfügen, um einen Alarm zu erstellen oder zu ändern, der EC2-Alarmaktionen ausführt. Eine Servicerolle ist eine IAM-Rolle, die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

Inhalt

Stoppaktionen zu CloudWatch Amazon-Alarmen hinzufügen

Sie können einen Alarm erstellen, mit dem eine Amazon EC2- Instance angehalten wird, sobald ein bestimmter Schwellenwert erreicht wird. Es kann beispielsweise sein, dass Sie Entwicklungs- oder Test-Instances ausführen und gelegentlich vergessen, diese herunterzufahren. Sie können einen Alarm einrichten, der ausgelöst wird, wenn die durchschnittliche prozentuale CPU-Auslastung 24 Stunden lang unter 10 Prozent fällt. Dies signalisiert, dass sich die Instance im Leerlauf befindet und nicht mehr verwendet wird. Sie können den Schwellenwert, die Dauer und den Zeitraum an Ihre Anforderungen anpassen. Außerdem haben Sie die Möglichkeit, eine Amazon-Simple-Notification-Service (Amazon SNS)-Benachrichtigung hinzuzufügen, damit Sie eine E-Mail erhalten, sobald der Alarm ausgelöst wird.

Instances, die ein Amazon EBS-Volume als Root-Gerät verwenden, können angehalten oder beendet werden. Instances, die den Instance-Speicher als Root-Gerät verwenden, können dagegen nur beendet werden. Daten auf Instance-Speicher-Volumes gehen verloren, wenn die Instance beendet oder gestoppt wird.

So erstellen Sie einen Alarm, um eine im Leerlauf befindliche Instance anzuhalten (Amazon EC2-Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.

   Alternativ können Sie das Pluszeichen (

) in der Spalte Alarm status (Alarmstatus) auswählen.
4. Gehen Sie auf der Seite „ CloudWatch Alarme verwalten“ wie folgt vor:

   a. Wählen Sie Create an alarm (Einen Alarm erstellen).

   b. Um eine E-Mail zu erhalten, wenn der Alarm ausgelöst wird, wählen Sie für Alarm notification (Alarmbenachrichtigung) ein vorhandenes Amazon SNS-Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

   c. Schalten Sie die Alarm action (Alarmaktion) ein und wählen Sie Stop (Anhalten).

   d. Wählen Sie für Group samples by (Beispiele gruppieren nach) und Type of data to sample (Datentypen, die in Beispielen aufgeführt werden sollen) eine Statistik und eine Metrik. Wählen Sie in diesem Beispiel die Optionen Average und CPU Utilization (CPU-Nutzung).

   e. Geben Sie für Alarm When (Alarm bei) und Percent (Prozent) den metrischen Schwellenwert an. In diesem Beispiel geben Sie <= und 10 Prozent an.

   f. Geben Sie für Consecutive period (Aufeinanderfolgender Zeitraum) und Period (Zeitraum) den Bewertungszeitraum für den Alarm an. Geben Sie in diesem Beispiel 1 aufeinanderfolgende Periode von 5 Minuten an.

   g. Amazon erstellt CloudWatch automatisch einen Alarmnamen für Sie. Um den Namen zu ändern, geben Sie für Alarm name (Alarmname) einen neuen Namen ein. Alarmnamen dürfen nur ASCII-Zeichen enthalten.

   > **Note**
   >
   > Sie können die Alarmkonfiguration vor dem Erstellen des Alarms gemäß Ihren eigenen Anforderungen anpassen oder diese später ändern. Dies umfasst die

Einstellungen für Metrik, Schwellenwert, Dauer, Aktion und Benachrichtigung. Nachdem Sie einen Alarm erstellt haben, können Sie seinen Namen aber nicht mehr bearbeiten.

h. Wählen Sie Create (Erstellen) aus.

Beendenaktionen zu CloudWatch Amazon-Alarmen hinzufügen

Sie können einen Alarm erstellen, mit dem eine EC2 Instance automatisch beendet wird, sobald ein bestimmter Schwellenwert erreicht wird (solange für die Instance kein Beendigungsschutz aktiviert ist). Es kann beispielsweise sein, dass Sie eine Instance beenden möchten, sobald diese ihre Arbeit abgeschlossen hat, und dass Sie die Instance nicht noch einmal benötigen. Wenn Sie die Instance unter Umständen später noch einmal verwenden möchten, sollten Sie die Instance nur anhalten, anstatt sie zu beenden. Daten auf Instance-Speicher-Volumes gehen verloren, wenn die Instance beendet wird. Informationen zum Aktivieren und Deaktivieren des Beendigungsschutzes für eine Instance finden Sie unter Aktivieren des Beendigungsschutzes.

So erstellen Sie einen Alarm, um eine im Leerlauf befindliche Instance zu beenden (Amazon EC2-Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instanz aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.

   Alternativ können Sie das Pluszeichen (

) in der Spalte Alarm status (Alarmstatus) auswählen.
4. Gehen Sie auf der Seite „ CloudWatch Alarme verwalten“ wie folgt vor:

   a. Wählen Sie Create an alarm (Einen Alarm erstellen).

   b. Um eine E-Mail zu erhalten, wenn der Alarm ausgelöst wird, wählen Sie für Alarm notification (Alarmbenachrichtigung) ein vorhandenes Amazon SNS-Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

c. Schalten Sie die Alarm action (Alarmaktion) ein und wählen Sie Terminate (Beenden).

d. Wählen Sie für Group samples by (Beispiele gruppieren nach) und Type of data to sample (Datentypen, die in Beispielen aufgeführt werden sollen) eine Statistik und eine Metrik. Wählen Sie in diesem Beispiel die Optionen Average und CPU Utilization (CPU-Nutzung).

e. Geben Sie für Alarm When (Alarm bei) und Percent (Prozent) den metrischen Schwellenwert an. In diesem Beispiel geben Sie => und 10 Prozent an.

f. Geben Sie für Consecutive period (Aufeinanderfolgender Zeitraum) und Period (Zeitraum) den Bewertungszeitraum für den Alarm an. Geben Sie in diesem Beispiel 24 aufeinanderfolgende Perioden von 1 Hour (einer Stunde) an.

g. Amazon erstellt CloudWatch automatisch einen Alarmnamen für Sie. Um den Namen zu ändern, geben Sie für Alarm name (Alarmname) einen neuen Namen ein. Alarmnamen dürfen nur ASCII-Zeichen enthalten.

> **Note**
>
> Sie können die Alarmkonfiguration vor dem Erstellen des Alarms gemäß Ihren eigenen Anforderungen anpassen oder diese später ändern. Dies umfasst die Einstellungen für Metrik, Schwellenwert, Dauer, Aktion und Benachrichtigung. Nachdem Sie einen Alarm erstellt haben, können Sie seinen Namen aber nicht mehr bearbeiten.

h. Wählen Sie Create (Erstellen) aus.

Neustartaktionen zu CloudWatch Amazon-Alarmen hinzufügen

Sie können einen CloudWatch Amazon-Alarm erstellen, der eine Amazon EC2-Instance überwacht und die Instance automatisch neu startet. Die Alarmaktion zum Neustarten wird für Instance-Zustandsprüfungsfehler empfohlen (im Gegensatz zur Alarmaktion zum Wiederherstellen, die sich für System-Zustandsprüfungsfehler eignet). Ein Neustart einer Instance entspricht einem Neustart des Betriebssystems. In den meisten Fällen dauert es nur wenige Minuten, um die Instance neu zu starten. Wenn Sie eine Instance neu starten, verbleibt sie auf demselben physischen Host, sodass die Instance ihren öffentlichen DNS- Namen, ihre private IP-Adresse sowie alle Daten auf ihren Instance-Speicher-Volumes behält.

Im Gegensatz zum Anhalten und erneuten Starten der Instance beginnt mit dem erneuten Hochfahren einer Instance kein neuer Instance-Abrechnungszeitraum (mit einer minimalen 1-

Minuten-Abrechnung). Daten auf Instance-Speicher-Volumes werden beibehalten, wenn die Instance neu gestartet wird. Die Instance-Speicher-Volumes müssen nach einem Neustart erneut in das Dateisystem gemountet werden. Weitere Informationen finden Sie unter Durchführen eines Neustarts Ihrer Instance.

> **Important**
>
> Um eine Race-Bedingung zwischen der Neustart- und der Wiederherstellungsaktion zu vermeiden, sollten Sie für den Neustartalarm und den Wiederherstellungsalarm nicht die gleiche Anzahl von Auswertungszeiträumen festlegen. Wir empfehlen, dass Sie Neustartalarme zu drei Auswertungszeiträumen von jeweils einer Minute festlegen. Weitere Informationen finden Sie unter Auswertung eines Alarms im CloudWatch Amazon-Benutzerhandbuch.

So erstellen Sie einen Alarm, um eine Instance neu zu starten (Amazon EC2-Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.

   Alternativ können Sie das Pluszeichen (

) in der Spalte Alarm status (Alarmstatus) auswählen.
4. Gehen Sie auf der Seite „ CloudWatch Alarme verwalten“ wie folgt vor:

   a. Wählen Sie Create an alarm (Einen Alarm erstellen).

   b. Um eine E-Mail zu erhalten, wenn der Alarm ausgelöst wird, wählen Sie für Alarm notification (Alarmbenachrichtigung) ein vorhandenes Amazon SNS-Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

   c. Schalten Sie die Alarm action (Alarmaktion) ein und wählen Sie Reboot (Neustart).

   d. Wählen Sie für Group samples by (Beispiele gruppieren nach) und Type of data to sample (Datentypen, die in Beispielen aufgeführt werden sollen) eine Statistik und eine Metrik.

In diesem Beispiel wählen Sie Average (Durchschnitt) und Status check failed: instance (Statusprüfung fehlgeschlagen: Instance).

e. Geben Sie für Consecutive period (Aufeinanderfolgender Zeitraum) und Period (Zeitraum) den Bewertungszeitraum für den Alarm an. Geben Sie in diesem Beispiel 3 aufeinanderfolgende Perioden von 5 Minuten an.

f. Amazon erstellt CloudWatch automatisch einen Alarmnamen für Sie. Um den Namen zu ändern, geben Sie für Alarm name (Alarmname) einen neuen Namen ein. Alarmnamen dürfen nur ASCII-Zeichen enthalten.

g. Wählen Sie Create (Erstellen) aus.

Wiederherstellungsaktionen zu CloudWatch Amazon-Alarmen hinzufügen

Sie können einen CloudWatch Amazon-Alarm erstellen, der eine Amazon EC2-Instance überwacht. Wenn die Instance aufgrund eines zugrunde liegenden Hardwarefehlers oder eines Problems, das eine Reparatur erfordert AWS , beeinträchtigt wird, können Sie die Instance automatisch wiederherstellen. Beendete Instances können nicht wiederhergestellt werden. Eine wiederhergestellte Instance ist mit der ursprünglichen Instance identisch. Dies schließt auch die Instance-ID, private IP-Adressen, Elastic IP-Adressen und alle Instance-Metadaten mit ein.

CloudWatch verhindert, dass Sie eine Wiederherstellungsaktion zu einem Alarm hinzufügen, der sich auf einer Instance befindet, die keine Wiederherstellungsaktionen unterstützt.

Wird der Alarm `StatusCheckFailed_System` ausgelöst und die Aktion zum Wiederherstellen initiiert, werden Sie über das Amazon SNS-Thema, das Sie bei der Erstellung des Alarms gewählt haben und das mit der Aktion zum Wiederherstellen verknüpft ist, darüber benachrichtigt. Während der Instance-Wiederherstellung wird die Instance bei einem Instance-Neustart migriert und alle im Speicher befindlichen Daten gehen verloren. Wenn der Vorgang abgeschlossen ist, wird die Information in dem SNS-Thema, das Sie für den Alarm konfiguriert haben, veröffentlicht. Alle Personen, die das SNS-Thema abonniert haben, erhalten eine Benachrichtigung per E-Mail, in der auch der Status des Wiederherstellungsversuchs und weitere Anweisungen enthalten sind. Sie bemerken, dass auf der wiederhergestellten Instance ein Instance-Neustart durchgeführt wird.

> **Note**
>
> Die Aktion zum Wiederherstellen kann nur mit `StatusCheckFailed_System` verwendet werden, nicht mit `StatusCheckFailed_Instance`.

Hier sind die Probleme aufgeführt, die dazu führen können, dass System-Statusprüfungen fehlschlagen:

- Verlust der Netzwerkverbindung
- Systemstromausfall
- Softwareprobleme auf dem physischen Host
- Hardwareprobleme auf dem physischen Host, die die Erreichbarkeit des Netzwerks beeinträchtigen

Die Wiederherstellungsaktion wird nur auf Instances unterstützt, die bestimmte Kriterien erfüllen. Weitere Informationen finden Sie unter Resilienz der Instanz.

Wenn Ihre Instance über eine öffentliche IP-Adresse verfügt, wird diese nach der Wiederherstellung beibehalten.

> **Important**
>
> Um eine Race-Bedingung zwischen der Neustart- und der Wiederherstellungsaktion zu vermeiden, sollten Sie für den Neustartalarm und den Wiederherstellungsalarm nicht die gleiche Anzahl von Auswertungszeiträumen festlegen. Wir empfehlen, dass Sie Wiederherstellungsalarme zu zwei Auswertungszeiträumen von jeweils einer Minute festlegen. Weitere Informationen finden Sie unter Auswertung eines Alarms im CloudWatch Amazon-Benutzerhandbuch.

So erstellen Sie einen Alarm, um eine Instance wiederherstellen (Amazon EC2-Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus und wählen Sie Aktionen, Überwachung und Fehlerbehebung, CloudWatch Alarme verwalten aus.

   Alternativ können Sie das Pluszeichen (

) in der Spalte Alarm status (Alarmstatus) auswählen.
4. Gehen Sie auf der Seite „ CloudWatch Alarme verwalten“ wie folgt vor:

   a. Wählen Sie Create an alarm (Einen Alarm erstellen).

b. Um eine E-Mail zu erhalten, wenn der Alarm ausgelöst wird, wählen Sie für Alarm notification (Alarmbenachrichtigung) ein vorhandenes Amazon SNS-Thema aus. Sie müssen zuerst mit der Amazon-SNS-Konsole ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Verwenden von Amazon SNS für application-to-person (A2P) -Messaging im Amazon Simple Notification Service Developer Guide.

> **Note**
>
> Benutzer müssen das angegebene SNS-Thema abonnieren, um E-Mail-Benachrichtigungen zu erhalten, wenn der Alarm ausgelöst wird. The erhält Root-Benutzer des AWS-Kontos immer E-Mail-Benachrichtigungen, wenn automatische Aktionen zur Instance-Wiederherstellung ausgeführt werden, auch wenn kein SNS-Thema angegeben ist oder der Root-Benutzer das angegebene SNS-Thema nicht abonniert hat.

c. Schalten Sie die Alarm action (Alarmaktion) ein und wählen Sie Recover (Wiederherstellen).

d. Wählen Sie für Group samples by (Beispiele gruppieren nach) und Type of data to sample (Datentypen, die in Beispielen aufgeführt werden sollen) eine Statistik und eine Metrik. In diesem Beispiel wählen Sie Average (Durchschnitt) und Status check failed: system (Statusprüfung fehlgeschlagen: System).

e. Geben Sie für Consecutive period (Aufeinanderfolgender Zeitraum) und Period (Zeitraum) den Bewertungszeitraum für den Alarm an. Geben Sie in diesem Beispiel 2 aufeinanderfolgende Perioden von 5 Minuten an.

f. Amazon erstellt CloudWatch automatisch einen Alarmnamen für Sie. Um den Namen zu ändern, geben Sie für Alarm name (Alarmname) einen neuen Namen ein. Alarmnamen dürfen nur ASCII-Zeichen enthalten.

g. Wählen Sie Create (Erstellen) aus.

Verwenden Sie die CloudWatch Amazon-Konsole, um den Alarm- und Aktionsverlauf einzusehen

Sie können den Alarm- und Aktionsverlauf in der CloudWatch Amazon-Konsole einsehen. Amazon CloudWatch speichert den Alarm- und Aktionsverlauf der letzten zwei Wochen.

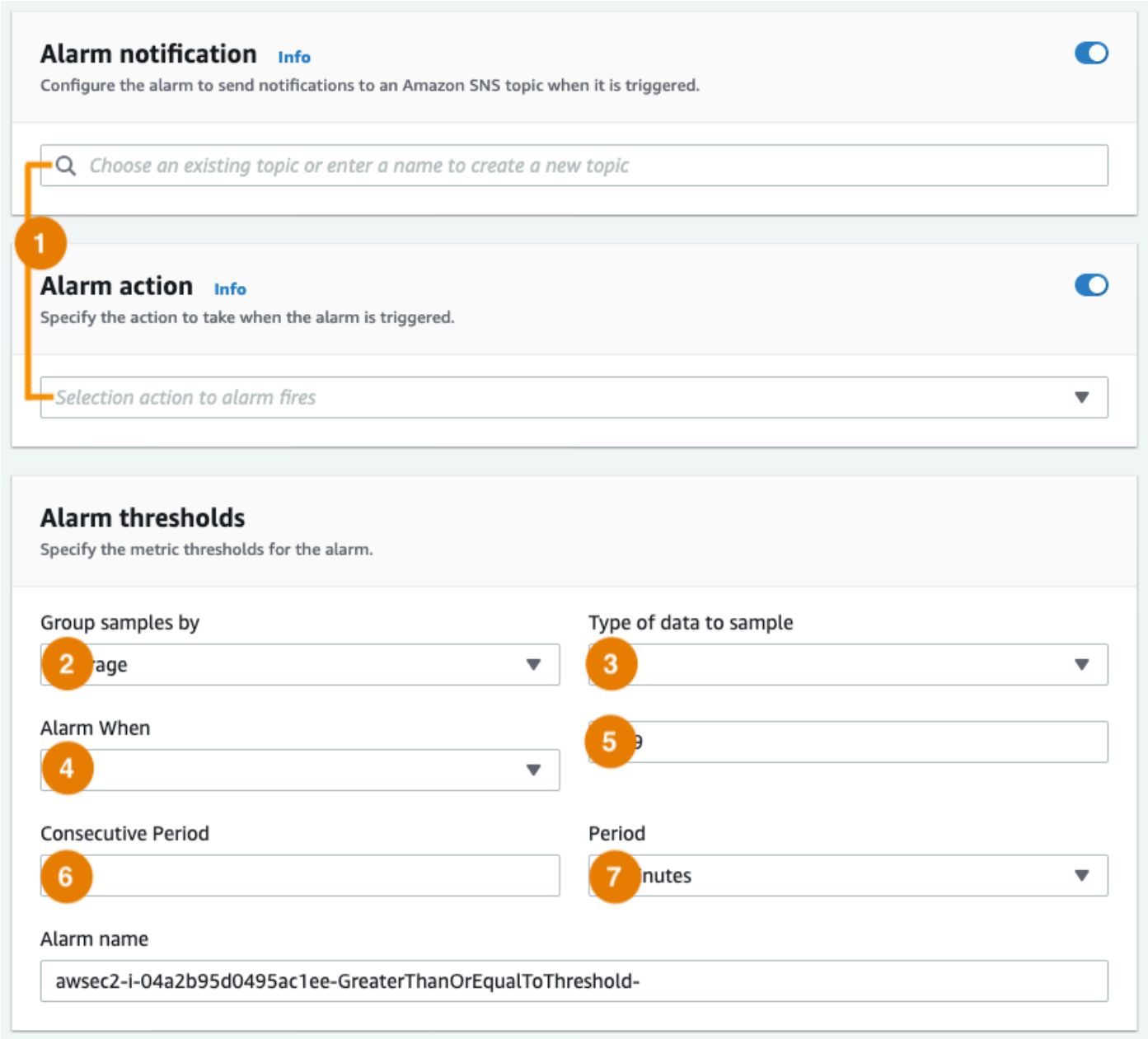
Um den Verlauf der ausgelösten Alarme und Aktionen einzusehen (CloudWatch Konsole)

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Klicken Sie im Navigationsbereich auf Alarme.
3. Wählen Sie einen Alarm aus.
4. Auf der Registerkarte Details wird neben den Zeit- und Metrikwerten der neueste Statusübergang angezeigt.
5. Wählen Sie die Registerkarte History (Verlauf), um die neuesten Verlaufseinträge anzuzeigen.

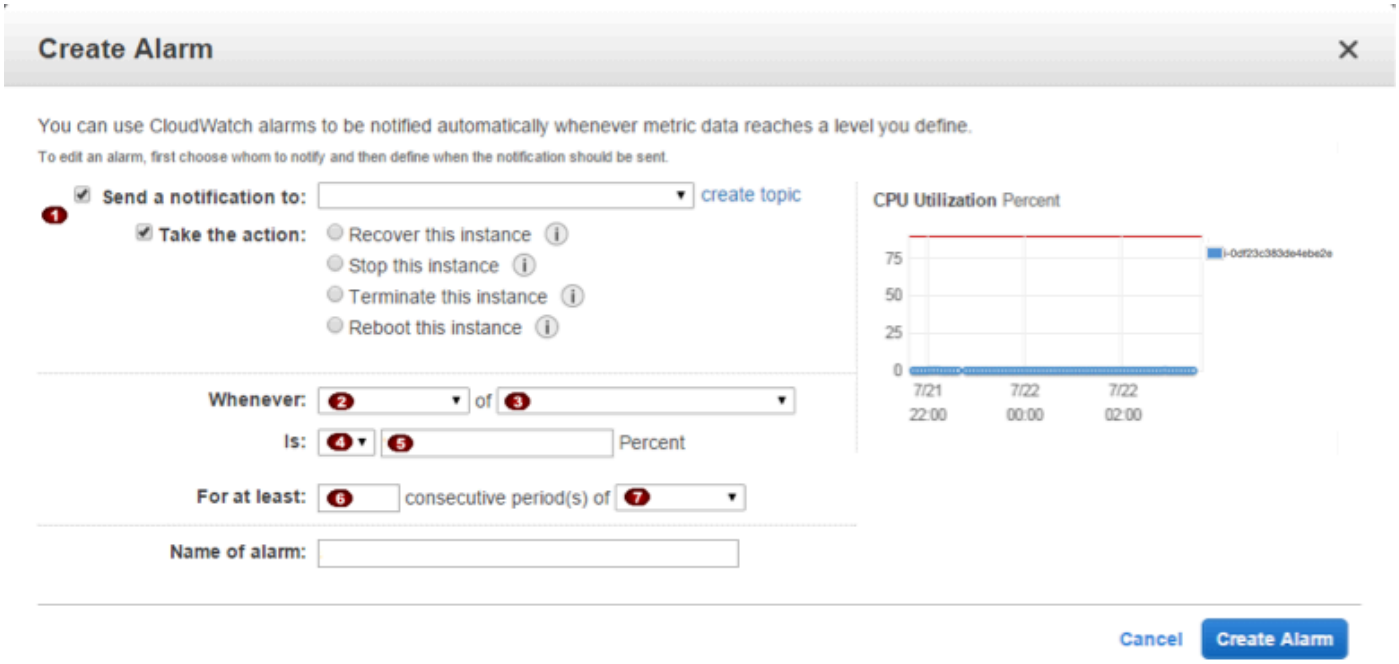
CloudWatch Amazon-Alarmaktionsszenarien

Sie können die Amazon EC2-Konsole zum Erstellen von Alarmaktionen verwenden, mit denen eine Amazon EC2 Instance angehalten oder beendet wird, wenn bestimmte Bedingungen erfüllt sind. In den folgenden Screenshots der Konsolenseite, auf der Sie die Alarmaktionen festlegen, haben wir die Einstellungen nummeriert. Wir haben auch die Einstellungen in den darauffolgenden Szenarien nummeriert, damit Sie die entsprechenden Aktionen leichter erstellen können.

New console


Alarm notification Info
Configure the alarm to send notifications to an Amazon SNS topic when it is triggered.
Choose an existing topic or enter a name to create a new topic
1
Alarm action Info
Specify the action to take when the alarm is triggered.
Selection action to alarm fires
Alarm thresholds
Specify the metric thresholds for the alarm.
Group samples by
2
Type of data to sample
3
Alarm When
4
5
Consecutive Period
6
Period
7
Alarm name
awsec2-i-04a2b95d0495ac1ee-GreaterThanOrEqualToThreshold-

Old console



Szenario 1: Anhalten von im Leerlauf befindlichen Entwicklungs- und Test-Instances

Erstellen Sie einen Alarm, mit dem eine für die Software-Entwicklung oder das Testing bestimmte Instance angehalten wird, wenn sie sich seit mindestens einer Stunde im Leerlauf befindet.

Einstellung	Wert
1	Stoppen
2	Maximum
3	CPU-Auslastung
4	<=
5	10 %
6	1
7	1 Stunde

Szenario 2: Anhalten von im Leerlauf befindlichen Instances

Erstellen Sie einen Alarm, mit dem eine Instance angehalten und eine E-Mail gesendet wird, wenn sich die Instance seit 24 Stunden im Leerlauf befindet.

Einstellung	Wert
1	Anhalten und Senden einer E-Mail
2	Durchschnitt
3	CPU-Auslastung
4	<=
5	5 %
6	24
7	1 Stunde

Szenario 3: Senden von E-Mails zu Webservern mit ungewöhnlich hohem Datenverkehrsaufkommen

Erstellen Sie einen Alarm, mit dem eine E-Mail gesendet wird, wenn für eine Instance pro Tag der Grenzwert von 10 GB an ausgehendem Netzwerkdatenverkehr überschritten wird.

Einstellung	Wert
1	E-Mail
2	Summe
3	Netzwerkausgang
4	>
5	10 GB
6	24

Einstellung	Wert
7	1 Stunde

Szenario 4: Anhalten von Webservern mit ungewöhnlich hohem Datenverkehrsaufkommen

Erstellen Sie einen Alarm, mit dem eine Instance angehalten und eine Textnachricht (SMS) gesendet wird, wenn der ausgehende Datenverkehr den Grenzwert von 1 GB pro Stunde überschreitet.

Einstellung	Wert
1	Anhalten und Senden einer SMS
2	Summe
3	Netzwerkausgang
4	>
5	1 GB
6	1
7	1 Stunde

Szenario 5: Anhalten einer beeinträchtigten Instance

Erstellen Sie einen Alarm, mit dem eine Instance angehalten wird, die drei aufeinander folgende Statusprüfungen (im Abstand von 5 Minuten) nicht bestanden hat.

Einstellung	Wert
1	Stoppen
2	Durchschnitt
3	Statusprüfung fehlgeschlagen: System
4	-

Einstellung	Wert
5	-
6	1
7	15 Minuten

Szenario 6: Beenden von Instances nach dem Abschluss von Stapelverarbeitungsaufträgen

Erstellen Sie einen Alarm, mit dem eine Instance für Stapelaufträge beendet wird, wenn keine Ergebnisdaten mehr gesendet werden.

Einstellung	Wert
1	Beenden
2	Maximum
3	Netzwerkausgang
4	<=
5	100 000 Bytes
6	1
7	5 Minuten

Automatisieren Sie Amazon EC2 mit EventBridge

Sie können Amazon verwenden EventBridge , um Systemereignisse wie Probleme mit der Anwendungsverfügbarkeit oder Ressourcenänderungen zu automatisieren AWS-Services und automatisch darauf zu reagieren. Ereignisse im AWS Rahmen von Services werden nahezu EventBridge in Echtzeit zugestellt. Sie können Regeln erstellen, um anzugeben, an welchen Ereignissen Sie interessiert sind, und welche Aktionen auszuführen sind, wenn ein Ereignis mit einer Regel übereinstimmt. Die folgenden Aktionen können beispielsweise automatisch ausgelöst werden:

- Rufen Sie eine Funktion auf AWS Lambda
- Aufrufen eines Amazon-EC2-Ausführungsbefehls
- Weitergabe des Ereignisses an Amazon Kinesis Data Streams
- Aktiviere eine AWS Step Functions Zustandsmaschine
- Benachrichtigen eines Amazon-SNS-Themas
- Benachrichtigen einer Amazon-SQS-Warteschlange

Im Folgenden finden Sie Beispiele für die Verwendung EventBridge mit Amazon EC2:

- Aktivieren Sie eine Lambda-Funktion immer dann, wenn eine Instance in den Ausführungsstatus übergeht.
- Benachrichtigen Sie ein Amazon-SNS-Thema, wenn ein Amazon-EBS-Volume erstellt oder geändert wird.
- Senden Sie mit Amazon EC2 Run Command einen Befehl an eine oder mehrere Amazon EC2 EC2-Instances, wenn ein bestimmtes Ereignis in einem anderen AWS Service eintritt.

Weitere Informationen finden Sie im EventBridge Amazon-Benutzerhandbuch.

Amazon-EC2-Ereignistypen

Amazon EC2 unterstützt die folgenden Ereignistypen:

- EC2-AMI-Statusänderung
- EC2 Schnellstart Benachrichtigung über Statusänderungen
- EC2-Flotten-Fehler
- Informationen zur EC2-Flotte
- Ändern der EC2-Flotten-Instance
- Ändern der Anforderung der EC2-Flotte-Spot-Instance
- Verändern des EC2-Flottenzustand
- Empfehlung zum Ausgleich einer EC2-Instance
- Benachrichtigung über die Statusänderung für eine EC2-Instance
- EC2-Spot-Flottenfehler
- Informationen zur EC2-Spot-Flotte

- Ändern der EC2-Spot-Flotten-Instance
- Ändern der Anforderung der EC2-Spot-Flotten-Spot-Instance
- Verändern des EC2-Spot-Flottenzustands
- Unterbrechungswarnung zur EC2-Spot-Instance
- Erfüllung einer EC2-Spot-Instance-Anforderung
- Benachrichtigung zur EC2-ODCR-Nichtauslastung

Informationen zu den von Amazon EBS unterstützten Ereignistypen finden Sie unter EventBridge Für Amazon EBS.

Amazon EC2 EC2-API-Aufrufe protokollieren mit AWS CloudTrail

Die Amazon EC2 EC2-API ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der von einem Benutzer, einer Rolle oder einem AWS-Service ausgeführten Aktionen bereitstellt. CloudTrail erfasst alle API-Aufrufe für Amazon EC2 als Ereignisse, einschließlich Aufrufe von der Konsole und von Codeaufrufen an die API-Operationen. Anhand der von gesammelten Informationen können Sie die Anfrage ermitteln CloudTrail, die an die Amazon EC2 EC2-API gestellt wurde, die IP-Adresse, von der aus die Anfrage gestellt wurde, wann sie gestellt wurde usw.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Amazon EC2 EC2-API-Informationen in CloudTrail

CloudTrail ist auf Ihrem aktiviert AWS-Konto , wenn Sie das Konto erstellen. Wenn Aktivitäten in Amazon EC2 und Amazon EBS auftreten, wird diese Aktivität zusammen mit anderen AWS-Service Ereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können in Ihrem AWS-Konto die neusten Ereignisse anzeigen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit dem CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS-Konto, einschließlich Ereignissen für Amazon EC2 und Amazon EBS, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen-Regionen. Der Trail protokolliert Ereignisse aus allen Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie hier:

- Erstellen Sie einen Trail für Ihren AWS-Konto
- AWS-Service Integrationen mit Protokollen CloudTrail
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle Amazon EC2 EC2-Aktionen und Amazon EBS-Verwaltungsaktionen werden von der Amazon EC2 EC2-API-Referenz protokolliert CloudTrail und sind in dieser dokumentiert. Aufrufe der RunInstances,- oder CreateImage-Aktionen generieren beispielsweise Einträge in den CloudTrail Protokolldateien. DescribeInstances

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Stammbenutzers oder des IAM-Benutzers gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde.

Weitere Informationen finden Sie unter dem CloudTrailuserIdentityElement.

Verstehen Sie die Einträge der Amazon EC2 EC2-API-Protokolldatei

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Der folgende Protokolldatensatz zeigt, dass ein Benutzer eine Instance beendet hat.

```
{
   "Records":[
      {
         "eventVersion":"1.03",
         "userIdentity":{
```

```
            "type":"Root",
            "principalId":"123456789012",
            "arn":"arn:aws:iam::123456789012:root",
            "accountId":"123456789012",
            "accessKeyId":"AKIAIOSFODNN7EXAMPLE",
            "userName":"user"
         },
         "eventTime":"2016-05-20T08:27:45Z",
         "eventSource":"ec2.amazonaws.com",
         "eventName":"TerminateInstances",
         "awsRegion":"us-west-2",
         "sourceIPAddress":"198.51.100.1",
         "userAgent":"aws-cli/1.10.10 Python/2.7.9 Windows/7botocore/1.4.1",
         "requestParameters":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d"
               }]
            }
         },
         "responseElements":{
            "instancesSet":{
               "items":[{
                  "instanceId":"i-1a2b3c4d",
                  "currentState":{
                     "code":32,
                     "name":"shutting-down"
                  },
                  "previousState":{
                     "code":16,
                     "name":"running"
                  }
               }]
            }
         },
         "requestID":"be112233-1ba5-4ae0-8e2b-1c302EXAMPLE",
         "eventID":"6e12345-2a4e-417c-aa78-7594fEXAMPLE",
         "eventType":"AwsApiCall",
         "recipientAccountId":"123456789012"
      }
   ]
}
```

Wird verwendet AWS CloudTrail , um Verbindungen zu prüfen, die mit EC2 Instance Connect hergestellt wurden

Wird verwendet AWS CloudTrail , um die Benutzer zu prüfen, die sich über EC2 Instance Connect mit Ihren Instances verbinden.

So überprüfen Sie die SSH-Aktivität über EC2 Instance Connect mithilfe der Konsole AWS CloudTrail

1. Öffnen Sie die CloudTrail Konsole unter https://console.aws.amazon.com/cloudtrail/.
2. Stellen Sie sicher, dass Sie sich in der korrekten Region befinden.
3. Wählen Sie im Navigationsbereich Event history (Ereignisverlauf) aus.
4. Wählen Sie für Filter Event source (Ereignisquelle), ec2-instance-connect.amazonaws.com aus.
5. (Optional) Wählen Sie für Time range (Zeitraum) einen Zeitraum aus.
6. Wählen Sie das Symbol Refresh events (Ereignisse aktualisieren) aus.
7. Die Seite zeigt die Ereignisse, die den SendSSHPublicKey-API-Aufrufen entsprechen. Erweitern Sie ein Ereignis mithilfe des Pfeils, um zusätzliche Details anzuzeigen, z. B. den Benutzernamen und den AWS Zugriffsschlüssel, mit denen die SSH-Verbindung hergestellt wurde, sowie die Quell-IP-Adresse.
8. Zum Anzeigen der vollständigen Ereignisinformationen im JSON-Format wählen Sie View event (Ereignis anzeigen). Das requestParameters-Feld enthält die Ziel-Instance-ID, den Benutzernamen für das Betriebssystem und den öffentlichen Schlüssel, der zur Herstellung der SSH-Verbindung verwendet wurde.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "ABCDEFGONGNOMOOCB6XYTQEXAMPLE",
        "arn": "arn:aws:iam::1234567890120:user/IAM-friendly-name",
        "accountId": "123456789012",
        "accessKeyId": "ABCDEFGUKZHNAW4OSN2AEXAMPLE",
        "userName": "IAM-friendly-name",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-09-21T21:37:58Z"}
        }
    },
```

```
    "eventTime": "2018-09-21T21:38:00Z",
    "eventSource": "ec2-instance-connect.amazonaws.com",
    "eventName": "SendSSHPublicKey ",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "123.456.789.012",
    "userAgent": "aws-cli/1.15.61 Python/2.7.10 Darwin/16.7.0 botocore/1.10.60",
    "requestParameters": {
        "instanceId": "i-0123456789EXAMPLE",
        "osUser": "ec2-user",
        "SSHKey": {
            "publicKey": "ssh-rsa ABCDEFGHIJKLMNO01234567890EXAMPLE"
        }
     },
    "responseElements": null,
    "requestID": "1a2s3d4f-bde6-11e8-a892-f7ec64543add",
    "eventID": "1a2w3d4r5-a88f-4e28-b3bf-30161f75be34",
    "eventType": "AwsApiCall",
    "recipientAccountId": "0987654321"
}
```


Wenn Sie Ihr AWS Konto so konfiguriert haben, dass CloudTrail Ereignisse in einem S3-Bucket erfasst werden, können Sie die Informationen programmgesteuert herunterladen und prüfen. Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Abrufen und Anzeigen Ihrer CloudTrail Protokolldateien.

Überwachen Sie Ihre .NET- und SQL Server-Anwendungen mit CloudWatch Application Insights

CloudWatch Application Insights unterstützt Sie bei der Überwachung Ihrer .NET- und SQL Server-Anwendungen, die Amazon EC2 EC2-Instances zusammen mit anderen AWS Anwendungsressourcen verwenden. Es identifiziert Schlüsselmetrikprotokolle und Alarme und richtet diese für Ihre Anwendungsressourcen und Ihren Technologie-Stack ein (z. B. Ihre Microsoft SQL Server-Datenbank, Web (IIS)- und Anwendungsserver, Betriebssystem, Load Balancer und Warteschlangen). Es überwacht kontinuierlich die Metriken und Protokolle, um Anomalien und Fehler zu erkennen und zu korrelieren. Wenn Fehler und Anomalien erkannt werden, generiert Application Insights CloudWatch Ereignisse, anhand derer Sie Benachrichtigungen einrichten oder Maßnahmen ergreifen können. Um die Fehlersuche zu erleichtern, erstellt es automatisierte Dashboards für die erkannten Probleme, die korrelierte Metrikanomalien und Protokollfehler sowie zusätzliche Erkenntnisse enthalten, die Sie auf die mögliche Ursache hinweisen. Die automatisierten Dashboards

helfen Ihnen, schnell Abhilfemaßnahmen zu ergreifen, um Ihre Anwendungen funktionstüchtig zu halten und Auswirkungen auf die Endbenutzer Ihrer Anwendung zu vermeiden.

Eine vollständige Liste der unterstützten Protokolle und Metriken finden Sie unter Von Amazon CloudWatch Application Insights unterstützte Protokolle und Metriken.

Informationen über erkannte Probleme:

- Eine kurze Zusammenfassung des Problems.
- Die Startzeit und das Datum des Problems.
- Der Schweregrad des Problems: Hoch/Mittel/Niedrig.
- Der Status des erkannten Problems: in Bearbeitung/gelöst.
- Einblicke: Automatisch generierte Erkenntnisse über das erkannte Problem und die mögliche Hauptursache.
- Feedback zu Erkenntnissen: Feedback, das Sie zur Nützlichkeit der mit CloudWatch Application Insights für .NET und SQL Server generierten Erkenntnisse gegeben haben
- Verwandte Beobachtungen: Eine detaillierte Übersicht über die Metrikanomalien und Fehlerausschnitte relevanter Protokolle im Zusammenhang mit dem Problem über verschiedene Anwendungskomponenten hinweg.

Feedback

Sie können Feedback zu den automatisch generierten Erkenntnissen über erkannte Probleme geben, indem Sie sie als nützlich oder nicht nützlich einstufen. Ihr Feedback zu den Erkenntnissen sowie Ihre Anwendungsdiagnose (Metrikanomalien und Protokollausnahmen) werden genutzt, um die zukünftige Erkennung ähnlicher Probleme zu verbessern.

Weitere Informationen finden Sie in der Dokumentation zu CloudWatchApplication Insights im CloudWatch Amazon-Benutzerhandbuch.

Verfolgen Sie Ihre Nutzung des kostenlosen Kontingents für Amazon EC2

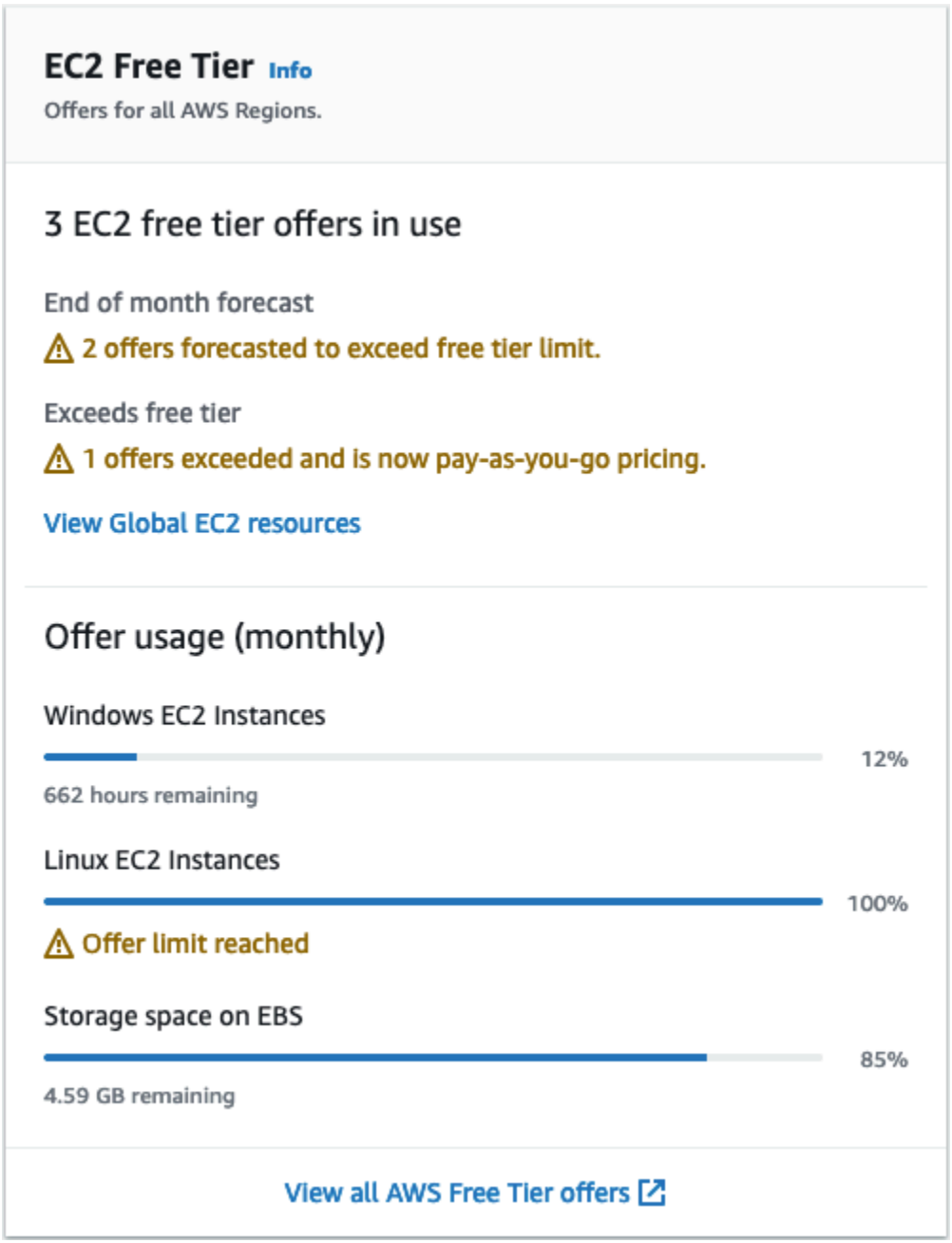
Sie können Amazon EC2 kostenlos nutzen, wenn Sie seit weniger als 12 Monaten AWS Kunde sind und die Kostenloses AWS-Kontingent Nutzungslimits einhalten. Es ist wichtig, dass Sie Ihre Nutzung des kostenlosen Kontingents nachverfolgen, um Überraschungen bei der Rechnungsstellung zu

vermeiden. Wenn Sie die Limits des kostenlosen Kontingents überschreiten, fallen Standardgebühren an. pay-as-go

> **Note**
>
> Wenn Sie seit mehr als 12 Monaten AWS Kunde sind, haben Sie keinen Anspruch mehr auf die Nutzung des kostenlosen Kontingents und das Feld „Kostenloses Kontingent für EC2“, das im folgenden Verfahren beschrieben wird, wird nicht angezeigt.

So können Sie Ihre Nutzung des kostenlosen Kontingents nachverfolgen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2 Dashboard (EC2-Dashboard) aus.
3. Suchen Sie das Feld Kostenloses Kontingent für EC2 (oben rechts).



4. Überprüfen Sie im Feld Kostenloses Kontingent für EC2 wie folgt Ihre Nutzung des kostenlosen Kontingents:

   - Beachten Sie unter In Anspruch genommene Angebote des kostenlosen EC2-Kontingents die folgenden Warnhinweise:
     - Prognose zum Monatsende – Diese Warnung gibt an, dass in diesem Monat Gebühren anfallen werden, wenn Sie Ihr derzeitiges Nutzungsmuster beibehalten.
     - Überschreitet das kostenlose Kontingent – Diese Warnung gibt an, dass Sie Ihr Limit für das kostenlose Kontingent überschritten haben und bereits Gebühren anfallen.

- Notieren Sie sich unter Nutzung des Angebots (monatlich) Ihre Nutzung von Linux-Instances, Windows-Instances und EBS-Speicher. Der Prozentsatz gibt an, wie viele der Limits Ihres kostenlosen Kontingents Sie in diesem Monat genutzt haben. Wenn Sie bei 100 % angelangt sind, fallen Gebühren für die weitere Nutzung an.

> **Note**
>
> Diese Informationen werden erst angezeigt, nachdem Sie eine Instance erstellt haben. Die Nutzungsinformationen werden jedoch nicht in Echtzeit aktualisiert, sondern dreimal täglich.

5. Um weitere Gebühren zu vermeiden, löschen Sie alle Ressourcen, für die entweder jetzt Gebühren anfallen oder für die Gebühren anfallen, wenn Sie Ihr Nutzungslimit für das kostenlose Kontingent überschreiten.

   - Anweisungen zum Löschen Ihrer Instance finden Sie im nächsten Schritt in diesem Tutorial.
   - Um zu überprüfen, ob Sie über Ressourcen in anderen Regionen verfügen, für die möglicherweise Gebühren anfallen, wählen Sie im Feld Kostenloses Kontingent für EC2 die Option Globale EC2-Ressourcen anzeigen aus, um die Globale EC2-Ansicht zu öffnen. Weitere Informationen finden Sie unter Amazon EC2 Global View.

6. Um Ihre Ressourcennutzung für alle AWS-Services anzuzeigen Kostenloses AWS-Kontingent, wählen Sie unten im Feld Kostenloses EC2-Kontingent die Option Alle Kostenloses AWS-Kontingent Angebote anzeigen aus. Weitere Informationen finden Sie unter Verwenden des Kostenloses AWS-Kontingent im Benutzerhandbuch für AWS -Fakturierung.

Netzwerk in Amazon EC2

Mit Amazon VPC können Sie AWS Ressourcen wie Amazon EC2 EC2-Instances in einem virtuellen Netzwerk starten, das Ihrem AWS Konto zugewiesen ist und als Virtual Private Cloud (VPC) bezeichnet wird. Wenn Sie eine Instance starten, können Sie ein Subnetz aus der VPC auswählen. Die Instance ist mit einer primären Netzwerkschnittstelle konfiguriert, bei der es sich um eine logische virtuelle Netzwerkkarte handelt. Die Instance erhält eine primäre private IP-Adresse von der IPv4-Adresse des Subnetzes und wird der primären Netzwerkschnittstelle zugewiesen.

Sie können steuern, ob die Instance eine öffentliche IP-Adresse aus dem Pool öffentlicher IP-Adressen von Amazon erhält. Die öffentliche IP-Adresse einer Instance wird Ihrer Instance nur zugeordnet, bis sie gestoppt oder beendet wird. Wenn Sie eine persistente öffentliche IP-Adresse benötigen, können Sie Ihrem AWS Konto eine Elastic IP-Adresse zuweisen und diese mit einer Instance oder einer Netzwerkschnittstelle verknüpfen. Eine Elastic IP-Adresse bleibt mit Ihrem AWS Konto verknüpft, bis Sie sie freigeben, und Sie können sie bei Bedarf von einer Instance auf eine andere verschieben. Sie können Ihren eigenen IP-Adressbereich in Ihr AWS -Konto bringen, wo er als Adresspool angezeigt wird, und dann Elastic IP-Adressen aus Ihrem Adresspool zuweisen.

Um die Netzwerkleistung zu erhöhen und die Latenz zu reduzieren, können Sie Instances in einer Placement-Gruppe starten. Mithilfe von Enhanced Networking können Sie eine deutlich höhere Paketleistung pro Sekunde (PPS) erzielen. Sie können High-Performance-Computing- und Machine-Learning-Anwendungen mit einem Elastic Fabric Adapter (EFA) beschleunigen. Dies ist ein Netzwerkgerät, das Sie an einen unterstützten Instance-Typ anschließen können.

Features

- Regionen und Zonen
- IP-Adressierung von Amazon EC2-Instances
- Hostnamentypen für Amazon-EC2-Instances
- Bring Your Own IP Addresses (BYOIP) in Amazon EC2
- Elastic-IP-Adressen
- Elastic-Network-Schnittstelle
- Netzwerkbandbreite für Amazon EC2-Instances
- Verbessertes Networking auf Amazon EC2
- Elastic Fabric Adapter

- Amazon-EC2-Instance-Topologie
- Placement-Gruppen
- Netzwerk-MTU (Maximum Transmission Unit) für Ihre EC2-Instance
- Virtuelle private Clouds für Ihre EC2-Instances

Regionen und Zonen

Amazon EC2 wird an mehreren Standorten weltweit gehostet. Diese Standorte bestehen aus AWS-Regionen Availability Zones, Local Zones und AWS Outposts Wavelength Zones.

- Jede Region ist ein separater geografischer Bereich.
- Availability Zones sind mehrere isolierte Standorte innerhalb jeder Region.
- Local Zones bieten Ihnen die Möglichkeit, Ressourcen wie Rechenleistung und Speicher an mehreren Standorten zu platzieren, die näher an Ihren Endbenutzern liegen.
- AWS Outposts bietet native AWS Dienste, Infrastrukturen und Betriebsmodelle für praktisch jedes Rechenzentrum, jeden Colocation-Bereich oder jede lokale Einrichtung.
- Mit Wavelength Zones können Developer Anwendungen mit äußerst niedriger Latenz für 5G-Geräte und Endbenutzer erstellen. Wavelength stellt AWS Standard-Rechen- und Speicherdienste am Rand der 5G-Netzwerke von Telekommunikationsanbietern bereit.

AWS betreibt state-of-the-art hochverfügbare Rechenzentren. In seltenen Fällen kann es aber zu Ausfällen kommen, die die Verfügbarkeit von Instances desselben Standorts beeinträchtigen. Wenn Sie alle Ihre Instances an einem einzigen Standort hosten, der von einem Ausfall dieser Art betroffen ist, ist keine Ihrer Instances verfügbar.

Informationen zur Ermittlung der für Sie am besten geeigneten Bereitstellung finden Sie unter Häufig gestellte Fragen zu AWS Wavelength.

Inhalt

Regionen

Jede -Region ist darauf ausgelegt, vollständig von den anderen -Regionen getrennt zu sein. Dies sorgt für die größtmögliche Fehlertoleranz und Stabilität.

Wenn Sie sich Ihre Ressourcen anzeigen lassen, werden nur die Ressourcen angezeigt, die mit der von Ihnen angegebenen Region verknüpft sind. Der Grund hierfür ist, dass die Regionen voneinander isoliert sind und Ressourcen nicht automatisch über unterschiedliche Regionen repliziert werden.

Beim Starten einer Instance müssen Sie ein AMI auswählen, das sich in derselben Region befindet. Wenn sich das AMI in einer anderen Region befindet, können Sie das AMI in die von Ihnen verwendete Region kopieren. Weitere Informationen finden Sie unter Kopieren eines AMI.

Beachten Sie, dass für die Datenübertragung zwischen Regionen eine Gebühr anfällt. Weitere Informationen hierzu erhalten Sie unter Amazon EC2-Preise – Datenübertragung.

Inhalt

Verfügbare Regionen

Ihr Konto bestimmt die Regionen, die für Sie verfügbar sind.

- An AWS-Konto bietet mehrere Regionen, sodass Sie Amazon EC2 EC2-Instances an Standorten starten können, die Ihren Anforderungen entsprechen. Beispielsweise kann es sinnvoll sein, Instances in Europa zu starten, damit sie sich in der Nähe Ihrer europäischen Kunden befinden oder um rechtliche Anforderungen zu erfüllen.
- Ein Konto AWS GovCloud (USA West) bietet Zugriff auf die Regionen AWS GovCloud (USA West) und die Region AWS GovCloud (USA Ost). Weitere Informationen finden Sie unter AWS GovCloud (US).
- Ein Amazon-Konto AWS (China) bietet nur Zugriff auf die Regionen Peking und Ningxia. Weitere Informationen finden Sie unter Amazon Web Services in China.

In der folgenden Tabelle sind die von an AWS-Konto bereitgestellten Regionen aufgeführt. Sie können von einer Region aus keine weiteren Regionen beschreiben AWS GovCloud (US) Regions oder darauf zugreifen AWS-Konto, z. B. die Region China. Um eine nach dem 20. März 2019 eingeführte Region verwenden zu können, müssen Sie die Region aktivieren. Weitere Informationen finden Sie im AWS Account Management Referenzhandbuch unter „Geben Sie an, welche AWS Regionen Ihr Konto verwenden kann“.

Code	Name	Aktivierungsstatus
us-east-2	USA Ost (Ohio)	Nicht erforderlich
us-east-1	USA Ost (Virginia)	Nicht erforderlich
us-west-1	US West (N. California)	Nicht erforderlich
us-west-2	USA West (Oregon)	Nicht erforderlich
af-south-1	Afrika (Kapstadt)	Erforderlich
ap-east-1	Asien-Pazifik (Hongkong)	Erforderlich
ap-south-2	Asien-Pazifik (Hyderabad)	Erforderlich
ap-southeast-3	Asien-Pazifik (Jakarta)	Erforderlich
ap-southeast-4	Asien-Pazifik (Melbourne)	Erforderlich
ap-south-1	Asien-Pazifik (Mumbai)	Nicht erforderlich
ap-northeast-3	Asien-Pazifik (Osaka)	Nicht erforderlich
ap-northeast-2	Asien-Pazifik (Seoul)	Nicht erforderlich
ap-southeast-1	Asia Pacific (Singapore)	Nicht erforderlich
ap-southeast-2	Asien-Pazifik (Sydney)	Nicht erforderlich
ap-northeast-1	Asien-Pazifik (Tokio)	Nicht erforderlich
ca-central-1	Kanada (Zentral)	Nicht erforderlich

Code	Name	Aktivierungsstatus
ca-west-1	Kanada West (Calgary)	Erforderlich
eu-central-1	Europa (Frankfurt)	Nicht erforderlich
eu-west-1	Europa (Irland)	Nicht erforderlich
eu-west-2	Europa (London)	Nicht erforderlich
eu-south-1	Europa (Milan)	Erforderlich
eu-west-3	Europa (Paris)	Nicht erforderlich
eu-south-2	Europa (Spain)	Erforderlich
eu-north-1	Europa (Stockholm)	Nicht erforderlich
eu-central-2	Europa (Zürich)	Erforderlich
il-central-1	Israel (Tel Aviv)	Erforderlich
me-south-1	Naher Osten (Bahrain)	Erforderlich
me-central-1	Naher Osten (VAE)	Erforderlich
sa-east-1	South America (São Paulo)	Nicht erforderlich

Weitere Informationen finden Sie unter AWS -Globale Infrastruktur.

Die Anzahl und Zuordnung der Availability Zones pro Region kann zwischen AWS-Konten variieren. Um die Availability Zones aufzulisten, die für Ihr Konto verfügbar sind, können Sie die Amazon-EC2-Konsole oder die Befehlszeilenschnittstelle verwenden. Weitere Informationen finden Sie unter Beschreiben Sie Ihre Regionen.

Regionen und Endpunkte

Wenn Sie über die Befehlszeilenschnittstelle oder über API-Aktionen mit einer Instance arbeiten, müssen Sie ihren regionalen Endpunkt angeben. Weitere Informationen über Regionen und Endpunkte für Amazon EC2 finden Sie unter Amazon-EC2-Endpunkte und -Kontingente im Allgemeine Amazon Web Services-Referenz.

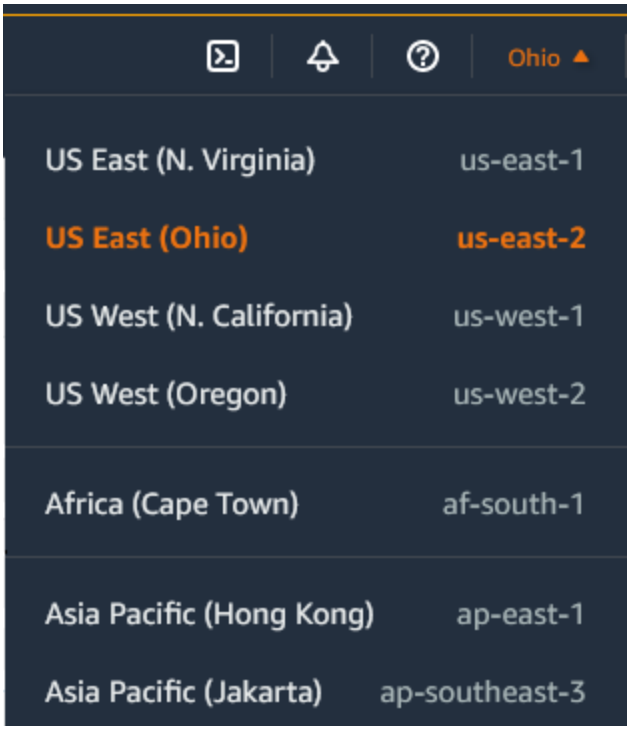
Weitere Informationen zu Endpunkten und Protokollen in AWS GovCloud (USA West) finden Sie im Benutzerhandbuch unter Service-Endpunkte.AWS GovCloud (US)

Beschreiben Sie Ihre Regionen

Sie können die Amazon EC2-Konsole oder die Befehlszeilenschnittstelle verwenden, um zu ermitteln, welche Regionen und für Ihr Konto verfügbar sind. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

So suchen Sie Ihre Regionen über die Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie in der Navigationsleiste auf die Auswahl der Regions (Regionen).



3. Ihre EC2-Ressourcen für diese Region werden im EC2-Dashboard im Abschnitt Ressourcen angezeigt.

So finden Sie Ihre Regionen mit dem AWS CLI

Beschreiben Sie wie folgt mit dem Befehl describe-regions die Regionen, die für Ihr Konto aktiviert sind.

```
aws ec2 describe-regions
```

Um alle Regionen zu beschreiben, einschließlich Regionen, die für Ihr Konto deaktiviert sind, fügen Sie wie folgt die Option `--all-regions` hinzu.

```
aws ec2 describe-regions --all-regions
```

Abrufen des Anzeigenamens der Region

Sie können den AWS Systems Manager Parameterspeicher verwenden, um den Anzeigenamen einer Region anzuzeigen. Jede Region verfügt über öffentliche Parameter im folgenden Pfad.

```
/aws/service/global-infrastructure/regions/region-code
```

Zu den öffentlichen Parametern für eine Region gehören die folgenden:

- /aws/service/global-infrastructure/regions/*region-code*/domain
- /aws/service/global-infrastructure/regions/*region-code*/geolocationCountry
- /aws/service/global-infrastructure/regions/*region-code*/geolocationRegion
- /aws/service/global-infrastructure/regions/*region-code*/longName
- /aws/service/global-infrastructure/regions/*region-code*/partition

Der Parameter `longName` enthält den Anzeigenamen der Region. Der folgende get-parameters-by-path-Befehl gibt den Anzeigenamen der `af-south-1`-Region zurück. Es benutzt die `--query`-Option, um die Ausgabe auf den Namen der Region zu beschränken. Unter Linux müssen Sie die Abfragezeichenfolge in einfache Anführungszeichen setzen. Um diesen Befehl über die Windows-Eingabeaufforderung auszuführen, lassen Sie entweder die einfachen Anführungszeichen weg oder ändern Sie sie in doppelte Anführungszeichen.

AWS CLI on Linux

```
aws ssm get-parameters-by-path \
    --path /aws/service/global-infrastructure/regions/af-south-1 \
    --query 'Parameters[?Name.contains(@,`longName`)].Value' \
    --output text
```

AWS CLI on Windows

```
aws ssm get-parameters-by-path ^
    --path /aws/service/global-infrastructure/regions/af-south-1 ^
```

```
    --query "Parameters[?Name.contains(@,`longName`)].Value" ^
    --output text
```

Tools for PowerShell

Wenn es nicht installiert ist, installieren Sie die AWS.Tools. SimpleSystemsFühren Sie das Verwaltungsmodul für Tools for PowerShell aus. `Install-AWSToolsModule AWS.Tools.SimpleSystemsManagement -CleanUp`

```
$parameterPath = "/aws/service/global-infrastructure/regions/af-south-1"
$substringToMatch = "longName"
$filteredParameters = Get-SSMParametersByPath -Path $parameterPath `
| Where-Object { $_.Name -like "*$substringToMatch*" } `
| ForEach-Object { Write-Output $_.Value }
$filteredParameters
```

Es folgt eine Beispielausgabe.

```
Africa (Cape Town)
```

Weitere Informationen finden Sie unter Arbeiten mit öffentlichen Parametern im AWS Systems Manager -Benutzerhandbuch.

Angeben der Region für eine Ressource

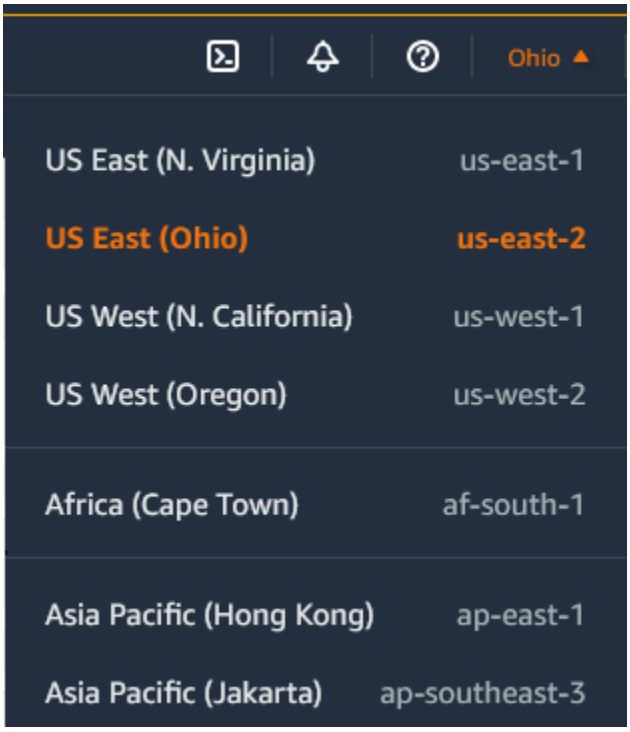
Bei jeder Erstellung einer Amazon EC2-Ressource können Sie die Region für die Ressource angeben. Sie können die Region für eine Ressource mithilfe der Befehlszeile AWS Management Console oder angeben.

Überlegungen

Einige AWS Ressourcen sind möglicherweise nicht in allen Regionen verfügbar. Stellen Sie sicher, dass Sie die benötigten Ressourcen in den gewünschten Regionen erstellen können, bevor Sie eine Instance starten.

So geben Sie die Region für eine Ressource mit der Konsole an

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie in der Navigationsleiste auf die Auswahl der Regions (Regionen) und wählen Sie dann die Region aus.



So geben Sie die Standardregion über die Befehlszeile an

Sie können den Wert einer Umgebungsvariablen auf den gewünschten regionalen Endpunkt festlegen (z. B, `https://ec2.us-east-2.amazonaws.com`):

- `AWS_DEFAULT_REGION` (AWS CLI)
- `Set-AWSDefaultRegion` (AWS Tools for Windows PowerShell)

Alternativ hierzu können Sie für jeden Befehl auch die Befehlszeilenoption `--region` (AWS CLI) oder `-Region` (AWS Tools for Windows PowerShell) verwenden. z. B. `--region us-east-2`.

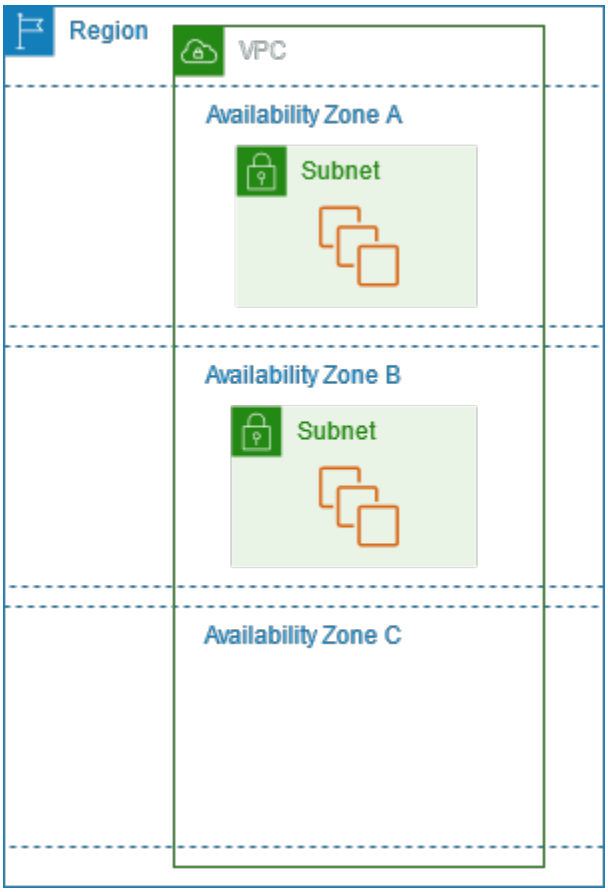
Weitere Informationen zu den Endpunkten für Amazon EC2 finden Sie unter Amazon EC2 EC2-Endpunkte und Kontingente in der. Allgemeine AWS-Referenz

Availability Zones

Jede Region verfügt über mehrere isolierte Standorte, die als Availability Zones bezeichnet werden. Der Code für Availability Zone ist der Regionscode gefolgt von einem Buchstaben als Bezeichner angegeben. Zum Beispiel `us-east-1a`.

Wenn Sie eine Instance starten, wählen Sie eine Region und eine Virtual Private Cloud (VPC) aus. Dann können Sie entweder ein Subnetz aus einer der Availability Zones auswählen oder uns eines für Sie auswählen lassen. Wenn Sie Ihre Instances auf mehrere Availability Zones verteilen, ist es sinnvoll, Ihre Anwendung so zu entwerfen, dass bei einem Ausfall einer Instance die Anforderungen von einer Instance in einer anderen Availability Zone verarbeitet werden können. Außerdem können Sie Elastic IP-Adressen verwenden, um den Ausfall einer Instance in einer Availability Zone zu maskieren, indem Sie die Adresse schnell einer Instance in einer anderen Availability Zone zuordnen.

Das folgende Diagramm zeigt mehrere Availability Zones in einer Region. AWS Availability Zone A und Availability Zone B haben jeweils ein Subnetz, und jedes Subnetz verfügt über Instances. Availability Zone C hat keine Subnetze, daher können Sie keine Instances in diese Availability Zone starten.



Da Availability Zones im Laufe der Zeit größer werden, werden die Erweiterungsmöglichkeiten in der Regel immer weiter eingeschränkt. Wenn dies eintritt, wird für Sie das Starten einer Instance in einer eingeschränkten Availability Zone unter Umständen verhindert, es sei denn, sie verfügen bereits über eine Instance in dieser Availability Zone. Es kann auch sein, dass wir die eingeschränkte Availability Zone aus der Liste mit den Availability Zones für neue Konten entfernen. Daher besteht

die Möglichkeit, dass Ihr Konto in einer Region über eine andere Anzahl von verfügbaren Availability Zones als ein anderes Konto verfügt.

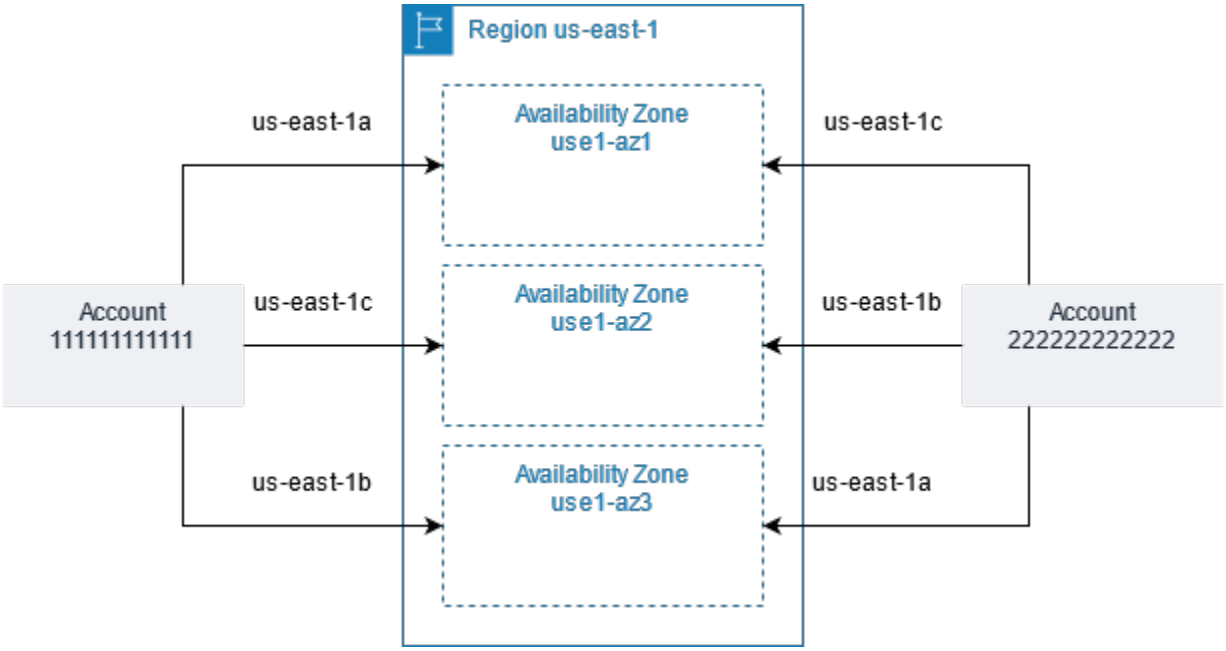
Inhalt

AZ-IDs

Um sicherzustellen, dass die Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones AWS-Konto in unseren ältesten Regionen unabhängig voneinander den Codes der einzelnen Availability Zones zu. Zum Beispiel AWS-Konto könnte es sein, dass der `us-east-1a` für Sie nicht derselbe physische Standort wie der `us-east-1a` für eine andere ist AWS-Konto.

Verwenden Sie die AZ-IDs, bei denen es sich um eindeutige und konsistente Kennungen für eine Availability Zone handelt, um Availability Zones zwischen Konten in allen Regionen zu koordinieren, auch wenn diese Availability Zones zuordnen. Dies `use1-az1` ist beispielsweise eine AZ-ID für die `us-east-1` Region, und sie hat in jeder AWS-Konto Region denselben physischen Standort. Mit der Anzeige von AZ-IDs für Ihr Konto können Sie den physischen Standort Ihrer Ressourcen im Verhältnis zu den Ressourcen in einem anderen Konto bestimmen. Wenn Sie beispielsweise ein Subnetz in der Availability Zone mit der AZ-ID `use1-az2` mit einem anderen Konto teilen, steht dieses Subnetz dem Konto in der Availability Zone zur Verfügung, dessen AZ-ID ebenfalls `use1-az2` ist.

Das folgende Diagramm veranschaulicht zwei Konten mit unterschiedlichen Mappings von Availability-Zone-Code zur AZ ID.



Beschreiben Ihrer Availability Zones

Sie können die Amazon EC2-Konsole oder die Befehlszeilenschnittstelle verwenden, um zu ermitteln, welche Regionen und Availability Zones für Ihr Konto verfügbar sind. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

So suchen Sie Ihre Availability Zones über die Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie in der Navigationsleiste auf die Auswahl der Regions (Regionen) und wählen Sie dann die Region aus.
3. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
4. Die Availability Zones sind im Bereich Service health (Servicezustand) erstellt.

Um Ihre Availability Zones zu finden, verwenden Sie den AWS CLI

- Beschreiben Sie wie folgt mit dem Befehl describe-availability-zones die Availability Zones in der angegebenen Region, die für Ihr Konto aktiviert sind.

```
aws ec2 describe-availability-zones --region region-name
```

- Beschreiben Sie wie folgt mit dem Befehl describe-availability-zones die Availability Zones, unabhängig vom Anmeldestatus.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Starten von Instances in einer Availability Zone

Wählen Sie beim Starten einer Instance eine Region aus, in der Instances näher an bestimmten Kunden platziert werden oder mit der rechtliche oder andere Anforderungen erfüllt werden. Indem Sie Instances in separaten Availability Zones starten, können Sie Ihre Anwendungen vor dem Ausfall eines einzelnen Standorts schützen.

Beim Starten einer Instance können Sie optional eine Availability Zone in der Region angeben, die Sie verwenden. Wenn Sie keine Availability Zone angeben, wählen wir eine Availability Zone für Sie aus. Beim Starten Ihrer ersten Instances ist es ratsam, die standardmäßig vorgegebene Availability Zone zu akzeptieren. Wir können so basierend auf dem Systemzustand und der verfügbaren Kapazität die beste Availability Zone für Sie auswählen. Geben Sie beim Starten weiterer Instances eine Availability Zone nur dann an, wenn Ihre Instances nah bei Ihren laufenden Instances oder getrennt davon angeordnet werden müssen.

Migrieren einer Instance zu einer anderen Availability Zone

Bei Bedarf können Sie eine Instance aus einer Availability Zone zu einer anderen migrieren. Wenn Sie beispielsweise versuchen, den Instance-Typ Ihrer Instance zu ändern, und sich keine Instance des neuen Instance-Typs in der aktuellen Availability Zone starten lässt, können Sie die Instance in eine Availability Zone mit Kapazität für den neuen Instance-Typ migrieren.

Der Migrationsprozess umfasst:

- das Erstellen eines AMI aus der ursprünglichen Instance
- das Starten einer Instance in der neuen Availability Zone
- das Aktualisieren der Konfiguration der neuen Instance, wie im folgenden Verfahren gezeigt

So migrieren Sie eine Instance zu einer anderen Availability Zone

1. Erstellen Sie aus der Instance ein AMI. Das Verfahren hängt vom Typ des Root-Geräte-Volumes für die Instanz ab. Weitere Informationen finden Sie in der Dokumentation, die Ihrem Root-Geräte-Volume entspricht:

   - Erstellen Sie ein Amazon EBS-backed AMI

- Erstellen einer Instance-Speicher-Backed Linux-AMI

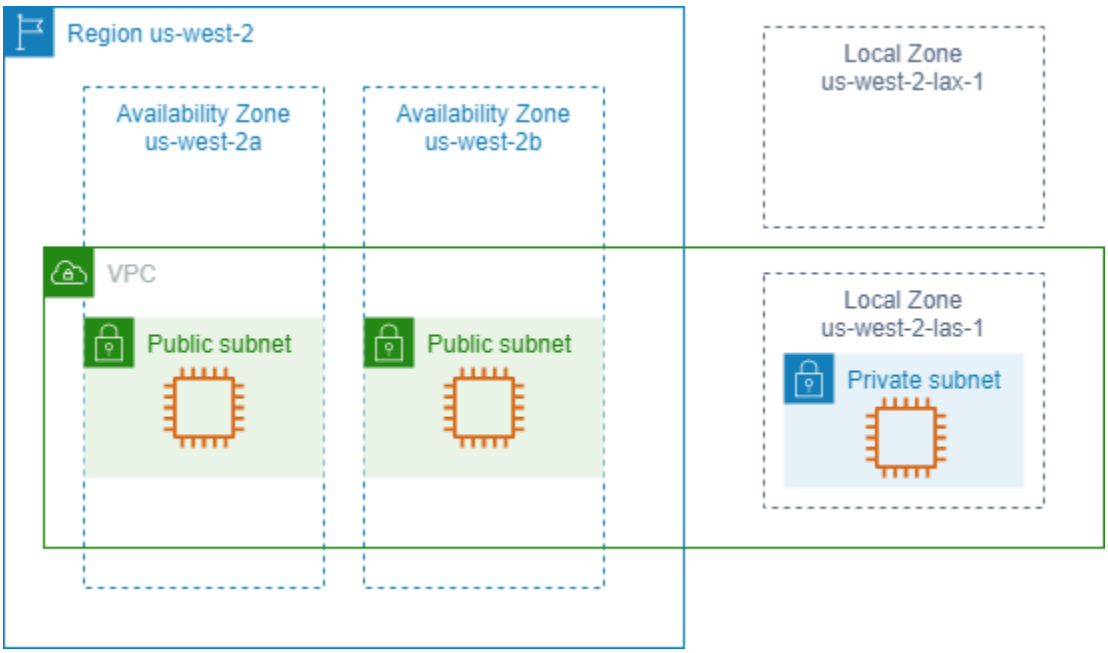
2. Wenn Sie die private IPv4-Adresse der Instance beibehalten möchten, müssen Sie das Subnetz in der aktuellen Availability Zone löschen und in der neuen Availability Zone dann ein Subnetz erstellen, das über den gleichen IPv4-Adressbereich wie das ursprüngliche Subnetz verfügt. Beachten Sie hierbei, das Sie in einem Subnetz alle Instances beenden müssen, bevor Sie es löschen können. Aus diesem Grund sollten Sie AMIs aus allen Instances in Ihrem Subnetz erstellen, damit Sie alle Instances aus dem aktuellen Subnetz in das neue Subnetz verschieben können.
3. Starten Sie eine Instance über das gerade erstellte AMI und geben Sie die neue Availability Zone bzw. das Subnetz an. Sie können den gleichen Instance-Typ wie für die ursprüngliche Instance verwenden oder einen neuen Instance-Typ wählen. Weitere Informationen finden Sie unter Starten von Instances in einer Availability Zone.
4. Wenn die ursprüngliche Instance über eine zugeordnete Elastic IP-Adresse verfügt, sollten Sie sie der neuen Instance zuordnen. Weitere Informationen finden Sie unter Aufheben der Zuordnung einer Elastic IP-Adresse.
5. Wenn die ursprüngliche Instance eine Reserved Instance ist, sollten Sie die Availability Zone für Ihre Reservierung ändern. (Falls Sie auch den Instance-Typ geändert haben, können Sie zusätzlich den Instance-Typ für Ihre Reservierung ändern.) Weitere Informationen finden Sie unter Senden von Änderungsanforderungen.
6. (Optional) Beenden Sie die ursprüngliche Instance. Weitere Informationen finden Sie unter Beenden einer Instance.

Local Zones

Eine lokale Zone ist eine Erweiterung einer AWS Region in geografischer Nähe zu Ihren Benutzern. Local Zones verfügen über eigene Verbindungen zum Internet und unterstützen sie AWS Direct Connect, sodass Ressourcen, die in einer lokalen Zone erstellt wurden, lokalen Benutzern mit Kommunikation mit niedriger Latenz dienen können. Weitere Informationen finden Sie unter Was sind AWS Local Zones? im AWS Local Zones User Guide.

Der Code für die lokale Zone wird durch einen Regionscode dargestellt, gefolgt von einer ID, die den physischen Standort angibt. Beispiel: `us-west-2-lax-1` in Los Angeles.

Das folgende Diagramm zeigt die AWS Region`us-west-2`, zwei ihrer Availability Zones und zwei ihrer Local Zones. Die VPC erstreckt sich über die Availability Zones und eine der lokalen Zonen. Jede Zone in der VPC hat ein Subnetz und jedes Subnetz eine Instance.



Um eine Local Zone verwenden zu können, müssen Sie diese zunächst aktivieren. Weitere Informationen finden Sie unter the section called “Anmelden für Local Zones”. Erstellen Sie als Nächstes ein Subnetz in der Local Zone. Starten Sie schließlich die Ressourcen im Subnetz der Local Zone, z. B. Instances, damit Ihre Anwendungen sich in der Nähe der Benutzer befinden.

Inhalt

Verfügbare Local Zones

Sie können über die Amazon-EC2-Konsole oder eine Befehlszeilenschnittstelle feststellen, welche Local Zones für Ihr Konto verfügbar sind. Eine vollständige Liste finden Sie unter Local Zones von AWS – Standorte.

So finden Sie Ihre Local Zones mithilfe der Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie in der Navigationsleiste auf die Auswahl der Regions (Regionen) und wählen Sie dann die übergeordnete Region aus.
3. Wählen Sie im Navigationsbereich EC2-Dashboard aus.

4. Wählen Sie in der oberen rechten Ecke der Seite Account Attributes (Kontoattribute), Zones (Zonen).aus.

So finden Sie Ihre Local Zones mit dem AWS CLI

Beschreiben Sie wie folgt mit dem Befehl describe-availability-zones alle Local Zones in der angegebenen Region, selbst wenn sie nicht aktiviert sind. Um nur die Local Zones zu beschreiben, die Sie aktiviert haben, lassen Sie die Option `--all-availability-zones` weg.

```
aws ec2 describe-availability-zones --region region-name --filters Name=zone-
type,Values=local-zone --all-availability-zones
```

Anmelden für Local Zones

Bevor Sie eine Local Zone für eine Ressource oder einen Service angeben können, müssen Sie sich für Local Zones anmelden

Überlegungen

Einige AWS Ressourcen sind möglicherweise nicht in allen Regionen verfügbar. Stellen Sie sicher, dass Sie die benötigten Ressourcen in den gewünschten Regionen oder Local Zones erstellen können, bevor Sie eine Instance in einer bestimmten Local Zone starten. Eine Liste der in den einzelnen Local Zones unterstützten Services finden Sie unter Local Zones von AWS – Features.

Anmelden für Local Zones mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der oberen linken Ecke der Seite New EC2 Experience (Neue EC2-Umgebung) aus. Sie können diese Aufgabe nicht mithilfe der alten Konsolenumgebung durchführen.
3. Klicken Sie in der Navigationsleiste auf die Auswahl der Regions (Regionen) und wählen Sie dann die übergeordnete Region aus.
4. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
5. Wählen Sie in der oberen rechten Ecke der Seite Account Attributes (Kontoattribute), Zones (Zonen).aus.
6. Wählen Sie eine Lokale Zone und dann Aktion > Zonengruppe verwalten.
7. Wählen Sie unter Opt-In-Status die Option Aktivieren aus.
8. Wählen Sie Aktualisieren.

Um sich für Local Zones anzumelden, verwenden Sie den AWS CLI

Verwenden Sie den Befehl modify-availability-zone-group.

Starten von Instances in einer Local Zone

Wenn Sie eine Instance starten, können Sie ein Subnetz angeben, das sich in einer Local Zone befindet. Sie weisen auch eine IP-Adresse aus einer Netzwerkgrenzgruppe zu. Eine Netzwerkgrenzgruppe ist ein eindeutiger Satz von Availability Zones, Local Zones oder Wavelength Zones, aus denen AWS IP-Adressen ankündigt, zum Beispiel `us-west-2-lax-1a`.

Sie können die folgenden IP-Adressen aus einer Netzwerkgrenzgruppe zuweisen:

- Elastische IPv4-Adressen, die von Amazon bereitgestellt werden
- Von Amazon bereitgestellte IPv6-VPC-Adressen (nur in den Zonen von Los Angeles verfügbar)

Weitere Informationen zum Starten einer Instance in einer Local Zone finden Sie unter Getting started with AWS Local Zones im AWS Local Zones User Guide.

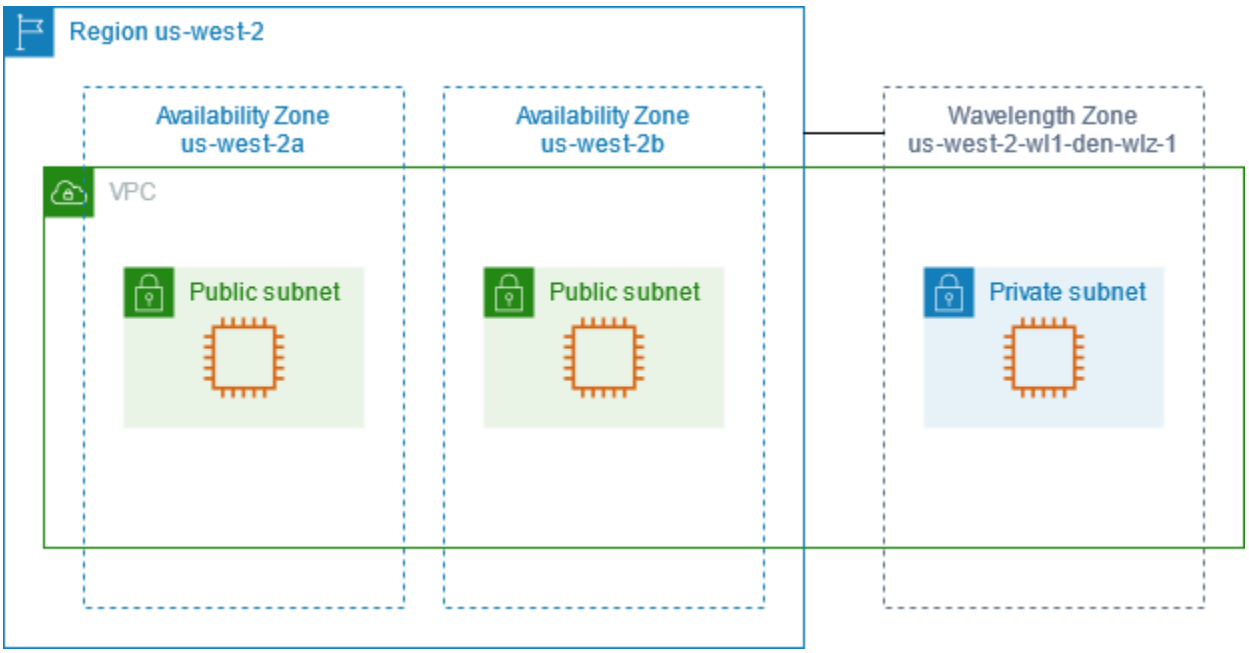
Wavelength Zones

AWS Wavelength ermöglicht es Entwicklern, Anwendungen zu entwickeln, die extrem niedrige Latenzen für mobile Geräte und Endbenutzer bieten. Wavelength stellt AWS Standard-Rechen- und Speicherdienste am Rand der 5G-Netzwerke von Telekommunikationsanbietern bereit. Entwickler können eine Virtual Private Cloud (VPC) auf eine oder mehrere Wellenlängenzonen erweitern und dann AWS Ressourcen wie Amazon EC2 EC2-Instances verwenden, um Anwendungen auszuführen, die eine extrem niedrige Latenz und eine Verbindung zu AWS Diensten in der Region erfordern.

Eine Wavelength-Zone ist eine isolierte Zone am Standort des Carriers, an dem die Wavelength-Infrastruktur bereitgestellt wird. Wavelength Zones sind an eine Region gebunden. Eine Wavelength-Zone ist eine logische Erweiterung einer Region und wird von der Steuerungsebene in der Region verwaltet.

Der Code für die Wavelength-Zone wird durch einen Regionscode dargestellt, gefolgt von einer ID, die den physischen Standort angibt. Beispiel: `us-east-1-wl1-bos-wlz-1` in Boston.

Das folgende Diagramm zeigt die AWS Region`us-west-2`, zwei ihrer Availability Zones und eine Wellenlängenzone. Die VPC erstreckt sich über die Availability Zones und die Wavelength-Zone. Jede Zone in der VPC hat ein Subnetz und jedes Subnetz eine Instance.



Um eine Wavelength-Zone zu verwenden, müssen Sie sich zunächst für die Zone anmelden. Weitere Informationen finden Sie unter the section called “Aktivieren von Wavelength Zones”. Erstellen Sie als Nächstes ein Subnetz in der Wavelength-Zone. Starten Sie schließlich Ihre Ressourcen im Subnetz „Wavelength Zones“, damit Ihre Anwendungen näher an den Endbenutzern liegen.

Wavelength Zones sind nicht in jeder Region verfügbar. Weitere Informationen zu den Regionen, die Wavelength Zones unterstützen, finden Sie unter Verfügbare Wavelength Zones im AWS Wavelength Developerhandbuch.

Inhalt

Beschreiben Ihrer Wavelength Zones

Sie können die Amazon-EC2-Konsole oder die Befehlszeilenschnittstelle verwenden, um zu ermitteln, welche Wavelength Zones für Ihr Konto verfügbar sind. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

So finden Sie Ihre Wavelength Zones über die Konsole:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Klicken Sie in der Navigationsleiste auf die Auswahl der Regions (Regionen) und wählen Sie dann die Region aus.
3. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
4. Wählen Sie in der oberen rechten Ecke der Seite Account Attributes (Kontoattribute), Zones (Zonen).aus.

So finden Sie Ihre Wellenlängenzonen mit dem AWS CLI

- Beschreiben Sie wie folgt mit dem Befehl describe-availability-zones die Wavelength Zones in der angegebenen Region, die für Ihr Konto aktiviert sind.

```
aws ec2 describe-availability-zones --region region-name
```

- Beschreiben Sie wie folgt mit dem Befehl describe-availability-zones die Wavelength Zones unabhängig vom Anmeldestatus.

```
aws ec2 describe-availability-zones --all-availability-zones
```

Aktivieren von Wavelength Zones

Bevor Sie eine Wavelength Zones für eine Ressource oder einen Service angeben, müssen Sie sich für Wavelength Zones anmelden.

Überlegungen

- Einige AWS Ressourcen sind nicht in allen Regionen verfügbar. Stellen Sie sicher, dass Sie die benötigten Ressourcen in der gewünschten Region oder Wavelength-Zone erstellen können, bevor Sie eine Instance in einer bestimmten Wavelength-Zone starten.

So melden Sie sich über die Konsole für eine Wavelength-Zone an:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der oberen linken Ecke der Seite New EC2 Experience (Neue EC2-Umgebung) aus. Sie können diese Aufgabe nicht mithilfe der alten Konsolenumgebung durchführen.
3. Klicken Sie in der Navigationsleiste auf die Auswahl der Regions (Regionen) und wählen Sie dann die Region aus.

4. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
5. Wählen Sie in der oberen rechten Ecke der Seite Account Attributes (Kontoattribute), Zones (Zonen).aus.
6. Wählen Sie eine Wellenlängenzone und wählen Sie Aktion > Gruppe „Zone verwalten“.
7. Wählen Sie unter Opt-In-Status die Option Aktivieren aus.
8. Wählen Sie Aktualisieren.

Um Wellenlängenzonen mit dem zu aktivieren AWS CLI

Verwenden Sie den Befehl modify-availability-zone-group.

Starten von Instances in einer Wavelength-Zone

Wenn Sie eine Instance starten, können Sie ein Subnetz angeben, das sich in einer Wavelength-Zone befindet. Sie weisen auch eine Carrier-IP-Adresse aus einer Netzwerkgrenzgruppe zu, bei der es sich um einen eindeutigen Satz von Availability Zones, Local Zones oder Wavelength Zones handelt, von denen AWS IP-Adressen präsentiert, zum Beispiel `us-east-1-wl1-bos-wlz-1`.

Weitere Informationen zum Starten einer Instance in einer Wavelength-Zone finden Sie unter Erste Schritte mit AWS Wavelength im AWS Wavelength Developerhandbuch.

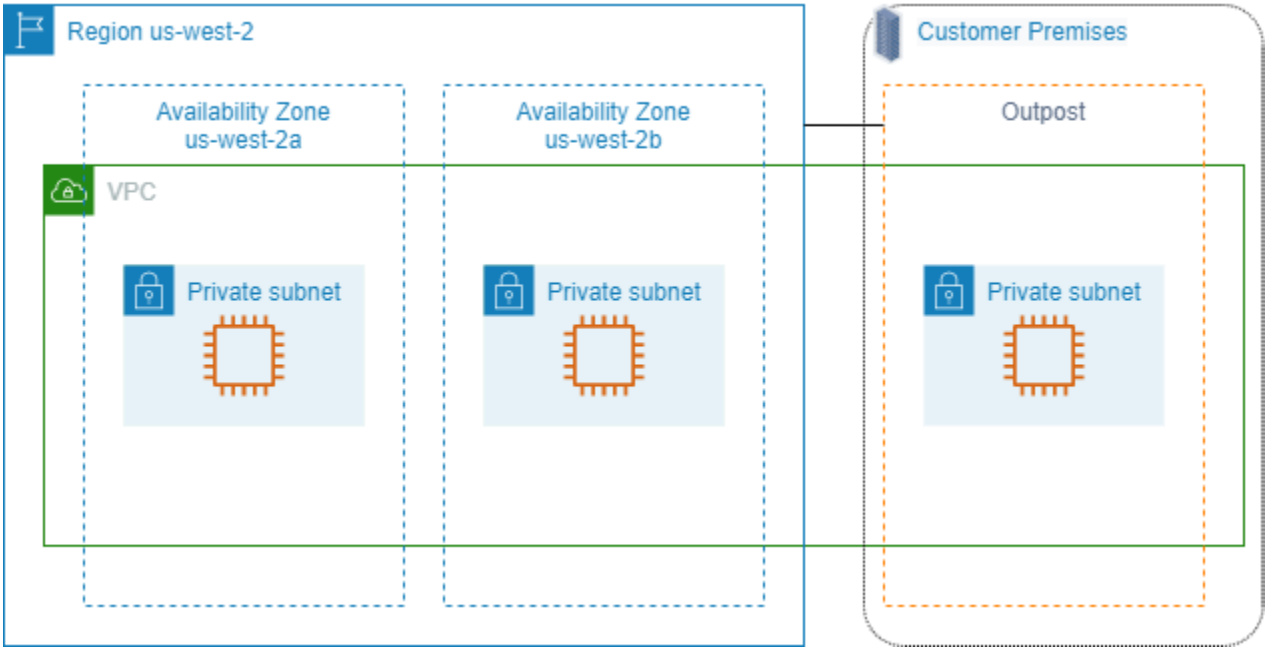
AWS Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur, Dienste, APIs und Tools auf Kundenstandorte ausdehnt. Durch den lokalen Zugriff auf die AWS verwaltete Infrastruktur AWS Outposts können Kunden Anwendungen vor Ort mit denselben Programmierschnittstellen wie in AWS Regionen erstellen und ausführen und gleichzeitig lokale Rechen- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen nutzen.

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazität, der am Standort eines Kunden bereitgestellt wird. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS Region. Sie können Subnetze in Ihrem Outpost erstellen und diese bei der Erstellung AWS von Ressourcen angeben. Instances in Outpost-Subnetzen kommunizieren mit anderen Instances in der AWS Region über private IP-Adressen, alle innerhalb derselben VPC.

Das folgende Diagramm zeigt die AWS Region`us-west-2`, zwei ihrer Availability Zones und einen Outpost. Die VPC erstreckt sich über die Availability Zones und den Outpost. Der Outpost befindet

sich in einem On-Premises Kundenrechenzentrum. Jede Zone in der VPC hat ein Subnetz und jedes Subnetz eine Instance.



Um mit der Nutzung zu beginnen AWS Outposts, müssen Sie einen Outpost erstellen und Outpost-Kapazität bestellen. Weitere Informationen zu Outpost-Konfigurationen finden Sie in unserem Katalog. Nach der Installation Ihres Outpost-Equipments steht Ihnen die Datenverarbeitungs- und Speicherkapazität zur Verfügung, wenn Sie Amazon-EC2-Instances auf Ihrem Outpost starten.

Starten von Instances auf einem Outpost

Sie können EC2-Instances im Outpost-Subnetz starten, das Sie erstellt haben. Sicherheitsgruppen steuern den eingehenden und ausgehenden Datenverkehr für Instances mit Elastic-Network-Schnittstelle in einem Outpost-Subnetz wie für Instances in einem Availability-Zone-Subnetz. Um eine Verbindung zu einer EC2-Instance in einem Outpost-Subnetz herzustellen, können Sie beim Starten der Instance ein Schlüsselpaar angeben, wie dies bei Instances in einem Availability Zone-Subnetz der Fall ist.

Wir empfehlen, das Root-Volume für eine Instance auf einem Outpost-Rack auf 30 GiB oder weniger zu beschränken. Sie können Daten-Volumes in der Blockgeräte-Zuweisung des AMI oder der Instance angeben, um zusätzlichen Speicher bereitzustellen. Informationen zum Entfernen ungenutzter Blöcke aus dem Startvolume finden Sie unter How to Build Sparse EBS Volumes im AWS Partner Network-Blog.

Es wird empfohlen, das NVMe-Timeout für das Root-Volume zu erhöhen. Weitere Informationen finden Sie unter Timeout für I/O-Operationen.

Informationen zum Erstellen eines Outposts finden Sie unter Erste Schritte mit AWS Outposts im AWS Outposts -Benutzerhandbuch.

Erstellen eines Volumes in einem Outpost-Rack

AWS Outposts bietet Rack- und Server-Formfaktoren. Wenn sich Ihre Kapazität in einem Outpost-Rack befindet, können Sie EBS-Volumes in dem Outpost-Subnetz erstellen, das Sie erstellt haben. Wenn Sie das Volume erstellen, geben Sie den Amazon-Ressourcennamen (ARN) des Outposts an.

Der folgende Befehl create-volume erstellt ein leeres 50 GB-Volume auf dem angegebenen Outpost.

```
aws ec2 create-volume --availability-zone us-east-2a --outpost-arn arn:aws:outposts:us-east-2:123456789012:outpost/op-03e6fecad652a6138 --size 50
```

Sie können die Größe Ihres Amazon EBS gp2-Volumes dynamisch ändern, ohne sie zu trennen. Weitere Informationen zum Ändern eines Volumes, ohne es zu trennen, finden Sie unter Beantragen von Änderungen an Ihren EBS-Volumes.

IP-Adressierung von Amazon EC2-Instances

Amazon EC2 und Amazon VPC unterstützen sowohl die IPv4- als auch IPv6-Adressierungsprotokolle. Standardmäßig verwendet Amazon VPC das IPv4-Adressierungsprotokoll; dieses Verhalten lässt sich nicht deaktivieren. Wenn Sie eine VPC erstellen, müssen Sie einen IPv4 CIDR-Block (einen privaten IPv4-Adressenbereich) angeben. Optional können Sie Ihrer VPC und einen IPv6-CIDR-Block zuordnen und den Instances in Ihrem Subnetz IPv6-Adressen von diesem Block zuweisen.

Inhalt

- Hostnamen der EC2-Instance
- Link-lokale Adressen

Private IPv4-Adressen

Eine private IPv4-Adresse ist eine IP-Adresse, die nicht über das Internet erreichbar ist. Sie können private IPv4-Adressen zur Kommunikation zwischen Instances im selben VPC verwenden. Weitere Informationen über die Standards und Spezifikationen vom privaten IPv4-Adressen finden Sie unter RFC 1918. Wir reservieren mit DHCP private IPv4-Adressen für Instances.

> **Note**
>
> Sie können eine VPC mit einem öffentlich routingfähigen CIDR-Block erstellen, der außerhalb der privaten, in RFC 1918 angegebenen IPv4-Adressbereiche fällt. Für die Zwecke dieser Dokumentation bezeichnen wir als private IPv4-Adressen (oder „private IP-Adressen“) die IP-Adressen, die innerhalb des IPv4 CIDR-Bereichs Ihrer VPC liegen.

VPC-Subnetze können einen der folgenden Typen haben:

VPC-Subnetze können einen der folgenden Typen haben:

- Nur-IPv4-Subnetze: Sie können nur Ressourcen in diesen Subnetzen erstellen, deren IPv4-Adressen zugewiesen sind.
- Nur-IPv6-Subnetze: Sie können nur Ressourcen in diesen Subnetzen erstellen, deren IPv6-Adressen zugewiesen sind.
- IPv4- und IPv6-Subnetze: Sie können Ressourcen in diesen Subnetzen erstellen, deren IPv4- oder IPv6-Adressen zugewiesen sind.

Wenn Sie eine EC2-Instance in einem reinen IPv4-oder Dual-Stack-Subnetz (IPv4 und IPv6) starten, erhält die Instance eine primäre private IP-Adresse vom IPv4-Adressbereich des Subnetzes. Weitere Informationen finden Sie unter IP-Adresse im Amazon-VPC-Benutzerhandbuch. Wenn Sie beim Start der Instance keine primäre private IP-Adresse angeben, wählen wir eine verfügbare IP-Adresse im IPv4-Bereich des Subnetzes für Sie aus. Jede Instance hat eine standardmäßige Netzwerkschnittstelle (eth0), die der primären privaten IPv4-Adresse zugeordnet ist. Sie können auch zusätzliche private IPv4-Adressen angeben, die auch als sekundäre private IPv4-Adressen bezeichnet werden. Im Gegensatz zu privaten IP-Adressen können sekundäre private IP-Adressen

von einer Instance zur anderen erneut zugewiesen werden. Weitere Informationen finden Sie unter Mehrere IP-Adressen für Ihre EC2-Instances.

Eine private IPv4-Adresse, unabhängig davon, ob es sich um eine primäre oder sekundäre Adresse handelt, bleibt der Netzwerkschnittstelle zugeordnet, wenn die Instance angehalten und neu gestartet oder in den Ruhezustand versetzt und gestartet wird, und wird freigegeben, wenn die Instance beendet wird.

Öffentliche IPv4-Adressen

Eine öffentliche IP-Adresse ist eine IPv4-Adresse, die über das Internet erreichbar ist. Sie können öffentliche Adressen zur Kommunikation zwischen Ihren Instances und dem Internet verwenden.

Wenn Sie eine Instance in einer Standard-VPC starten, weisen wir ihr standardmäßig eine öffentliche IP-Adresse zu. Wenn Sie eine Instance in einer nicht standardmäßigen VPC starten, hat Ihr Subnetz ein Attribut, durch das festgelegt wird, ob in diesem Subnetz gestartete Instances eine öffentliche IP-Adresse aus dem Pool öffentlicher IPv4-Adressen erhalten. Standardmäßig weisen wir Instances, die in einem nicht standardmäßigen Subnetz gestartet wurden, keine öffentliche IP-Adresse zu.

Anhand der folgenden Schritte können Sie kontrollieren, ob Ihre Instance eine öffentliche IP-Adresse erhält:

- Ändern des öffentlichen IP-Adressierungsattributs Ihres Subnetzes. Weitere Informationen finden Sie unter Ändern des öffentlichen IPv4-Adressierungsattributs für Ihr Subnetz im Amazon-VPC-Benutzerhandbuch.
- Aktivieren oder Deaktivieren des öffentlichen IP-Adressierungsfeatures während des Starts, wodurch das öffentliche IP-Adressierungsattribut des Subnetzes überschrieben wird. Weitere Informationen finden Sie unter Zuweisen einer öffentlichen IPv4-Adresse beim Start einer Instance.
- Sie können die Zuweisung einer öffentlichen IP-Adresse zu Ihrer Instance nach dem Start aufheben, indem Sie die mit einer Netzwerkschnittstelle verknüpften IP-Adressen verwalten.

Ihrer Instance wird aus dem Pool öffentlicher IPv4-Adressen von Amazon eine öffentliche IP-Adresse zugewiesen, die nicht mit Ihrem AWS Konto verknüpft ist. Wenn eine öffentliche IP-Adresse von Ihrer Instance getrennt wurde, wird sie an den Pool öffentlicher IPv4-Adressen zurückgegeben, und Sie können sie nicht erneut verwenden.

In bestimmten Fällen geben wir die öffentliche IP-Adresse Ihrer Instance frei oder weisen ihr eine neue zu:

- Wir geben die öffentliche IP-Adresse für Ihre Instance frei, wenn diese angehalten, in den Ruhezustand versetzt oder beendet wird. Ihre angehaltene oder im Ruhezustand befindliche Instance erhält beim Start eine neue öffentliche IP-Adresse.
- Wir geben die öffentliche IP-Adresse Ihrer Instance frei, wenn Sie ihr eine Elastic IP-Adresse zuweisen. Wenn Sie die Elastic IP-Adresse von Ihrer Instance trennen, erhält sie eine neue öffentliche IP-Adresse.
- Wenn die öffentliche IP-Adresse Ihrer Instance in einer VPC freigegeben ist, erhält sie keine neue, wenn mehr als eine Netzwerkschnittstelle mit Ihrer Instance verbunden ist.
- Wenn die öffentliche IP-Adresse Ihrer Instance freigegeben wird, während sie eine zweite private IP-Adresse hat, die einer Elastic-IP-Adresse zugeordnet ist, erhält die Instance keine neue öffentliche IP-Adresse.

Wenn Sie eine persistente öffentliche IP-Adresse benötigen, die Instances nach Bedarf zugeordnet werden kann, verwenden Sie eine Elastic IP-Adresse.

Wenn Sie dynamisches DNS verwenden, um einen existierenden DNS-Namen der öffentlichen IP-Adresse einer neuen Instance zuzuordnen, kann es bis zu 24 Stunden dauern, bis die IP-Adresse im Internet übernommen wird. Infolgedessen erhalten neue Instances möglicherweise keinen Datenverkehr, während beendete Instances weiterhin Anfragen erhalten. Verwenden Sie eine Elastic IP-Adresse, um dieses Problem zu lösen. Sie können Ihre eigene Elastic IP-Adresse zuweisen und sie mit Ihrer Instance verknüpfen. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

> **Note**
>
> - AWS Gebühren für alle öffentlichen IPv4-Adressen, einschließlich öffentlicher IPv4-Adressen, die mit laufenden Instances verknüpft sind, und Elastic IP-Adressen. Weitere Informationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite Preise für Amazon VPC.
> - Für Instances, die auf andere Instances über ihre öffentliche NAT-IP-Adresse zugreifen, werden Gebühren für regionale oder Internet-Datenübertragung berechnet, je nachdem, ob sich die Instances in derselben Region befinden.

Optimierung öffentlicher IPv4-Adressen

AWS Gebühren für alle öffentlichen IPv4-Adressen, einschließlich öffentlicher IPv4-Adressen, die mit laufenden Instances verknüpft sind, und Elastic IP-Adressen. Weitere Informationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite Preise für Amazon VPC.

Die folgende Liste enthält Maßnahmen, die Sie ergreifen können, um die Anzahl der von Ihnen verwendeten öffentlichen IPv4-Adressen zu optimieren:

- Verwenden Sie einen Elastic Load Balancer, um den Datenverkehr zu Ihren EC2-Instances zu verteilen, und deaktivieren Sie die automatische Zuweisung öffentlicher IP-Adressen auf der primären ENI, die den Instances zugewiesen ist. Load Balancer verwenden eine einzige öffentliche IPv4-Adresse, sodass die Anzahl Ihrer öffentlichen IPv4-Adressen reduziert wird. Möglicherweise möchten Sie auch vorhandene Load Balancer konsolidieren, um die Anzahl der öffentlichen IPv4-Adressen weiter zu reduzieren.
- Wenn der einzige Grund für die Verwendung eines NAT-Gateways die SSH-Verbindung zu einer EC2-Instance in einem privaten Subnetz für Wartungs- oder Notfälle ist, sollten Sie stattdessen EC2 Instance Connect Endpoint verwenden. Mit EC2 Instance Connect Endpoint können Sie über das Internet eine Verbindung zu einer Instance herstellen, ohne dass die Instance über eine öffentliche IPv4-Adresse verfügen muss.
- Wenn sich Ihre EC2-Instances in einem öffentlichen Subnetz befinden und ihnen öffentliche IP-Adressen zugewiesen sind, sollten Sie erwägen, die Instances in ein privates Subnetz zu verschieben, die öffentlichen IP-Adressen zu entfernen und ein öffentliches NAT-Gateway zu verwenden, um den Zugriff auf und von Ihren EC2-Instances zu ermöglichen. Bei der Verwendung von NAT-Gateways müssen die Kosten berücksichtigt werden. Verwenden Sie diese Berechnungsmethode, um zu entscheiden, ob NAT-Gateways kostengünstig sind. Sie können die für diese Berechnung `Number of public IPv4 addresses` erforderlichen Informationen abrufen, indem Sie einen AWS Abrechnungskosten- und Nutzungsbericht erstellen.

  ```
  NAT gateway per hour + NAT gateway public IPs + NAT gateway transfer / Existing
   public IP cost
  ```

  Wobei gilt:

  - `NAT gateway per hour = $0.045 * 730 hours in a month * Number of Availability Zones the NAT gateways are in`
  - `NAT gateway public IPs = $0.005 * 730 hours in a month * Number of IPs associated with your NAT gateways`

  - `NAT gateway transfer = $0.045 * Number of GBs that will go through the NAT gateway in a month`
  - `Existing public IP cost = $0.005 * 730 hours in a month * Number of public IPv4 addresses`

  Wenn die Summe weniger als 1 ist, sind NAT-Gateways günstiger als öffentliche IPv4-Adressen.
- Wird verwendet AWS PrivateLink, um private Verbindungen zu AWS Diensten oder Diensten herzustellen, die von anderen AWS Konten gehostet werden, anstatt öffentliche IPv4-Adressen und Internet-Gateways zu verwenden.
- Bringen Sie Ihren eigenen IP-Adressbereich (BYOIP) mit AWS und verwenden Sie den Bereich für öffentliche IPv4-Adressen, anstatt öffentliche IPv4-Adressen im Besitz von Amazon zu verwenden.
- Deaktivieren Sie die automatische Zuweisung einer öffentlichen IPv4-Adresse für Instances, die in Subnetzen gestartet wurden. Diese Option ist in der Regel standardmäßig für VPCs deaktiviert, wenn Sie ein Subnetz erstellen. Sie sollten jedoch Ihre vorhandenen Subnetze überprüfen, um sicherzustellen, dass sie deaktiviert ist.
- Wenn Sie über EC2-Instances verfügen, die keine öffentlichen IPv4-Adressen benötigen, überprüfen Sie, ob für die Netzwerkschnittstellen, die an Ihre Instances angeschlossen sind, die automatische Zuweisung öffentlicher IP-Adressen deaktiviert ist.
- Konfigurieren Sie Accelerator-Endpunkte AWS Global Accelerator für EC2-Instances in privaten Subnetzen, damit der Internetverkehr direkt zu den Endpunkten in Ihren VPCs fließen kann, ohne dass öffentliche IP-Adressen erforderlich sind. Sie können auch Ihre eigenen Adressen angeben AWS Global Accelerator und Ihre eigenen IPv4-Adressen für die statischen IP-Adressen Ihres Accelerators verwenden.

Elastic IP-Adressen (IPv4)

Eine Elastic IP-Adresse ist eine öffentliche IPv4-Adresse, die Sie Ihrem Konto zuordnen können. Sie können sie nach Bedarf mit Instances verknüpfen bzw. sie von Instances trennen. Sie wird Ihrem Konto zugewiesen, bis Sie sie freigeben. Weitere Informationen über Elastic IP-Adressen und deren Nutzung finden Sie unter Elastic-IP-Adressen.

Elastic IP-Adressen werden für IPv6 nicht unterstützt.

IPv6-Adressen

Optional können Sie Ihrer VPC auch einen IPv6 CIDR-Block und Ihren Subnetzen IPv6 CIDR-Blöcke zuweisen. Der IPv6 CIDR-Block für Ihre VPC wird automatisch aus dem Amazon-Pool mit IPv6-Adressen zugewiesen; Sie können den Bereich nicht selbst auswählen. Weitere Informationen finden Sie unter den folgenden Themen im Amazon VPC Benutzerhandbuch:

- IP-Adressierung für Ihre VPCs und Subnetze
- Hinzufügen eines IPv6-CIDR-Blocks zu Ihrer VPC
- Hinzufügen eines IPv6-CIDR-Blocks zu Ihrem Subnetz

IPv6-Adressen sind global eindeutig und können so konfiguriert werden, dass sie privat oder über das Internet erreichbar sind. Ihre Instance erhält eine IPv6-Adresse, wenn Ihrer VPC und Ihrem Subnetz ein IPv6 CIDR-Block zugewiesen ist und eine der folgenden Bedingungen zutrifft:

- Ihr Subnetz ist so konfiguriert, dass einer Instance beim Start automatisch eine IPv6-Adresse zugewiesen wird. Weitere Informationen finden Sie unter Ändern des IPv6-Adressierungsattributs für Ihr Subnetz.
- Sie weisen Ihrer Instance beim Start manuell eine IPv6-Adresse zu.
- Sie weisen der primären Netzwerkschnittstelle Ihrer Instance nach dem Start eine IPv6-Adresse zu.
- Sie weisen einer Netzwerkschnittstelle eine IPv6-Adresse im gleichen Subnetz zu und fügen die Netzwerkschnittstelle nach dem Start Ihrer Instance hinzu.

Wenn Ihre Instance beim Start eine IPv6-Adresse erhält, wird die Adresse mit der primären Netzwerkschnittstelle (eth0) der Instance verknüpft. Sie können die IPv6-Adresse der primären Netzwerkschnittstelle (eth0) Ihrer Instance auf folgende Weise verwalten:

- Zuweisung und Aufhebung der Zuweisung von IPv6-Adressen an der Netzwerkschnittstelle. Die Anzahl der IPv6-Adressen, die Sie einer Netzwerkschnittstelle zuweisen können, und die Anzahl der Netzwerkschnittstellen, die Sie einer Instance zuweisen können, ist abhängig vom Instance-Typ. Weitere Informationen finden Sie unter IP-Adressen pro Netzwerkschnittstelle pro Instance-Typ.
- Aktivieren Sie eine primäre IPv6-Adresse. Mit einer primären IPv6-Adresse können Sie eine Unterbrechung des Datenverkehrs zu Instances oder ENIs vermeiden. Weitere Informationen finden Sie unter Erstellen einer Netzwerkschnittstelle oder Verwalten von IP-Adressen.

Eine IPv6-Adresse bleibt beim Anhalten und Starten oder beim Versetzen in den Ruhezustand und Starten Ihrer Instance bestehen und wird beim Beenden Ihrer Instance freigegeben. Solange eine IPv6-Adresse einer anderen Netzwerkschnittstelle zugewiesen ist, können Sie sie nicht erneut zuordnen – Sie müssen die Zuweisung zunächst aufheben.

Sie können kontrollieren, ob Instances über ihre IPv6-Adressen erreichbar sind, indem Sie entweder das Routing Ihres Subnetzes steuern oder Sicherheitsgruppen und Netzwerk-ACL-Regeln verwenden. Weitere Informationen finden Sie unter Datenschutz im Internet-Netzwerk im Amazon VPC-Benutzerhandbuch.

Weitere Informationen über reservierte IPv6-Adressbereiche finden Sie unter IANA IPv6 Special-Purpose Address Registry und RFC4291.

Arbeiten mit den IPv4-Adressen für Ihre Instances

Sie können Ihrer Instance beim Start eine öffentliche IPv4-Adresse zuweisen. Sie können die IPv4-Adressen für Ihre Instance in der Konsole über die Seite Instances oder die Seite Network Interfaces (Netzwerkschnittstellen) anzeigen.

Inhalt

Anzeigen der IPv4-Adressen

Sie können die Amazon-EC2-Konsole verwenden, um die privaten und öffentlichen IPv4-Adressen Ihrer Instances anzuzeigen. Sie können auch die öffentlichen und privaten IPv4-Adressen Ihrer Instance innerhalb Ihrer Instance mithilfe von Instance-Metadaten bestimmen. Weitere Informationen finden Sie unter Arbeiten mit Instance-Metadaten.

Die öffentliche IPv4-Adresse wird als Eigenschaft der Netzwerkschnittstelle auf der Konsole angezeigt, jedoch ist sie mit der primären privaten IPv4-Adresse über NAT verknüpft. Daher wird die öffentliche IPv4-Adresse bei einer Überprüfung der Eigenschaften Ihrer Netzwerkschnittstelle auf Ihrer Instance, beispielsweise über `ifconfig` (Linux) oder `ipconfig` (Windows), nicht angezeigt. Um die öffentliche IPv4-Adresse Ihrer Instance anhand der Instance zu bestimmen, verwendenden Sie Instance-Metadaten.

So zeigen Sie die IPv4-Adressen für eine Instance über die Befehlszeile an

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell).

So bestimmen Sie die IPv4-Adressen Ihrer Instance mithilfe der Instance-Metadaten

1. Verbinden Sie sich mit der Instance. Weitere Informationen finden Sie unter Connect zu Ihrer EC2-Instance her.
2. Verwenden Sie den folgenden Befehl, um auf die private IP-Adresse zuzugreifen.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/local-ipv4
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/local-ipv4
   ```

3. Verwenden Sie den folgenden Befehl, um auf die öffentliche IP-Adresse zuzugreifen. Wenn der Instance eine Elastic IP-Adresse zugewiesen ist, gehört der zurückgegebene Wert zu der Elastic IP-Adresse.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/public-ipv4
   ```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-ipv4
```

Tools for Windows PowerShell

```
PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/public-ipv4
```

Zuweisen einer öffentlichen IPv4-Adresse beim Start einer Instance

Alle Subnetze haben ein Attribut, das bestimmt, ob den Instances, die in diesem Subnetz gestartet werden, eine öffentliche IP-Adresse zugewiesen wird. Standardmäßig ist dieses Attribut bei nicht standardmäßigen Subnetzen auf „false“ eingestellt. Bei standardmäßigen Subnetzen ist es auf „true“ eingestellt. Wenn Sie eine Instance starten, steht Ihnen auch ein öffentliches IPv4-Adressierungsfeature zur Verfügung, um zu kontrollieren, ob Ihrer Instance eine öffentliche IPv4-Adresse zugewiesen wurde. Sie können das Standardverhalten des IP-Adressierungsattributs des Subnetzes außer Kraft setzen. Die öffentliche IPv4-Adresse wird aus dem Pool öffentlicher IPv4-Adressen von Amazon zugeordnet. Sie wird der Netzwerkschnittstelle mit dem Geräteindex eth0 zugewiesen. Dieses Feature ist von bestimmten Bedingungen zum Zeitpunkt des Starts Ihrer Instance abhängig.

Überlegungen

- Sie können die Zuweisung der öffentlichen IP-Adresse zu Ihrer Instance nach dem Start aufheben, indem Sie die IP-Adressen verwalten, die einer Netzwerkschnittstelle zugeordnet sind. Weitere Informationen über öffentliche IPv4-Adressen finden Sie unter Öffentliche IPv4-Adressen.
- Sie können eine öffentliche IP-Adresse nicht automatisch zuweisen, wenn Sie mehr als eine Netzwerkschnittstelle angeben. Darüber hinaus können Sie die Einstellung des Subnetzes auch nicht mithilfe des automatischen Zuweisungsfeatures für öffentliche IP-Adressen überschreiben, wenn Sie für eth0 eine vorhandene Netzwerkschnittstelle angeben.
- Unabhängig davon, ob Sie Ihrer Instance beim Start eine öffentliche IP-Adresse zuweisen oder nicht, können Sie Ihrer Instance nach dem Start eine Elastic IP-Adresse zuordnen. Weitere Informationen finden Sie unter Elastic-IP-Adressen. Sie können auch das Adressierungsverhaltens Ihres Subnetzes für öffentliche IPv4-Adressen ändern. Weitere Informationen finden Sie unter Ändern des öffentlichen IPv4-Adressierungsattributs für Ihr Subnetz.

So weisen Sie eine öffentliche IPv4-Adresse beim Start einer Instance zu

Folgen Sie dem Verfahren unter Eine Instance starten und wenn Sie dabei sind, die Netzwerk-Einstellungen zu konfigurieren, wählen Sie die Option Auto-assign Public IP (Öffentliche IP-Adresse automatisch zuweisen).

So aktivieren oder deaktivieren Sie das Adressierungsfeature für öffentliche IP-Adressen mit der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- Verwenden Sie die Optionen `--associate-public-ip-address` oder `--no-associate-public-ip-address` mit dem Befehl run-instances (AWS CLI).
- Verwenden Sie den `-AssociatePublicIp` Parameter mit dem New-EC2InstanceBefehl (AWS Tools for Windows PowerShell)

Arbeiten mit den IPv6-Adressen für Ihre Instances

Sie können die Ihrer Instance zugewiesenen IPv6-Adressen anzeigen, Ihrer Instance eine öffentliche IPv6-Adresse zuweisen oder die Zuweisung einer IPv6-Adresse zu Ihrer Instance aufheben. Sie können diese Adressen in der Konsole über die Seite Instances oder die Seite Netzwerkschnittstellen anzeigen.

Inhalt

Anzeigen der IPv6-Adressen

Sie können die Amazon EC2 EC2-Konsole und Instance-Metadaten verwenden AWS CLI, um die IPv6-Adressen für Ihre Instances anzuzeigen.

So zeigen Sie die IPv6-Adressen für eine Instance mit der Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Suchen Sie auf der Registerkarte Netzwerk die Option IPv6-Adressen.

So zeigen Sie die IPv6-Adressen für eine Instance über die Befehlszeile an

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell).

So zeigen Sie die IPv6-Adressen für eine Instance mithilfe von Instance-Metadaten an

1. Verbinden Sie sich mit der Instance. Weitere Informationen finden Sie unter Connect zu Ihrer EC2-Instance her.
2. Rufen Sie die MAC-Adresse der Instance von ab. `http://169.254.169.254/latest/meta-data/network/interfaces/macs/`
3. Verwenden Sie den folgenden Befehl, um die IPv6-Adresse anzuzeigen.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/network/interfaces/macs/mac-address/ipv6s
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/network/interfaces/
   macs/mac-address/ipv6s
   ```

   Tools for Windows PowerShell

   ```
   PS C:\> Invoke-RestMethod http://169.254.169.254/latest/meta-data/network/
   interfaces/macs/mac-address/ipv6s
   ```

Zuweisen einer IPv6-Adresse zu einer Instance

Wenn Ihrer VPC und dem Subnetz IPv6 CIDR-Blöcke zugeordnet sind, können Sie Ihrer Instance während oder nach dem Start eine IPv6-Adresse zuweisen. Die IPv6-Adresse wird aus dem IPv6-Adressenbereich des Subnetzes zugeordnet. Sie wird der Netzwerkschnittstelle mit dem Geräteindex eth0 zugewiesen.

So weisen Sie IPv6-Adresse beim Start einer Instance zu

Folgen Sie dem Verfahren zum Zuweisen einer IPv6-Adresse beim Start einer Instance unter Eine Instance starten und wenn Sie Netzwerk-Einstellungen konfigurieren, wählen Sie die Option Auto-assign IPv6 IP (IPv6-IP-Adresse automatisch zuweisen).

So weisen Sie nach dem Start eine IPv6-Adresse zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance und anschließend Aktionen, Netzwerk, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie unter IPv6-Adressen die Option Neue IP-Adresse zuweisen aus. Geben Sie eine IPv6-Adresse aus dem Bereich des Subnetzes ein oder lassen Sie das Feld leer, damit Amazon eine IPv6-Adresse für Sie auswählen kann.
5. Wählen Sie Speichern.

So weisen Sie eine IPv6-Adresse mit der Befehlszeile zu

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- Verwenden Sie die Option `--ipv6-addresses` mit dem Befehl run-instances (AWS CLI).
- Verwenden Sie die `Ipv6Addresses` Eigenschaft for `-NetworkInterface` im New-EC2InstanceBefehl ()AWS Tools for Windows PowerShell
- assign-ipv6-addresses (AWS CLI)
- Register-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Aufheben der Zuweisung einer IPv6-Adresse zu einer Instance

Sie können die Zuweisung einer IPv6-Adresse zu einer Instance jederzeit aufheben.

Sie können die Zuweisung einer IPv6-Adresse zu einer Instance mithilfe der Konsole aufheben.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance und anschließend Aktionen, Netzwerk, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie unter IPv6-Adressen die Option Zuweisung aufheben neben der IPv6-Adresse aus.
5. Wählen Sie Speichern.

So heben Sie die Zuweisung einer IPv6-Adresse zu einer Instance über die Befehlszeile auf

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2IpvAddressList(6AWS Tools for Windows PowerShell).

Mehrere IP-Adressen für Ihre EC2-Instances

Sie können Sie mehrere private IPv4- und IPv6-Adressen für Ihre Instances angeben. Die Anzahl von Netzwerkschnittstellen und privaten IPv4- und IPv6-Adressen, die Sie für eine Instance angeben können, hängt vom Instance-Typ ab. Weitere Informationen finden Sie unter IP-Adressen pro Netzwerkschnittstelle pro Instance-Typ.

Es kann nützlich sein, einer Instance in Ihrer VPC mehrere IP-Adresse zuzuweisen, um folgende Aktionen durchzuführen:

- Hosten mehrerer Websites auf einem einzelnen Server, indem mehrere SSL-Zertifikate auf einem einzelnen Server verwendet werden und jedem Zertifikat eine spezifische IP-Adresse zugeordnet wird.
- Betreiben von Netzwerkgeräten, beispielsweise Firewalls oder Load Balancers, die über mehrere IP-Adressen für jede Netzwerkschnittstelle verfügen.
- Umleiten von internem Datenverkehr zu einer Standby-Instance für den Fall, dass Ihre Instance ausfällt, wobei die sekundäre IP-Adresse der Standby-Instance zugewiesen wird.

Inhalt

So funktionieren mehrere IP-Adressen

In der folgenden Liste wird erklärt, wie mehrere IP-Adressen mit Netzwerkschnittstellen zusammen funktionieren:

- Sie können jeder Netzwerkschnittstelle eine sekundäre private IPv4-Adresse zuweisen.
- Sie können mehrere IPv6-Adressen einer Netzwerkschnittstelle in einem Subnetz zuweisen, dem ein IPv6 CIDR-Block zugeordnet ist.
- Sie müssen die sekundäre IPv4-Adresse für die Netzwerkschnittstelle aus dem IPv4 CIDR-Blockbereich des Subnetzes auswählen.
- Sie müssen IPv6-Adressen für die Netzwerkschnittstelle aus dem IPv6 CIDR-Blockbereich des Subnetzes auswählen.
- Sie weisen den Netzwerkschnittstellen Sicherheitsgruppen und keine einzelnen IP-Adressen zu. Daher unterliegt jede IP-Adresse, die Sie in einer Netzwerkschnittstelle angeben, der Sicherheitsgruppe dieser Netzwerkschnittstelle.
- Es kann eine Zuweisung mehrerer IP-Adressen zu Netzwerkschnittstellen erfolgen oder aufgehoben werden, die an laufende oder angehaltene Instances angefügt sind.
- Sekundäre private IPv4-Adressen, die einer Netzwerkschnittstelle zugewiesen sind, können einer anderen Schnittstelle erneut zugewiesen werden, wenn Sie dies ausdrücklich erlauben.
- Eine IPv6-Adresse kann einer anderen Netzwerkschnittstelle nicht erneut zugewiesen werden; Sie müssen zuerst die Zuordnung der IPv6-Adresse zu der bestehenden Netzwerkschnittstelle aufheben.
- Wenn Sie einer Netzwerkschnittstelle mit den Befehlszeilen-Tools oder der API mehrere IP-Adressen zuweisen, schlägt die gesamte Operation fehl, wenn eine der IP-Adressen nicht zugewiesen werden kann.
- Primäre private IPv4-, sekundäre private IPv4-, Elastic IP- und IPv6-Adressen bleiben mit einer sekundären Netzwerkschnittstelle verknüpft, wenn sie von einer Instance getrennt oder an eine Instance angefügt wird.

- Obwohl es nicht möglich ist, die primäre Netzwerkschnittstelle von einer Instance zu trennen, können Sie die sekundäre private IPv4-Adresse der primären Netzwerkschnittstelle einer anderen Netzwerkschnittstelle zuweisen.

In der folgenden Liste wird erklärt, wie mehrere IP-Adressen mit Elastic IP-Adressen (nur IPv4) zusammen funktionieren:

- Jede private IPv4-Adresse kann einer einzelnen Elastic IP-Adresse zugewiesen werden und umgekehrt.
- Wenn eine sekundäre private IPv4-Adresse einer anderen Schnittstelle erneut zugewiesen wird, bleibt die Verknüpfung dieser Adresse mit einer Elastic IP-Adresse bestehen.
- Wenn eine sekundäre private IPv4-Adresse von einer Schnittstelle getrennt wird, wird die Zuordnung einer verknüpften Elastic IP-Adresse von der sekundären privaten IPv4-Adresse automatisch aufgehoben.

Arbeiten mit mehreren IPv4-Adressen

Sie können einer Instance eine sekundäre private IPv4-Adresse zuweisen, einer sekundären privaten IPv4-Adresse eine Elastic IPv4-Adresse zuordnen und die Zuordnung einer sekundären privaten IPv4-Adresse aufheben.

Aufgaben

- Zuweisen einer sekundären privaten IPv4-Adresse
- Konfigurieren Sie das Betriebssystem so, dass es sekundäre private IPv4-Adressen erkennt
- Zuweisen einer Elastic-IP-Adresse zur sekundären privaten IPv4-Adresse
- Anzeigen Ihrer sekundären privaten IPv4-Adressen
- Aufheben der Zuweisung einer sekundären privaten IPv4-Adresse

Zuweisen einer sekundären privaten IPv4-Adresse

Sie können der Netzwerkschnittstelle für eine Instance die sekundäre private IPv4-Adresse zuweisen, während Sie die Instance starten oder wenn die Instance ausgeführt wird.

Zuweisen einer sekundären privaten IPv4-Adresse beim Starten einer Instance

1. Befolgen Sie das Verfahren zum Starten einer Instance. Wählen Sie für Netzwerkeinstellungen die Option Bearbeiten aus.
2. Wählen Sie eine VPC und ein Subnetz aus.
3. Erweiterte Netzwerkkonfiguration erweitert
4. Wählen Sie für Sekundäre IP die Option Automatisch zuweisen und geben Sie die Anzahl der IP-Adressen ein (Amazon weist automatisch sekundäre IPv4-Adressen zu) oder wählen Sie Manuell zuweisen und die IPv4-Adressen eingeben.
5. Führen Sie die verbleibenden Schritte zum Starten der Instance aus.

So weisen Sie beim Start eine sekundäre IPv4-Adresse mit der Befehlszeile zu

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- Die Option `--secondary-private-ip-addresses` mit dem Befehl (AWS CLI) run-instances
- Definieren `-NetworkInterface` und spezifizieren Sie den `PrivateIpAddresses` Parameter mit dem New-EC2InstanceBefehl ().AWS Tools for Windows PowerShell

So weisen Sie einer Netzwerkschnittstelle eine sekundäre private IPv4-Adresse zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Netzwerkschnittstellen und dann die Netzwerkschnittstelle für die Instanz aus.
3. Wählen Sie Actions, Manage IP Addresses aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie unter IPv4-Adressen die Option Neue IP-Adresse zuweisen aus.
5. Geben Sie eine bestimmte IPv4-Adresse ein, die innerhalb des Subnetzbereichs für die Instance liegt, oder lassen Sie das Feld leer, damit Amazon eine IPv4-Adresse für Sie auswählen kann.
6. (Optional) Wählen Sie Zulassen aus, damit die sekundäre private IP-Adresse erneut zugewiesen werden kann, wenn sie bereits einer anderen Netzwerkschnittstelle zugewiesen ist.
7. Wählen Sie Speichern.

Alternativ dazu können Sie einer Instance eine sekundäre private IPv4-Adresse zuweisen. Wählen Sie im Navigationsbereich Instances aus, wählen Sie die Instance und anschließend Aktionen, Netzwerk, IP-Adressen verwalten aus. Sie können die Konfiguration mit den gleichen Informationen wie in den vorherigen Schritten vornehmen. Die IP-Adresse wird der primären Netzwerkschnittstelle (eth0) der Instance zugewiesen.

Um einer vorhandenen Instanz über die Befehlszeile eine sekundäre private IPv4-Adresse zuzuweisen

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- assign-private-ip-addresses (AWS CLI)
- Register-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Konfigurieren Sie das Betriebssystem so, dass es sekundäre private IPv4-Adressen erkennt

Nachdem Sie Ihrer Instance eine sekundäre private IPv4-Adresse zugewiesen haben, müssen Sie das Betriebssystem auf der Instance so konfigurieren, dass es die sekundäre private IP-Adresse erkennt.

Linux-Instances

- Wenn Sie Amazon Linux verwenden, kann das Paket ec2-net-utils diesen Schritt für Sie übernehmen. Es konfiguriert zusätzliche Netzwerkschnittstellen, die Sie anfügen, während die Instance ausgeführt wird, aktualisiert sekundäre IPv4-Adressen während der Erneuerung der DHCP-Lease und aktualisiert die zugehörigen Routing-Regeln. Sie können die Liste der Schnittstellen sofort aktualisieren, indem Sie den Befehl verwenden `sudo service network restart` und die up-to-date Liste dann mit `ip addr li` anzeigen. Wenn Sie eine manuelle Kontrolle über Ihre Netzwerkkonfiguration benötigen, können Sie das Paket ec2-net-utils entfernen. Weitere Informationen finden Sie unter Konfigurieren Sie Ihre Netzwerkschnittstelle mit ec2-net-utils für Amazon Linux 2.
- Wenn Sie eine andere Linux-Verteilung verwenden, ziehen Sie die Dokumentation für Ihre Linux-Distribution zurate. Suchen Sie nach Informationen zum Konfigurieren zusätzlicher Netzwerkschnittstellen und sekundärer IPv4-Adressen. Wenn die Instance zwei oder mehr Schnittstellen in demselben Subnetz hat, suchen Sie nach Informationen zur Verwendung von Routing-Regeln, um asymmetrisches Routing zu umgehen.

Windows-Instances

Weitere Informationen finden Sie unter Konfigurieren einer sekundären privaten IPv4-Adresse für Ihre Windows-Instance.

Zuweisen einer Elastic-IP-Adresse zur sekundären privaten IPv4-Adresse

So weisen Sie einer sekundären privaten IPv4-Adresse eine Elastic IP-Adresse zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Aktivieren Sie das Kontrollkästchen für die Elastic IP-Adresse
4. Wählen Sie Aktionen, Elastic IP Address zuordnen aus.
5. Wählen Sie als Ressourcentyp die Option Netzwerkschnittstelle aus. Wählen Sie die Netzwerkschnittstelle und dann die sekundäre IP-Adresse aus der Liste der privaten IP-Adressen aus.
6. Wählen Sie für Netzwerkschnittstelle die Netzwerkschnittstelle aus. Wählen Sie die sekundäre IP-Adresse aus der Liste Private IP-Adressen aus.
7. Wählen Sie für Private IP-Adresse die sekundäre IP-Adresse aus.
8. Wählen Sie Associate aus.

So weisen Sie einer sekundären privaten IPv4-Adresse eine Elastic IP-Adresse mit der Befehlszeile zu

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- associate-address (AWS CLI)
- Register-EC2Address (AWS Tools for Windows PowerShell)

Anzeigen Ihrer sekundären privaten IPv4-Adressen

So zeigen Sie private IPv4-Adressen an, die einer Netzwerkschnittstelle zugewiesen sind

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.

4. Suchen Sie auf der Registerkarte Details unter IP-Adressen nach Private IPv4-Adresse und Sekundäre private IPv4-Adressen.

So zeigen Sie private IPv4-Adressen an, die einer Instance zugewiesen sind

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Aktivieren Sie das Kontrollkästchen für die Instance.
4. Suchen Sie auf der Registerkarte Netzwerk unter Netzwerkdetails nach Private IPv4-Adressen und Sekundäre private IPv4-Adressen.

Aufheben der Zuweisung einer sekundären privaten IPv4-Adresse

Wenn Sie eine sekundäre private IPv4-Adresse nicht länger benötigen, können Sie die Zuweisung zu der Instance oder der Netzwerkschnittstelle aufheben. Wird die Zuweisung einer sekundären privaten IPv4-Adresse zu einer Netzwerkschnittstelle aufgehoben, wird die Zuordnung der Elastic IP-Adresse (falls vorhanden) ebenfalls getrennt.

So heben Sie die Zuweisung einer sekundären privaten IPv4-Adresse zu einer Instance auf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine Instance und anschließend Aktionen, Netzwerk, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie für IPv4-Adressen Unassign für die IPv4-Adresse, deren Zuweisung aufgehoben werden soll.
5. Wählen Sie Speichern.

So heben Sie die Zuweisung einer sekundären privaten IPv4-Adresse zu einer Netzwerkschnittstelle auf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie die Netzwerkschnittstelle aus, wählen Sie Aktionen, IP-Adressen verwalten.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie für IPv4-Adressen Unassign aus, um die Zuweisung der IPv4-Adresse aufzuheben.

5. Wählen Sie Speichern.

So heben Sie die Zuweisung einer privaten IPv4-Adresse mit der Befehlszeile auf

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- unassign-private-ip-addresses (AWS CLI)
- Unregister-EC2PrivateIpAddress (AWS Tools for Windows PowerShell)

Arbeiten mit mehreren IPv6-Adressen

Sie können Ihrer Instance mehrere IPv6-Adressen zuweisen, die der Instance zugewiesenen IPv6-Adressen anzeigen und die Zuweisung der IPv6-Adressen zu Ihre Instance aufheben.

Inhalt

Zuweisen von mehreren IPv6-Adressen

Sie können Ihrer Instance beim Start oder nach dem Start eine oder mehrere IPv6-Adressen zuweisen. Um der Instance eine IPv6-Adresse zuzuweisen, müssen die VPC und das Subnetz, in dem Sie die Instance starten, einen zugeordneten IPv6 CIDR-Block haben.

So weisen Sie mehrere IPv6-Adressen beim Start zu

1. Befolgen Sie das Verfahren zum Starten einer Instance. Wählen Sie für Netzwerkeinstellungen die Option Bearbeiten aus.
2. Wählen Sie eine VPC und ein Subnetz aus.
3. Erweiterte Netzwerkkonfiguration erweitert
4. Wählen Sie für IPv6-IPs Automatisch zuweisen und die Anzahl der IP-Adressen (Amazon weist die IPv6-Adressen automatisch zu) oder wählen Sie Manuell zuweisen und die IPv6-Adressen eingeben.
5. Führen Sie die verbleibenden Schritte zum Starten der Instance aus.

Sie können den Bildschirm Instances in der Amazon EC2-Konsole verwenden, um einer bestehenden Instance mehrere IPv6-Adressen zuzuweisen. Dadurch wird die IPv6-Adresse der primären Netzwerkschnittstelle (eth0) der Instance zugewiesen. Um der Instance eine spezifische IPv6-Adresse zuzuweisen, überprüfen Sie, ob die IPv6-Adresse nicht bereits einer anderen Instance oder Netzwerkschnittstelle zugewiesen ist.

So weisen Sie einer bestehenden Instance mehrere IPv6-Adressen zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance aus, wählen Sie Aktionen, Netzwerke, IP-Adressen verwalten.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie für IPv6-Adressen für jede hinzuzufügende IPv6-Adresse die Option Neue IP-Adresse zuweisen aus. Sie können eine IPv6-Adresse aus dem Bereich des Subnetzes angeben oder das Feld leer lassen, damit Amazon eine IPv6-Adresse für Sie auswählen kann.
5. Wählen Sie Speichern.

Alternativ können Sie einer bestehenden Netzwerkschnittstelle mehrere IPv6-Adressen zuweisen. Die Netzwerkschnittstelle muss in einem Subnetz erstellt worden sein, dem ein IPv6 CIDR-Block zugeordnet ist. Um der Netzwerkschnittstelle eine spezifische IPv6-Adresse zuzuweisen, müssen Sie überprüfen, ob die IPv6-Adresse nicht bereits einer anderen Netzwerkschnittstelle zugewiesen ist.

So weisen Sie einer Netzwerkschnittstelle mehrere IPv6-Adressen zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie Ihre Netzwerkschnittstelle aus, wählen Sie Aktionen, IP-Adressen verwalten.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie für IPv6-Adressen für jede hinzuzufügende IPv6-Adresse die Option Neue IP-Adresse zuweisen aus. Sie können eine IPv6-Adresse aus dem Bereich des Subnetzes angeben oder das Feld leer lassen, damit Amazon eine IPv6-Adresse für Sie auswählen kann.
5. Wählen Sie Speichern.

CLI-Übersicht

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- Zuweisen einer IPv6-Adresse beim Start:
  - Verwenden Sie die Option `--ipv6-addresses` oder `--ipv6-address-count` mit dem Befehl (AWS CLI) run-instances.
  - Definieren `-NetworkInterface` und spezifizieren Sie die `Ipv6AddressCount` Parameter `Ipv6Addresses` oder mit dem New-EC2InstanceBefehl ().AWS Tools for Windows PowerShell
- Zuweisen einer IPv6-Adresse zu einer Netzwerkschnittstelle:
  - assign-ipv6-addresses (AWS CLI)
  - Register-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Anzeigen Ihrer IPv6-Adressen

Sie können die IPv6-Adressen für eine Instance oder eine Netzwerkschnittstelle anzeigen lassen.

So zeigen Sie die IPv6-Adressen an, die einer Instance zugewiesen sind

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie das Kontrollkästchen für Ihre Instance aus.
4. Suchen Sie auf der Registerkarte Netzwerk das Feld IPv6-Adressen.

So zeigen Sie die einer Netzwerkschnittstelle zugewiesenen IPv6-Adressen an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Aktivieren Sie das Kontrollkästchen für Ihre Netzwerkschnittstelle.
4. Suchen Sie auf der Registerkarte Details unter IP-Adressen das Feld IPv6-Adressen.

CLI-Übersicht

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- Anzeigen der IPv6-Adressen für eine Instance:
  - describe-instances (AWS CLI)
  - Get-EC2Instance (AWS Tools for Windows PowerShell).
- Anzeigen der IPv6-Adressen für eine Netzwerkschnittstelle:
  - describe-network-interfaces (AWS CLI)
  - Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Aufheben der Zuweisung einer IPv6-Adresse

Sie können die Zuweisung einer IPv6-Adresse zur primären Netzwerkschnittstelle einer Instance oder zu einer Netzwerkschnittstelle aufheben.

So heben Sie die Zuweisung einer IPv6-Adresse zu einer Instance auf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Aktivieren Sie das Kontrollkästchen für Ihre Instance und wählen Sie dann Aktionen, Netzwerk, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie unter IPv6-Adressen die Option Zuweisung aufheben neben der IPv6-Adresse aus.
5. Wählen Sie Speichern.

So heben Sie die Zuweisung einer IPv6-Adresse zu einer Netzwerkschnittstelle auf

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Aktivieren Sie das Kontrollkästchen für Ihre Netzwerkschnittstelle und wählen Sie dann Aktionen, IP-Adressen verwalten aus.
4. Erweitern Sie die Netzwerkschnittstelle. Wählen Sie unter IPv6-Adressen die Option Zuweisung aufheben neben der IPv6-Adresse aus.
5. Wählen Sie Speichern.

CLI-Übersicht

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- unassign-ipv6-addresses (AWS CLI)
- Unregister-EC2IpvAddressList(6AWS Tools for Windows PowerShell)

Konfigurieren einer sekundären privaten IPv4-Adresse für Ihre Windows-Instance

Sie können Sie mehrere private IPv4-Adressen für Ihre Instances angeben. Nachdem Sie einer Instance eine sekundäre private IPv4-Adresse zugewiesen haben, müssen Sie das Betriebssystem auf der Instance so konfigurieren, dass es die sekundäre private IPv4-Adresse erkennt.

> **Note**
>
> Diese Anweisungen basieren auf Windows Server 2022. Die Implementierung dieser Schritte kann je nach Betriebssystem der Windows-Instanz variieren.

Aufgaben

- Voraussetzungen
- Schritt 1: Konfigurieren Sie die statische IP-Adressierung in Ihrer Instanz
- Schritt 2: Konfigurieren einer sekundären privaten IP-Adresse für Ihre Instance
- Schritt 3: Konfigurieren von Anwendungen für die Verwendung der sekundären privaten IP-Adresse

Voraussetzungen

1. Weisen Sie der Netzwerkschnittstelle für die Instance die sekundäre private IPv4-Adresse zu. Sie können die sekundäre private IPv4-Adresse zuweisen, wenn Sie die Instance starten oder nachdem die Instance ausgeführt wird. Weitere Informationen finden Sie unter Zuweisen einer sekundären privaten IPv4-Adresse.
2. Weisen Sie eine elastische IP-Adresse zu und verknüpfen Sie sie mit der sekundären privaten IPv4-Adresse. Weitere Informationen erhalten Sie unter Zuweisen einer Elastic-IP-Adresse und Zuweisen einer Elastic-IP-Adresse zur sekundären privaten IPv4-Adresse.

Schritt 1: Konfigurieren Sie die statische IP-Adressierung in Ihrer Instanz

Um für Ihre Windows-Instance die Verwendung von mehreren IP-Adressen zuzulassen, müssen Sie Ihre Instance so konfigurieren, dass anstelle eines DHCP-Servers die statische IP-Adresszuweisung verwendet wird.

> **Important**
>
> Wenn Sie die statische IP-Adressierung in Ihrer Instance konfigurieren, muss die IP-Adresse genau mit dem übereinstimmen, was in der Konsole, CLI oder API angezeigt wird. Die Instance ist u. U. nicht erreichbar, wenn Sie diese IP-Adressen falsch eingeben.

So konfigurieren Sie die statische IP-Adresszuweisung auf einer Windows-Instance

1. Verbinden Sie sich mit der Instance.
2. Suchen Sie nach der IP-Adresse, der Subnetzmaske und den Standard-Gateway-Adressen für die Instance, indem Sie die folgenden Schritte ausführen:
   - Führen Sie den folgenden Befehl aus in PowerShell:

     ```
     ipconfig /all
     ```

     Überprüfen Sie die Ausgabe und notieren Sie sich die Werte für IPv4-Adresse, Subnetzmaske, Standard-Gateway und DNS-Server für die Netzwerkschnittstelle. Ihre Ausgabe sollte dem folgenden Beispiel ähneln:

     ```
     ...

     Ethernet adapter Ethernet 4:

        Connection-specific DNS Suffix  . : us-west-2.compute.internal
        Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
        Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
        IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Lease Obtained. . . . . . . . . . : Monday, April 8, 2024 12:19:29 PM
     ```

```
   Lease Expires . . . . . . . . . . : Monday, April 8, 2024 4:49:30 PM
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCP Server . . . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-
E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

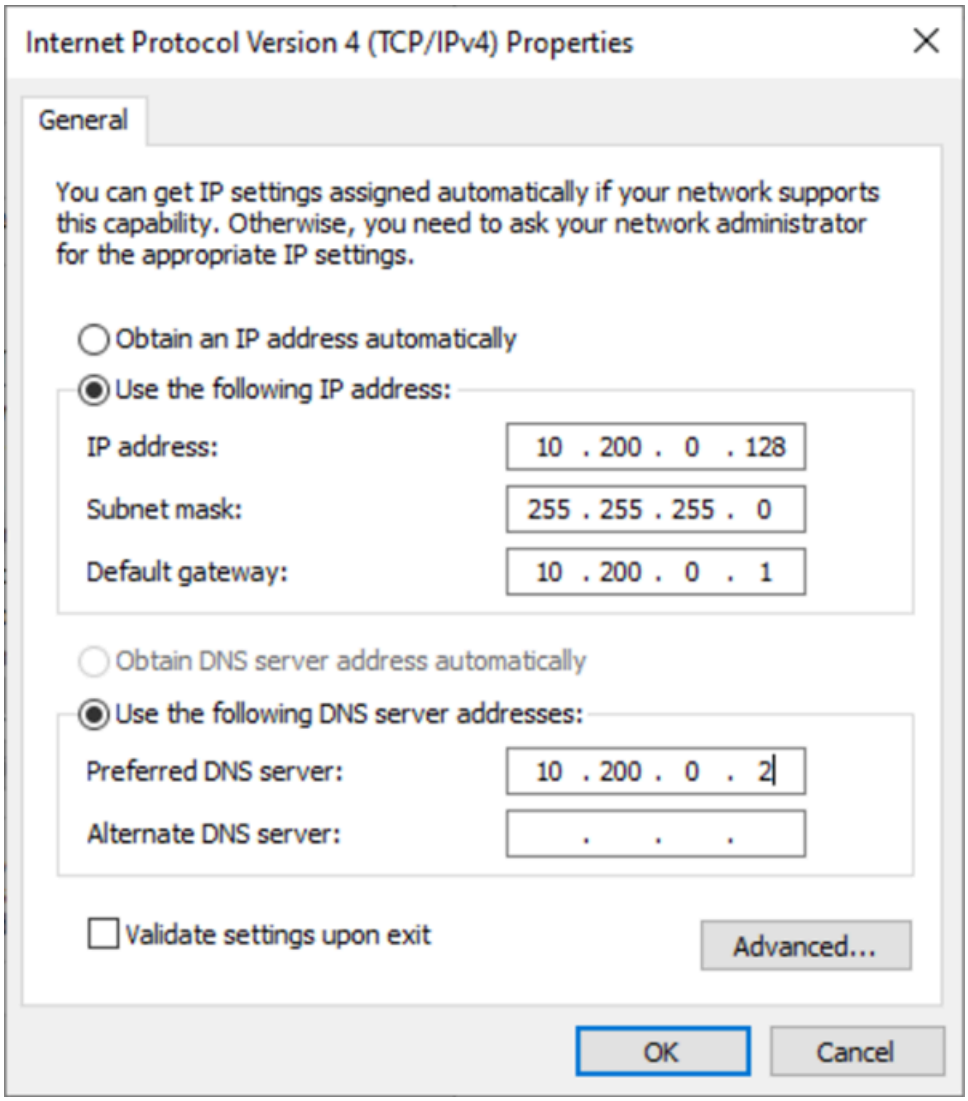
3. Öffnen Sie das Network and Sharing Center, indem Sie den folgenden Befehl in ausführen PowerShell:

```
& $env:SystemRoot\system32\control.exe ncpa.cpl
```

4. Öffnen Sie das Kontextmenü (Rechtsklick) für die Netzwerkschnittstelle (LAN-Verbindung oder Ethernet) und wählen Sie Eigenschaften.
5. Wählen Sie Internetprotokoll Version 4 (TCP/IPv4) und dann Eigenschaften aus.
6. Wählen Sie im Dialogfeld Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4) die Option Folgende IP-Adresse verwenden: aus, geben Sie folgende Werte ein und wählen Sie anschließend OK.

Feld	Value
IP-Adresse	Die oben in Schritt 2 ermittelte IPv4-Adresse.
Subnetzmaske	Die oben in Schritt 2 ermittelte Subnetzmaske.
Standard-Gateway	Das oben in Schritt 2 ermittelte Standard-Gateway.
Bevorzugter DNS-Server	Der oben in Schritt 2 ermittelte DNS-Server.
Alternativer DNS-Server	Der oben in Schritt 2 ermittelte alternative DNS-Server. Lassen Sie dieses Feld leer, wenn kein alternativer DNS-Server aufgeführt wurde.

> **Important**
>
> Wenn Sie die IP-Adresse auf einen beliebigen anderen Wert als die aktuelle IP-Adresse festlegen, geht die Verbindung zur Instance verloren.



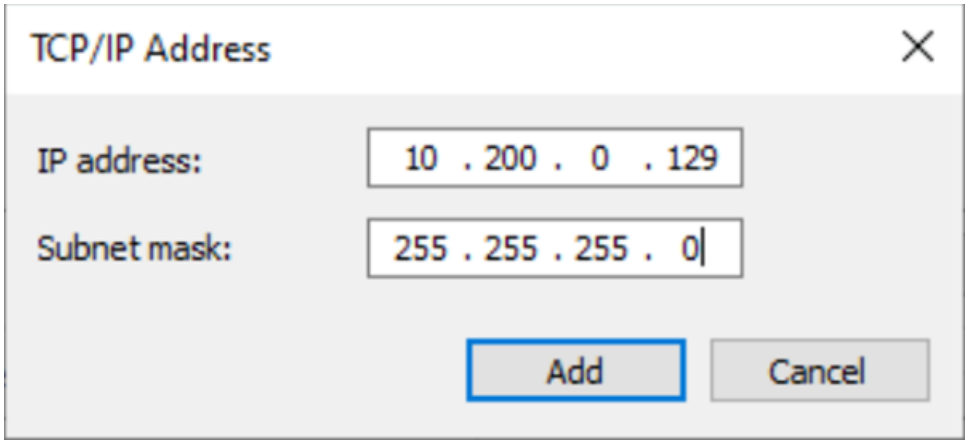
Die RDP-Verbindung zur Windows-Instance geht für einige Sekunden verloren, während die Instance von der DHCP-Adresszuweisung zur statischen Adresszuweisung wechselt. Die Instance behält dieselben IP-Adressinformationen wie zuvor, allerdings sind diese Informationen jetzt statisch und werden nicht vom DHCP-Server verwaltet.

Schritt 2: Konfigurieren einer sekundären privaten IP-Adresse für Ihre Instance

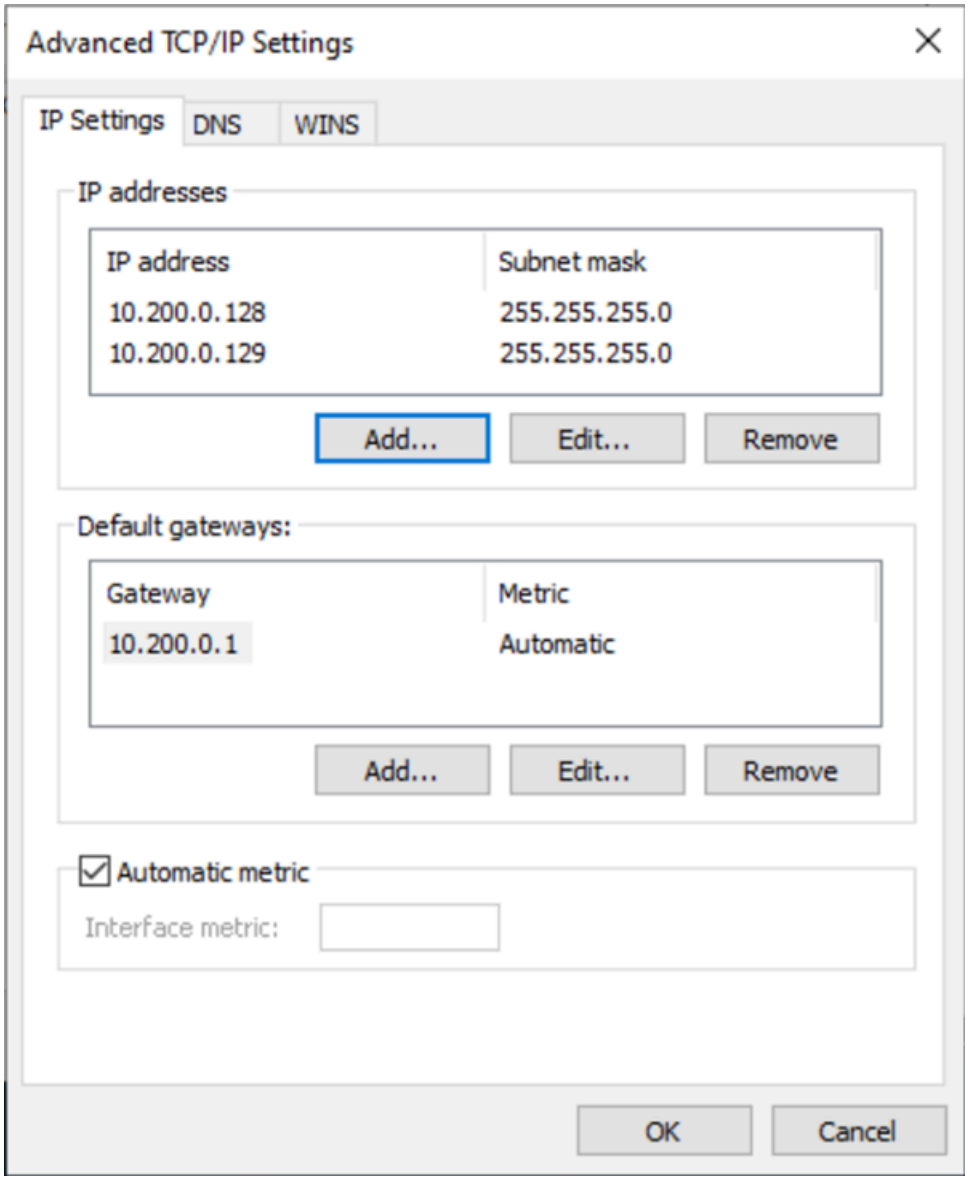
Nachdem Sie die statische IP-Adresszuweisung auf Ihrer Windows-Instance eingerichtet haben, können Sie jetzt eine zweite private IP-Adresse vorbereiten.

So konfigurieren Sie eine sekundäre IP-Adresse

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Notieren Sie sich die auf Networking (Netzwerk) die sekundäre IP-Adresse.
4. Verbinden Sie sich mit der Instance.
5. Wählen Sie auf Ihrer Windows-Instance die Optionen Start und anschließend Systemsteuerung aus.
6. Wählen Sie dann Netzwerk und Internet und anschließend Netzwerk- und Freigabecenter aus.
7. Wählen Sie die Netzwerkschnittstelle (Local Area Connection oder Ethernet) aus und wählen Sie Eigenschaften.
8. Wählen Sie auf der Seite Eigenschaften von LAN-Verbindung die Option Internetprotokoll Version 4 (TCP/IPv4) und dann Eigenschaften und Erweitert aus.
9. Wählen Sie Add (Hinzufügen) aus.
10. Geben Sie im Dialogfeld TCP/IP-Adresse die sekundäre private IP-Adresse als IP-Adresse ein. Geben Sie unter Subnetzmaske dieselbe Subnetzmaske ein, die Sie für die primäre private IP-Adresse unter Schritt 1: Konfigurieren Sie die statische IP-Adressierung in Ihrer Instanz eingegeben haben, und wählen Sie anschließend Hinzufügen aus.



11. Überprüfen Sie die Einstellungen der IP-Adresse und wählen Sie OK.



12. Wählen Sie zuerst OK und dann Schließen aus.
13. Um zu bestätigen, dass die sekundäre IP-Adresse zum Betriebssystem hinzugefügt wurde, führen Sie den `ipconfig /all` Befehl in aus PowerShell. Die Ausgabe sollte in etwa wie folgt aussehen:

```
Ethernet adapter Ethernet 4:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Amazon Elastic Network Adapter #2
   Physical Address. . . . . . . . . : 02-9C-3B-FC-8E-67
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
```

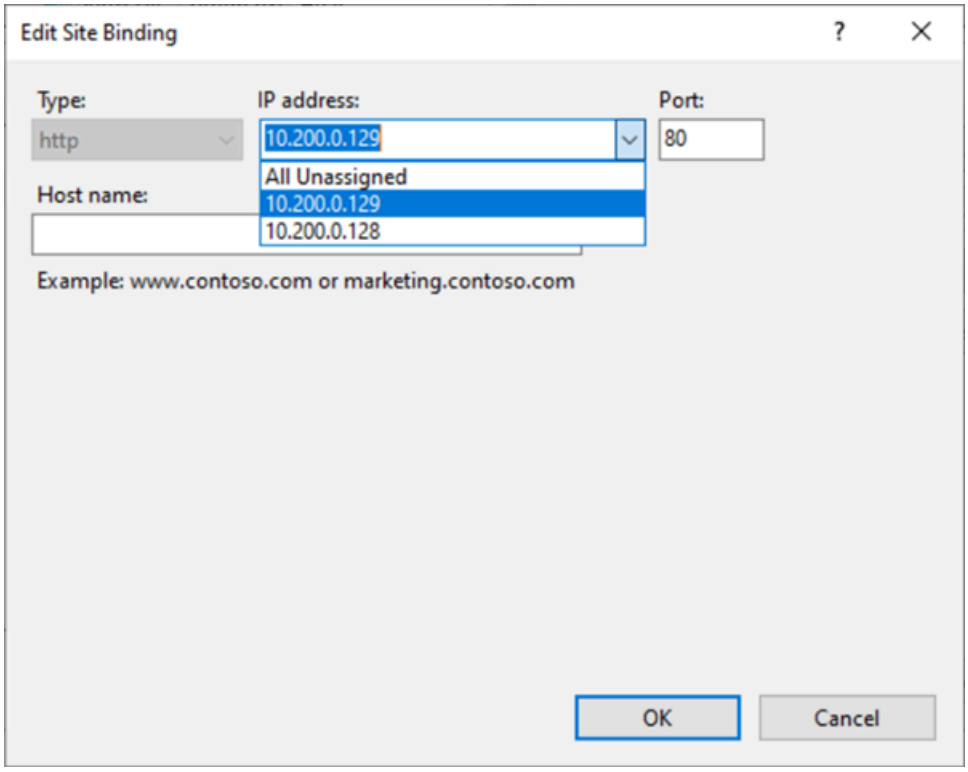
```
   Link-local IPv6 Address . . . . . : fe80::f4d1:a773:5afa:cd1%7(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.200.0.128(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.200.0.129(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.200.0.1
   DHCPv6 IAID . . . . . . . . . . . : 151166011
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-67-AC-FC-12-34-9A-BE-A5-E7
   DNS Servers . . . . . . . . . . . : 10.200.0.2
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Schritt 3: Konfigurieren von Anwendungen für die Verwendung der sekundären privaten IP-Adresse

Sie können beliebige Anwendungen für die Verwendung der sekundären privaten IP-Adresse konfigurieren. Beispiel: Wenn Ihre Instance eine Website unter IIS ausführt, können Sie IIS so konfigurieren, dass die sekundäre private IP-Adresse verwendet wird.

So konfigurieren Sie IIS für die Verwendung der sekundären privaten IP-Adresse

1. Verbinden Sie sich mit der Instance.
2. Öffnen Sie den Internetinformationsdienste-Manager (IIS).
3. Erweitern Sie im Bereich Verbindungen die Option Sites.
4. Öffnen Sie das Kontextmenü (rechte Maustaste) für Ihre Website und wählen Sie Bindungen bearbeiten aus.
5. Wählen Sie im Dialogfeld Sitebindungen unter Typ die Option http und anschließend Bearbeiten aus.
6. Wählen Sie im Dialogfeld Sitebindung bearbeiten unter IP-Adresse die sekundäre private IP-Adresse aus. (Standardmäßig akzeptiert jede Website HTTP-Anforderungen von allen IP-Adressen.)



7. Wählen Sie zuerst OK und dann Schließen aus.

Hostnamen der EC2-Instance

Wenn Sie eine EC2-Instance erstellen, AWS erstellt ein Hostname für diese Instance. Weitere Informationen zu den Hostnamentypen und deren Bereitstellung durch finden Sie unter. AWSHostnamentypen für Amazon-EC2-Instances Amazon bietet einen DNS-Server, der von Amazon bereitgestellten Hostnamen zu IPv4- und IPv6-Adressen auflöst. Der Amazon DNS-Server befindet sich an der Basis Ihres VPC-Netzwerkbereichs plus zwei. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Link-lokale Adressen

Link-Local-Adressen sind bekannte, nicht weiterleitbare IP-Adressen. Amazon EC2 verwendet Adressen aus dem Link-lokalen Adressraum, um Services bereitzustellen, auf die nur von einer EC2-Instance aus zugegriffen werden kann. Diese Services werden nicht auf der Instance ausgeführt, sondern auf dem zugrunde liegenden Host. Wenn Sie auf die Link-lokalen Adressen für diese Services zugreifen, kommunizieren Sie entweder mit dem Xen-Hypervisor oder dem Nitro-Controller.

Link-lokale Adressbereiche

- IPv4 – 169.254.0.0/16 (169.254.0.0 bis 169.254.255.255)
- IPv6 – fe80::/10

Services, auf die Sie über Link-lokale Adressen zugreifen

- Instance-Metadatenservice
- Amazon Route 53 Resolver (auch bekannt als Amazon DNS-Server)
- Amazon Time Sync Service

Hostnamentypen für Amazon-EC2-Instances

In diesem Abschnitt werden die Hostnamentypen der Amazon-EC2-Instance beschrieben, die verfügbar sind, wenn Sie Instances in Ihren VPC-Subnetzen starten.

Der Hostname unterscheidet die EC2-Instances in Ihrem Netzwerk. Sie können den Hostnamen einer Instance verwenden, wenn Sie beispielsweise Skripte ausführen möchten, um mit einigen oder allen Instances in Ihrem Netzwerk zu kommunizieren.

Inhalt

Typen von EC2-Hostnamen

Es gibt zwei Hostnamentypen für den Hostnamen des Gastbetriebssystems, wenn EC2-Instances in einer VPC gestartet werden:

- IP Name (IP-Name): Das Legacy-Namensschema, in dem beim Start einer Instance die Private IPv4-Adresse die Instance im Hostnamen der Instance enthalten ist. Der IP-Adressenname existiert für die Lebensdauer der EC2-Instance. Wenn er als privater DNS-Hostname verwendet wird, wird nur die private IPv4-Adresse (Ein Datensatz) zurückgegeben.

- Resource name (Ressourcenname): Beim Start einer Instance ist die EC2-Instance-ID im Hostnamen der Instance enthalten. Der Ressourcenname existiert für die Lebensdauer der EC2-Instance. Wenn er als privater DNS-Hostname verwendet wird, kann er sowohl die private IPv4-Adresse (A-Datensatz) und/oder die IPv6-Global-Unicast-Adresse (AAAA-Datensatz) zurückgeben.

Der Hostname des EC2-Instance-Gastbetriebssystems hängt von den Subnetzeinstellungen ab:

- Wenn die Instance in ein reines IPv4-Subnetz gestartet wird, können Sie entweder den IP-Namen oder den Ressourcennamen auswählen.
- Wenn die Instance in einem Dual-Stack-Subnetz (IPv4+IPv6) gestartet wird, können Sie entweder den IP-Namen oder den Ressourcennamen auswählen.
- Wenn die Instance in ein reines IPv6-Subnetz gestartet wird, wird automatisch der Ressourcenname verwendet.

Inhalt

IP-Name

Wenn Sie eine EC2-Instance mit dem Hostname-Typ von IP-Name starten, wird der Hostname des Gastbetriebssystems so konfiguriert, dass er die private IPv4-Adresse verwendet.

- Format für eine Instance in us-east-1: *`private-ipv4-address`*`.ec2.internal`
- Beispiel: *`ip-10-24-34-0`*`.ec2.internal`
- Format für eine Instanz in einer anderen AWS Region: *`private-ipv4-address.region`*`.compute.internal`
- Beispiel: *`ip-10-24-34-0.us-west-2`*`.compute.internal`

Ressourcenname

Wenn Sie EC2-Instances in reinen IPv6-Subnetzen starten, wird der Hostname type (Hostname-Typ) Resource name (Ressourcenname) standardmäßig ausgewählt. Wenn Sie eine Instance in

reinen IPv4-Subnetzen oder Dual-Stack-Subnetzen (IPv4+IPv6) starten, ist der Resource name (Ressourcenname) eine Option, die Sie auswählen können. Nach dem Start einer Instance können Sie die Hostnamenkonfiguration verwalten. Weitere Informationen finden Sie unter Ändern des Hostnamen-Typs und der DNS-Hostname-Konfigurationen.

Wenn Sie eine EC2-Instance mit einem Hostname type (Hostname-Typ) Resource name (Ressourcenname) starten, wird der Hostname des Gastbetriebssystems so konfiguriert, dass er die EC2-Instance-ID verwendet.

- Format für eine Instance in us-east-1: *ec2-instance-id*.ec2.internal
- Beispiel: *i-0123456789abcdef*.ec2.internal
- Format für eine Instanz in einer anderen AWS Region: *ec2-instance-id.region*.compute.internal
- Beispiel: *i-0123456789abcdef.us-west-2*.compute.internal

Der Unterschied zwischen IP-Name und Ressourcenname

DNS-Abfragen für IP-Namen und Ressourcennamen existieren nebeneinander, um die Abwärtskompatibilität zu gewährleisten und Ihnen die Migration von der IP-basierten Benennung für Hostnamen zur ressourcenbasierten Benennung zu ermöglichen. Für private DNS-Hostnamen basierend auf IP-Namen können Sie nicht konfigurieren, ob eine DNS-A-Datensatzabfrage für die Instance beantwortet wird oder nicht. DNS-A-Datensatzabfragen werden unabhängig von den Hostnameneinstellungen des Gastbetriebssystems immer beantwortet. Im Gegensatz dazu können Sie für private DNS-Hostnamen basierend auf dem Ressourcennamen konfigurieren, ob DNS-A- und/oder DNS-AAAA-Abfragen für die Instance beantwortet werden oder nicht. Sie konfigurieren das Antwortverhalten, wenn Sie eine Instance starten oder ein Subnetz ändern. Weitere Informationen finden Sie unter Ändern des Hostnamen-Typs und der DNS-Hostname-Konfigurationen.

Wo Sie den Ressourcennamen und den IP-Namen sehen

In diesem Abschnitt wird beschrieben, wo die Hostname-Typen „Ressourcenname“ und „IP-Name“ in der EC2-Konsole angezeigt werden.

Inhalt

Beim Erstellen einer EC2-Instance

Wenn Sie eine EC2-Instance erstellen, sind je nachdem, welchen Subnetztyp Sie auswählen, Hostname type (Hostname-Typ) und Resource name (Ressourcenname), verfügbar oder er ist möglicherweise ausgewählt und nicht modifizierbar. In diesem Abschnitt wird die Szenarien beschrieben, wo Sie die Hostname-Typen „Ressourcenname“ und „IP-Name“ sehen können.

Szenario 1

Sie erstellen eine EC2-Instance im Assistenten (siehe Starten einer Instance mit dem neuen Launch Instance Wizard) und wählen bei der Konfiguration der Details ein Subnetz aus, das Sie als nur IPv6 konfiguriert haben.

In diesem Fall wird der Hostname type (Hostname-Typ) Resource name (Ressourcenname) automatisch ausgewählt und kann nicht geändert werden. Die Optionen für den DNS-Hostnamen Enable IP name IPv4 (A record) DNS requests (IP-Namen-IPv4-DNS-Anforderungen (A-Datensatz) aktivieren) und Ressourcenbasierte IP-Namen-IPv4-DNS-Anforderungen (A-Datensatz) aktivieren) werden automatisch deaktiviert und können nicht geändert werden. Enable resource-based IPv6 (AAAA record) DNS requests (Ressourcenbasierte IPv6-DNS-Anfragen (AAAA-Datensatz) aktibieren) ist standardmäßig ausgewählt, aber modifizierbar. Wenn diese Option aktiviert ist, werden DNS-Anfragen an den Ressourcennamen in die IPv6-Adresse (AAAA-Datensatz) dieser EC2-Instance aufgelöst.

Szenario 2

Sie erstellen eine EC2-Instance im Assistenten (siehe Starten einer Instance mit dem neuen Launch Instance Wizard) und wählen bei der Konfiguration der Details ein Subnetz aus, das mit einem IPv4-CIDR-Block oder einem IPv4- und IPv6-CIDR-Block („Dual-Stack“) konfiguriert ist.

In diesem Fall ist Enable IP name IPv4 (A record) DNS requests (IP-Namen-IPv4-DNS-Anforderungen (A-Datensatz) aktivieren) automatisch ausgewählt und nicht modifizierbar. Dies bedeutet, dass Anfragen an den IP-Namen an die IPv4-Adresse (A-Datensatz) dieser EC2-Instance aufgelöst werden.

Die Optionen sind standardmäßig auf die Konfigurationen des Subnetzes festgelegt, aber Sie können die Optionen für diese Instance abhängig von den Subnetzeinstellungen ändern:

- Hostname type (Hostnamen-Typ): Bestimmt, ob der Hostname des Gastbetriebssystems der EC2-Instance der Ressourcenname oder der IP-Name sein soll. Der Standardwert ist IP name (IP-Name).

- Enable resource-based IPv4 (A record) DNS requests (Ressourcenbasierte IPv4-DNS-Anforderungen (A-Datensatz) aktivieren): Bestimmt, ob Anforderungen an Ihren Ressourcennamen an die private IPv4-Adresse (A-Datensatz) dieser EC2-Instance aufgelöst werden. Diese Option ist standardmäßig ausgewählt.
- Enable resource-based IPv6 (AAAA record) DNS requests (Ressourcenbasierte IPV6-DNS-Anforderungen (AAAA-Datensatz) aktivieren): Bestimmt, ob Anfragen an Ihren Namen der Ressource an die private IPv6-GUA-Adresse (AAAA-Datensatz) dieser EC2-Instance aufgelöst werden. Diese Option ist standardmäßig nicht ausgewählt.

Beim Anzeigen der Details einer vorhandenen EC2-Instance

Sie können die Hostnamenwerte für eine vorhandene EC2-Instance auf der Registerkarte Details (Details) für die EC2-Instance anzeigen.

- Hostname type (Hostnamen-Typ): Der Hostname im IP-Namen- oder im Ressourcennamenformat.
- Private IP DNS name (IPv4 only) (Privater IP-DNS-Name (nur IPv4)): Der IP-Name, der immer an die private IPv4-Adresse der Instance aufgelöst wird.
- Private resource DNS name (DNS-Name der privaten Ressource): Der Ressourcenname, der zu den für diese Instance ausgewählten DNS-Datensätzen aufgelöst wird.
- Answer private resource DNS name (Mit privatem Ressourcen-DNS-Namen antworten): Der Ressourcenname wird in IPv4 (A)-, IPv6 (AAAA)- oder IPv4- und IPv6-DNS-Datensätze (A und AAAA) aufgelöst.

Wenn Sie sich außerdem direkt über SSH mit Ihrer EC2-Instance verbinden und den `hostname`-Befehl eingeben, wird der Hostname entweder im IP- oder im Ressourcennamenformat angezeigt.

So entscheiden Sie, ob Sie den Ressourcennamen oder den IP-Namen wählen

Wenn beim Starten einer EC2-Instance (siehe Starten einer Instance mit dem neuen Launch Instance Wizard) für den Hostname type (Hostname-Typ) und Resource name (Ressourcenname) entscheiden, wird die EC2-Instance mit einem Hostnamen im Ressourcennamenformat gestartet. In solchen Fällen kann der DNS-Datensatz für diese EC2-Instance auch auf den Ressourcennamen verweisen. Dies gibt Ihnen die Flexibilität zu wählen, ob dieser Hostname in die IPv4-Adresse, die IPv6-Adresse oder sowohl die IPv4- als auch die IPv6-Adresse der Instance aufgelöst wird. Wenn Sie planen, IPv6 in Zukunft zu verwenden oder wenn Sie heute Dual-Stack-Subnetze verwenden, ist

es am besten, einen Hostname type (Hostname-Typ) des Resource name (Ressourcennamens) zu verwenden, damit Sie die DNS-Auflösung für die Hostnamen Ihrer Instances ändern können, ohne die DNS-Einträge selbst zu ändern. Der Ressourcenname ermöglicht es Ihnen, IPv4- und IPv6-DNS-Auflösung bei einer EC2-Instance hinzuzufügen und zu entfernen.

Wenn Sie stattdessen einen Hostname type (Hostnamen-Typ) des IP name (IP-Namens) und ihn als DNS-Hostnamen verwenden, kann er nur an die IPv4-Adresse der Instance aufgelöst werden. Er wird nicht an die IPv6-Adresse der Instance aufgelöst, selbst wenn der Instance sowohl eine IPv4-Adresse als auch eine IPv6-Adresse zugeordnet ist.

Ändern des Hostnamen-Typs und der DNS-Hostname-Konfigurationen

Führen Sie die Schritte in diesem Abschnitt aus, um die Konfigurationen des Hostnamen-Typs und des DNS-Hostnamens für Subnetze oder EC2-Instances zu ändern, nachdem diese gestartet worden sind.

Inhalt

Subnetze

Ändern Sie die Konfigurationen für ein Subnetz, indem Sie ein Subnetz in der VPC-Konsole auswählen und Actions (Aktionen), Edit subnet settings (Subnetzeinstellungen bearbeiten) auswählen.

> **Note**
>
> Das Ändern der Subnetzeinstellungen ändert nicht die Konfiguration von EC2-Instances, die bereits im Subnetz gestartet wurden.

- Hostname type (Hostnamen-Typ): Legt fest, ob die Standardeinstellung des Hostnamens des Gastbetriebssystems der im Subnetz gestarteten EC2-Instance der Ressourcenname oder der IP-Name sein soll.
- Enable DNS hostname IPv4 (A record) requests (DNS Hostname IPv4 (A-Datensatz)-Anforderungen aktivieren): Bestimmt, ob DNS-Anforderungen/-Abfragen an Ihren

Ressourcennamen in die private IPv4-Adresse (A-Datensatz) dieser EC2-Instance aufgelöst werden.

- DNS-Hostnamen-IPv6-Anforderungen (AAAA-Datensatz) aktivieren: Bestimmt, ob DNS-Anfragen/-Anforderungen an Ihren Ressourcennamen in die IPv6-Adresse (AAAA-Datensatz) dieser EC2-Instance aufgelöst werden.

EC2-Instances

Befolgen Sie die Schritte in diesem Abschnitt, um die Konfigurationen des Hostnamen-Typs und des DNS-Hostnamens für eine EC2-Instance zu ändern.

> **Important**
>
> - Um die Einstellung Use resource based naming as guest OS hostname (Ressourcenbasierte Benennungen als Hostnamen des Gastbetriebssystems verwenden) zu ändern, müssen Sie zuerst die Instance stoppen. Um die Einstellungen für IPv4 (A-Datensatz)-Anforderung des DNS-Hostnamens beantworten oder IPv6-Anforderungen für DNS-Hostnamen (AAAA-Datensatz) beantworten zu ändern, müssen Sie die Instance nicht stoppen.
> - Um eine der Einstellungen für nicht von EBS-unterstützte EC2-Instance-Typen zu ändern, können Sie die Instance nicht stoppen. Sie müssen die Instance beenden und eine neue Instance mit den gewünschten Konfigurationen des Hostnamen-Typs und des DNS-Hostnamens starten.

So ändern Sie die Konfigurationen des Hostnamen-Typs und des DNS-Hostnamens für eine EC2-Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wenn Sie die Einstellung Use resource based naming as guest OS hostname (Ressourcenbasierte Benennungen als Hostnamen des Gastbetriebssystems verwenden) ändern möchten, stoppen Sie zuerst die EC2-Instance. Andernfalls überspringen Sie diesen Schritt.

   Um die Instance zu stoppen, wählen Sie die Instance aus und wählen Sie Instance-Status, Instance stoppen.

3. Wählen Sie die Instance aus und wählen Sie Aktionen, Instance-Einstellungen, Optionen für die ressourcenbasierte Benennung ändern.

   - Use resource based naming as guest OS hostname (Ressourcenbasierte Benennungen als Hostnamen des Gastbetriebssystems verwenden): Bestimmt, ob der Hostname des Gastbetriebssystems der EC2-Instance der Ressourcenname oder der IP-Name sein soll.
   - Answer DNS hostname IPv4 (A record) requests (Auf DNS Hostnamen IPv4 (A-Datensatz)-Anforderungen antworten): Bestimmt, ob DNS-Anforderungen/-Abfragen an Ihren Ressourcennamen in die private IPv4-Adresse dieser EC2-Instance aufgelöst werden.
   - Auf DNS-Hostnamen-IPv6-Anforderungen (AAAA-Datensatz) antworten: Bestimmt, ob DNS-Anfragen/-Anforderungen an Ihren Ressourcennamen in die IPv6-Adresse (AAAA-Datensatz) dieser EC2-Instance aufgelöst werden.

4. Wählen Sie Speichern.
5. Wenn Sie die Instance gestoppt haben, starten Sie sie erneut.

Bring Your Own IP Addresses (BYOIP) in Amazon EC2

Sie können Ihren öffentlich routbaren IPv4- oder IPv6-Adressbereich ganz oder teilweise aus Ihrem lokalen Netzwerk auf Ihr Konto übertragen. AWS Sie haben weiterhin die Kontrolle über den Adressbereich und können den Adressbereich im Internet über bewerben. AWS Nachdem Sie den Adressbereich aktiviert haben AWS, erscheint er in Ihrem AWS Konto als Adresspool.

Die Liste der Regionen, in denen BYOIP verfügbar ist, finden Sie unter Regionale Verfügbarkeit.

> **Note**
>
> - In den Schritten auf dieser Seite wird beschrieben, wie Sie Ihren eigenen IP-Adressbereich zur ausschließlichen Verwendung in Amazon EC2 verwenden.
> - Informationen zur Verwendung in AWS Global Accelerator Ihrem eigenen IP-Adressbereich finden Sie unter Bring your own IP Addresses (BYOIP) im AWS Global Accelerator Entwicklerhandbuch.
> - Informationen zur Verwendung mit Amazon VPC IP Address Manager Ihrem eigenen IP-Adressbereich finden Sie unter Tutorial: Bringen Sie Ihre IP-Adressen zu IPAM im Amazon VPC IPAM-Benutzerhandbuch.

Inhalt

BYOIP-Definitionen

- Selbstsigniertes X.509-Zertifikat – ein Zertifikatsstandard, der am häufigsten zum Verschlüsseln und Authentifizieren von Daten innerhalb eines Netzwerks verwendet wird. Es ist ein Zertifikat, das verwendet wird AWS , um die Kontrolle über den IP-Bereich anhand eines RDAP-Datensatzes zu validieren. Weitere Informationen zu X.509-Zertifikaten finden Sie unter RFC 3280.
- Autonome Systemnummer (ASN) – Eine weltweit eindeutige Kennung, die eine Gruppe von IP-Präfixen definiert, die von einem oder mehreren Netzwerkbetreibern betrieben werden und eine einzige, klar definierte Routing-Richtlinie einhalten.
- Regional Internet Registry (RIR) – Eine Organisation, die die Zuweisung und Registrierung von IP-Adressen und ASNs innerhalb einer Region der Welt verwaltet.
- Registry Data Access Protocol (RDAP) – Ein schreibgeschütztes Protokoll zur Abfrage aktueller Registrierungsdaten innerhalb einer RIR. Einträge in der abgefragten RIR-Datenbank werden als „RDAP-Einträge“ bezeichnet. Bestimmte Datensatztypen müssen von Kunden über einen von RIR bereitgestellten Mechanismus aktualisiert werden. Diese Datensätze werden von abgefragt, AWS um die Kontrolle über einen Adressraum im RIR zu überprüfen.
- Route Origin Authorization (ROA) – ein von RIRs erstelltes Objekt, mit dem Kunden IP-Ankündigungen, insbesondere autonomer Systeme, authentifizieren können. Eine Übersicht finden Sie unter Route Origin Authorizations (ROAs) auf der ARIN-Website.
- Local Internet Registry (LIR) – Organisationen wie Internet-Serviceanbieter, die ihren Kunden einen Block von IP-Adressen aus einem RIR zuweisen.

Voraussetzungen und Kontingente

- Der Adressbereich muss bei Ihrer Regional Internet Registry (RIR) registriert sein. Alle Richtlinien in Bezug auf geografische Regionen finden Sie in Ihrem RIR. BYOIP unterstützt derzeit die Registrierung im American Registry for Internet Numbers (ARIN), dem Réseaux IP Européens Network Coordination Centre (RIPE) oder dem Asia-Pacific Network Information Centre (APNIC). Er muss auf ein Unternehmen oder eine juristische Person registriert sein und kann nicht auf eine natürliche Person registriert werden.
- Der spezifischste IPv4-Adressbereich, den Sie aufnehmen können, ist /24.
- Der spezifischste IPv6-Adressbereich, den Sie angeben können, ist /48 für CIDRs, die öffentlich beworben werden können, und /56 für CIDRs, die nicht öffentlich beworben werden können.
- ROAs sind nicht erforderlich für CIDR-Bereiche, die nicht öffentlich beworben werden können. Die RDAP-Datensätze müssen aber weiterhin aktualisiert werden.
- Sie können jeden Adressbereich jeweils einer Region zuordnen. AWS
- Sie können Ihrem Konto insgesamt fünf BYOIP-IPv4- und IPv6-Adressbereiche pro AWS Region hinzufügen. AWS Sie können die Kontingente für BYOIP-CIDRs nicht über die Service Quotas-Konsole anpassen, aber Sie können eine Erhöhung des Kontingents beantragen, indem Sie sich an das AWS Support Center wenden, wie unter AWS Service Quotas in der beschrieben. Allgemeine AWS-Referenz
- Sie können Ihren IP-Adressbereich nicht mit anderen Konten teilen, AWS RAM es sei denn, Sie verwenden Amazon VPC IP Address Manager (IPAM) und integrieren IPAM mit Organizations. AWS Weitere Informationen finden Sie unter Integrate IPAM with AWS Organizations im Amazon VPC IPAM-Benutzerhandbuch.
- Die Adressen im IP-Adressbereich müssen über einen sauberen Verlauf verfügen. Wir könnten die Reputation des IP-Adressbereichs untersuchen und uns das Recht vorbehalten, einen IP-Adressbereich abzulehnen, wenn er eine IP-Adresse enthält, die eine schlechte Reputation hat oder mit schädlichem Verhalten in Verbindung gebracht wird.
- Für den Legacy-Adressraum, also den IPv4-Adressraum, der vor der Einrichtung des Regional Internet Registry (RIR)-Systems von der zentralen Registrierungsstelle der Internet Assigned Numbers Authority (IANA) verteilt wurde, ist weiterhin ein entsprechendes ROA-Objekt erforderlich.
- Bei LIRs ist es üblich, dass sie die Datensätze mithilfe eines manuellen Prozesses aktualisieren. Die Bereitstellung kann je nach LIR mehrere Tage dauern.

- Für einen großen CIDR-Block werden ein einzelnes ROA-Objekt und ein RDAP-Datensatz benötigt. Sie können mehrere kleinere CIDR-Blöcke aus diesem Bereich mithilfe eines einzigen Objekts und Datensatzes in mehrere AWS Regionen übertragen. AWS
- BYOIP wird für Wellenlängenzonen oder aktiviert nicht unterstützt. AWS Outposts
- Nehmen Sie keine manuellen Änderungen für BYOIP in RADb oder irgendeinem anderen IRR vor. BYOIP aktualisiert RADb automatisch. Alle manuellen Änderungen, welche die BYOIP-ASN beinhalten, führen dazu, dass der BYOIP-Bereitstellungsvorgang fehlschlägt.
- Sobald Sie einen IPv4-Adressbereich AWS eingerichtet haben, können Sie alle IP-Adressen im Bereich verwenden, einschließlich der ersten Adresse (der Netzwerkadresse) und der letzten Adresse (der Broadcast-Adresse).

Onboarding-Voraussetzungen für Ihren BYOIP-Adressbereich

Der Onboarding-Prozess für BYOIP hat zwei Phasen, für die Sie drei Schritte ausführen müssen. Diese Schritte werden im folgenden Diagramm dargestellt. Wir schließen manuelle Schritte in diese Dokumentation ein, aber Ihr RIR bietet möglicherweise verwaltete Services an, um Sie bei diesen Schritten zu unterstützen.

Vorbereitungsphase

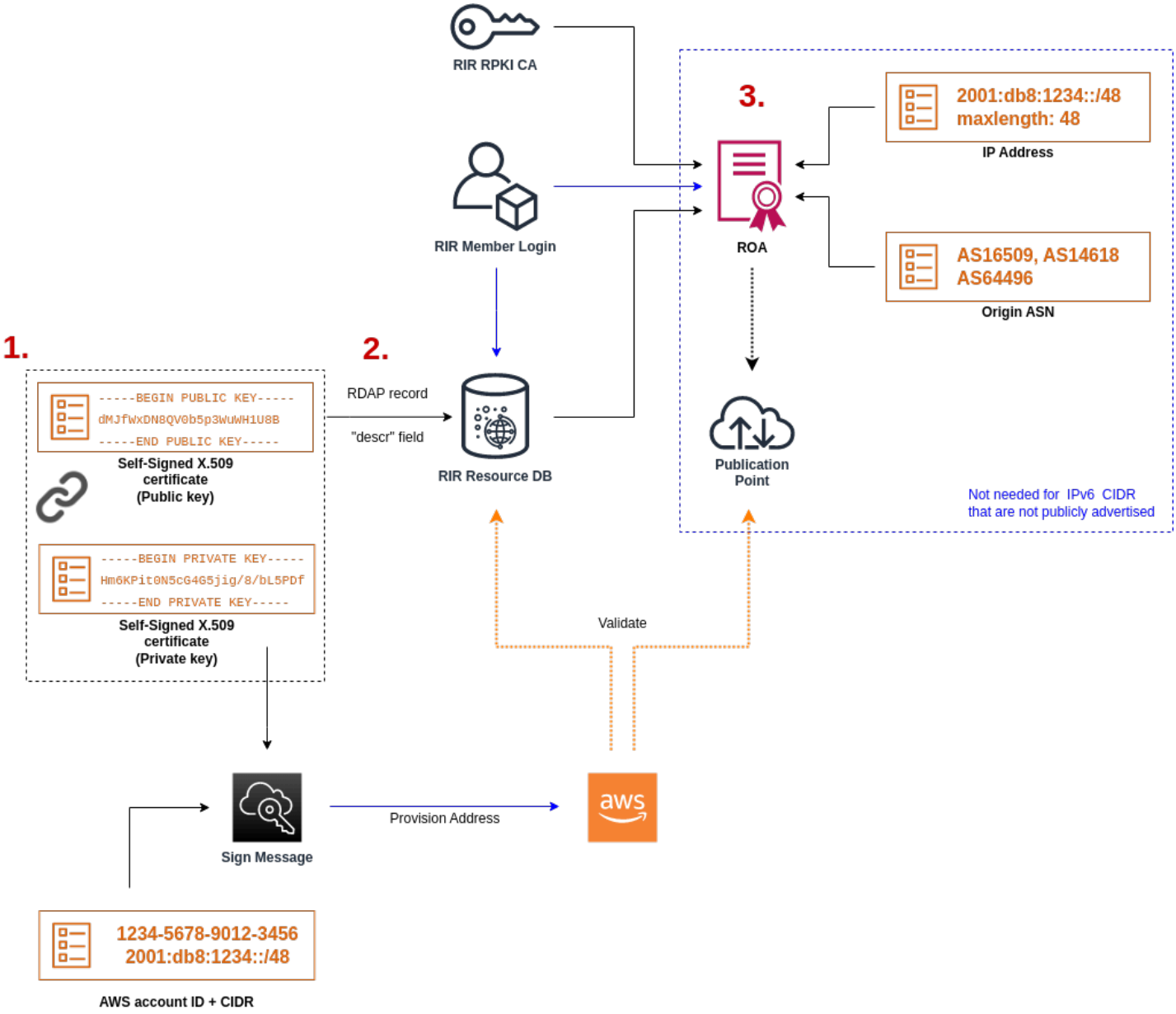
1. Erstellen Sie ein privates Schlüsselpaar und verwenden Sie es zum Generieren eines selbstsignierten X.509-Zertifikats. Dieses Zertifikat wird nur während der Bereitstellungsphase verwendet.

RIR-Konfigurationsphase

2. Laden Sie das selbstsignierte Zertifikat in Ihre Kommentare zum RDAP-Datensatz hoch.

3. Erstellen Sie ein ROA-Objekt in Ihrem RIR. Die ROA definiert den gewünschten Adressbereich, die zum Veröffentlichen des Adressbereichs zulässigen Autonomous System Numbers (ASNs) und ein Ablaufdatum zum Registrieren bei der Resource Public Key Infrastructure (RPKI) Ihres RIR.

> **Note**
>
> Für nicht öffentlich beworbene IPv6-Adressumgebungen ist kein ROA erforderlich.



Um mehrere nicht zusammenhängende Adressbereiche einzubeziehen, müssen Sie diesen Vorgang mit jedem Adressbereich wiederholen. Die Vorbereitungs- und RIR-Konfigurationsschritte müssen jedoch nicht wiederholt werden, wenn ein zusammenhängender Block auf mehrere verschiedene Regionen aufgeteilt wird. AWS

Das Aktivieren eines Adressbereichs hat keine Auswirkungen auf Adressbereiche, die Sie zuvor aktiviert haben.

> **Important**
>
> Die folgenden Voraussetzungen müssen vor dem Onboarding des Adressbereichs erfüllt sein. Die Aufgaben in diesem Abschnitt erfordern ein Linux-Terminal und können mit Linux AWS CloudShell, dem oder dem Windows-Subsystem für Linux ausgeführt werden.

1. Einen privaten Schlüssel erstellen und ein X.509-Zertifikat generieren

Gehen Sie zum Erstellen eines selbsignierten X.509-Zertifikats folgendermaßen vor und fügen Sie es dann zum RDAP-Datensatz für Ihr RIR hinzu. Dieses Schlüsselpaar dient zur Authentifizierung des Adressbereichs im RIR. Für die openssl-Befehle ist OpenSSL Version 1.0.2 oder höher erforderlich.

Kopieren Sie die folgenden Befehle und ersetzen Sie nur die Platzhalterwerte (in farbigem kursivem Text).

Dieses Verfahren folgt der bewährten Methode, Ihren privaten RSA-Schlüssel zu verschlüsseln und zum Zugriff darauf eine Passphrase zu erfordern.

1. Generieren Sie einen privaten RSA-Schlüssel mit 2 048 Bit, wie im Folgenden gezeigt.

   ```
   $ openssl genpkey -aes256 -algorithm RSA -pkeyopt rsa_keygen_bits:2048 -out
    private-key.pem
   ```

   Der Parameter `-aes256` gibt den Algorithmus an, der zum Verschlüsseln des privaten Schlüssels verwendet wird. Der Befehl gibt die folgende Ausgabe zurück, einschließlich Aufforderungen zum Festlegen einer Passphrase:

   ```
   ......+++
   .+++
   Enter PEM pass phrase: xxxxxxx
   Verifying - Enter PEM pass phrase: xxxxxxx
   ```

   Sie können den Schlüssel mit dem folgenden Befehl prüfen:

   ```
   $ openssl pkey -in private-key.pem -text
   ```

   Dadurch wird eine Eingabeaufforderung für die Passphrase und der Inhalt des Schlüssels zurückgegeben, der etwa wie folgt aussehen sollte:

```
Enter pass phrase for private-key.pem: xxxxxxx
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDFBXHRI4HVKAhh
3seiciooizCRTbJe1+YsxNTja4XyKypVGIFWDGhZs44FCHlPOOSVJ+NqP74w96oM
7DPS3xo9kaQyZBFn2YEp2EBq5vf307KHNRmZZUmkn0zHOSEpNmY2fMxISBxewlxR
FAniwmSd/8TDvHJMY9FvAIvWuTsv5l0tJKk+a91K4+tO3UdDR7Sno5WXExfsBrW3
g1ydo3TBsx8i5/YiVOcNApy7ge2/FiwY3aCXJB6r6nuF6H8mRgI4r4vkMRsOlAhJ
DnZPNeweboo+K3Q3lwbgbmOKD/z9svk8N/+hUTBtIX0fRtbG+PLIw3xWRHGrMSn2
BzsPVuDLAgMBAAECggEACiJUj2hfJkKv47Dc3es3Zex67A5uDVjXmxfox2Xhdupn
fAcNqAptV6fXt0SPUNbhUxbBKNbshoJGufFwXPli1SXnpzvkdU4Hyco4zgbhXFsE
RNYjYfOGzTPwdBLpNMB6k3Tp4RHse6dNrlH0jDhpioL8cQEBdBJyVF5X0wymEbmV
mC0jgH/MxsBAPWW6ZKicg9ULMlWiAZ3MRAZPjHHgpYkAAsUWKAbCBwVQcVjGO59W
jfZjzTX5pQtVVH68ruciH88DTZCwjCkjBhxg+OIkJBLE5wkh82jIHSivZ63flwLw
z+E0+HhELSZJrn2MY6Jxmik3qNNUOF/Z+3msdj2luQKBgQDjwlC/3jxp8zJy6P8o
JQKv7TdvMwUj4VSWOHZBHLv4evJaaia0uQjIo1UDa8AYitqhX1NmCCehGH8yuXj/
v6V3CzMKDkmRr1NrONnSz5QsndQ04Z6ihAQlPmJ96g4wKtgoC7AYpyP0g1a+4/sj
b1+o3YQI4pD/F71c+qaztH7PRwKBgQDdc23yNmT3+Jyptf0fKjEvONK+xwUKzi9c
L/OzBq5yOIC1Pz2T85gOe1i8kwZws+xlpG6uBT6lmIJELd0k59FyupNu4dPvX5SD
6GGqdx4jk9KvI74usGeOBohmF0phTHkrWKBxXiyT0oS8zjnJlEn8ysIpGgO28jjr
LpaHNZ/MXQKBgQDfLNcnS0LzpsS2aK0tzyZU8SMyqVHOGMxj7quhneBq2T6FbiLD
T9TVlYaGNZ0j71vQaLI19qOubWymbautH0Op5KV8owdf4+bf1/NJaPIOzhDUSIjD
Qo01WW31Z9XDSRhKFTnWzmCjBdeIcajyzf10YKsycaAW9lItu8aBrMndnQKBgQDb
nNp/JyRwqjOrNljk7DHEs+SD39kHQzzCfqd+dnTPv2sc06+cpym3yulQcbokULpy
fmRo3bin/pvJQ3aZX/Bdh9woTXqhXDdrrSwWInVYMQPyPk8f/D9mIOJp5FUWMwHD
U+whIZSxsEeE+jtixlWtheKRYkQmzQZXbWdIhYyI3QKBgD+F/6wcZ85QW8nAUykA
3WrSIx/3cwDGdm4NRGct8ZOZjTHjiy9ojMOD1L7iMhRQ/3k3hUsin5LDMp/ryWGG
x4uIaLat40kiC7T4I66DM7P59euqdz3w0PD+VU+h7GSivvsFDdySUt7bNK0AUVLh
dMJfWxDN8QV0b5p3WuWH1U8B
-----END PRIVATE KEY-----
Private-Key: (2048 bit)
modulus:
    00:c5:05:71:d1:23:81:d5:28:08:61:de:c7:a2:72:
    2a:28:8b:30:91:4d:b2:5e:d7:e6:2c:c4:d4:e3:6b:
    85:f2:2b:2a:55:18:81:56:0c:68:59:b3:8e:05:08:
    79:4f:38:e4:95:27:e3:6a:3f:be:30:f7:aa:0c:ec:
    33:d2:df:1a:3d:91:a4:32:64:11:67:d9:81:29:d8:
    40:6a:e6:f7:f7:d3:b2:87:35:19:99:65:49:a4:9f:
    4c:c7:39:21:29:36:66:36:7c:cc:48:48:1c:5e:c2:
    5c:51:14:09:e2:c2:64:9d:ff:c4:c3:bc:72:4c:63:
    d1:6f:00:8b:d6:b9:3b:2f:e6:5d:2d:24:a9:3e:6b:
    dd:4a:e3:eb:4e:dd:47:43:47:b4:a7:a3:95:97:13:
    17:ec:06:b5:b7:83:5c:9d:a3:74:c1:b3:1f:22:e7:
    f6:22:54:e7:0d:02:9c:bb:81:ed:bf:16:2c:18:dd:
```

```
    a0:97:24:1e:ab:ea:7b:85:e8:7f:26:46:02:38:af:
    8b:e4:31:1b:0e:94:08:49:0e:76:4f:35:ec:1e:6e:
    8a:3e:2b:74:37:97:06:e0:6e:63:8a:0f:fc:fd:b2:
    f9:3c:37:ff:a1:51:30:6d:21:7d:1f:46:d6:c6:f8:
    f2:c8:c3:7c:56:44:71:ab:31:29:f6:07:3b:0f:56:
    e0:cb
publicExponent: 65537 (0x10001)
privateExponent:
    0a:22:54:8f:68:5f:26:42:af:e3:b0:dc:dd:eb:37:
    65:ec:7a:ec:0e:6e:0d:58:d7:9b:17:e8:c7:65:e1:
    76:ea:67:7c:07:0d:a8:0a:6d:57:a7:d7:b7:44:8f:
    50:d6:e1:53:16:c1:28:d6:ec:86:82:46:b9:f1:70:
    5c:f9:62:d5:25:e7:a7:3b:e4:75:4e:07:c9:ca:38:
    ce:06:e1:5c:5b:04:44:d6:23:61:f3:86:cd:33:f0:
    74:12:e9:34:c0:7a:93:74:e9:e1:11:ec:7b:a7:4d:
    ae:51:f4:8c:38:69:8a:82:fc:71:01:01:74:12:72:
    54:5e:57:d3:0c:a6:11:b9:95:98:2d:23:80:7f:cc:
    c6:c0:40:3d:65:ba:64:a8:9c:83:d5:0b:32:55:a2:
    01:9d:cc:44:06:4f:8c:71:e0:a5:89:00:02:c5:16:
    28:06:c2:07:05:50:71:58:c6:3b:9f:56:8d:f6:63:
    cd:35:f9:a5:0b:55:54:7e:bc:ae:e7:22:1f:cf:03:
    4d:90:b0:8c:29:23:06:1c:60:f8:e2:24:24:12:c4:
    e7:09:21:f3:68:c8:1d:28:af:67:ad:df:97:02:f0:
    cf:e1:34:f8:78:44:2d:26:49:ae:7d:8c:63:a2:71:
    9a:29:37:a8:d3:54:38:5f:d9:fb:79:ac:76:3d:a5:
    b9
prime1:
    00:e3:c2:50:bf:de:3c:69:f3:32:72:e8:ff:28:25:
    02:af:ed:37:6f:33:05:23:e1:54:96:38:76:41:1c:
    bb:f8:7a:f2:5a:6a:26:b4:b9:08:c8:a3:55:03:6b:
    c0:18:8a:da:a1:5f:53:66:08:27:a1:18:7f:32:b9:
    78:ff:bf:a5:77:0b:33:0a:0e:49:91:af:53:6b:38:
    d9:d2:cf:94:2c:9d:d4:34:e1:9e:a2:84:04:25:3e:
    62:7d:ea:0e:30:2a:d8:28:0b:b0:18:a7:23:f4:83:
    56:be:e3:fb:23:6f:5f:a8:dd:84:08:e2:90:ff:17:
    bd:5c:fa:a6:b3:b4:7e:cf:47
prime2:
    00:dd:73:6d:f2:36:64:f7:f8:9c:a9:b5:fd:1f:2a:
    31:2f:38:d2:be:c7:05:0a:ce:2f:5c:2f:f3:b3:06:
    ae:72:38:80:b5:3f:3d:93:f3:98:0e:7b:58:bc:93:
    06:70:b3:ec:65:a4:6e:ae:05:3e:a5:98:82:44:2d:
    dd:24:e7:d1:72:ba:93:6e:e1:d3:ef:5f:94:83:e8:
    61:aa:77:1e:23:93:d2:af:23:be:2e:b0:67:8e:06:
    88:66:17:4a:61:4c:79:2b:58:a0:71:5e:2c:93:d2:
```

```
    84:bc:ce:39:c9:94:49:fc:ca:c2:29:1a:03:b6:f2:
    38:eb:2e:96:87:35:9f:cc:5d
exponent1:
    00:df:2c:d7:27:4b:42:f3:a6:c4:b6:68:ad:2d:cf:
    26:54:f1:23:32:a9:51:ce:18:cc:63:ee:ab:a1:9d:
    e0:6a:d9:3e:85:6e:22:c3:4f:d4:d5:95:86:86:35:
    9d:23:ef:5b:d0:68:b2:35:f6:a3:ae:6d:6c:a6:6d:
    ab:ad:1f:43:a9:e4:a5:7c:a3:07:5f:e3:e6:df:d7:
    f3:49:68:f2:0e:ce:10:d4:48:88:c3:42:8d:35:59:
    6d:f5:67:d5:c3:49:18:4a:15:39:d6:ce:60:a3:05:
    d7:88:71:a8:f2:cd:fd:74:60:ab:32:71:a0:16:f6:
    52:2d:bb:c6:81:ac:c9:dd:9d
exponent2:
    00:db:9c:da:7f:27:24:70:aa:33:ab:36:58:e4:ec:
    31:c4:b3:e4:83:df:d9:07:43:3c:c2:7e:a7:7e:76:
    74:cf:bf:6b:1c:d3:af:9c:a7:29:b7:ca:e9:50:71:
    ba:24:50:ba:72:7e:64:68:dd:b8:a7:fe:9b:c9:43:
    76:99:5f:f0:5d:87:dc:28:4d:7a:a1:5c:37:6b:ad:
    2c:16:22:75:58:31:03:f2:3e:4f:1f:fc:3f:66:20:
    e2:69:e4:55:16:33:01:c3:53:ec:21:21:94:b1:b0:
    47:84:fa:3b:62:c6:55:ad:85:e2:91:62:44:26:cd:
    06:57:6d:67:48:85:8c:88:dd
coefficient:
    3f:85:ff:ac:1c:67:ce:50:5b:c9:c0:53:29:00:dd:
    6a:d2:23:1f:f7:73:00:c6:76:6e:0d:44:67:2d:f1:
    93:99:8d:31:e3:8b:2f:68:8c:c3:83:d4:be:e2:32:
    14:50:ff:79:37:85:4b:22:9f:92:c3:32:9f:eb:c9:
    61:86:c7:8b:88:68:b6:ad:e3:49:22:0b:b4:f8:23:
    ae:83:33:b3:f9:f5:eb:aa:77:3d:f0:d0:f0:fe:55:
    4f:a1:ec:64:a2:be:fb:05:0d:dc:92:52:de:db:34:
    ad:00:51:52:e1:74:c2:5f:5b:10:cd:f1:05:74:6f:
    9a:77:5a:e5:87:d5:4f:01
```

Bewahren Sie Ihren privaten Schlüssel an einem sicheren Ort auf, wenn er nicht verwendet wird.

2. Generieren Sie ein X.509-Zertifikat unter Verwendung des im vorherigen Schritt erstellten privaten Schlüssels. In diesem Beispiel läuft das Zertifikat nach 365 Tagen ab und ist dann nicht mehr vertrauenswürdig. Stellen Sie sicher, das Sie das Ablaufdatum korrekt festlegen. Das Zertifikat darf nur für die Dauer des Bereitstellungsprozesses gültig sein. Sie können das Zertifikat nach Abschluss der Bereitstellung aus Ihrem RIR-Datensatz entfernen. Der `tr -d "\n"`-Befehl entfernt Zeilenvorschubzeichen (Zeilenumbrüche) aus der Ausgabe. Sie müssen

einen Common Name angeben, wenn Sie dazu aufgefordert werden, aber die übrigen Felder können leer gelassen werden.

```
$ openssl req -new -x509 -key private-key.pem -days 365 | tr -d "\n" >
 certificate.pem
```

Daraus resultiert eine Ausgabe ähnlich der folgenden:

```
Enter pass phrase for private-key.pem: xxxxxxx
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:
State or Province Name (full name) []:
Locality Name (eg, city) []:
Organization Name (eg, company) []:
Organizational Unit Name (eg, section) []:
Common Name (eg, fully qualified host name) []:example.com
Email Address []:
```

> **Note**
>
> Der Common Name wird für AWS die Bereitstellung nicht benötigt. Der Domain-Name kann intern oder öffentlich sein.

Sie können das Zertifikat mit dem folgenden Befehl prüfen:

```
$ cat certificate.pem
```

Die Ausgabe sollte eine lange, PEM-codierte Zeichenfolge ohne Zeilenumbrüche sein, eingeleitet durch `-----BEGIN CERTIFICATE-----` und gefolgt von `-----END CERTIFICATE-----`.

2. Das X.509-Zertifikat in den RDAP-Eintrag in Ihrem RIR hochladen

Fügen Sie das zuvor erstellte Zertifikat zum RDAP-Datensatz für Ihr RIR hinzu. Achten Sie darauf, dass die `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----`-Zeichenfolgen vor und nach dem kodierten Teil enthalten sind. Der gesamte Inhalt muss sich in einer einzigen, langen Zeile befinden. Das Verfahren zum Aktualisieren des RDAP hängt von Ihrem RIR ab:

- Verwenden Sie für ARIN das Accountmanager-Portal, um das Zertifikat im Abschnitt „Öffentliche Kommentare“ für das Objekt „Netzwerkinformationen“ hinzuzufügen, das Ihren Adressbereich darstellt. Fügen Sie es nicht dem Kommentarbereich Ihrer Organisation hinzu.
- Für RIPE fügen Sie das Zertifikat als neues „descr“-Feld zum Objekt „inetnum“ oder „inet6num“ hinzu, das Ihren Adressbereich darstellt. Diese finden Sie normalerweise im Bereich „Meine Ressourcen“ des RIPE-Datenbankportals. Fügen Sie es nicht dem Kommentarbereich für Ihre Organisation oder dem Feld „Anmerkungen“ der oben genannten Objekte hinzu.
- Senden Sie für APNIC das Zertifikat per E-Mail an helpdesk@apnic.net, um es manuell in das Feld „remarks“ (Anmerkungen) für Ihren Adressbereich aufzunehmen. Senden Sie die E-Mail für die IP-Adressen über den von APNIC autorisierten Kontakt.

Sie können das Zertifikat aus dem Verzeichnis Ihres RIRs entfernen, nachdem die nachfolgende Bereitstellungsphase abgeschlossen ist.

3. Erstellen eines ROA-Objekts in Ihrem RIR

Erstellen Sie ein ROA-Objekt, um die Amazon-ASNs 16509 und 14618 zu autorisieren, Ihren Adressbereich zu bewerben, sowie die ASNs, die derzeit autorisiert sind, den Adressbereich zu veröffentlichen. Autorisieren Sie für die AWS GovCloud (US) Regions ASN 8987 anstelle von 16509 und 14618. Sie müssen die maximale Länge auf die Größe des CIDR festlegen, das Sie einbinden möchten. Das spezifischste IPv4-Präfix, das Sie aufnehmen können, ist /24. Der spezifischste IPv6-Adressbereich, den Sie einbringen können, ist /48 für CIDRs, die öffentlich beworben werden können und /56 für CIDRs, die nicht öffentlich beworben werden können.

> **Important**
>
> Wenn Sie ein ROA-Objekt für Amazon VPC IP Address Manager (IPAM) erstellen, müssen Sie bei der Erstellung der ROAs für IPv4-CIDRs die maximale Länge eines IP-Adresspräfixes auf `/24` festlegen. Wenn Sie IPv6-CIDRs zu einem werbefähigen Pool hinzufügen, darf die maximale Länge eines IP-Adresspräfixes `/48` sein. Dies stellt sicher,

dass Sie bei der Aufteilung Ihrer öffentlichen IP-Adresse auf verschiedene Regionen die volle Flexibilität haben. AWS IPAM erzwingt die von Ihnen festgelegte maximale Länge. Weitere Informationen zu BYOIP-Adressen für IPAM finden Sie im Tutorial: BYOIP-Adress-CIDRs für IPAM im Amazon-VPC-IPAM-Benutzerhandbuch.

Es kann bis zu 24 Stunden dauern, bis das ROA für Amazon verfügbar ist. Weitere Informationen erhalten Sie von Ihrem RIR:

- ARIN: — ROA-Anforderungen
- RIPE: — Verwalten von ROAs
- APNIC — Routenmanagement

Wenn Sie Werbung von einem lokalen Workload zu einem migrieren AWS, müssen Sie einen ROA für Ihre bestehende ASN erstellen, bevor Sie die ROAs für die ASNs von Amazon erstellen. Andernfalls könnte der Vorgang Auswirkungen auf Ihr vorhandenes Routing und Ihre Anzeigen haben.

Important

Damit Amazon Ihren IP-Adressbereich bewerben und weiterhin bewerben kann, müssen Ihre ROAs mit Amazon ASNs den oben genannten Richtlinien entsprechen. Wenn Ihre ROAs ungültig sind oder nicht den oben genannten Richtlinien entsprechen, behält sich Amazon das Recht vor, die Werbung für Ihren IP-Adressbereich einzustellen.

Note

Dieser Schritt ist nicht erforderlich, wenn die IPv6-Adressumgebung nicht öffentlich beworben werden kann.

Onboarding Ihres BYOIP

Der Onboarding-Prozess für BYOIP umfasst je nach Ihren Bedürfnissen die folgenden Aufgaben.

Aufgaben

Einen öffentlich beworbener Adressbereich in AWS bereitstellen

Wenn Sie einen Adressbereich zur Verwendung mit angeben, bestätigen Sie AWS, dass Sie die Kontrolle über den Adressbereich haben, und autorisieren Amazon, für ihn zu werben. Wir bestätigen ebenso mit einer signierten Autorisierungsnachricht, dass Sie den Adressbereich kontrollieren. Diese Nachricht ist mit dem selbstsignierten X.509-Schlüsselpaar signiert, das Sie bei der Aktualisierung des RDAP-Eintrags mit dem X.509-Zertifikat verwendet haben. AWS erfordert eine kryptografisch signierte Autorisierungsnachricht, die dem RIR vorgelegt wird. Das RIR authentifiziert die Signatur mit dem Zertifikat, das Sie zum RDAP hinzugefügt haben, und vergleicht die Autorisierungsdetails mit dem ROA.

Aufheben der Bereitstellung des Adressbereichs

1. Verfassen einer Nachricht

   Verfassen Sie die Nur-Text-Autorisierungsnachricht. Das Format der Nachricht ist wie folgt, wobei das Datum das Ablaufdatum der Nachricht ist:

   ```
   1|aws|account|cidr|YYYYMMDD|SHA256|RSAPSS
   ```

   Ersetzen Sie die Kontonummer, den Adressbereich und das Ablaufdatum mit Ihren eigenen Werten, um eine Nachricht zu erstellen, die der folgenden ähnelt:

   ```
   text_message="1|aws|0123456789AB|198.51.100.0/24|20211231|SHA256|RSAPSS"
   ```

   Dies ist nicht mit einer ROA-Nachricht zu verwechseln, die ähnlich aussieht.

2. Nachrichten signieren

   Signieren Sie die Nur-Text-Nachricht mit dem privaten Schlüssel, den Sie zuvor erstellt haben. Die vom Befehl zurückgegebene Signatur ist eine lange Zeichenfolge, die Sie für den nächsten Schritt nutzen müssen.

> **Important**
>
> Es wird empfohlen, diesen Befehl zu kopieren und einzufügen. Ändern oder ersetzen Sie mit Ausnahme des Nachrichteninhalts keine Werte.

```
signed_message=$( echo -n $text_message | openssl dgst -sha256 -sigopt
 rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -sign private-key.pem -keyform PEM
 | openssl base64 | tr -- '+=/' '-_~' | tr -d "\n")
```

3. Adresse zur Verfügung stellen

   Verwenden Sie den Befehl AWS CLI provision-byoip-cidr, um den Adressbereich bereitzustellen. Die Option `--cidr-authorization-context` verwendet die Nachrichten- und Signaturzeichenfolgen, die Sie zuvor erstellt haben.

   > **Important**
   >
   > Sie müssen die AWS Region angeben, in der der BYOIP-Bereich bereitgestellt werden soll, falls er von Ihrer Konfiguration abweicht.AWS CLI `Default region name`

   ```
   aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
    Message="$text_message",Signature="$signed_message" --region us-east-1
   ```

   Die Bereitstellung eines Adressbereichs ist eine asynchrone Operation. Daher gibt der Aufruf sofort Daten zurück, der Adressbereich ist jedoch erst zur Verwendung bereit, wenn der Status von `pending-provision` zu `provisioned` wechselt.

4. Überwachen des Fortschritts

   Während die meisten Bereitstellungen innerhalb von zwei Stunden abgeschlossen sein werden, kann es bis zu einer Woche dauern, bis der Bereitstellungsprozess für öffentlich beworbene Bereiche abgeschlossen ist. Verwenden Sie den Befehl describe-byoip-cidrs, um den Fortschritt zu überwachen, wie in diesem Beispiel gezeigt:

   ```
   aws ec2 describe-byoip-cidrs --max-results 5 --region us-east-1
   ```

Wenn während der Bereitstellung Probleme auftreten und der Status in `failed-provision` wechselt, müssen Sie den `provision-byoip-cidr`-Befehl erneut ausführen, nachdem die Probleme behoben wurden.

Einen nicht öffentlich zugänglichen IPv6-Adressbereich bereitstellen

Standardmäßig wird ein Adressbereich bereitgestellt, der öffentlich im Internet beworben wird. Sie können einen IPv6-Adressbereich bereitstellen, der nicht öffentlich beworben werden kann. Bei Routen ohne öffentliches Advertising ist der Bereitstellungsprozess in der Regel innerhalb von Minuten abgeschlossen. Wenn Sie einen IPv6-CIDR-Block aus einem nicht öffentlichen Adressbereich einer VPC zuordnen, kann auf das IPv6-CIDR nur über hybride Konnektivitätsoptionen zugegriffen werden, die IPv6 unterstützen, z. B. AWS Direct Connect, AWS Site-to-Site VPN oder Amazon VPC Transit Gateways.

Eine ROA ist nicht erforderlich, um einen nicht-öffentlichen Adressbereich bereitzustellen.

> **Important**
>
> - Sie können nur während der Bereitstellung angeben, ob ein Adressbereich öffentlich beworben werden kann. Sie können den Anzeigenstatus nachträglich nicht mehr ändern.
> - Amazon VPC unterstützt keine Unique Local Address (ULA)-CIDRs. Alle VPCs müssen über eindeutige IPv6-CIDRs verfügen. Zwei VPCs können nicht denselben IPv6-CIDR-Bereich haben.

Um einen IPv6-Adressbereich bereitzustellen, der nicht öffentlich angekündigt werden kann, verwenden Sie den folgenden provision-byoip-cidr-Befehl.

```
aws ec2 provision-byoip-cidr --cidr address-range --cidr-authorization-context
 Message="$text_message",Signature="$signed_message" --no-publicly-advertisable --
region us-east-1
```

Bewerben Sie den Adressbereich über AWS

Nachdem der Adressbereich bereitgestellt wurde, kann er veröffentlicht werden. Sie müssen den genauen Adressbereich ankündigen, den Sie bereitgestellt haben. Sie können nur einen Teil des bereitgestellten Adressbereichs ankündigen.

Wenn Sie einen IPv6-Adressbereich bereitgestellt haben, der nicht öffentlich angekündigt wird, müssen Sie diesen Schritt nicht ausführen.

Wir empfehlen Ihnen, den Adressbereich oder einen Teil des Adressbereichs nicht mehr an anderen Standorten zu bewerben, bevor Sie ihn über diese Website bewerben AWS. Wenn Sie Ihren IP-Adressbereich oder einen Teil davon weiterhin von anderen Standorten aus bewerben, können wir dies nicht zuverlässig unterstützen oder Probleme beheben. Insbesondere können wir nicht garantieren, dass der Datenverkehr in den Adressbereich oder einen Teil des Bereichs in unser Netzwerk gelangt.

Um Ausfallzeiten zu minimieren, können Sie Ihre AWS Ressourcen so konfigurieren, dass sie eine Adresse aus Ihrem Adresspool verwenden, bevor sie veröffentlicht wird, und dann gleichzeitig die Werbung am aktuellen Standort beenden und mit der Werbung beginnen. AWS Weitere Informationen zur Zuweisung einer Elastic IP-Adresse aus Ihrem Adresspool finden Sie unter Zuweisen einer Elastic-IP-Adresse.

Einschränkungen

- Sie können den Befehl advertise-byoip-cidr höchstens alle 10 Sekunden ausführen, auch wenn Sie jedes Mal einen anderen Adressbereich angeben.
- Sie können den Befehl withdraw-byoip-cidr höchstens alle 10 Sekunden ausführen, auch wenn Sie jedes Mal einen anderen Adressbereich angeben.

Um den Adressbereich zu veröffentlichen, verwenden Sie den folgenden advertise-byoip-cidr-Befehl.

```
aws ec2 advertise-byoip-cidr --cidr address-range --region us-east-1
```

Um die Veröffentlichung für den Adressbereich einzustellen, verwenden Sie den folgenden witw-byoip-cidr-Befehl.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Aufheben der Bereitstellung des Adressbereichs

Um die Verwendung Ihres Adressbereichs mit zu beenden AWS, geben Sie zunächst alle Elastic IP-Adressen frei und trennen Sie die Zuordnung aller IPv6-CIDR-Blöcke, die noch dem Adresspool zugewiesen sind. Beenden Sie dann die Veröffentlichung des Adressbereichs und heben Sie schließlich die Bereitstellung des Adressbereichs auf.

Sie können die Bereitstellung eines Teils des Adressbereichs nicht aufheben. Wenn Sie einen spezifischeren Adressbereich mit verwenden möchten AWS, heben Sie die Bereitstellung des gesamten Adressbereichs auf und stellen Sie einen spezifischeren Adressbereich bereit.

(IPv4) Um jede Elastic IP-Adresse freizugeben, verwenden Sie den folgenden release-address-Befehl.

```
aws ec2 release-address --allocation-id eipalloc-12345678abcabcabc --region us-east-1
```

(IPv6) Um die Zuordnung eines IPv6-CIDR-Blocks zu trennen, verwenden Sie den folgenden disassociate-vpc-cidr-block-Befehl.

```
aws ec2 disassociate-vpc-cidr-block --association-id vpc-cidr-assoc-12345abcd1234abc1
 --region us-east-1
```

Um die Veröffentlichung für den Adressbereich einzustellen, verwenden Sie den folgenden witw-byoip-cidr-Befehl.

```
aws ec2 withdraw-byoip-cidr --cidr address-range --region us-east-1
```

Um den Adressbereich zu deaktivieren, verwenden Sie den folgenden deprovision-byoip-cidr-Befehl.

```
aws ec2 deprovision-byoip-cidr --cidr address-range --region us-east-1
```

Es kann bis zu einem Tag dauern, bis die Bereitstellung eines Adressbereichs aufgehoben wird.

Arbeiten mit Ihrem Adressbereich

Sie können die IPv4- und IPv6-Adressbereiche anzeigen und mit denen arbeiten, die Sie in Ihrem Konto bereitgestellt haben.

IPv4-Adressbereiche

Sie können eine Elastic IP-Adresse aus Ihrem IPv4-Adresspool erstellen und sie mit Ihren AWS Ressourcen wie EC2-Instances, NAT-Gateways und Network Load Balancers verwenden.

Um Informationen zu den IPv4-Adresspools anzuzeigen, die Sie in Ihrem Konto bereitgestellt haben, verwenden Sie den folgenden describe-public-ipv4-pools-Befehl.

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Verwenden Sie den Befehl allocate-address, um eine Elastic IP-Adresse aus Ihrem IPv4-Adresspool zu erstellen. Mit der Option `--public-ipv4-pool` können Sie die ID des von `describe-byoip-cidrs` zurückgegebenen Adressbereichs angeben. Oder Sie können die Option `--address` verwenden, um eine Adresse aus dem von Ihnen bereitgestellten Adressbereich anzugeben.

IPv6-Adressbereiche

Um Informationen zu den IPv6-Adresspools anzuzeigen, die Sie in Ihrem Konto bereitgestellt haben, verwenden Sie den folgenden describe-ipv6-pools-Befehl.

```
aws ec2 describe-ipv6-pools --region us-east-1
```

Verwenden Sie den folgenden create-vpc-Befehl, um eine VPC zu erstellen und eine IPv6-CIDR aus Ihrem IPv6-Adresspool anzugeben. Damit Amazon die IPv6-CIDR aus Ihrem IPv6-Adresspool auswählen kann, lassen Sie die `--ipv6-cidr-block`-Option aus.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --ipv6-cidr-block ipv6-cidr --ipv6-
pool pool-id --region us-east-1
```

Um einen IPv6-CIDR-Block aus Ihrem IPv6-Adresspool einer VPC zuzuordnen, verwenden Sie den folgenden associate-vpc-cidr-block-Befehl. Damit Amazon die IPv6-CIDR aus Ihrem IPv6-Adresspool auswählen kann, lassen Sie die `--ipv6-cidr-block`-Option aus.

```
aws ec2 associate-vpc-cidr-block --vpc-id vpc-123456789abc123ab --ipv6-cidr-block ipv6-
cidr --ipv6-pool pool-id --region us-east-1
```

Verwenden Sie den describe-vpcs-Befehl, um Ihre VPCs und die zugehörigen IPv6-Adresspool-Informationen anzuzeigen. Um Informationen zu zugeordneten IPv6-CIDR-Blöcken aus einem bestimmten IPv6-Adresspool anzuzeigen, verwenden Sie den folgenden get-associated-ipv6-pool-cidrs-Befehl.

```
aws ec2 get-associated-ipv6-pool-cidrs --pool-id pool-id --region us-east-1
```

Wenn Sie den IPv6-CIDR-Block von Ihrer VPC trennen, wird er wieder in Ihren IPv6-Adresspool freigegeben.

Validieren Ihres BYOIP

1. Validieren des selbstsignierten x.509-Schlüsselpaars

Validieren Sie, ob das Zertifikat hochgeladen wurde, und seine Gültigkeit mit dem Befehl whois.

Verwenden Sie für ARIN `whois -h whois.arin.net r + 2001:0DB8:6172::/48`, um den RDAP-Datensatz für Ihren Adressbereich nachzuschlagen. Überprüfen Sie den `Public Comments`-Abschnitt für `NetRange` (Netzwerkbereich) in der Befehlsausgabe. Das Zertifikat sollte im `Public Comments`-Abschnitt für den Adressbereich hinzugefügt werden.

Sie können `Public Comments` mit dem Zertifikat als Inhalt mit dem folgenden Befehl prüfen:

```
whois -h whois.arin.net r + 2001:0DB8:6172::/48 | grep Comments | grep BEGIN
```

Dadurch wird eine Ausgabe mit dem Inhalt des Schlüssels zurückgegeben, der etwa wie folgt aussehen sollte:

```
Public Comments:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Verwenden Sie für RIPE `whois -r -h whois.ripe.net` *2001:0DB8:7269::/48*, um den RDAP-Datensatz für Ihren Adressbereich nachzuschlagen. Überprüfen Sie den `descr`-Abschnitt für das `inetnum`-Objekt (Netzwerkbereich) in der Befehlsausgabe. Das Zertifikat sollte als neues `descr`-Feld für den Adressbereich hinzugefügt werden.

Sie können `descr` mit dem Zertifikat als Inhalt mit dem folgenden Befehl prüfen:

```
whois -r -h whois.ripe.net 2001:0DB8:7269::/48 | grep descr | grep BEGIN
```

Dadurch wird eine Ausgabe mit dem Inhalt des Schlüssels zurückgegeben, der etwa wie folgt aussehen sollte:

```
descr:
-----BEGIN CERTIFICATE-----MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8
RDAHSP+I1TowDQYJKoZIhvcNAQELBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAg
MCEF1Y2tsYW5kMREwDwYDVQQHDAhBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIF
dlYiBTZXJ2aWNlczETMBEGA1UECwwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPS
VAgRGVtbzAeFw0yMTEyMDcyMDI0NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNV
BAYTAk5aMREwDwYDVQQIDAhBdWNrbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDA
aBgNVBAoME0FtYXpvbiBXZWIgU2VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW
8xEzARBgNVBAMMCkJZT0lQIERlbW8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwg
gEKAoIBAQCfmacvDp0wZ0ceiXXcR/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanA
EskgAseyFypwEEQr4CJijI/5hp9prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3
stsI5QesHVRwOaXUdprAnndaTugmDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq
35wU/x+wXlAqBXg4MZK2KoUu27kYt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp
1ZnVIc7NqnhdeIW48QaYjhMlUEfxdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2r
GlHWkJsbhr0VEUyAGu1bwkgcdww3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBS
tFyujN6SYBr2glHpGt0XGF7GbGTAfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0
XGF7GbGTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6Y
Lhz521lfyVfxY0t6o3410bQAeAF08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyL
xngwMYN0XY5tVhDQqk4/gmDNEKSZy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9
wySL507XQz76Uk5cFypBOzbnk35UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8
mBGqVpPpey+dXpzzzv1iBKN/VY4ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGC
vRDl/qdO/GIDJi77dmZWkh/ic90MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoN
PyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

Verwenden Sie für APNIC `whois -h whois.apnic.net` *2001:0DB8:6170::/48*, um den RDAP-Datensatz für Ihren BYOIP-Adressbereich nachzuschlagen. Überprüfen Sie den `remarks`-

Abschnitt für das `inetnum`-Objekt (Netzwerkbereich) in der Befehlsausgabe. Das Zertifikat sollte als neues `remarks`-Feld für den Adressbereich hinzugefügt werden.

Sie können `remarks` mit dem Zertifikat als Inhalt mit dem folgenden Befehl prüfen:

```
whois -h whois.apnic.net 2001:0DB8:6170::/48 | grep remarks | grep BEGIN
```

Dadurch wird eine Ausgabe mit dem Inhalt des Schlüssels zurückgegeben, der etwa wie folgt aussehen sollte:

```
remarks:
-----BEGIN CERTIFICATE-----
MIID1zCCAr+gAwIBAgIUBkRPNSLrPqbRAFP8RDAHSP+I1TowDQYJKoZIhvcNAQE
LBQAwezELMAkGA1UEBhMCTloxETAPBgNVBAgMCEF1Y2tsYW5kMREwDwYDVQQHDA
hBdWNrbGFuZDEcMBoGA1UECgwTQW1hem9uIFdlYiBTZXJ2aWNlczETMBEGA1UEC
wwKQllPSVAgRGVtbzETMBEGA1UEAwwKQllPSVAgRGVtbzAeFw0yMTEyMDcyMDI0
NTRaFw0yMjEyMDcyMDI0NTRaMHsxCzAJBgNVBAYTAk5aMREwDwYDVQQIDAhBdWN
rbGFuZDERMA8GA1UEBwwIQXVja2xhbmQxHDAaBgNVBAoME0FtYXpvbiBXZWIgU2
VydmljZXMxEzARBgNVBAsMCkJZT0lQIERlbW8xEzARBgNVBAMMCkJZT0lQIERlb
W8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCfmacvDp0wZ0ceiXXc
R/q27mHI/U5HKt7SST4X2eAqufR9wXkfNanAEskgAseyFypwEEQr4CJijI/5hp9
prh+jsWHWwkFRoBRR9FBtwcU/45XDXLga7D3stsI5QesHVRwOaXUdprAnndaTug
mDPkD0vrl475JWDSIm+PUxGWLy+60aBqiaZq35wU/x+wXlAqBXg4MZK2KoUu27k
Yt2zhmy0S7Ky+oRfRJ9QbAiSu/RwhQbh5Mkp1ZnVIc7NqnhdeIW48QaYjhMlUEf
xdaqYUinzz8KpjfADZ4Hvqj9jWZ/eXo/9b2rGlHWkJsbhr0VEUyAGu1bwkgcdww
3A7NjOxQbAgMBAAGjUzBRMB0GA1UdDgQWBBStFyujN6SYBr2glHpGt0XGF7GbGT
AfBgNVHSMEGDAWgBStFyujN6SYBr2glHpGt0XGF7GbGTAPBgNVHRMBAf8EBTADA
QH/MA0GCSqGSIb3DQEBCwUAA4IBAQBX6nn6YLhz521lfyVfxY0t6o3410bQAeAF
08ud+ICtmQ4IO4A4B7zV3zIVYr0clrOOaFyLxngwMYN0XY5tVhDQqk4/gmDNEKS
Zy2QkX4Eg0YUWVzOyt6fPzjOvJLcsqc1hcF9wySL507XQz76Uk5cFypBOzbnk35
UkWrzA9KK97cXckfIESgK/k1N4ecwxwG6VQ8mBGqVpPpey+dXpzzzv1iBKN/VY4
ydjgH/LBfdTsVarmmy2vtWBxwrqkFvpdhSGCvRDl/qdO/GIDJi77dmZWkh/ic90
MNk1f38gs1jrCj8lThoar17Uo9y/Q5qJIsoNPyQrJRzqFU9F3FBjiPJF
-----END CERTIFICATE-----
```

2. Überprüfung der Erstellung eines ROA-Objekts

   Validieren Sie die erfolgreiche Erstellung der ROA-Objekte mit Hilfe der RIPEstat-Data-API. Testen Sie Ihren Adressbereich mit den Amazon ASNs 16509 und 14618 sowie den ASNs, die derzeit zur Veröffentlichung des Adressbereichs autorisiert sind.

Sie können die ROA-Objekte aus verschiedenen Amazon-ASNs mit Ihrem Adressbereich mit dem folgenden Befehl untersuchen:

```
curl --location --request GET "https://stat.ripe.net/data/rpki-validation/data.json?
resource=ASN&prefix=CIDR
```

In dieser Beispielausgabe hat die Antwort ein Ergebnis von `"status": "valid"` für die Amazon ASN 16509. Dies gibt an, dass das ROA-Objekt für den Adressbereich erfolgreich erstellt wurde:


```
{
    "messages": [],
    "see_also": [],
    "version": "0.3",
    "data_call_name": "rpki-validation",
    "data_call_status": "supported",
    "cached": false,
    "data": {
        "validating_roas": [
            {
                "origin": "16509",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "valid"
            },
            {
                "origin": "14618",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            },
            {
                "origin": "64496",
                "prefix": "2001:0DB8::/32",
                "max_length": 48,
                "validity": "invalid_asn"
            }
        ],
        "status": "valid",
        "validator": "routinator",
        "resource": "16509",
        "prefix": "2001:0DB8::/32"
```

```
    },
    "query_id": "20230224152430-81e6384e-21ba-4a86-852a-31850787105f",
    "process_time": 58,
    "server_id": "app116",
    "build_version": "live.2023.2.1.142",
    "status": "ok",
    "status_code": 200,
    "time": "2023-02-24T15:24:30.773654"
}
```


Der Status "`unknown`" gibt an, dass das ROA-Objekt für den Adressbereich nicht erstellt wurde. Der Status "`invalid_asn`" gibt an, dass das ROA-Objekt für den Adressbereich nicht erfolgreich erstellt wurde.

Regionale Verfügbarkeit

Das BYOIP-Feature ist derzeit in allen kommerziellen AWS -Regionen mit Ausnahme der Regionen China verfügbar.

Verfügbarkeit der Local Zone

Eine lokale Zone ist eine Erweiterung einer AWS Region in geografischer Nähe zu Ihren Benutzern. Local Zones werden in „Netzwerkgrenzgruppen“ gruppiert. Bei AWS einer Netzwerkgrenzgruppe handelt es sich um eine Sammlung von Availability Zones (AZs), Local Zones oder Wavelength Zones, von denen aus AWS eine öffentliche IP-Adresse beworben wird. Local Zones können andere Netzwerkgrenzgruppen haben als die AZs in einer AWS Region, um eine minimale Latenz oder physische Entfernung zwischen dem AWS Netzwerk und den Kunden sicherzustellen, die auf die Ressourcen in diesen Zonen zugreifen.

Mit der `--network-border-group`-Option können Sie BYOIPv4-Adressbereiche für die folgenden Netzwerkgrenzgruppen der Local Zone bereitstellen und diese dort bewerben:

- us-east-1-dfw-2
- us-west-2-lax-1
- us-west-2-phx-2

Wenn Sie Local Zones aktiviert haben (siehe Eine Local Zone aktivieren), können Sie eine Netzwerkgrenzgruppe für Local Zones auswählen, wenn Sie ein BYOIPv4-CIDR bereitstellen und

bewerben. Wählen Sie die Netzwerkgrenzgruppe sorgfältig aus, da sich die EIP und die AWS Ressource, der sie zugeordnet ist, in derselben Netzwerkgrenzgruppe befinden müssen.

> **Note**
>
> Sie können derzeit keine BYOIP6-Adressbereiche in Local Zones bereitstellen oder bewerben.

Weitere Informationen

Weitere Informationen finden Sie im AWS Online-Tech-Talk Deep Dive zum Thema Bring Your Own IP.

Elastic-IP-Adressen

Eine Elastic IP-Adresse ist eine statische IPv4-Adresse, die für dynamisches Cloud Computing konzipiert ist. Ihrem AWS Konto wird eine Elastic IP-Adresse zugewiesen, die Ihnen gehört, bis Sie sie freigeben. Durch Verwenden einer Elastic IP-Adresse können Sie Ausfälle bei Instances oder Software maskieren. Weisen Sie dazu die Adresse einer anderen Instance in Ihrem Konto neu zu. Alternativ können Sie die Elastic IP-Adresse in einem DNS-Eintrag für Ihre Domain angeben, damit Ihre Domain auf Ihre Instance verweist. Weitere Informationen finden Sie in der Dokumentation Ihres Domain-Registrars.

Eine Elastic IP-Adresse ist eine öffentliche IPv4-Adresse, die über das Internet erreichbar ist. Wenn Ihre Instance keine öffentliche IPv4-Adresse hat, können Sie eine Elastic IP-Adresse mit der Instance verknüpfen, damit diese mit dem Internet kommunizieren kann. So können Sie beispielsweise von Ihrem lokalen Computer aus eine Verbindung zu Ihrer Instance herstellen.

Inhalt

Grundlagen zu Elastic IP-Preisen

AWS Gebühren für alle öffentlichen IPv4-Adressen, einschließlich öffentlicher IPv4-Adressen, die mit laufenden Instances verknüpft sind, und Elastic IP-Adressen. Weitere Informationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite Preise für Amazon VPC.

Grundlagen zu Elastic IP-Adressen

Im Folgenden finden Sie eine Auflistung der grundlegenden Merkmale einer Elastic IP-Adresse:

- Eine Elastic IP-Adresse ist statisch; sie ändert sich im Laufe der Zeit nicht.
- Eine Elastic IP-Adresse ist nur für die Verwendung in einer bestimmten Region bestimmt und kann nicht in eine andere Region verschoben werden.
- Eine Elastic IP-Adresse stammt aus dem IPv4-Adresspool von Amazon oder aus einem benutzerdefinierten IPv4-Adresspool, den Sie Ihrem Konto hinzugefügt haben. AWS
- Um eine Elastic IP-Adresse zu verwenden, verknüpfen Sie sie zuerst mit Ihrem Konto und anschließend mit Ihrer Instance oder Netzwerkschnittstelle.
- Wenn Sie einer Instance eine Elastic IP-Adresse zuordnen, wird sie auch der primären Netzwerkschnittstelle der Instance zugeordnet. Wenn Sie eine Elastic IP-Adresse einer Netzwerkschnittstelle zuordnen, die einer Instance zugewiesen ist, wird sie auch der Instance zugeordnet.
- Wenn Sie einer Instance oder ihrer primären Netzwerkschnittstelle eine Elastic IP-Adresse zuordnen und der Instance bereits eine öffentliche IPv4-Adresse zugeordnet ist, wird diese öffentliche IPv4-Adresse wieder in den Pool der öffentlichen IPv4-Adressen von Amazon freigegeben und die Elastic IP-Adresse wird stattdessen der Instance zugeordnet. Sie können die öffentliche IPv4-Adresse, die zuvor mit der Instance verknüpft war, nicht wiederverwenden und Sie können diese öffentliche IPv4-Adresse nicht in eine Elastic IP-Adresse konvertieren. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen.
- Sie können die Zuordnung einer Elastic IP-Adresse zu einer Ressource aufheben und die Adresse einer anderen Ressource erneut zuordnen. Um unerwartetes Verhalten zu vermeiden, stellen Sie sicher, dass alle aktiven Verbindungen zu der in der vorhandenen Zuordnung genannten Ressource geschlossen werden, bevor Sie die Änderung vornehmen. Nachdem Sie Ihre Elastic IP-Adresse einer anderen Ressource zugeordnet haben, können Sie Ihre Verbindungen mit der neu verknüpften Ressource erneut öffnen.
- Eine getrennte Elastic IP-Adresse bleibt mit Ihrem Konto verknüpft, bis Sie sie explizit freigeben. Ihnen werden alle Elastic IP-Adressen in Ihrem Konto in Rechnung gestellt, unabhängig davon,

ob sie mit einer Instance verknüpft oder getrennt sind. Weitere Informationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite Preise für Amazon VPC.

- Wenn Sie eine Elastic IP-Adresse einer Instance zuordnen, die zuvor eine öffentliche IPv4-Adresse hatte, ändert sich der öffentliche DNS-Hostname der Instance so, dass er mit der Elastic IP-Adresse übereinstimmt.
- Wir lösen den öffentlichen DNS-Hostnamen zur öffentlichen IPv4-Adresse oder zur Elastic IP-Adresse der Instance außerhalb des Netzwerks der Instance bzw. der privaten IPv4-Adresse der Instance innerhalb des Netzwerks der Instance auf.
- Wenn Sie eine Elastic IP-Adresse aus einem IP-Adresspool zuweisen, den Sie Ihrem AWS Konto hinzugefügt haben, wird diese nicht auf Ihre Elastic IP-Adresslimits angerechnet. Weitere Informationen finden Sie unter Kontingent für Elastic-IP-Adressen.
- Wenn Sie die Elastic IP-Adressen zuweisen, können Sie die Elastic IP-Adressen einer Netzwerkgrenzgruppe zuordnen. Dies ist der Ort, von dem aus wir den CIDR-Block bewerben. Durch Festlegen der Netzwerkgrenzgruppe wird der CIDR-Block auf dieser Gruppe beschränkt. Wenn Sie die Netzwerkgrenzgruppe nicht angeben, legen wir die Grenzgruppe fest, die alle Availability Zones in der Region enthält (z. B. `us-west-2`).
- Eine elastische IP-Adresse ist nur zur Verwendung in einer spezifischen Netzwerkgrenzgruppe bestimmt.

Arbeiten mit Elastic-IP-Adressen

In den folgenden Abschnitten wird beschrieben, wie Sie mit Elastic-IP-Adressen arbeiten können.

Aufgaben

- Zuweisen einer Elastic-IP-Adresse
- Beschreiben Ihrer Elastic-IP-Adressen
- Markieren einer Elastic IP-Adresse
- Zuordnen einer Elastic IP-Adresse zu einer Instance oder Netzwerkschnittstelle
- Aufheben der Zuordnung einer Elastic IP-Adresse
- Übertragen von Elastic-IP-Adressen
- Freigeben einer Elastic IP-Adresse
- Wiederherstellen einer Elastic-IP-Adresse
- Verwenden von Reverse DNS für E-Mail-Anwendungen

Zuweisen einer Elastic-IP-Adresse

Sie können eine Elastic IP-Adresse aus dem Pool öffentlicher IPv4-Adressen von Amazon oder aus einem benutzerdefinierten IP-Adresspool, den Sie Ihrem Konto hinzugefügt haben, zuweisen. AWS Weitere Informationen darüber, wie Sie Ihrem AWS Konto Ihren eigenen IP-Adressbereich hinzufügen können, finden Sie unter. Bring Your Own IP Addresses (BYOIP) in Amazon EC2

Sie können eine Elastic IP-Adresse mit einer der folgenden Methoden zuweisen.

Console

So weisen Sie eine Elastic IP-Adresse zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Network & Security Elastic IPs aus.
3. Wählen Sie Elastic IP-Adresse zuweisen aus.
4. (Optional) Wenn Sie eine Elastic IP-Adresse (EIP) zuweisen, wählen Sie die Netzwerkgrenzgruppe aus, der die EIP zugewiesen werden soll. Eine Netzwerkgrenzgruppe ist eine Sammlung von Availability Zones (AZs), Local Zones oder Wavelength Zones, von denen aus AWS eine öffentliche IP-Adresse beworben wird. Local Zones und Wellenlängenzonen können andere Netzwerkgrenzgruppen haben als die AZs in einer Region, um eine minimale Latenz oder physische Entfernung zwischen dem AWS Netzwerk und den Kunden sicherzustellen, die auf die Ressourcen in diesen Zonen zugreifen.

   > **Important**
   >
   > Sie müssen eine EIP derselben Netzwerkgrenzgruppe zuordnen wie die AWS Ressource, die der EIP zugeordnet werden soll. Eine EIP in einer Netzwerkgrenzgruppe kann nur in Zonen dieser Netzwerkgrenzgruppe angekündigt werden und nicht in anderen Zonen, die durch andere Netzwerkgrenzgruppen repräsentiert werden.

   Wenn Sie Local Zones oder Wavelength Zones aktiviert haben (weitere Informationen finden Sie unter Aktivieren einer lokalen Zone oder Aktivieren von Wavelength Zones), können Sie eine Netzwerkgrenzgruppe für AZs, Local Zones oder Wellenlängenzonen auswählen. Wählen Sie die Netzwerkgrenzgruppe sorgfältig aus, da sich die EIP und die AWS Ressource, der sie zugeordnet ist, in derselben Netzwerkgrenzgruppe befinden müssen. Sie

können die EC2-Konsole verwenden, um die Netzwerkgrenzgruppe anzuzeigen, in der sich Ihre Availability Zones, Local Zones oder Wavelength Zones befinden. In der Regel gehören alle Availability Zones in einer Region derselben Netzwerkgrenzgruppe an, wohingegen Local Zones oder Wavelength Zones zu ihren eigenen separaten Netzwerkgrenzgruppen gehören.

Wenn Sie Local Zones oder Wavelength Zones nicht aktiviert haben, ist bei der Zuweisung einer EIP die Netzwerkgrenzgruppe, die alle AZs für die Region darstellt (z. B.`us-west-2`), für Sie vordefiniert und Sie können sie nicht ändern. Das bedeutet, dass die EIP, die Sie dieser Netzwerkgrenzgruppe zuweisen, in allen AZs in der Region, in der Sie sich befinden, angekündigt wird.

5. Wählen Sie für Pool mit öffentlichen IPv4-Adressen eine der folgenden Optionen:

   - Amazon‘s pool of IPv4 addresses (Amazon-Pool von IPv4-Adressen)—Wenn Sie möchten, dass eine IPv4-Adresse aus dem Amazon-Pool von IP-Adressen zugewiesen werden soll.
   - Öffentliche IPv4-Adresse, die Sie Ihrem AWS Konto hinzufügen — Wenn Sie eine IPv4-Adresse aus einem IP-Adresspool zuweisen möchten, den Sie zu Ihrem Konto hinzugefügt haben. AWS Diese Option ist deaktiviert, wenn Sie keine IP-Adresspools haben.
   - Customer owned pool of IPv4 addresses (Kundeneigener Pool von IPv4-Adressen) – Wenn Sie eine IPv4-Adresse aus einem Pool zuweisen möchten, der aus Ihrem On-Premises-Netzwerk zur Verwendung mit einem AWS Outpost erstellt wurde. Diese Option ist deaktiviert, wenn Sie keinen Outpost haben. AWS

6. (Optional) Hinzufügen oder Entfernen eines Tags (Markierung).

   [Tag (Markierung) hinzufügen] Wählen Sie Add new tag (Neuen Tag (Markierung) hinzufügen), und führen Sie die folgenden Schritte aus:

   - Geben Sie bei Key (Schlüssel) den Schlüsselnamen ein.
   - Geben Sie bei Value (Wert) den Wert des Schlüssels ein.

   [Tag (Markierung) entfernen] Wählen Sie Remove (Entfernen) rechts neben dem Schlüssel und dem Wert des Tags (Markierung).

7. Wählen Sie Allocate aus.

AWS CLI

So weisen Sie eine Elastic IP-Adresse zu

Verwenden Sie den AWS CLI -Befehl allocate-address .

PowerShell

So weisen Sie eine Elastic IP-Adresse zu

Benutze den New-EC2Address AWS Tools for Windows PowerShell Befehl.

Beschreiben Ihrer Elastic-IP-Adressen

Sie können eine Elastic IP-Adresse mit einer der folgenden Methoden beschreiben.

Console

So beschreiben Sie Ihre Elastic IP-Adressen:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die Elastic IP-Adresse, die angezeigt werden soll, und wählen Sie Actions (Aktionen), View details (Details anzeigen).

AWS CLI

So beschreiben Sie Ihre Elastic IP-Adressen:

Verwenden Sie den Befehl describe-addresses AWS CLI .

PowerShell

So beschreiben Sie Ihre Elastic IP-Adressen:

Verwenden Sie den Befehl Get-EC2Address AWS Tools for Windows PowerShell .

Markieren einer Elastic IP-Adresse

Sie können benutzerdefinierte Tags (Markierungen) Ihren Elastic IP-Adressen zuweisen, um sie auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. So können Sie eine spezifische Elastic IP-Adresse basierend auf den ihr zugewiesenen benutzerdefinierten Tags (Markierung) schnell finden.

Die Nachverfolgung der Kostenzuordnung mithilfe von Elastic IP-Adressen-Tags (Markierungen) wird nicht unterstützt.

Sie können eine Elastic IP-Adresse mit einer der folgenden Methoden markieren.

Console

Markieren einer Elastic IP-Adresse

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die zu markierende Elastic IP-Adresse aus, und wählen Sie Actions (Aktionen(, View details (Details anzeigen).
4. Wählen Sie im Abschnitt Tags (Markierungen) die Option Manage tags (Tags (Markierungen) verwalten).
5. Geben Sie ein Tag (Markierung)-Schlüssel/Wert-Paar an.
6. (Optional) Wählen Sie Add tag (Tag (Markierung) hinzufügen), um zusätzliche Tags (Markierungen) hinzuzufügen.
7. Wählen Sie Save (Speichern) aus.

AWS CLI

Markieren einer Elastic IP-Adresse

Verwenden Sie den Befehl create-tags AWS CLI .

```
aws ec2 create-tags --resources eipalloc-12345678 --tags Key=Owner,Value=TeamA
```

PowerShell

Markieren einer Elastic IP-Adresse

Verwenden Sie den Befehl New-EC2Tag AWS Tools for Windows PowerShell .

Der Befehl `New-EC2Tag` benötigt einen `Tag`-Parameter, der den Schlüssel und das Schlüsselpaar angibt, die für den Elastic IP-Adressen-Tag (Markierung) verwendet werden. Die folgenden Befehle erstellen den Parameter `Tag`.

```
PS C:\> $tag = New-Object Amazon.EC2.Model.Tag
 PS C:\> $tag.Key = "Owner"
 PS C:\> $tag.Value = "TeamA"
```

```
PS C:\> New-EC2Tag -Resource eipalloc-12345678 -Tag $tag
```

Zuordnen einer Elastic IP-Adresse zu einer Instance oder Netzwerkschnittstelle

Wenn Sie Ihrer Instance eine Elastic IP-Adresse zuordnen, um die Kommunikation mit dem Internet zu ermöglichen, müssen Sie sicherstellen, dass sich Ihre Instance in einem öffentlichen Subnetz befindet. Weitere Informationen finden Sie unter Internet-Gateways im Amazon-VPC-Benutzerhandbuch.

Mit einer der folgenden Methoden können Sie eine Elastic IP-Adresse einer Instance oder einer Netzwerkschnittstelle zuordnen.

Console

Zuordnen einer Elastic IP-Adresse zu einer Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die zu verknüpfende Elastic IP-Adresse aus, und wählen Sie Actions (Aktionen), Associate Elastic IP address (Elastic IP-Adresse zuordnen).
4. Wählen Sie für Resource type (Ressourcentyp) die Option Instance aus.
5. Wählen Sie die Instance aus, der die Elastic IP-Adresse zugeordnet werden soll. Sie können auch Text eingeben, um nach einer bestimmten Instance zu suchen.
6. (Optional) Geben Sie für Private IP address (Private IP-Adresse) eine private IP-Adresse an, mit der die Elastic IP-Adresse verknüpft werden soll.
7. Wählen Sie Associate aus.

So ordnen Sie einer Elastic IP-Adresse eine Netzwerkschnittstelle zu:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.

3. Wählen Sie die zu verknüpfende Elastic IP-Adresse aus, und wählen Sie Actions (Aktionen), Associate Elastic IP address (Elastic IP-Adresse zuordnen).
4. Wählen Sie für Resource type (Ressourcentyp) Network interface (Netzwerkschnittstelle) aus.
5. Wählen Sie für Network interface (Netzwerkschnittstelle) die Netzwerkschnittstelle aus, der die Elastic IP-Adresse zugeordnet werden soll. Sie können auch Text eingeben, um nach einer bestimmten Netzwerkschnittstelle zu suchen.
6. (Optional) Geben Sie für Private IP address (Private IP-Adresse) eine private IP-Adresse an, mit der die Elastic IP-Adresse verknüpft werden soll.
7. Wählen Sie Associate aus.

AWS CLI

So ordnen Sie eine Elastic IP-Adresse zu:

Verwenden Sie den Befehl associate-address AWS CLI .

PowerShell

So ordnen Sie eine Elastic IP-Adresse zu:

Verwenden Sie den Befehl Register-EC2Address AWS Tools for Windows PowerShell .

Aufheben der Zuordnung einer Elastic IP-Adresse

Sie können die Zuordnung einer Elastic IP-Adresse jederzeit von einer Instance oder einer Netzwerkschnittstelle trennen. Nachdem Sie die Elastic IP-Adresse getrennt haben, können Sie sie erneut einer anderen Ressource zuordnen.

Sie können die Zuordnung einer Elastic IP-Adresse mit einer der folgenden Methoden aufheben.

Console

So heben Sie die Zuordnung einer Elastic IP-Adresse auf und ordnen sie wieder zu:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die Elastic IP-Adresse, deren Zuordnung Sie aufheben möchten, und wählen Sie Actions (Aktionen), Disassociate Elastic IP address (Elastic IP-Adresse trennen).

4. Wählen Sie Disassociate (Zuordnung aufheben) aus.

AWS CLI

So heben Sie die Zuordnung einer Elastic-IP-Adresse auf

Verwenden Sie den Befehl disassociate-address AWS CLI .

PowerShell

So heben Sie die Zuordnung einer Elastic-IP-Adresse auf

Verwenden Sie den Unregister-EC2Address-Befehl. AWS Tools for Windows PowerShell

Übertragen von Elastic-IP-Adressen

In diesem Abschnitt wird beschrieben, wie Sie Elastic-IP-Adressen von einem AWS-Konto auf ein anderes übertragen. Die Übertragung von Elastic-IP-Adressen kann in den folgenden Situationen hilfreich sein:

- Organisatorische Umstrukturierung — Verwenden Sie Elastic IP-Adressübertragungen, um Workloads schnell von einem zum anderen zu verlagern. AWS-Konto Sie müssen nicht warten, bis neue Elastic-IP-Adressen in Ihren Sicherheitsgruppen und NACLs auf die Zulassungsliste gesetzt werden.
- Zentralisierte Sicherheitsadministration — Verwenden Sie ein zentrales AWS Sicherheitskonto, um Elastic IP-Adressen zu verfolgen und zu übertragen, die auf Einhaltung der Sicherheitsbestimmungen überprüft wurden.
- Notfallwiederherstellung – Verwenden Sie Elastic-IP-Adressübertragungen, um IPs für öffentlich zugängliche Internet-Workloads bei Notfallereignissen schnell neu zuzuordnen.

Für die Übertragung von Elastic-IP-Adressen fallen keine Gebühren an.

Aufgaben

- Übertragung für Elastic-IP-Adressen aktivieren
- Deaktivieren der Übertragung von Elastic-IP-Adressen
- Akzeptieren einer übertragenen Elastic-IP-Adresse

Übertragung für Elastic-IP-Adressen aktivieren

In diesem Abschnitt wird beschrieben, wie Sie eine übertragene Elastic-IP-Adresse akzeptieren. Beachten Sie die folgenden Einschränkungen in Bezug auf die Aktivierung von Elastic-IP-Adressen für die Übertragung:

- Sie können Elastic IP-Adressen von einem beliebigen Konto AWS-Konto (Quellkonto) auf jedes andere AWS Konto in derselben AWS Region (Transferkonto) übertragen.
- Wenn Sie eine Elastic-IP-Adresse übertragen, findet ein zweistufiger Handshake zwischen den AWS-Konten statt. Wenn das Quellkonto die Übertragung startet, haben die Übertragungskonten sieben Tage Zeit, die Übertragung der Elastic-IP-Adresse zu akzeptieren. Während dieser sieben Tage kann das Quellkonto die ausstehende Übertragung einsehen (z. B. in der AWS Konsole oder mithilfe des Befehls AWS CLI describe-address-transfers). Nach sieben Tagen läuft die Übertragung ab und das Eigentum an der Elastic-IP-Adresse geht zurück an das Quellkonto.
- Akzeptierte Übertragungen sind für das Quellkonto (z. B. in der AWS Konsole oder mithilfe des AWS CLI Befehls describe-address-transfers) drei Tage lang sichtbar, nachdem die Übertragungen akzeptiert wurden.
- AWS benachrichtigt Übertragungskonten nicht über ausstehende Elastic IP-Adressübertragungsanfragen. Der Besitzer des Quellkontos muss den Besitzer des Übertragungskontos darüber informieren, dass eine Elastic-IP-Adressübertragungsanforderung vorliegt, die er akzeptieren muss.
- Alle Tags, die einer übertragenen Elastic-IP-Adresse zugeordnet sind, werden zurückgesetzt, wenn die Übertragung abgeschlossen ist.
- Sie können Elastic IP-Adressen, die Ihnen aus öffentlichen IPv4-Adresspools zugewiesen wurden, nicht in Ihre eigenen AWS-Konto — allgemein als Bring Your Own IP (BYOIP) -Adresspools (Bring Your Own IP) bezeichnet — übertragen.
- Wenn Sie versuchen, eine Elastic-IP-Adresse zu übertragen, der ein umgekehrter DNS-Eintrag zugeordnet ist, können Sie zwar mit der Übertragung beginnen, aber das Übertragungskonto kann die Übertragung erst dann akzeptieren, wenn der zugeordnete DNS-Eintrag entfernt wurde.
- Wenn Sie Elastic aktiviert und konfiguriert haben AWS Outposts, haben Sie Elastic IP-Adressen möglicherweise aus einem kundeneigenen IP-Adresspool (CoIP) zugewiesen. Sie können keine Elastic-IP-Adressen übertragen, die von einem CoIP zugewiesen wurden. Sie können es jedoch verwenden, AWS RAM um eine CoIP mit einem anderen Konto zu teilen. Weitere Informationen finden Sie unter Kundeneigene IP-Adressen im AWS Outposts -Benutzerhandbuch.
- Sie können Amazon VPC IPAM verwenden, um die Übertragung von Elastic-IP-Adressen an Konten in einer Organisation von AWS Organizations zu verfolgen. Weitere Informationen finden

Sie unter Anzeigen des IP-Adressverlaufs. Wenn eine Elastic-IP-Adresse auf ein AWS-Konto außerhalb des Unternehmens übertragen wird, geht der IPAM-Prüfungsverlauf für die Elastic-IP-Adresse verloren.

Diese Schritte müssen vom Quellkonto ausgeführt werden.

Console

So aktivieren Sie die Übertragung von Elastic-IP-Adressen

1. Stellen Sie sicher, dass Sie das AWS Quellkonto verwenden.
2. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Elastic IPs.
4. Wählen Sie eine oder mehrere Elastic-IP-Adressen aus, die für die Übertragung aktiviert werden sollen, und wählen Sie Actions (Aktionen), Enable transfer (Übertragung aktivieren).
5. Wenn Sie mehrere Elastic-IP-Adressen übertragen, wird Ihnen die Option Transfer type (Übertragungstyp) angezeigt. Wählen Sie eine der folgenden Optionen:
   - Wählen Sie Einzelkonto, wenn Sie die Elastic-IP-Adressen auf ein einzelnes AWS Konto übertragen möchten.
   - Wählen Sie Mehrere Konten, wenn Sie die Elastic IP-Adressen auf mehrere AWS Konten übertragen möchten.
6. Geben Sie unter Transfer account ID (Konto-ID übertragen) die IDs der AWS -Konten ein, auf die Sie die Elastic-IP-Adressen übertragen möchten.
7. Bestätigen Sie die Übertragung, indem Sie **`enable`** in das Textfeld eingeben.
8. Wählen Sie Absenden aus.
9. Informationen zum Akzeptieren der Übertragung finden Sie unter Akzeptieren einer übertragenen Elastic-IP-Adresse. Informationen zum Deaktivieren der Übertragung finden Sie unter Deaktivieren der Übertragung von Elastic-IP-Adressen.

AWS CLI

So aktivieren Sie die Übertragung von Elastic-IP-Adressen

Verwenden Sie den Befehl enable-address-transfer.

PowerShell

So aktivieren Sie die Übertragung von Elastic-IP-Adressen

Verwenden Sie den Enable-EC2AddressTransfer-Befehl.

Deaktivieren der Übertragung von Elastic-IP-Adressen

In diesem Abschnitt wird beschrieben, wie Sie eine Elastic-IP-Übertragung deaktivieren, nachdem die Übertragung aktiviert wurde.

Diese Schritte müssen von dem Quellkonto ausgeführt werden, das die Übertragung aktiviert hat.

Console

So deaktivieren Sie die Übertragung einer Elastic-IP-Adresse

1. Stellen Sie sicher, dass Sie das AWS Quellkonto verwenden.
2. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Elastic IPs.
4. Stellen Sie in der Ressourcenliste der Elastic-IPs sicher, dass Sie die Eigenschaft aktiviert haben, die die Spalte Transfer status (Übertragungsstatus) anzeigt.
5. Wählen Sie eine oder mehrere Elastic-IP-Adressen aus, die den Transfer status (Übertragungsstatus) Pending (Ausstehend) haben, und wählen Sie Actions (Aktionen), Disable transfer (Übertragung deaktivieren) aus.
6. Bestätigen Sie durch Eingabe von **`disable`** in das Textfeld.
7. Wählen Sie Absenden aus.

AWS CLI

So deaktivieren Sie die Übertragung von Elastic-IP-Adressen

Verwenden Sie den Befehl disable-address-transfer.

PowerShell

So deaktivieren Sie die Übertragung von Elastic-IP-Adressen

Verwenden Sie den Disable-EC2AddressTransfer-Befehl.

Akzeptieren einer übertragenen Elastic-IP-Adresse

In diesem Abschnitt wird beschrieben, wie Sie eine übertragene Elastic-IP-Adresse akzeptieren.

Wenn Sie eine Elastic-IP-Adresse übertragen, findet ein zweistufiger Handshake zwischen den AWS-Konten statt. Wenn das Quellkonto die Übertragung startet, haben die Übertragungskonten sieben Tage Zeit, die Übertragung der Elastic-IP-Adresse zu akzeptieren. Während dieser sieben Tage kann das Quellkonto die ausstehende Übertragung einsehen (z. B. in der AWS Konsole oder mithilfe des Befehls AWS CLI describe-address-transfers). Nach sieben Tagen läuft die Übertragung ab und das Eigentum an der Elastic-IP-Adresse geht zurück an das Quellkonto.

Beachten Sie bei dem Akzeptieren von Übertragungen die folgenden Ausnahmen, die auftreten können, und wie Sie sie beheben können:

- AddressLimitÜberschritten: Wenn Ihr Übertragungskonto das Elastic IP-Adresskontingent überschritten hat, kann das Quellkonto die Elastic IP-Adressübertragung aktivieren. Diese Ausnahme tritt jedoch auf, wenn das Übertragungskonto versucht, die Übertragung zu akzeptieren. Standardmäßig sind alle AWS Konten auf 5 Elastic IP-Adressen pro Region beschränkt. Anweisungen zur Erhöhung des Limits finden Sie unter Kontingent für Elastic-IP-Adressen.
- InvalidTransfer. AddressCustomPtrSet: Wenn Sie oder jemand in Ihrer Organisation die Elastic IP-Adresse, die Sie übertragen möchten, für die umgekehrte DNS-Suche konfiguriert haben, kann das Quellkonto die Übertragung für die Elastic IP-Adresse ermöglichen. Diese Ausnahme tritt jedoch auf, wenn das Übertragungskonto versucht, die Übertragung zu akzeptieren. Um dieses Problem zu beheben, muss das Quellkonto den DNS-Datensatz für die Elastic-IP-Adresse entfernen. Weitere Informationen finden Sie unter Verwenden von Reverse DNS für E-Mail-Anwendungen.
- InvalidTransfer. AddressAssociated: Wenn eine Elastic IP-Adresse mit einer ENI- oder EC2-Instance verknüpft ist, kann das Quellkonto die Übertragung für die Elastic IP-Adresse ermöglichen. Diese Ausnahme tritt jedoch auf, wenn das Übertragungskonto versucht, die Übertragung zu akzeptieren. Um dieses Problem zu beheben, muss die Zuordnung für das Quellkonto der Elastic-IP-Adresse aufgehoben worden. Weitere Informationen finden Sie unter Aufheben der Zuordnung einer Elastic IP-Adresse.

Für alle anderen Ausnahmen wenden Sie sich an AWS Support.

Diese Schritte müssen von dem Übertragungskonto ausgeführt werden.

Console

So akzeptieren Sie die Übertragung einer Elastic-IP-Adresse

1. Stellen Sie sicher, dass Sie das Übertragungskonto verwenden.
2. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
3. Wählen Sie im Navigationsbereich Elastic IPs.
4. Wählen Sie Actions (Aktionen), Accept transfer (Übertragung akzeptieren).
5. Wenn Sie die Übertragung akzeptieren, werden keine Tags, die der übertragenen Elastic-IP-Adresse zugeordnet sind, mit der Elastic-IP-Adresse übertragen. Wenn Sie ein Tag Name für die von Ihnen akzeptierte Elastic-IP-Adresse definieren möchten, wählen Sie Create a tag with a key of 'Name' and a value that you specify (Erstellen eines Tags mit dem Schlüssel „Name“ und einem von Ihnen angegebenen Wert) aus.
6. Geben Sie die Elastic-IP-Adresse ein, die Sie übertragen möchten.
7. Wenn Sie mehrere übertragene Elastic-IP-Adressen akzeptieren, wählen Sie Add address (Adresse hinzufügen), um eine zusätzliche Elastic-IP-Adresse einzugeben.
8. Wählen Sie Absenden aus.

AWS CLI

So akzeptieren Sie die Übertragung einer Elastic-IP-Adresse

Verwenden Sie den Befehl accept-address-transfer.

PowerShell

So akzeptieren Sie die Übertragung einer Elastic-IP-Adresse

Verwenden Sie den Approve-EC2AddressTransfer-Befehl.

Freigeben einer Elastic IP-Adresse

Wenn Sie eine Elastic IP-Adresse nicht mehr benötigen, empfehlen wir, sie mit einer der folgenden Methoden freizugeben. Die Adresse, die freigegeben werden soll, darf derzeit keiner AWS Ressource zugeordnet sein, z. B. einer EC2-Instance, einem NAT-Gateway oder einem Network Load Balancer.

> **Note**
>
> Wenn Sie den AWS Support kontaktiert haben, um Reverse-DNS für eine Elastic IP (EIP) - Adresse einzurichten, können Sie das Reverse-DNS entfernen, aber Sie können die Elastic IP-Adresse nicht freigeben, da sie vom Support gesperrt wurde. AWS Wenden Sie sich an den AWS Support, um die elastische IP-Adresse zu entsperren. Nachdem die Elastic IP-Adresse entsperrt wurde, können Sie die Elastic IP-Adresse freigeben.

Console

So geben Sie eine Elastic IP-Adresse frei

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die Elastic IP-Adresse, die freigegeben werden soll, und wählen Sie Actions (Aktionen), Release Elastic IP addresses (Elastic IP-Adressen freigeben).
4. Wählen Sie Release (Freigeben).

AWS CLI

So geben Sie eine Elastic-IP-Adresse frei

Verwenden Sie den Befehl release-address AWS CLI .

PowerShell

So geben Sie eine Elastic-IP-Adresse frei

Verwenden Sie den Befehl Remove-EC2Address AWS Tools for Windows PowerShell .

Wiederherstellen einer Elastic-IP-Adresse

Wenn Sie Ihre Elastic IP-Adresse freigegeben haben, können Sie sie möglicherweise wiederherstellen. Es gelten die folgenden Regeln:

- Sie können eine Elastic IP-Adresse nicht wiederherstellen, wenn sie einem anderen AWS -Konto zugeordnet wurde oder wenn dies dazu führen würde, dass Sie Ihren Elastic IP-Adressgrenzwert überschreiten.

- Sie können keine Tags (Markierungen) wiederherstellen, die einer Elastic IP-Adresse zugeordnet sind.
- Sie können eine Elastic IP-Adresse nur mithilfe der Amazon EC2-API oder eines Befehlszeilen-Tools wiederherstellen.

AWS CLI

So stellen Sie eine Elastic IP-Adresse wieder her:

Verwenden Sie den AWS CLI Befehl allocate-address und geben Sie die IP-Adresse mithilfe des `--address` Parameters wie folgt an.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

PowerShell

So stellen Sie eine Elastic IP-Adresse wieder her:

Verwenden Sie den New-EC2Address AWS Tools for Windows PowerShell Befehl und geben Sie die IP-Adresse mithilfe des `-Address` Parameters wie folgt an.

```
PS C:\> New-EC2Address -Address 203.0.113.3 -Domain vpc -Region us-east-1
```

Verwenden von Reverse DNS für E-Mail-Anwendungen

Wenn Sie beabsichtigen, E-Mails von einer Instance an Dritte zu senden, empfehlen wir Ihnen, eine oder mehrere Elastic IP-Adressen bereitzustellen und den Elastic IP-Adressen, die Sie zum Senden von E-Mails verwenden, statische Reverse-DNS-Einträge zuzuweisen. Auf diese Weise können Sie verhindern, dass Ihre E-Mail von einigen Anti-Spam-Organisationen als Spam gekennzeichnet wird. AWS arbeitet mit ISPs und Internet-Anti-Spam-Organisationen zusammen, um die Wahrscheinlichkeit zu verringern, dass Ihre von diesen Adressen gesendeten E-Mails als Spam gekennzeichnet werden.

Überlegungen

- Bevor Sie einen Reverse-DNS-Datensatz erstellen, müssen Sie einen entsprechenden Forward-DNS-Datensatz (Record-Typ A) einrichten, der auf Ihre Elastic IP-Adresse verweist.
- Wenn einer Elastic IP-Adresse ein Reverse-DNS-Datensatz zugewiesen ist, wird die Elastic IP-Adresse fest mit Ihrem Konto verknüpft und kann von dem Konto nur freigegeben werden, wenn der Datensatz entfernt wird.

- AWS GovCloud (US) Region

  Sie können mit der Konsole oder keinen Reverse-DNS-Eintrag erstellen. AWS CLI AWS muss Ihnen die statischen Reverse-DNS-Einträge zuweisen. Öffnen Sie Anforderung zum Entfernen von Reverse-DNS und Einschränkungen beim Senden von E-Mails und stellen Sie uns Ihre Elastic IP-Adressen und Reverse-DNS-Einträge zur Verfügung.

Erstellen eines Reverse-DNS-Datensatzes

Um einen Reverse-DNS-Eintrag zu erstellen, wählen Sie die Registerkarte aus, die Ihrer bevorzugten Methode entspricht.

Console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die Elastic IP-Adresse aus und wählen Sie Actions (Aktionen), Reverse-DNS aktualisieren.
4. Geben Sie für Reverse DNS domain name (Reverse-DNS-Domain-Name) den Domain-Namen ein.
5. Geben Sie **`update`** zur Bestätigung ein.
6. Wählen Sie Update (Aktualisieren) aus.

AWS CLI

Verwenden Sie den modify-address-attribute Befehl in AWS CLI, wie im folgenden Beispiel gezeigt:

```
aws ec2 modify-address-attribute --allocation-id eipalloc-abcdef01234567890  --
domain-name example.com
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.net."
            "PtrRecordUpdate": {
                "Value": "example.com.",
                "Status": "PENDING"
```

```
        }
    ]
}
```

Entfernen eines Reverse-DNS-Datensatzes

Um einen Reverse-DNS-Eintrag zu entfernen, wählen Sie die Registerkarte aus, die Ihrer bevorzugten Methode entspricht.

Console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die Elastic IP-Adresse aus und wählen Sie Actions (Aktionen), Reverse-DNS aktualisieren.
4. Löschen Sie für Reverse DNS domain name (Reverse-DNS-Domain-Name) den Domain-Namen.
5. Geben Sie **`update`** zur Bestätigung ein.
6. Wählen Sie Update (Aktualisieren) aus.

AWS CLI

Verwenden Sie den reset-address-attribute Befehl in AWS CLI, wie im folgenden Beispiel gezeigt:

```
aws ec2 reset-address-attribute --allocation-id eipalloc-abcdef01234567890 --
attribute domain-name
{
    "Addresses": [
        {
            "PublicIp": "192.0.2.0",
            "AllocationId": "eipalloc-abcdef01234567890",
            "PtrRecord": "example.com."
            "PtrRecordUpdate": {
                "Value": "example.net.",
                "Status": "PENDING"
        }
    ]
}
```

> **Note**
>
> Wenn Sie bei der Ausführung des Befehls die folgende Fehlermeldung erhalten, können Sie eine Anfrage zur Aufhebung der Einschränkungen beim Senden von E-Mails an uns senden, um AWS Support Unterstützung zu erhalten.
> Die Adresse mit Zuordnungs-ID kann nicht freigegeben werden, da sie fest mit Ihrem Konto verknüpft ist.

Kontingent für Elastic-IP-Adressen

Standardmäßig haben alle AWS Konten ein Kontingent von fünf (5) Elastic IP-Adressen pro Region, da öffentliche (IPv4) Internetadressen eine knappe öffentliche Ressource sind. Wir empfehlen Ihnen dringend, eine Elastic IP-Adresse in erster Linie wegen der Möglichkeit zu verwenden, die Adresse im Fall eines Instance-Ausfalls einer anderen Instance zuzuweisen und für alle anderen Kommunikationen zwischen Knoten DNS-Hostnamen zu verwenden.

So überprüfen Sie, wie viele Elastic IP-Adressen verwendet werden

Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/ und wählen Sie im Navigationsbereich Elastic IPs (Elastische IP-Adressen) aus.

So überprüfen Sie Ihr aktuelles Kontokontingent für Elastic IP-Adressen

1. Öffnen Sie die Service-Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/.
2. Wählen Sie auf der Navigationsleiste (oben auf dem Bildschirm) eine Region aus.
3. Wählen Sie auf dem Dashboard die Option Amazon Elastic Compute Cloud (Amazon EC2) aus.

   Wenn Amazon Elastic Compute Cloud (Amazon EC2) nicht im Dashboard aufgeführt ist, wählen Sie AWS services aus, geben **`EC2`** in das Suchfeld ein und wählen dann Amazon Elastic Compute Cloud (Amazon EC2) aus.
4. Geben Sie auf der Seite „Amazon-EC2-Service-Quotas“ in das Suchfeld **`IP`** ein. Das Limit ist EC2-VPC Elastic IPs. Für weitere Informationen wählen Sie das Limit.

Wenn Ihre Architektur zusätzliche Elastic IP-Adressen erfordert, können Sie direkt in der Service-Quotas-Konsole eine Erhöhung des Kontingents anfordern. Zum Anfordern einer Erhöhung für ein Kontingent wählen Sie Erhöhung auf Kontoebene beantragen. Weitere Informationen finden Sie unter Amazon-EC2-Service Quotas.

Elastic-Network-Schnittstelle

Eine Elastic-Network-Schnittstelle ist eine logische Netzwerkkomponente in einer VPC, die eine virtuelle Netzwerkkarte darstellt. Es kann die folgenden Attribute enthalten:

- Eine primäre private IPv4-Adresse aus dem IPv4-Adressbereich Ihrer VPC
- Eine primäre IPv6-Adresse aus dem IPv6-Adressbereich Ihrer VPC
- Eine oder mehrere sekundäre private IPv4-Adressen aus dem IPv4-Adressbereich Ihrer VPC
- Eine Elastic IP-Adresse (IPv4) für jede private IPv4-Adresse
- Eine öffentliche IPv4-Adresse
- Eine oder mehrere IPv6-Adressen
- Eine oder mehrere Sicherheitsgruppen
- Eine MAC-Adresse
- Eine Quell-/Zielprüfungsmarkierung
- Eine Beschreibung

Sie können Netzwerkschnittstellen erstellen und konfigurieren und sie an Instances in derselben Availability Zone anfügen. Ihr Konto verfügt möglicherweise auch über vom Antragsteller verwaltete Netzwerkschnittstellen, die von Diensten erstellt und verwaltet werden, sodass Sie andere Ressourcen und AWS Dienste nutzen können. Sie können diese Netzwerkschnittstellen nicht selbst verwalten. Weitere Informationen finden Sie unter Vom Anforderer verwaltete Netzwerkschnittstellen.

Diese AWS Ressource wird in der AWS Management Console und der Amazon EC2 EC2-API als Netzwerkschnittstelle bezeichnet. Daher verwenden wir „Netzwerkschnittstelle“ in dieser Dokumentation anstelle von „Elastic-Network-Schnittstelle“. Der Begriff „Netzwerkschnittstelle“ in dieser Dokumentation bedeutet immer „Elastic-Network-Schnittstelle“.

Inhalt

- Vom Anforderer verwaltete Netzwerkschnittstellen
- Zuweisen von Präfixen zu Amazon EC2 Netzwerkschnittstellen

Netzwerkschnittstellen – Grundlagen

Sie können eine Netzwerkschnittstelle erstellen, diese an eine Instance anfügen, sie von einer Instance trennen und sie an eine andere Instance anfügen. Die Attribute einer Netzwerkschnittstelle folgen der Netzwerkschnittstelle, wenn diese an eine Instance angefügt oder von dieser getrennt und erneut an eine andere Instance angefügt wird. Wenn Sie eine Netzwerkschnittstelle von einer Instance zu einer anderen verschieben, wird der Netzwerkdatenverkehr zur neuen Instance umgeleitet.

Primäre Netzwerkschnittstelle

Jede Instance verfügt über eine Standard-Netzwerkschnittstelle, die als primäre Netzwerkschnittstelle bezeichnet wird. Sie können eine primäre Netzwerkschnittstelle nicht von einer Instance trennen. Sie können zusätzliche Netzwerkschnittstellen erstellen und anfügen. Die maximale Anzahl von Netzwerkschnittstellen, die Sie verwenden können, variiert je nach Instance-Typ. Weitere Informationen finden Sie unter IP-Adressen pro Netzwerkschnittstelle pro Instance-Typ.

Öffentliche IPv4-Adressen für Netzwerkschnittstellen

In einer VPC verfügen alle Subnetze über ein anpassbares Attribut, über das festlegt wird, ob die in einem Subnetz erstellten Netzwerkschnittstellen (und somit Instances, die in diesem Subnetz gestartet wurden) einer öffentlichen IPv4-Adresse zugeordnet sind. Weitere Informationen finden Sie unter Subnetz-Einstellungen im Amazon-VPC-Benutzerhandbuch. Die öffentliche IPv4-Adresse wird aus dem Pool öffentlicher IPv4-Adressen von Amazon zugewiesen. Wenn Sie eine Instance starten, wird die IP-Adresse der erstellten primären Netzwerkschnittstelle zugewiesen.

Wenn Sie eine Netzwerkschnittstelle erstellen, erhält diese das öffentliche IPv4-Adressierungsattribut des Subnetzes. Falls Sie das öffentliche IPv4-Adressierungsattribut des Subnetzes später ändern, behält die Netzwerkschnittstelle die Einstellung bei, die bei ihrer Erstellung wirksam war. Wenn Sie eine Instance starten und eine vorhandene Netzwerkschnittstelle als primäre Netzwerkschnittstelle angeben, wird das öffentliche IPv4-Adressattribut von dieser Netzwerkschnittstelle bestimmt.

Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen.

Elastic IP-Adressen für Netzwerkschnittstelle

Wenn Sie über eine Elastic IP-Adresse verfügen, können Sie diese Adresse einer der privaten IPv4-Adressen für die Netzwerkschnittstelle zuordnen. Sie können eine Elastic IP-Adresse jeder privaten IPv4-Adresse zuordnen.

Wenn Sie eine Elastic IP-Adresse von einer Netzwerkschnittstelle trennen, können Sie sie wieder in den Adresspool freigeben. Dies ist die einzige Möglichkeit, eine Elastic IP-Adresse einer Instance in einem anderen Subnetz oder einer anderen VPC zuzuordnen. Netzwerkschnittstellen gelten speziell für bestimmte Subnetze.

IPv6-Adressen für Netzwerkschnittstellen

Wenn Sie IPv6-CIDR-Blöcke Ihrer VPC und Ihrem Subnetz zuordnen, können Sie einer Netzwerkschnittstelle eine oder mehrere IPv6-Adressen aus dem Subnetzbereich zuweisen. Jede IPv6-Adresse kann einer Netzwerkschnittstelle zugewiesen werden.

Alle Subnetze verfügen über ein anpassbares Attribut, über das festlegt wird, ob den in einem Subnetz erstellten Netzwerkschnittstellen (und somit Instances, die in diesem Subnetz gestartet wurden) automatisch eine IPv6-Adresse aus dem Subnetzbereich zugewiesen wird. Weitere Informationen finden Sie unter Subnetz-Einstellungen im Amazon-VPC-Benutzerhandbuch. Wenn Sie eine Instance starten, wird die IPv6-Adresse der erstellten primären Netzwerkschnittstelle zugewiesen.

Weitere Informationen finden Sie unter IPv6-Adressen.

Präfixdelegierung

Ein Präfix für die Präfixdelegierung ist ein reservierter privater IPv4- oder IPv6-CIDR-Bereich, den Sie zur automatischen oder manuellen Zuweisung zu Netzwerkschnittstellen zuweisen, die einer Instance zugeordnet sind. Mithilfe von delegierten Präfixen können Sie Dienste schneller starten, indem Sie einen Bereich von IP-Adressen als einzelnes Präfix zuweisen.

Beendigungsverhalten

Sie können das Beendigungsverhalten für eine Netzwerkschnittstelle ändern, die mit einer Instance verbunden ist. Sie können angeben, ob die Netzwerkschnittstelle automatisch gelöscht werden soll, wenn Sie die Instance beenden, mit der sie verbunden ist.

Quell-/Zielprüfung

Sie können Quell-/Zielprüfungen aktivieren oder deaktivieren, die sicherstellen, dass die Instance entweder die Quelle oder das Ziel eines Datenverkehrs ist, den sie empfängt. Die Quell-/

Zielprüfungen sind standardmäßig aktiviert. Sie müssen Quell-/Zielprüfungen deaktivieren, wenn die Instance Services wie Network Address Translation, Routing oder Firewalls ausführt.

Überwachen von IP-Datenverkehr

Sie können ein VPC-Flow-Protokoll auf Ihrer Netzwerkschnittstelle aktivieren, um Informationen über den IP-Datenverkehr zu und von einer Netzwerkschnittstelle zu erfassen. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie dessen Daten in Amazon CloudWatch Logs anzeigen und abrufen. Weitere Informationen finden Sie unter VPC-Flow-Protokolle im Amazon-VPC-Benutzerhandbuch.

Automatische Zuweisung von öffentlichen IPv4-Adressen

Sie können die automatische Zuweisung einer öffentlichen IPv4-Adresse zu einer Netzwerkschnittstelle aktivieren und deaktivieren. Diese Option kann für jede Netzwerkschnittstelle aktiviert werden, gilt jedoch nur für die primäre Netzwerkschnittstelle (eth0). Weitere Informationen finden Sie unter Verwalten von IP-Adressen.

Netzwerkkarten

Instances mit mehreren Netzwerkkarten bieten eine höhere Netzwerkleistung, einschließlich Bandbreitenfähigkeiten über 100 Gbit/s und verbesserte Paketratenleistung. Jede Netzwerkschnittstelle ist mit einer Netzwerkkarte verbunden. Die primäre Netzwerkschnittstelle muss dem Netzwerkkartenindex 0 zugewiesen sein.

Wenn Sie Elastic Fabric Adapter (EFA) aktivieren, wenn Sie eine Instance starten, die mehrere Netzwerkkarten unterstützt, sind alle Netzwerkkarten verfügbar. Sie können bis zu einem EFA pro Netzwerkkarte zuweisen. Ein EFA zählt als Netzwerkschnittstelle.

Die folgenden Instances unterstützen mehrere Netzwerkkarten. Alle anderen Instance-Typen unterstützen eine Netzwerkkarte.

Instance-Typ	Anzahl der Netzwerkkarten
`c6in.32xlarge`	2
`c6in.metal`	2
`dl1.24xlarge`	4
`hpc6id.32xlarge`	2

Instance-Typ	Anzahl der Netzwerkkarten
hpc7a.12xlarge	2
hpc7a.24xlarge	2
hpc7a.48xlarge	2
hpc7a.96xlarge	2
m6idn.32xlarge	2
m6idn.metal	2
m6in.32xlarge	2
m6in.metal	2
p4d.24xlarge	4
p4de.24xlarge	4
p5.48xlarge	32
r6idn.32xlarge	2
r6idn.metal	2
r6in.32xlarge	2
r6in.metal	2
trn1.32xlarge	8
trn1n.32xlarge	16
u7in-16tb.224xlarge	2
u7in-24tb.224xlarge	2
u7in-32tb.224xlarge	2

IP-Adressen pro Netzwerkschnittstelle pro Instance-Typ

Jeder Instance-Typ unterstützt eine maximale Anzahl von Netzwerkschnittstellen, eine maximale Anzahl von privaten IPv4-Adressen pro Netzwerkschnittstelle und eine maximale Anzahl von IPv6-Adressen pro Netzwerkschnittstelle. Der Grenzwert für IPv6-Adressen ist unabhängig vom Grenzwert für private IPv4-Adressen pro Netzwerkschnittstelle. Nicht alle Instance-Typen unterstützen die IPv6-Adressierung.

Verfügbare Netzwerkschnittstellen

Der Amazon EC2 Instance Types Guide enthält Informationen zu den Netzwerkschnittstellen, die für jeden Instance-Typ verfügbar sind. Weitere Informationen finden Sie hier:

- Netzwerkspezifikationen — Allgemeiner Zweck
- Netzwerkspezifikationen — Für Rechenleistung optimiert
- Netzwerkspezifikationen — Speicheroptimiert
- Netzwerkspezifikationen — Speicheroptimiert
- Netzwerkspezifikationen — Beschleunigtes Rechnen
- Netzwerkspezifikationen — Hochleistungsrechnen
- Netzwerkspezifikationen — Vorgängergeneration

Um Netzwerkschnittstelleninformationen mit dem abzurufen AWS CLI

Sie können den AWS CLI Befehl describe-instance-types verwenden, um Informationen über einen Instance-Typ anzuzeigen, z. B. die unterstützten Netzwerkschnittstellen und IP-Adressen pro Schnittstelle. Im folgenden Beispiel werden diese Informationen für alle C5-Instances angezeigt.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*" --query
 "InstanceTypes[].{Type: InstanceType, MaxENI: NetworkInfo.MaximumNetworkInterfaces,
 IPv4addr: NetworkInfo.Ipv4AddressesPerInterface}" --output table
----------------------------------------
|        DescribeInstanceTypes         |
+----------+----------+---------------+
| IPv4addr | MaxENI   |     Type      |
+----------+----------+---------------+
|  30      |  8       |  c5.4xlarge   |
|  50      |  15      |  c5.24xlarge  |
|  15      |  4       |  c5.xlarge    |
```

```
|  30      |  8       |  c5.12xlarge  |
|  10      |  3       |  c5.large     |
|  15      |  4       |  c5.2xlarge   |
|  50      |  15      |  c5.metal     |
|  30      |  8       |  c5.9xlarge   |
|  50      |  15      |  c5.18xlarge  |
+----------+----------+---------------+
```

Arbeiten mit Netzwerkschnittstellen

Sie können mit Netzwerkschnittstellen unter Verwendung der Amazon EC2-Konsole oder über die Befehlszeile arbeiten.

Inhalt

Erstellen einer Netzwerkschnittstelle

Sie können eine Netzwerkschnittstelle in einem Subnetz erstellen. Sie können die Netzwerkschnittstelle nach der Erstellung nicht in ein anderes Subnetz verschieben. Sie müssen eine Netzwerkschnittstelle an eine Instance in derselben Availability Zone anfügen.

So erstellen Sie eine Netzwerkschnittstelle mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).
4. (Optional) Geben Sie unter Description (Beschreibung) einen aussagekräftigen Namen ein.

5. Wählen Sie für Subnet (Subnetz) ein Subnetz aus. Die in den nachfolgenden Schritten verfügbaren Optionen ändern sich je nach ausgewähltem Subnetztyp (nur IPv4, nur IPv6 oder Dual-Stack (IPv4 und IPv6)).
6. Führen Sie für Private IPv4 address (Private IPv4-Adresse) einen der folgenden Schritte aus:
   - Wählen Sie Auto-assign (Automatisch zuweisen), um Amazon EC2 zu erlauben eine IPv4-Adresse aus dem Subnetz auszuwählen.
   - Wählen Sie Custom (Benutzerdefiniert) und geben Sie eine IPv4-Adresse ein, die Sie aus dem Subnetz auswählen.
7. (Nur Subnetze mit IPv6-Adressen) Für IPv6-Adresse, führen Sie einen der folgenden Schritte aus:
   - Wählen Sie None (Kein), wenn Sie der Netzwerkschnittstelle keine IPv6-Adresse zuweisen möchten.
   - Wählen Sie Auto-assign (Automatisch zuweisen) um Amazon EC2 zu erlauben, eine IPv6-Adresse aus dem Subnetz auszuwählen.
   - Wählen Sie Custom (Benutzerdefiniert) und geben Sie eine IPv6-Adresse ein, die Sie aus dem Subnetz auswählen.
8. (Optional) Wenn Sie eine Netzwerkschnittstelle in einem Dual-Stack- oder Nur-IPv6-Subnetz erstellen, haben Sie die Option Primäre IPv6-IP zuzuweisen. Dadurch wird der Netzwerkschnittstelle eine primäre globale IPv6-Unicast-Adresse (GUA) zugewiesen. Durch die Zuweisung einer primären IPv6-Adresse können Sie eine Unterbrechung des Datenverkehrs zu Instances oder ENIs vermeiden. Wählen Sie Aktivieren, wenn die Instance, an die diese ENI angehängt wird, darauf angewiesen ist, dass sich ihre IPv6-Adresse nicht ändert. AWS weist automatisch eine IPv6-Adresse, die der mit Ihrer Instance verbundenen ENI zugeordnet ist, als primäre IPv6-Adresse zu. Sobald Sie eine IPv6-GUA-Adresse als primäre IPv6-Adresse aktiviert haben, können Sie sie nicht mehr deaktivieren. Wenn Sie eine IPv6-GUA-Adresse als primäre IPv6-Adresse aktivieren, wird die erste IPv6-GUA zur primären IPv6-Adresse gemacht, bis die Instance beendet oder die Netzwerkschnittstelle getrennt wird. Wenn Ihrer Instance mehrere IPv6-Adressen mit einer angefügten ENI zugeordnet sind und Sie eine primäre IPv6-Adresse aktivieren, wird die erste IPv6-GUA-Adresse, die der ENI zugeordnet ist, zur primären IPv6-Adresse.
9. (Optional) So erstellen Sie ein Elastic Fabric Adapter, wählen Sie Elastic Fabric Adapter, Aktivieren.
10. (Optional) Ändern Sie unter Erweiterte Einstellungen für Timeout für Nachverfolgung von Leerlaufverbindungen die standardmäßigen Timeouts für Leerlaufverbindungen. Weitere

Informationen zu diesen Optionen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

- Timeout für bestehende TCP-Verbindungen: Timeout (in Sekunden) für bestehende TCP-Verbindungen im Leerlauf. Min: 60 Sekunden. Max: 432 000 Sekunden (fünf Tage). Standard: 432 000 Sekunden. Empfohlen: Weniger als 432 000 Sekunden.
- UDP-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, bei denen Datenverkehr nur in eine Richtung oder nur in einer einzelnen Anforderung-Antwort-Transaktion übermittelt wurde. Min: 30 Sekunden. Max: 60 Sekunden. Standard: 30 Sekunden.
- UDP-Stream-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, die als Streams klassifiziert sind, bei denen mehr als eine Anforderung-Antwort-Transaktion stattgefunden hat. Min: 60 Sekunden. Max: 180 Sekunden (3 Minuten) Standard: 180 Sekunden.

11. Wählen Sie unter Security groups (Sicherheitsgruppen) eine oder mehrere Sicherheitsgruppen aus.
12. (Optional) Wählen Sie für jeden Tag (Markierung) Neuen Tag (Markierung) hinzufügen und geben Sie einen Tag (Markierung)-Schlüssel und einen optionalen Tag (Markierung)-Wert ein.
13. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).

So erstellen Sie eine Netzwerkschnittstelle mithilfe der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- create-network-interface (AWS CLI)
- New-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Anzeigen von Details zu einer Netzwerkschnittstelle

Sie können alle Netzwerkschnittstellen in Ihrem Konto anzeigen.

So beschreiben Sie eine Netzwerkschnittstelle mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.

3. Um die Detailseite für eine Netzwerkschnittstelle anzuzeigen, wählen Sie die ID der Netzwerkschnittstelle aus. Um Informationen anzuzeigen, ohne die Seite Netzwerkschnittstellen zu verlassen, aktivieren Sie alternativ das Kontrollkästchen für die Netzwerkschnittstelle.

So beschreiben Sie eine Netzwerkschnittstelle mithilfe der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

So beschreiben Sie ein Netzwerkschnittstellenattribut mithilfe der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-network-interface-attribute (AWS CLI)
- Get-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Zuordnen einer Netzwerkschnittstelle zu einer Instance

Sie können eine Netzwerkschnittstelle an eine beliebige Instance in derselben Availability Zone wie die Netzwerkschnittstelle anhängen, indem Sie entweder die Seite Instances oder Netzwerkschnittstellen der Amazon-EC2-Konsole verwenden. Alternativ können Sie beim Starten einer Instance eine vorhandene Netzwerkschnittstelle anhängen.

> **Important**
>
> Wenn Sie bei EC2-Instances in einem reinen IPv6-Subnetz eine sekundäre Netzwerkschnittstelle an die Instance anschließen, wird der private DNS-Hostname der zweiten Netzwerkschnittstelle an die erste IPv6-Adresse auf der ersten Netzwerkschnittstelle der Instance aufgelöst. Weitere Informationen zu privaten DNS-Hostnamen für EC2-Instances finden Sie unter Hostnamentypen für Amazon-EC2-Instances.

Wenn die öffentliche IPv4-Adresse auf Ihrer Instance freigegeben wird, erhält sie keine neue Adresse, falls mehr als eine Netzwerkschnittstelle an die Instance angefügt ist. Weitere Informationen zum Verhalten von öffentlichen IPv4-Adressen erhalten Sie unter Öffentliche IPv4-Adressen.

Instances page

So fügen Sie über die Seite Instances eine Netzwerkschnittstelle an eine Instance an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Aktivieren Sie das Kontrollkästchen für die Instance.
4. Wählen Sie Aktionen, Netzwerk, Netzwerkschnittstelle, anhängen.
5. Wählen Sie eine VPC aus. Wenn Sie der Instance eine sekundäre Netzwerkschnittstelle hinzufügen, kann sich die Netzwerkschnittstelle in derselben VPC wie Ihre Instance oder in einer anderen VPC befinden, die Sie besitzen (sofern sich die Netzwerkschnittstelle in einem Subnetz befindet, das sich in derselben Availability Zone wie Ihre Instance befindet). Dadurch können Sie VPC-übergreifend mehrfach vernetzte Instances mit unterschiedlichen Netzwerk- und Sicherheitskonfigurationen erstellen.
6. Wählen Sie eine Netzwerkschnittstelle aus. Wenn die Instance mehrere Netzwerkkarten unterstützt, können Sie eine Netzwerkkarte wählen.
7. Wählen Sie Attach (Anfügen) aus.

Network Interfaces page

So fügen Sie über die Seite Network Interfaces eine Netzwerkschnittstelle an eine Instance an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Wählen Sie Actions (Aktionen) und Attach (Anfügen).
5. Wählen einer Instance Wenn die Instance mehrere Netzwerkkarten unterstützt, können Sie eine Netzwerkkarte wählen.
6. Wählen Sie Attach (Anfügen) aus.

So fügen Sie mithilfe der Befehlszeile eine Netzwerkschnittstelle an eine Instance an

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

> **Note**
>
> Sie können eine Netzwerkschnittstelle, die sich in einer anderen VPC (aber in derselben Availability Zone) befindet, mit dem Befehl AWS CLI attach-network-interface an eine Instance anhängen. Sie können dies nicht mit dem tun. AWS Management Console

- attach-network-interface (AWS CLI)
- Add-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Trennen einer Netzwerkschnittstelle von einer Instance

Sie können eine sekundäre Netzwerkschnittstelle, die einer EC2-Instance angefügt ist, jederzeit über die Seite Instances (Instances) oder Network Interfaces (Netzwerkschnittstellen) der Amazon EC2-Konsole trennen.

Wenn Sie versuchen, eine Netzwerkschnittstelle, die mit einer Ressource verbunden ist, von einem anderen Dienst zu trennen, z. B. einem Elastic Load Balancing Load Balancer, einer Lambda-Funktion WorkSpace, einem oder einem NAT-Gateway, erhalten Sie die Fehlermeldung, dass Sie nicht berechtigt sind, auf die Ressource zuzugreifen. Um herauszufinden, welcher Service die mit einer Netzwerkschnittstelle verbundene Ressource erstellt hat, überprüfen Sie die Beschreibung der Netzwerkschnittstelle. Wenn Sie die Ressource löschen, wird ihre Netzwerkschnittstelle gelöscht.

Instances page

So trennen Sie eine Netzwerkschnittstelle von einer Instance über die Seite „Instances“

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Aktivieren Sie das Kontrollkästchen für die Instance. Überprüfen Sie den Abschnitt Netzwerk interfaces (Netzwerkschnittstellen) des Reiters Networking (Netzwerk), um zu überprüfen, ob die Netzwerkschnittstelle als sekundäre Netzwerkschnittstelle mit einer Instance verbunden ist.

4. Wählen Sie Aktionen, Netzwerk, Netzwerkschnittstelle trennen.
5. Wählen Sie die Netzwerkschnittstelle aus und klicken Sie auf Detach.

Network Interfaces page

So trennen Sie eine Netzwerkschnittstelle von einer Instance über die Seite „Network Interfaces“

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle. Überprüfen Sie den Abschnitt Instance details (Instance-Details) des Reiters Einzelheiten, um zu überprüfen, ob die Netzwerkschnittstelle als sekundäre Netzwerkschnittstelle mit einer Instance verbunden ist.
4. Wählen Sie Actions (Aktionen), Loslösen (Detach).
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Trennen.
6. Wenn die Netzwerkschnittstelle nicht von der Instance getrennt wird, können Sie die Option Force detachment (Trennung erzwingen), Aktivieren (Enable) auswählen und den Vorgang erneut ausführen. Wir empfehlen, die Loslösung nur als letzten Ausweg zu erzwingen. Das Erzwingen einer Trennung kann verhindern, dass Sie demselben Index eine andere Netzwerkschnittstelle anfügen, bis Sie die Instance neu starten. Es kann auch verhindern, dass die Instance-Metadaten das Trennen der Netzwerkschnittstelle widerspiegeln, bis Sie die Instance neu starten.

So trennen Sie eine Netzwerkschnittstelle mithilfe der Befehlszeile:

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- detach-network-interface (AWS CLI)
- Dismount-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Verwalten von IP-Adressen

Sie können die folgenden IP-Adressen für Ihre Netzwerkschnittstellen verwalten:

- Elastic IP-Adressen (eine pro privater IPv4-Adresse)

- IPv4-Adressen
- IPv6-Adressen
- Primäre IPv6-Adresse

So verwalten Sie die Elastic-IP-Adressen einer Netzwerkschnittstelle über die Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Um eine Elastic IP-Adresse zuzuordnen, gehen Sie wie folgt vor:
   a. Wählen Sie Aktionen, Adresse zuweisen aus.
   b. Wählen Sie unter Elastic IP-Adresse die Elastic IP-Adresse aus.
   c. Wählen Sie unter Private IPv4 address die private IPv4-Adresse aus, die Sie der Elastic IP-Adresse zuordnen möchten.
   d. (Optional) Wählen Sie Zulassen einer erneuten Verknüpfung der Elastic IP-Adresse, wenn die Netzwerkschnittstelle derzeit mit einer anderen Instance oder Netzwerkschnittstelle verknüpft ist.
   e. Wählen Sie Associate aus.
5. Um die Zuordnung einer Elastic IP-Adresse aufzuheben, gehen Sie folgendermaßen vor:
   a. Wählen Sie Actions, Disassociate address aus.
   b. Wählen Sie unter Öffentliche IP-Adresse die Elastic IP-Adresse aus.
   c. Wählen Sie Disassociate (Zuordnung aufheben) aus.

So verwalten Sie die IPv4- und IPv6-Adressen einer Netzwerkschnittstelle über die Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Wählen Sie die Netzwerkschnittstelle aus.
4. Wählen Sie Actions, Manage IP addresses (IP-Adressen verwalten) aus.
5. Erweitern Sie die Netzwerkschnittstelle.
6. Ändern Sie bei IPv4 addresses (IPv4-Adressen) die IP-Adressen nach Bedarf. Um eine IPv4-Adresse zuzuweisen, wählen Sie Neue IP-Adresse zuweisen und geben Sie dann eine

IPv4-Adresse aus dem Subnetzbereich an oder lassen Sie sich eine auswählen. AWS Um die Zuweisung einer IPv4-Adresse aufzuheben, wählen Sie neben der Adresse die Option Zuweisung aufheben.

7. Um einer Netzwerkschnittstelle eine öffentliche IPv4-Adresse zuzuweisen oder deren Zuweisung aufzuheben, wählen Sie Öffentliche IP automatisch zuweisen. Diese Option kann für jede Netzwerkschnittstelle aktiviert oder deaktiviert werden, gilt jedoch nur für die primäre Netzwerkschnittstelle (eth0).
8. Ändern Sie bei IPv6-Adressen die IP-Adressen nach Bedarf. Um eine IPv6-Adresse zuzuweisen, wählen Sie Neue IP-Adresse zuweisen und geben Sie dann eine IPv6-Adresse aus dem Subnetzbereich an oder lassen AWS Sie sich eine auswählen. Um die Zuweisung einer IPv6-Adresse aufzuheben, wählen Sie neben der Adresse die Option Zuweisung aufheben.
9. (Optional) Wenn Sie eine Netzwerkschnittstelle in einem Dual-Stack- oder Nur-IPv6-Subnetz ändern, haben Sie die Möglichkeit, Primäre IPv6-IP zuzuweisen. Durch die Zuweisung einer primären IPv6-Adresse können Sie eine Unterbrechung des Datenverkehrs zu Instances oder ENIs vermeiden. Wählen Sie Aktivieren, wenn die Instanz, an die diese ENI angehängt wird, darauf angewiesen ist, dass sich ihre IPv6-Adresse nicht ändert. AWS weist automatisch eine IPv6-Adresse, die der mit Ihrer Instance verbundenen ENI zugeordnet ist, als primäre IPv6-Adresse zu. Sobald Sie eine IPv6-GUA-Adresse als primäre IPv6-Adresse aktiviert haben, können Sie sie nicht mehr deaktivieren. Wenn Sie eine IPv6-GUA-Adresse als primäre IPv6-Adresse aktivieren, wird die erste IPv6-GUA zur primären IPv6-Adresse gemacht, bis die Instance beendet oder die Netzwerkschnittstelle getrennt wird. Wenn Ihrer Instance mehrere IPv6-Adressen mit einer angefügten ENI zugeordnet sind und Sie eine primäre IPv6-Adresse aktivieren, wird die erste IPv6-GUA-Adresse, die der ENI zugeordnet ist, zur primären IPv6-Adresse.
10. Wählen Sie Speichern.

Um die IP-Adressen einer Netzwerkschnittstelle mit dem zu verwalten AWS CLI

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- assign-ipv6-addresses
- associate-address
- disassociate-address
- unassign-ipv6-addresses

Um die IP-Adressen einer Netzwerkschnittstelle mit den Tools für Windows zu verwalten PowerShell

Verwenden Sie einen der folgenden Befehle.

- Register-EC2Address
- Register-EC2Ipv6 AddressList
- Unregister-EC2Address
- Unregister-EC2Ipv6 AddressList

Ändern der Netzwerkschnittstellenattribute

Sie können die folgenden Netzwerkschnittstellenattribute ändern:

- Beschreibung
- Sicherheitsgruppen
- Beim Beenden löschen
- Quell-/Zielprüfung

So ändern Sie die Beschreibung für eine Netzwerkschnittstelle mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Wählen Sie Actions (Aktionen), Change description (Beschreibung ändern).
5. Geben Sie unter Description (Beschreibung) eine Beschreibung für die Netzwerkschnittstelle ein.
6. Wählen Sie Save aus.

So ändern Sie die Sicherheitsgruppen für eine Netzwerkschnittstelle mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.

4. Wählen Sie Actions (Aktionen), Change security groups (Ändern von Sicherheitsgruppen).
5. Wählen Sie unter Zugehörige Sicherheitsgruppen die zu verwendenden Sicherheitsgruppen aus und wählen Sie dann Speichern.

   Die Sicherheitsgruppe und die Netzwerkschnittstelle müssen für dieselbe VPC erstellt werden. Um die Sicherheitsgruppe für Schnittstellen zu ändern, die im Besitz anderer Services sind, z. B. Elastic Load Balancing, nehmen Sie die Änderung über den betreffenden Service vor.

So ändern Sie das Beendigungsverhalten für eine Netzwerkschnittstelle mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Wählen Sie Aktionen, Beendigungsverhalten ändern .
5. Auswählen oder löschen Delete on Termination (Bei Beenden löschen), Aktivieren nach Bedarf, und wählen Sie dann Speichern.

So ändern Sie die Quell-/Zielprüfung für eine Netzwerkschnittstelle mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Wählen Sie Actions (Aktionen), Change source/dest check (Ändern Quell-/Zielprüfung).
5. Auswählen oder löschen Quell-/Zielprüfung, Aktivieren nach Bedarf, und wählen Sie dann Speichern.

So ändern Sie Timeouts für die Nachverfolgung von Leerlaufverbindungen:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
4. Wählen Sie Aktionen, Verbindungs-Timeout ändern.

5. Ändern Sie die Timeouts für die Nachverfolgung von Leerlaufverbindungen. Weitere Informationen zu diesen Optionen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

   - Timeout für bestehende TCP-Verbindungen: Timeout (in Sekunden) für bestehende TCP-Verbindungen im Leerlauf. Min: 60 Sekunden. Max: 432 000 Sekunden (fünf Tage). Standard: 432 000 Sekunden. Empfohlen: Weniger als 432 000 Sekunden.
   - UDP-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, bei denen Datenverkehr nur in eine Richtung oder nur in einer einzelnen Anforderung-Antwort-Transaktion übermittelt wurde. Min: 30 Sekunden. Max: 60 Sekunden. Standard: 30 Sekunden.
   - UDP-Stream-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, die als Streams klassifiziert sind, bei denen mehr als eine Anforderung-Antwort-Transaktion stattgefunden hat. Min: 60 Sekunden. Max: 180 Sekunden (3 Minuten) Standard: 180 Sekunden.

6. Wählen Sie Speichern.

So ändern Sie Netzwerkschnittstellenattribute über die Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- modify-network-interface-attribute (AWS CLI)
- Edit-EC2NetworkInterfaceAttribute (AWS Tools for Windows PowerShell)

Hinzufügen oder Bearbeiten von Tags (Markierungen)

Tags (Markierungen) sind Metadaten, die Sie einer Netzwerkschnittstelle hinzufügen können. Tags (Markierungen) sind privat und nur unter Ihrem Konto sichtbar. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert. Weitere Informationen zu Tags erhalten Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

So fügen Sie Tags (Markierungen) einer Netzwerkschnittstelle mithilfe der Konsole hinzu oder bearbeiten sie

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.

4. Wählen Sie in der Registerkarte Tags (Markierungen) die Option Manage tags (Tags (Markierungen) verwalten).
5. Wählen Sie für jeden zu erstellenden Tag (Markierung) Neuen Tag (Markierung) hinzufügen und geben Sie einen Schlüssel und einen optionalen Wert ein. Klicken Sie abschließend auf Save.

So fügen Sie Tags (Markierungen) einer Netzwerkschnittstelle mithilfe der Befehlszeile hinzu oder bearbeiten sie

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Löschen einer Netzwerkschnittstelle

Durch das Löschen einer Netzwerkschnittstelle werden alle mit der Schnittstelle verknüpften Attribute entfernt und sämtliche privaten IP-Adressen oder Elastic IP-Adressen freigegeben, damit diese von einer anderen Instance verwendet werden können.

Sie können eine verwendete Netzwerkschnittstelle nicht löschen. Zuerst müssen Sie die Netzwerkschnittstelle trennen.

So löschen Sie eine Netzwerkschnittstelle mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle und wählen Sie dann Actions (Aktionen), Delete (Löschen) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

So löschen Sie eine Netzwerkschnittstelle mithilfe der Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- delete-network-interface (AWS CLI)

- Remove-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Bewährte Methoden zum Konfigurieren von Netzwerkschnittstellen

- Sie können eine Netzwerkschnittstelle an eine Instance anfügen, während diese ausgeführt wird („Hot Attach“), wenn sie angehalten ist („Warm Attach“) oder wenn die Instance gestartet wird („Cold Attach“).
- Sie können sekundäre Netzwerkschnittstellen sowohl von ausgeführten als auch von angehaltenen Instances trennen. Die primäre Netzwerkschnittstelle können Sie jedoch nicht trennen.
- Sie können eine sekundäre Netzwerkschnittstelle zwischen Instances verschieben, solange sich die Instances in derselben Availability Zone und VPC, aber in verschiedenen Subnetzen befinden.
- Beim Starten einer Instance mithilfe der CLI, API oder eines SDK können Sie die primäre Netzwerkschnittstelle sowie zusätzliche Netzwerkschnittstellen angeben.
- Beim Starten einer Amazon Linux- oder Windows Server-Instance mit mehreren Netzwerkschnittstellen werden Schnittstellen, private IPv4-Adressen und Routing-Tabellen auf dem Betriebssystem der Instance automatisch konfiguriert.
- Ein „Warm Attach“ oder „Hot Attach“ einer zusätzlichen Netzwerkschnittstelle erfordert u. U., dass Sie die zweite Schnittstelle manuell aufrufen, die private IPv4-Adresse konfigurieren und die Routing-Tabelle entsprechend ändern. Instances, auf denen Amazon Linux oder Windows Server ausgeführt wird, erkennen den „Warm Attach“ oder „Hot Attach“ automatisch und konfigurieren sich selbst.
- Das Anfügen einer anderen Netzwerkschnittstelle an eine Instance (z. B. eine NIC-Teaming-Konfiguration) kann jedoch nicht genutzt werden, um die Netzwerkbandbreite zur bzw. von der doppelt vernetzten Instance zu erhöhen oder zu verdoppeln.
- Wenn Sie eine oder mehrere Netzwerkschnittstellen aus demselben Subnetz an eine Instance anfügen, kann es zu Netzwerkproblemen, z. B. asymmetrischem Routing, kommen. Verwenden Sie stattdessen möglichst eine sekundäre private IPv4-Adresse für die primäre Netzwerkschnittstelle.
- Windows-Instanzen — Wenn Sie mehrere Netzwerkschnittstellen verwenden, müssen Sie die Netzwerkschnittstellen so konfigurieren, dass sie statisches Routing verwenden.

Konfigurieren Sie Ihre Netzwerkschnittstelle mit ec2-net-utils für Amazon Linux 2

> **Note**
>
> Für AL2023 generiert das `amazon-ec2-net-utils` Paket schnittstellenspezifische Konfigurationen im Verzeichnis. `/run/systemd/network` Weitere Informationen finden Sie unter Networking-Service im Benutzerhandbuch zu Amazon Linux 2023.

Amazon Linux 2-AMIs können zusätzliche Skripts enthalten, die von AWS, so genannten ec2-net-utils, installiert wurden. Mit diesen Skripts kann die Konfiguration Ihrer Netzwerkschnittstellen optional automatisiert werden. Diese Skripts stehen nur für Amazon Linux 2 zur Verfügung.

Verwenden Sie den folgenden Befehl, um das Paket unter Amazon Linux 2 zu installieren, sofern dies noch nicht durchgeführt wurde. Führen Sie ein Update durch, wenn es installiert ist und zusätzliche Updates zur Verfügung stehen:

```
$ yum install ec2-net-utils
```

Die folgenden Komponenten sind Teil von ec2-net-utils:

udev-Regeln (`/etc/udev/rules.d`)

Identifiziert Netzwerkschnittstellen, wenn sie an eine laufende Instance angefügt, von ihr getrennt oder wieder angefügt werden, und stellt sicher, dass das Hotplug-Skript ausgeführt wird (`53-ec2-network-interfaces.rules`). Ordnet die MAC-Adresse einem Gerätenamen zu (`75-persistent-net-generator.rules`, der `70-persistent-net.rules` generiert).

Hotplug-Skript

Generiert eine Schnittstellenkonfigurationsdatei, die mit DHCP verwendet werden kann (`/etc/sysconfig/network-scripts/ifcfg-ethN`). Generiert zudem eine Routing-Konfigurationsdatei (`/etc/sysconfig/network-scripts/route-ethN`).

DHCP-Skript

Wenn die Netzwerkschnittstelle einen neuen DHCP-Lease erhält, fragt dieses Skript die Instance-Metadaten nach Elastic IP-Adressen ab. Für jede Elastic IP-Adresse fügt es der Datenbank eine Regel für die Routing-Richtlinien hinzu, um sicherzustellen, dass für ausgehenden Datenverkehr die richtige Netzwerkschnittstelle verwendet wird. Sie fügt der Netzwerkschnittstelle darüber hinaus jede private IP-Adresse als sekundäre Adresse hinzu.

ec2ifup ethN (`/usr/sbin/`)

Erweitert die Funktionalität des ifup-Standardbefehls. Nachdem dieses Skript die Konfigurationsdateien `ifcfg-ethN` und `route-ethN` neu geschrieben hat, führt es den Befehl ifup aus.

ec2ifdown ethN (`/usr/sbin/`)

Erweitert die Funktionalität des ifdown-Standardbefehls. Nachdem dieses Skript sämtliche Regeln für die Netzwerkschnittstelle aus der Datenbank für die Routing-Richtlinien entfernt hat, führt es den Befehl ifdown aus.

ec2ifscan (`/usr/sbin/`)

Führt eine Prüfung auf unkonfigurierte Netzwerkschnittstellen durch und konfiguriert sie.

Dieses Skript ist in der ersten Version von ec2-net-utils nicht verfügbar.

Verwenden Sie den folgenden Befehl, um sämtliche Konfigurationsdateien aufzulisten, die von ec2-net-utils generiert wurden:

```
$ ls -l /etc/sysconfig/network-scripts/*-eth?
```

Um die Automatisierung zu deaktivieren, können Sie `EC2SYNC=no` der entsprechenden Datei `ifcfg-ethN` hinzufügen. Verwenden Sie z. B. den folgenden Befehl, um die Automatisierung für die Schnittstelle eth1 zu deaktivieren:

```
$ sed -i -e 's/^EC2SYNC=yes/EC2SYNC=no/' /etc/sysconfig/network-scripts/ifcfg-eth1
```

Zum vollständigen Deaktivieren der Automatisierung können Sie das Paket mithilfe des folgenden Befehls entfernen:

```
$ yum remove ec2-net-utils
```

Szenarien für Netzwerkschnittstellen

In den folgenden Fällen ist das Anfügen von mehreren Netzwerkschnittstellen an eine Instance sinnvoll:

- Erstellen eines Verwaltungsnetzwerks

- Verwenden Sie Netzwerk- und Sicherheitsanwendungen in Ihrer Virtual Private Cloud (VPC).
- Erstellen von doppelt vernetzten Instances mit Workloads/Rollen in verschiedenen Subnetzen
- Erstellen von kostengünstigen Hochverfügbarkeitslösungen

Erstellen eines Verwaltungsnetzwerks

Das folgende Szenario beschreibt, wie Sie ein Verwaltungsnetzwerk mit Netzwerkschnittstellen erstellen können, wenn Sie folgende Kriterien und Einstellungen beachten (Image folgt).

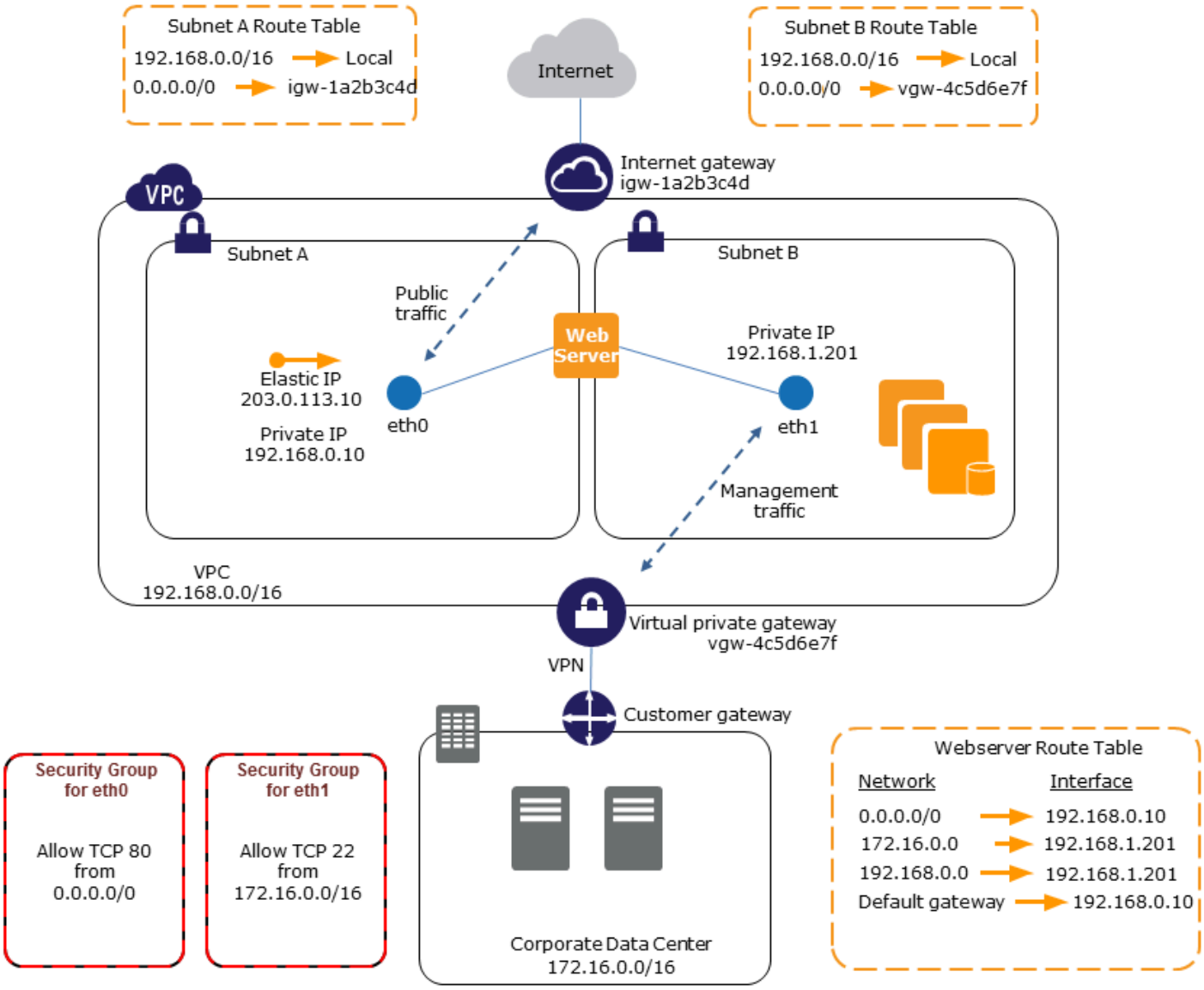
Kriterien

- Die primäre Netzwerkschnittstelle (eth0) der Instance verarbeitet den öffentlichen Datenverkehr.
- Die sekundäre Netzwerkschnittstelle der Instance (eth1) verarbeitet den Backend-Verwaltungsverkehr. Sie ist mit einem separaten Subnetz verbunden, das über restriktivere Zugriffskontrollen verfügt und sich in derselben Availability Zone (AZ) befindet wie die primäre Netzwerkschnittstelle.

Einstellungen

- Die primäre Netzwerkschnittstelle, welche sich möglicherweise hinter einem Load Balancer befindet, verfügt über eine zugeordnete Sicherheitsgruppe, welche den Zugriff auf den Server über das Internet ermöglicht. Erlauben Sie beispielsweise die TCP-Ports 80 und 443 vom `0.0.0.0/0` oder vom Load Balancer.
- Der sekundären Netzwerkschnittstelle ist eine Sicherheitsgruppe zugeordnet, die nur SSH-Zugriff ermöglicht und von einem der folgenden Standorte aus initiiert wird:
  - Ein zulässiger Bereich von IP-Adressen, entweder innerhalb der VPC oder aus dem Internet.
  - Ein privates Subnetz innerhalb derselben AZ wie die primäre Netzwerkschnittstelle.
  - Ein Virtual Private Gateway.

> **Note**
>
> Um Failover-Funktionen zu ermöglichen, sollten Sie eine sekundäre private IPv4-Adresse für eingehenden Datenverkehr auf einer Netzwerkschnittstelle verwenden. Bei einem Instance-Ausfall können Sie die Schnittstelle und/oder die sekundäre private IPv4-Adresse auf eine Standby-Instance verschieben.



Verwenden von Netzwerk- und Sicherheitsanwendungen in Ihrer VPC

Für einige Netzwerk- und Sicherheitsanwendungen (z. B. Load Balancer, Network Address Translation (NAT)-Server und Proxy-Server) wird die Konfiguration mit mehreren Netzwerkschnittstellen bevorzugt. Sie können sekundäre Netzwerkschnittstellen erstellen und an Instances anfügen, die diese Arten von Anwendungen ausführen und zusätzliche Schnittstellen mit ihren eigenen öffentlichen und privaten IP-Adressen, Sicherheitsgruppen und Quell-/Zielprüfung konfigurieren.

Erstellen von doppelt vernetzten Instances mit Workloads/Rollen in verschiedenen Subnetzen

Sie können eine Netzwerkschnittstelle auf jedem Ihrer Webserver einrichten, der mit einem Netzwerk der mittleren Schicht verbunden ist, in dem sich ein Anwendungsserver befindet. Der Anwendungsserver kann auch doppelt mit einem Backend-Netzwerk (Subnetz), in dem sich der Datenbankserver befindet, vernetzt sein. Statt Netzwerkpakete durch die doppelt vernetzten Instances weiterzuleiten, empfängt und verarbeitet jede doppelt vernetzte Instance Anfragen vom Frontend, stellt eine Verbindung zum Backend her und sendet die Anfragen dann an die Server im Backend-Netzwerk.

Erstellen von doppelt vernetzten Instances mit Workloads/Rollen in unterschiedlichen VPCs innerhalb desselben Kontos

Sie können eine EC2-Instance in einer VPC starten und eine sekundäre ENI von einer anderen VPC (jedoch in derselben Availability Zone) an die Instance anfügen. Dadurch können Sie VPC-übergreifend mehrfach vernetzte Instances mit unterschiedlichen Netzwerk- und Sicherheitskonfigurationen erstellen. Sie können keine mehrfach vernetzten Instanzen für mehrere VPCs mit unterschiedlichen Konten erstellen. AWS

In den folgenden Anwendungsfällen können Sie mehrfach vernetzte Instances VPC-übergreifend verwenden:

- Überwinden von CIDR-Überschneidungen zwischen zwei VPCs, die nicht miteinander verbunden werden können: Sie können ein sekundäres CIDR in einer VPC nutzen und einer Instance die Kommunikation über zwei sich nicht überschneidende IP-Bereiche ermöglichen.
- Mehrere VPCs innerhalb eines einzigen Kontos verbinden: Ermöglichen Sie die Kommunikation zwischen einzelnen Ressourcen, die normalerweise durch VPC-Grenzen getrennt wären.

Erstellen einer kostengünstigen Hochverfügbarkeitslösung

Wenn eine Ihrer Instances, die eine bestimmte Funktion erfüllt, ausfällt, besteht folgende Möglichkeit: Die zugehörige Netzwerkschnittstelle kann an eine Ersatz-Instance oder eine Hot Standby-Instance, die für die gleiche Funktion vorkonfiguriert wurde, angefügt werden, um den Service schnell wiederherzustellen. Sie können eine Netzwerkschnittstelle beispielsweise als primäre oder sekundäre Netzwerkschnittstelle für einen kritischen Service wie eine Datenbank- oder NAT-Instance verwenden. Wenn für die Instance ein Fehler auftritt (bzw. für den Code, der für Sie

ausgeführt wird), können Sie die Netzwerkschnittstelle an eine Hot Standby-Instance anfügen. Da die Schnittstelle ihre privaten IP-Adressen, Elastic IP-Adressen und MAC-Adressen beibehält, fließt der Netzwerkdatenverkehr zur Standby-Instance, sobald Sie die Netzwerkschnittstelle an die Ersatz-Instance angefügt haben. Zwischen dem Ausfall der Instance und dem Anfügen der Netzwerkschnittstelle an die Standby-Instance fällt die Verbindung für Benutzer kurzzeitig aus. Es sind jedoch keine Änderungen an der Routing-Tabelle oder an Ihrem DNS-Server erforderlich.

Vom Anforderer verwaltete Netzwerkschnittstellen

Eine vom Anforderer verwaltete Netzwerkschnittstelle ist eine Netzwerkschnittstelle, die ein AWS-Service in Ihrer VPC für Sie erstellt. Die Netzwerkschnittstelle ist mit einer Ressource für einen anderen Dienst verknüpft, z. B. einer DB-Instance von Amazon RDS, einem NAT-Gateway oder einem Schnittstellen-VPC-Endpunkt von AWS PrivateLink.

Überlegungen

- Sie können die vom Anforderer verwalteten Netzwerkschnittstellen in Ihrem Konto anzeigen. Sie können Tags hinzufügen oder entfernen, aber Sie können andere Eigenschaften einer vom Anforderer verwalteten Netzwerkschnittstelle nicht ändern.
- Sie können eine vom Anforderer verwaltete Netzwerkschnittstelle nicht trennen.
- Wenn Sie die Ressource löschen, die einer vom Anforderer verwalteten Netzwerkschnittstelle zugeordnet ist, wird die Netzwerkschnittstelle AWS-Service getrennt und gelöscht. Wenn der Service eine Netzwerkschnittstelle getrennt hat, sie jedoch nicht gelöscht hat, können Sie die getrennte Netzwerkschnittstelle löschen.

So zeigen Sie vom Anforderer verwaltete Netzwerkschnittstellen in der Konsole an

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich unter Network & Security (Netzwerk und Sicherheit) auf Network Interfaces (Netzwerkschnittstellen).
3. Wählen Sie die ID der Netzwerkschnittstelle aus, um die Detailseite zu öffnen.
4. Im Folgenden finden Sie die Schlüsselfelder, mit denen Sie den Zweck der Netzwerkschnittstelle ermitteln können:

    - Beschreibung: Eine Beschreibung vom AWS -Dienst, der die Schnittstelle erstellt hat. Zum Beispiel: „VPC Endpoint Interface vpce 089f2123488812123“.
    - Vom Anforderer verwaltet: Gibt an, ob die Netzwerkschnittstelle von verwaltet wird. AWS

- Anforderer-ID: Der Alias oder die AWS Konto-ID des Prinzipals oder Dienstes, der die Netzwerkschnittstelle erstellt hat. Wenn Sie die Netzwerkschnittstelle erstellt haben, ist dies Ihre AWS-Konto ID. Andernfalls hat ein anderer Prinzipal oder Dienst sie erstellt.

Um die vom Anforderer verwalteten Netzwerkschnittstellen anzuzeigen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl describe-network-interfaces folgendermaßen.

```
aws ec2 describe-network-interfaces --filters Name=requester-managed,Values=true
```

Im Folgenden finden Sie eine Beispielausgabe, die die Schlüsselfelder anzeigt, mit denen Sie den Zweck der Netzwerkschnittstelle ermitteln können: `Description` und `InterfaceType`.

```
{
     ...
    "Description": "VPC Endpoint Interface vpce-089f2123488812123",
    ...
    "InterfaceType": "vpc_endpoint",
    ...
    "NetworkInterfaceId": "eni-0d11e3ccd2c0e6c57",
    ...
    "RequesterId": "727180483921",
    "RequesterManaged": true,
    ...
}
```

Um vom Anforderer verwaltete Netzwerkschnittstellen mit den Tools für Windows anzuzeigen PowerShell

Verwenden Sie das Get-EC2NetworkInterfaceCmdlet wie folgt.

```
Get-EC2NetworkInterface -Filter @{ Name="requester-managed"; Values="true" }
```

Im Folgenden finden Sie eine Beispielausgabe, die die Schlüsselfelder anzeigt, mit denen Sie den Zweck der Netzwerkschnittstelle ermitteln können: `Description` und `InterfaceType`.

```
Description        : VPC Endpoint Interface vpce-089f2123488812123
...
InterfaceType      : vpc_endpoint
```

```
...
NetworkInterfaceId : eni-0d11e3ccd2c0e6c57
...
RequesterId        : 727180483921
RequesterManaged   : True
...
```

Zuweisen von Präfixen zu Amazon EC2 Netzwerkschnittstellen

Sie können Ihren Netzwerkschnittstellen einen privaten IPv4- oder IPv6-CIDR-Bereich entweder automatisch oder manuell zuweisen. Durch das Zuweisen von Präfixen können Sie die Verwaltung von Anwendungen skalieren und vereinfachen, einschließlich Container- und Netzwerkanwendungen, für die mehrere IP-Adressen in einer Instance erforderlich sind. Weitere Informationen über IPv4- und IPv6-Adressen finden Sie unter IP-Adressierung von Amazon EC2-Instances.

Die folgenden Zuweisungs-Optionen sind verfügbar:

- Automatische Zuweisung — AWS wählt das Präfix aus dem IPv4- oder IPv6-CIDR-Block Ihres VPC-Subnetzes aus und weist es Ihrer Netzwerkschnittstelle zu.
- Manuelle Zuweisung — Sie geben das Präfix aus dem IPv4- oder IPv6-CIDR-Block Ihres VPC-Subnetzes an und AWS überprüfen, ob das Präfix nicht bereits anderen Ressourcen zugewiesen ist, bevor Sie es Ihrer Netzwerkschnittstelle zuweisen.

Die Zuweisung von Präfixen hat folgende Vorteile:

- Erhöhte IP-Adressen auf einer Netzwerkschnittstelle – Wenn Sie ein Präfix verwenden, weisen Sie im Gegensatz zu einzelnen IP-Adressen einen Block von IP-Adressen zu. Dadurch wird die Anzahl der IP-Adressen für eine Netzwerkschnittstelle erhöht.
- Vereinfachte VPC Verwaltung für Container – In Containeranwendungen benötigt jeder Container eine eindeutige IP-Adresse. Das Zuweisen von Präfixen zu Ihrer Instance vereinfacht die Verwaltung Ihrer VPCs, da Sie Container starten und beenden können, ohne Amazon EC2 APIs für individuelle IP-Zuweisungen aufrufen zu müssen.

Inhalt

Grundlagen zum Zuweisen von Präfixen

- Sie können neuen oder vorhandenen Netzwerkschnittstellen ein Präfix zuweisen.
- Wenn Sie Präfixe verwenden möchten, weisen Sie Ihrer Netzwerkschnittstelle ein Präfix zu, fügen die Netzwerkschnittstelle Ihrer Instance an und konfigurieren dann das Betriebssystem.
- Wenn Sie die Option zum Angeben eines Präfix auswählen, muss das Präfix folgende Anforderungen erfüllen:
  - Das IPv4-Präfix, das Sie angeben können, ist `/28`.
  - Das IPv6-Präfix, das Sie angeben können, ist `/80`.
  - Das Präfix befindet sich im Subnetz-CIDR der Netzwerkschnittstelle und überschneidet sich nicht mit anderen Präfixen oder IP-Adressen, die vorhandenen Ressourcen im Subnetz zugewiesen sind.
- Sie können der primären oder sekundären Netzwerkschnittstelle ein Präfix zuweisen.
- Sie können einer Netzwerkschnittstelle eine Elastic IP-Adresse zuweisen, deren ein Präfix zugewiesen ist.
- Sie können dem IP-Adressteil des zugewiesenen Präfix auch eine Elastic-IP-Adresse zuweisen.
- Wir lösen den privaten DNS-Hostname einer Instance zur privaten IPv4-Adresse auf.
- Wir weisen jede private IPv4-Adresse für eine Netzwerkschnittstelle, einschließlich der von Präfixen, mit den folgenden Formaten zu:
  - `us-east-1`-Region

    ```
    ip-private-ipv4-address.ec2.internal
    ```

  - Alle anderen Regionen

    ```
    ip-private-ipv4-address.region.compute.internal
    ```

Überlegungen und Grenzwerte für Präfixe

Berücksichtigen Sie Folgendes, wenn Sie Präfixe verwenden:

- Netzwerkschnittstellen mit Präfixen werden von Instances unterstützt, die auf dem Nitro-System basieren. AWS
- Präfixe für Netzwerkschnittstellen sind auf IPv6- und private IPv4-Adressen beschränkt.

- Die maximale Anzahl der IP-Adressen, die Sie einer Netzwerkschnittstelle zuweisen können, hängt vom Instance-Typ ab. Jedes Präfix, das Sie einer Netzwerkschnittstelle zuweisen, zählt als eine IP-Adresse. Zum Beispiel hat eine `c5.large`-Instance ein Limit von `10` IPv4-Adressen pro Netzwerkschnittstelle. Jede Netzwerkschnittstelle für diese Instance hat eine primäre IPv4-Adresse. Wenn eine Netzwerkschnittstelle keine sekundären IPv4-Adressen hat, können Sie der Netzwerkschnittstelle bis zu 9 Präfixe zuweisen. Für jede weitere IPv4-Adresse, die Sie einer Netzwerkschnittstelle zuweisen, können Sie der Netzwerkschnittstelle ein Präfix weniger zuweisen. Weitere Informationen finden Sie unter IP-Adressen pro Netzwerkschnittstelle pro Instance-Typ.
- Präfixe sind bei Quell-/Zielprüfungen enthalten.

Arbeiten mit Präfixen

Sie können wie folgt Präfixe für Ihre Netzwerkschnittstellen verwenden.

Aufgaben

- Präfixe während der Erstellung der Netzwerkschnittstelle zuweisen
- Zuweisen von Präfixen zu vorhandenen Netzwerkschnittstellen
- Konfigurieren Sie Ihr Betriebssystem für Netzwerkschnittstellen mit Präfixen
- Anzeigen der Präfixe, die Ihren Netzwerkschnittstellen zugewiesen sind
- Entfernen Sie Präfixe von Ihren Netzwerkschnittstellen

Präfixe während der Erstellung der Netzwerkschnittstelle zuweisen

Wenn Sie die automatische Zuweisungsoption verwenden, können Sie einen Block von IP-Adressen in Ihrem Subnetz reservieren. AWS wählt die Präfixe aus diesem Block aus. Weitere Informationen erhalten Sie unter Subnetz-CIDR-Reservierungen im Amazon VPC Benutzerhandbuch.

Nachdem Sie die Netzwerkschnittstelle erstellt haben, verwenden Sie den AWS CLI Befehl attach-network-interface, um die Netzwerkschnittstelle mit Ihrer Instance zu verbinden. Sie müssen Ihr Betriebssystem so konfigurieren, dass es mit Netzwerkschnittstellen mit Präfixen arbeitet. Weitere Informationen finden Sie unter Konfigurieren Sie Ihr Betriebssystem für Netzwerkschnittstellen mit Präfixen.

Aufgaben

- Automatische Präfixe während der Erstellung der Netzwerkschnittstelle zuweisen
- Zuweisen bestimmter Präfixe während der Erstellung der Netzwerkschnittstelle

Automatische Präfixe während der Erstellung der Netzwerkschnittstelle zuweisen

Sie können automatische Präfixe beim Erstellen der Netzwerkschnittstelle mit einer der folgenden Methoden zuweisen.

Console

So weisen Sie automatische Präfixe während der Erstellung der Netzwerkschnittstelle zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Network Interfaces (Netzwerkschnittstellen) und wählen Sie dann Netzwerkschnittstelle erstellen aus.
3. Geben Sie eine Beschreibung für die Netzwerkschnittstelle an, wählen Sie das Subnetz aus, in dem die Netzwerkschnittstelle erstellt werden soll, und konfigurieren Sie die privaten IPv4- und IPv6-Adressen.
4. Erweitern Sie Fortgeschrittene Einstellungen und:
   a. Um ein IPv4-Präfix automatisch zuzuweisen, wählen Sie für die IPv4-Präfixdelegierung die Automatische Zuweisungaus. Geben Sie dann für die Anzahl der IPv4-Präfixe die Anzahl der zuzuweisenden Präfixe an.
   b. Um automatisch ein IPv6-Präfix zur IPv6-Präfixdelegierung zuzuweisen, wählen Sie Automatische Zuweisung aus. Geben Sie dann für die Anzahl der IPv6-Präfixe die Anzahl der zuzuweisenden Präfixe an.

   > **Note**
   >
   > IPv6-Präfixdelegierung wird nur angezeigt, wenn das ausgewählte Subnetz für IPv6 aktiviert ist.
5. Wählen Sie die Sicherheitsgruppen aus, die der Netzwerkschnittstelle zugeordnet werden sollen, und weisen Sie ggf. Ressourcen-Tags zu.
6. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).

AWS CLI

So weisen Sie während der Erstellung der Netzwerkschnittstelle automatische IPv4-Präfixe zu

Verwenden Sie den create-network-interfaceBefehl und legen Sie `--ipv4-prefix-count` die Anzahl der Präfixe fest, die Sie zuweisen möchten. AWS AWS Weist im folgenden Beispiel ein Präfix zu. 1

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv4 automatic example" \
--ipv4-prefix-count 1
```

Beispielausgabe


```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv4 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:98:65:dd:18:47",
        "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.62",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.62"
            }
        ],
        "Ipv4Prefixes": [
            {
                "Ipv4Prefix": "10.0.0.208/28"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
```

```
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

So weisen Sie während der Erstellung der Netzwerkschnittstelle automatische IPv6-Präfixe zu

Verwenden Sie den create-network-interfaceBefehl und stellen Sie `--ipv6-prefix-count` die Anzahl der Präfixe ein, die Sie zuweisen AWS möchten. AWS Weist im folgenden Beispiel ein Präfix zu. 1

```
$ C:\> aws ec2 create-network-interface \
--subnet-id subnet-047cfed18eEXAMPLE \
--description "IPv6 automatic example" \
--ipv6-prefix-count 1
```

Beispielausgabe

```
{
    "NetworkInterface": {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv6 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
```

```
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```

Zuweisen bestimmter Präfixe während der Erstellung der Netzwerkschnittstelle

Sie können bestimmte Präfixe beim Erstellen der Netzwerkschnittstelle mit einer der folgenden Methoden zuweisen.

Console

So weisen Sie während der Erstellung der Netzwerkschnittstelle bestimmte Präfixe zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Network Interfaces (Netzwerkschnittstellen) und wählen Sie dann Netzwerkschnittstelle erstellen aus.
3. Geben Sie eine Beschreibung für die Netzwerkschnittstelle an, wählen Sie das Subnetz aus, in dem die Netzwerkschnittstelle erstellt werden soll, und konfigurieren Sie die privaten IPv4- und IPv6-Adressen.
4. Erweitern Sie Fortgeschrittene Einstellungen und:
    a. Um ein bestimmtes IPv4-Präfix zuzuweisen, geben Sie für die IPv4-Präfixdelegierung Benutzerdefiniert an. Wählen Sie dann Hinzufügen eines Präfix und geben Sie das zu verwendende Präfix ein.
    b. Um ein bestimmtes IPv6-Präfix zur IPv6-Präfixdelegierung zuzuweisen, wählen Sie Benutzerdefiniert aus. Wählen Sie dann Hinzufügen eines Präfix und geben Sie das zu verwendende Präfix ein.

> **Note**
>
> IPv6-Präfixdelegierung wird nur angezeigt, wenn das ausgewählte Subnetz für IPv6 aktiviert ist.

5. Wählen Sie die Sicherheitsgruppen aus, die der Netzwerkschnittstelle zugeordnet werden sollen, und weisen Sie ggf. Ressourcen-Tags zu.
6. Klicken Sie auf Create network interface (Netzwerkschnittstellen erstellen).

AWS CLI

So weisen Sie während der Erstellung der Netzwerkschnittstelle bestimmte IPv4-Präfixe zu

Verwenden Sie den create-network-interfaceBefehl und stellen Sie `--ipv4-prefixes` die Präfixe ein. AWS wählt IP-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR `10.0.0.208/28`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv4 manual example" \
    --ipv4-prefixes Ipv4Prefix=10.0.0.208/28
```

Beispielausgabe

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 manual example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
```

```
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateIpAddress": "10.0.0.62"
                }
            ],
            "Ipv4Prefixes": [
                {
                    "Ipv4Prefix": "10.0.0.208/28"
                }
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "pending",
            "SubnetId": "subnet-047cfed18eEXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    }
```

So weisen Sie während der Erstellung der Netzwerkschnittstelle bestimmte IPv6-Präfixe zu

Verwenden Sie den create-network-interfaceBefehl und stellen Sie `--ipv6-prefixes` die Präfixe ein. AWS wählt IP-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR `2600:1f13:fc2:a700:1768::/80`.

```
$ C:\> aws ec2 create-network-interface \
    --subnet-id subnet-047cfed18eEXAMPLE \
    --description "IPv6 manual example" \
    --ipv6-prefixes Ipv6Prefix=2600:1f13:fc2:a700:1768::/80
```

Beispielausgabe

```
{
        "NetworkInterface": {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv6 automatic example",
            "Groups": [
                {
```

```
                "GroupName": "default",
                "GroupId": "sg-044c2de2c4EXAMPLE"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
        ],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "pending",
        "SubnetId": "subnet-047cfed18eEXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b21EXAMPLE"
    }
}
```


Zuweisen von Präfixen zu vorhandenen Netzwerkschnittstellen

Nachdem Sie die Präfixe zugewiesen haben, verwenden Sie den attach-network-interface AWS CLI Befehl, um die Netzwerkschnittstelle mit Ihrer Instance zu verbinden. Sie müssen Ihr Betriebssystem so konfigurieren, dass es mit Netzwerkschnittstellen mit Präfixen arbeitet. Weitere Informationen finden Sie unter Konfigurieren Sie Ihr Betriebssystem für Netzwerkschnittstellen mit Präfixen.

Aufgaben

- Zuweisen von automatischen Präfixen zu einer vorhandenen Netzwerkschnittstelle
- Zuweisen bestimmter Präfixe zu einer vorhandenen Netzwerkschnittstelle

Zuweisen von automatischen Präfixen zu einer vorhandenen Netzwerkschnittstelle

Mit einer der folgenden Methoden können Sie einer vorhandenen Netzwerkschnittstelle automatische Präfixe zuweisen.

Console

So weisen Sie einer vorhandenen Netzwerkschnittstelle automatische Präfixe zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie die Netzwerkschnittstelle aus, der Sie die Präfixe zuweisen möchten, und wählen Sie Aktionen, Präfixe verwaltenaus.
4. Um ein IPv4-Präfix automatisch zuzuweisen, wählen Sie für die IPv4-Präfixdelegierung die Automatische Zuweisungaus. Geben Sie dann für die Anzahl der IPv4-Präfixe die Anzahl der zuzuweisenden Präfixe an.
5. Um automatisch ein IPv6-Präfix zur IPv6-Präfixdelegierung zuzuweisen, wählen Sie Automatische Zuweisung aus. Geben Sie dann für die Anzahl der IPv6-Präfixe die Anzahl der zuzuweisenden Präfixe an.

   > **Note**
   >
   > IPv6-Präfixdelegierung wird nur angezeigt, wenn das ausgewählte Subnetz für IPv6 aktiviert ist.

6. Wählen Sie Speichern.

AWS CLI

Sie können den Befehl assign-ipv6-addresses nutzen, um IPv6-Präfixe zuzuweisen, und den Befehl assign-private-ip-addresses, um vorhandenen Netzwerkschnittstellen IPv4-Präfixe zuzuweisen.

So weisen Sie einer vorhandenen Netzwerkschnittstelle automatische IPv4-Präfixe zu

Verwenden Sie den assign-private-ip-addressesBefehl und legen Sie `--ipv4-prefix-count` die Anzahl der Präfixe fest, die Sie zuweisen AWS möchten. AWS Weist im folgenden Beispiel ein 1 IPv4-Präfix zu.

```
$ C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefix-count 1
```

Beispielausgabe

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
        {
            "Ipv4Prefix": "10.0.0.176/28"
        }
    ]
}
```

So weisen Sie einer vorhandenen Netzwerkschnittstelle automatische IPv6-Präfixe zu

Verwenden Sie den Befehl assign-ipv6-addresses und stellen Sie ihn auf die Anzahl der Präfixe ein`--ipv6-prefix-count`, die Sie zuweisen möchten. AWS Weist im folgenden Beispiel ein IPv6-Präfix zu. AWS 1

```
$ C:\> aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix-count 1
```

Beispielausgabe

```
{
    "AssignedIpv6Prefixes": [
        "2600:1f13:fc2:a700:18bb::/80"
    ],
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE"
}
```

Zuweisen bestimmter Präfixe zu einer vorhandenen Netzwerkschnittstelle

Mit einer der folgenden Methoden können Sie einer vorhandenen Netzwerkschnittstelle bestimmte Präfixe zuweisen.

Console

So weisen Sie einer vorhandenen Netzwerkschnittstelle bestimmte Präfixe zu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie die Netzwerkschnittstelle aus, der Sie die Präfixe zuweisen möchten, und wählen Sie Aktionen, Präfixe verwaltenaus.
4. Um ein bestimmtes IPv4-Präfix zuzuweisen, geben Sie für die IPv4-Präfixdelegierung Benutzerdefiniert an. Wählen Sie dann Hinzufügen eines Präfix und geben Sie das zu verwendende Präfix ein.
5. Um ein bestimmtes IPv6-Präfix zur IPv6-Präfixdelegierung zuzuweisen, wählen Sie Benutzerdefiniert aus. Wählen Sie dann Hinzufügen eines Präfix und geben Sie das zu verwendende Präfix ein.

   > **Note**
   >
   > IPv6-Präfixdelegierung wird nur angezeigt, wenn das ausgewählte Subnetz für IPv6 aktiviert ist.

6. Wählen Sie Speichern.

AWS CLI

Zuweisen bestimmter IPv4-Präfixe zu einer vorhandenen Netzwerkschnittstelle

Verwenden Sie den assign-private-ip-addressesBefehl und setzen Sie ihn `--ipv4-prefixes` auf das Präfix. AWS wählt IPv4-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR `10.0.0.208/28`.

```
$ C:\> aws ec2 assign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.208/28
```

Beispielausgabe

```
{
    "NetworkInterfaceId": "eni-081fbb4095EXAMPLE",
    "AssignedIpv4Prefixes": [
```

```
        {
            "Ipv4Prefix": "10.0.0.208/28"
        }
    ]
}
```

Zuweisen bestimmter IPv6-Präfixe zu einer vorhandenen Netzwerkschnittstelle

Verwenden Sie den Befehl assign-ipv6-addresses und setzen Sie ihn auf das Präfix. `--ipv6-prefixes` AWS wählt IPv6-Adressen aus diesem Bereich aus. Im folgenden Beispiel lautet das Präfix-CIDR `2600:1f13:fc2:a700:18bb::/80`.

```
$ C:\> aws ec2 assign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefixes 2600:1f13:fc2:a700:18bb::/80
```

Beispielausgabe

```
{
    "NetworkInterfaceId": "eni-00d577338cEXAMPLE",
    "AssignedIpv6Prefixes": [
        {
            "Ipv6Prefix": "2600:1f13:fc2:a700:18bb::/80"
        }
    ]
}
```

Konfigurieren Sie Ihr Betriebssystem für Netzwerkschnittstellen mit Präfixen

Amazon Linux-AMIs können zusätzliche Skripts enthalten, die von installiert wurden AWS, bekannt als`ec2-net-utils`. Mit diesen Skripts kann die Konfiguration Ihrer Netzwerkschnittstellen optional automatisiert werden. Diese Skripts stehen nur für Amazon Linux zur Verfügung.

Wenn Sie Amazon Linux nicht verwenden, können Sie ein Container Network Interface (CNI) für das Kubernetes-Plug-in verwenden oder `dockerd`, wenn Sie Docker verwenden, um Ihre Container zu verwalten.

Anzeigen der Präfixe, die Ihren Netzwerkschnittstellen zugewiesen sind

Sie können die Präfixe, die Ihren Netzwerkschnittstellen zugewiesen wurden, mit einer der folgenden Methoden anzeigen.

Console

So zeigen Sie die automatischen Präfixe an, die einer vorhandenen Netzwerkschnittstelle zugewiesen sind

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie die Netzwerkschnittstelle aus, deren Präfixe Sie anzeigen möchten, und wählen Sie die Registerkarte Details.
4. Die IPv4-Präfixdelegierung listet die zugewiesenen IPv4-Präfixe auf und die IPv6-Präfixdelegierung listet die zugewiesenen IPv6-Präfixe auf.

AWS CLI

Sie können den describe-network-interfaces AWS CLI Befehl verwenden, um die Präfixe anzuzeigen, die Ihren Netzwerkschnittstellen zugewiesen sind.

```
$ C:\> aws ec2 describe-network-interfaces
```

Beispielausgabe

```
{
    "NetworkInterfaces": [
        {
            "AvailabilityZone": "us-west-2a",
            "Description": "IPv4 automatic example",
            "Groups": [
                {
                    "GroupName": "default",
                    "GroupId": "sg-044c2de2c4EXAMPLE"
                }
            ],
            "InterfaceType": "interface",
            "Ipv6Addresses": [],
            "MacAddress": "02:98:65:dd:18:47",
            "NetworkInterfaceId": "eni-02b80b4668EXAMPLE",
            "OwnerId": "123456789012",
            "PrivateIpAddress": "10.0.0.62",
            "PrivateIpAddresses": [
                {
```

```
                "Primary": true,
                "PrivateIpAddress": "10.0.0.62"
            }
        ],
        "Ipv4Prefixes": [
            {
                "Ipv4Prefix": "10.0.0.208/28"
            }
        ],
        "Ipv6Prefixes": [],
        "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
        "RequesterManaged": false,
        "SourceDestCheck": true,
        "Status": "available",
        "SubnetId": "subnet-05eef9fb78EXAMPLE",
        "TagSet": [],
        "VpcId": "vpc-0e12f52b2146bf252"
    },
    {
        "AvailabilityZone": "us-west-2a",
        "Description": "IPv6 automatic example",
        "Groups": [
            {
                "GroupName": "default",
                "GroupId": "sg-044c2de2c411c91b5"
            }
        ],
        "InterfaceType": "interface",
        "Ipv6Addresses": [],
        "MacAddress": "02:bb:e4:31:fe:09",
        "NetworkInterfaceId": "eni-006edbcfa4EXAMPLE",
        "OwnerId": "123456789012",
        "PrivateIpAddress": "10.0.0.73",
        "PrivateIpAddresses": [
            {
                "Primary": true,
                "PrivateIpAddress": "10.0.0.73"
            }
        ],
        "Ipv4Prefixes": [],
        "Ipv6Prefixes": [
            {
                "Ipv6Prefix": "2600:1f13:fc2:a700:1768::/80"
            }
```

```
            ],
            "RequesterId": "AIDAIV5AJI5LXF5XXDPCO",
            "RequesterManaged": false,
            "SourceDestCheck": true,
            "Status": "available",
            "SubnetId": "subnet-05eef9fb78EXAMPLE",
            "TagSet": [],
            "VpcId": "vpc-0e12f52b21EXAMPLE"
        }
    ]
}
```

Entfernen Sie Präfixe von Ihren Netzwerkschnittstellen

Sie können Präfixe aus Ihren Netzwerkschnittstellen mit einer der folgenden Methoden entfernen.

Console

So entfernen Sie die Präfixe einer Netzwerkschnittstelle

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie die Netzwerkschnittstelle aus, aus der die Präfixe entfernt werden sollen, und wählen Sie Aktionen, Präfixe verwalten aus.
4. Führen Sie eine der folgenden Aktionen aus:
   - Um alle zugewiesenen Präfixe zu entfernen, wählen Sie für IPv4-Präfixdelegierung und IPv6-Präfixdelegierung Nicht zuweisen aus.
   - Um bestimmte zugewiesene Präfixe zu entfernen, wählen Sie für IPv4 prefix delegation (IPv4-Präfixdelegierung) oder IPv6 prefix delegation (IPv6-Präfixdelegierung) Custom (Benutzerdefiniert) und wählen Sie dann neben den Präfixen, die entfernt werden sollen, Unassign (Zuweisung aufheben).

> **Note**
>
> IPv6-Präfixdelegierung wird nur angezeigt, wenn das ausgewählte Subnetz für IPv6 aktiviert ist.

5. Wählen Sie Speichern.

AWS CLI

Sie können den Befehl unassign-ipv6-addresses nutzen, um IPv6-Präfixe zu entfernen und den Befehl unassign-private-ip-addresses, um IPv4-Präfixe aus Ihren vorhandenen Netzwerkschnittstellen zu entfernen.

So entfernen Sie IPv4-Präfixe aus einer Netzwerkschnittstelle

Verwenden Sie den Befehl unassign-private-ip-addresses und stellen Sie `--ipv4-prefix` auf die Adresse ein, die Sie entfernen möchten.

```
$ C:\> aws ec2 unassign-private-ip-addresses \
--network-interface-id eni-081fbb4095EXAMPLE \
--ipv4-prefixes 10.0.0.176/28
```

So entfernen Sie IPv6-Präfixe aus einer Netzwerkschnittstelle

Verwenden Sie den Befehl unassign-ipv6-addresses und stellen Sie `--ipv6-prefix` auf die Adresse ein, die Sie entfernen möchten.

```
$ C:\> aws ec2 unassign-ipv6-addresses \
--network-interface-id eni-00d577338cEXAMPLE \
--ipv6-prefix 2600:1f13:fc2:a700:18bb::/80
```

Netzwerkbandbreite für Amazon EC2-Instances

Spezifikationen der Instance-Bandbreite gelten sowohl für eingehenden als auch für ausgehenden Datenverkehr der Instance. Wenn eine Instance beispielsweise eine Bandbreite von bis zu 10 Gbit/s angibt, bedeutet dies, dass sie über eine Bandbreite von bis zu 10 Gbit/s für eingehenden Datenverkehr und bis zu 10 Gbit/s für ausgehenden Datenverkehr verfügt. Die für eine EC2-Instance verfügbare Netzwerkbandbreite hängt wie folgt von mehreren Faktoren ab.

Multi-Flow-Datenverkehr

Die Bandbreite für aggregierten Multiflow-Datenverkehr, der einer Instance zur Verfügung steht, hängt vom Ziel des Datenverkehrs ab.

- Innerhalb der Region – Der Datenverkehr kann die gesamte Netzwerkbandbreite nutzen, die der Instance zur Verfügung steht.
- Zu anderen Regionen, einem Internet-Gateway, Direct Connect oder lokalen Gateways (LGW) – Der Datenverkehr kann bis zu 50 % der Netzwerkbandbreite nutzen, die für eine Instance der aktuellen Generation mit mindestens 32 vCPUs verfügbar ist. Die Bandbreite für eine Instance der aktuellen Generation mit weniger als 32 vCPUs ist auf 5 Gbit/s begrenzt.

Single-Flow-Datenverkehr

Die Basisbandbreite für Single-Flow-Datenverkehr ist auf 5 Gbit/s begrenzt, wenn sich Instances nicht in der gleichen Cluster-Placement-Gruppe befinden. Um die Latenz zu verringern und die Single-Flow-Bandbreite zu erhöhen, versuchen Sie Folgendes:

- Verwenden Sie eine Cluster-Placement-Gruppe, um eine Bandbreite von bis zu 10 Gbit/s für Instances innerhalb derselben Platzierungsgruppe zu erreichen.
- Richten Sie mehrere Pfade zwischen zwei Endpunkten ein, um mit Multipath TCP (MPTCP) eine höhere Bandbreite zu erreichen.
- Konfigurieren Sie ENA Express für berechtigte Instances innerhalb desselben Subnetzes, um bis zu 25 Gbit/s zwischen diesen Instances zu erreichen.

Verfügbare Instance-Bandbreite

Die verfügbare Netzwerkbandbreite einer Instance hängt von der Anzahl der vCPUs ab, die sie besitzt. Eine `m5.8xlarge`-Instance verfügt beispielsweise über 32 vCPUs und 10 Gbit/s Netzwerkbandbreite und eine `m5.16xlarge`-Instance verfügt über 64 vCPUs und 20 Gbit/s Netzwerkbandbreite. Instances erreichen diese Bandbreite jedoch möglicherweise nicht, beispielsweise, wenn sie Netzwerkzuteilungen auf Instance-Ebene überschreiten, z. B. bei den Paketen pro Sekunde oder der Anzahl verfolgter Verbindungen. Wie viel der verfügbaren Bandbreite der Datenverkehr nutzen kann, hängt von der Anzahl der vCPUs und dem Ziel ab. Eine `m5.16xlarge`-Instance verfügt beispielsweise über 64 vCPUs, sodass der Datenverkehr zu einer anderen Instance in der Region die volle verfügbare Bandbreite (20 Gbit/s) nutzen kann. Der Datenverkehr zu einer anderen Instance in einer anderen Region kann jedoch nur 50 % der verfügbaren Bandbreite (10 Gbit/s) nutzen.

Typischerweise werden Instances mit 16 vCPUs oder weniger (Größe `4xlarge`und kleiner) als „bis“ zu einer bestimmten Bandbreite dokumentiert, z. B. „bis zu 10 Gbit/s“. Diese Instances

haben eine Basisbandbreite. Um zusätzlichen Bedarf zu decken, können sie einen Netzwerk-I/O-Guthabenmechanismus nutzen, der ihre Basisbandbreite übersteigt. Instances können Aufteilungsbandbreite für einen begrenzten Zeitraum verwenden, in der Regel zwischen 5 und 60 Minuten, abhängig von der Instancegröße.

Eine Instance erhält beim Start die maximale Anzahl von Netzwerk-I/O-Credits. Wenn die Instance ihre Netzwerk-I/O-Credits ausschöpft, kehrt sie zu ihrer Basisbandbreite zurück. Eine laufende Instance erhält Netzwerk-I/O-Credits, wenn sie weniger Netzwerkbandbreite benötigt als die Basisbandbreite. Eine gestoppte Instance erhält keine Netzwerk-I/O-Credits. Instance Burst basiert auf bestem Aufwand, selbst wenn für die Instance Credits verfügbar sind, da die Burstbandbreite eine gemeinsam genutzte Ressource ist.

Für ein- und ausgehenden Datenverkehr gibt es unterschiedliche Netzwerk-I/O-Credit-Buckets.

Basis- und Burst-Netzwerkleistung

Der Amazon EC2 Instance Types Guide beschreibt die Netzwerkleistung für jeden Instance-Typ sowie die Basis-Netzwerkbandbreite, die für Instances verfügbar ist, die Burst-Bandbreite verwenden können. Weitere Informationen finden Sie hier:

- Netzwerkspezifikationen — Allgemeiner Zweck
- Netzwerkspezifikationen — Für Rechenleistung optimiert
- Netzwerkspezifikationen — Speicheroptimiert
- Netzwerkspezifikationen — Speicheroptimiert
- Netzwerkspezifikationen — Beschleunigtes Rechnen
- Netzwerkspezifikationen — Hochleistungsrechnen
- Netzwerkspezifikationen — Vorgängergeneration

Um die Netzwerkleistung mit dem zu überprüfen AWS CLI

Sie können den AWS CLI Befehl describe-instance-types verwenden, um Informationen über einen Instance-Typ anzuzeigen. Im folgenden Beispiel werden Informationen zur Netzwerkleistung für alle C5-Instances angezeigt.

```
aws ec2 describe-instance-types --filters "Name=instance-type,Values=c5.*"
 --query "InstanceTypes[].[InstanceType, NetworkInfo.NetworkPerformance,
 NetworkInfo.NetworkCards[0].BaselineBandwidthInGbps]" --output table
```

```
-----------------------------------------
|           DescribeInstanceTypes           |
+--------------+--------------------+-------+
|  c5.4xlarge  |  Up to 10 Gigabit  |  5.0  |
|  c5.xlarge   |  Up to 10 Gigabit  |  1.25 |
|  c5.12xlarge |  12 Gigabit        |  12.0 |
|  c5.24xlarge |  25 Gigabit        |  25.0 |
|  c5.metal    |  25 Gigabit        |  25.0 |
|  c5.9xlarge  |  12 Gigabit        |  12.0 |
|  c5.2xlarge  |  Up to 10 Gigabit  |  2.5  |
|  c5.large    |  Up to 10 Gigabit  |  0.75 |
|  c5.18xlarge |  25 Gigabit        |  25.0 |
+--------------+--------------------+-------+
```

Überwachen der Instance-Bandbreite

Sie können CloudWatch Metriken verwenden, um die Netzwerkbandbreite der Instance und die gesendeten und empfangenen Pakete zu überwachen. Sie können die vom Elastic Network Adapter (ENA)-Treiber bereitgestellten Netzwerkleistungsmetriken verwenden, um zu beobachten, wenn Datenverkehr die Netzwerkzuteilungen überschreitet, die Amazon EC2 auf Instance-Ebene definiert.

Sie können konfigurieren, ob Amazon EC2 Metrikdaten für die Instance in Zeiträumen CloudWatch von einer Minute oder fünf Minuten sendet. Es ist möglich, dass die Netzwerkleistungsmetriken zeigen, dass eine zulässige Menge überschritten wurde und Pakete verworfen wurden, während dies bei den CloudWatch Instance-Metriken nicht der Fall ist. Dies kann passieren, wenn die Instance einen kurzen Anstieg der Nachfrage nach Netzwerkressourcen (bekannt als Microburst) hat, die CloudWatch Metriken aber nicht detailliert genug sind, um diese Mikrosekundenspitzen widerzuspiegeln.

Weitere Informationen

- Instance-Metriken
- Netzwerkleistungsmetriken

Verbessertes Networking auf Amazon EC2

Enhanced Networking verwendet Single Root I/O Virtualization (SR-IOV), um Hochleistungsnetzwerk-Funktionen in unterstützten Instance-Typen bereitzustellen. SR-IOV ist eine Methode zur Gerätevirtualisierung, die im Vergleich zu herkömmlichen virtualisierten Netzwerkschnittstellen

eine höhere I/O-Leistung bei niedrigerer CPU-Auslastung bietet. Die optimierte Netzwerkleistung ermöglicht eine größere Bandbreite, mehr Pakete pro Sekunde (PPS) und konstant niedrigere Latenzzeiten zwischen Instances. Für die Nutzung von Enhanced Networking fallen keine zusätzlichen Gebühren an.

Weitere Informationen zur unterstützten Netzwerkgeschwindigkeit für die einzelnen Instance-Typen finden Sie unter Amazon EC2-Instance-Typen.

Inhalt

Unterstützung von Enhanced Networking

Alle Instance-Typen der aktuellen Generation, mit Ausnahme von T2-Instances, unterstützen das Enhanced Networking.

Sie können das Enhanced Networking mit einem der folgenden Mechanismen aktivieren:

Elastic Network Adapter (ENA)

Der Elastic Network Adapter (ENA) unterstützt Netzwerkgeschwindigkeiten von bis zu 100 Gbit/s für unterstützte Instance-Typen.

Alle auf dem AWS Nitro System aufgebauten Instances verwenden ENA für erweiterte Netzwerke. Darüber hinaus unterstützen die folgenden Xen-Instance-Typen ENA: H1, G3, `m4.16xlarge`, P2, P3, P3dn und R4.

Weitere Informationen finden Sie unter Aktivieren Sie Enhanced Networking mit dem Elastic Network Adapter (ENA) auf Ihren EC2-Instances.

Intel 82599 Virtual Function-Schnittstelle (VF)

Die Intel 82599 Virtual Function-Schnittstelle unterstützt Netzwerkgeschwindigkeiten von bis zu 10 Gbit/s für unterstützte Instance-Typen.

Die folgenden Instance-Typen verwenden die Intel-82599-VF-Schnittstelle für erweiterte Netzwerke: C3, C4, D2, I2, M4 (ausgenommen m4.16xlarge) und R3.

Weitere Informationen finden Sie unter Aktivieren Sie Enhanced Networking mit der Intel 82599 VF-Schnittstelle auf Ihren EC2-Instances.

Aktivieren Sie Enhanced Networking mit dem Elastic Network Adapter (ENA) auf Ihren EC2-Instances

Amazon EC2 bietet optimierte Netzwerkfunktionen über den Elastic Network Adapter (ENA). Um Enhanced Networking nutzen zu können, müssen Sie das erforderliche ENA-Modul installieren und die ENA-Unterstützung aktivieren.

Inhalt

Voraussetzungen

Zur Vorbereitung für Enhanced Networking mit ENA sollten Sie Ihre Instance wie folgt einrichten:

- Starten Sie eine Instanz, die auf dem AWS Nitro System basiert.
- Überprüfen Sie, ob der Instance eine Verbindung zum Internet fehlt.
- Wenn Sie wichtige Daten auf der Instance gespeichert haben, die Sie erhalten möchten, sollten Sie diese Daten jetzt sichern, indem Sie ein AMI von Ihrer Instance erstellen. Die Aktualisierung

von Kernels und Kernel-Modulen sowie die Aktivierung des Attributs `enaSupport` kann dazu führen, dass Instances inkompatibel oder Betriebssysteme unerreichbar werden. Wenn Sie über ein aktuelles Backup verfügen, gehen die Daten nicht verloren, falls das geschieht.

- Linux-Instances — Starten Sie die Instance mit einer unterstützten Version des Linux-Kernels und einer unterstützten Distribution, sodass ENA Enhanced Networking automatisch für Ihre Instance aktiviert wird. Weitere Informationen finden Sie unter ENA Linux Kernel Driver Release Notes.
- Windows-Instanzen — Wenn auf der Instance Windows Server 2008 R2 SP1 ausgeführt wird, stellen Sie sicher, dass sie über das Update zur Unterstützung von SHA-2-Codesignaturen verfügt.
- Verwenden Sie AWS CloudShelldas AWS Management Console oder installieren und konfigurieren Sie das AWS CLIoder AWS Tools for Windows PowerShellauf einem beliebigen Computer Ihrer Wahl, vorzugsweise auf Ihrem lokalen Desktop oder Laptop. Weitere Informationen finden Sie unter Zugriff auf Amazon EC2 oder im AWS CloudShell -Benutzerhandbuch. Enhanced Networking kann nicht über die Amazon EC2-Konsole verwaltet werden.

Enhanced Networking-Leistung

Die folgende Dokumentation bietet eine Übersicht über die Netzwerkleistung für die Instance-Typen, die ENA Enhanced Networking unterstützen:

- Netzwerkspezifikationen für beschleunigte Recheninstanzen
- Netzwerkspezifikationen für rechenoptimierte Instanzen
- Netzwerkspezifikationen für Allzweckinstanzen
- Netzwerkspezifikationen für Hochleistungsverarbeitung
- Netzwerkspezifikationen für speicheroptimierte Instances
- Netzwerkspezifikationen für speicheroptimierte Instances

Linux-AMIs mit dem erforderlichen Modul

Die folgenden AMIs enthalten das erforderliche ENA-Modul und haben ENA-Unterstützung aktiviert:

- AL2023
- Amazon Linux 2
- Amazon-Linux-AMI 2018.03 und höher
- Ubuntu 14.04 oder höher mit `linux-aws`-Kernel

> **Note**
>
> AWS Graviton-basierte Instance-Typen erfordern Ubuntu 18.04 oder höher mit Kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 oder höher
- SUSE Linux Enterprise Server 12 SP2 oder höher
- CentOS 7.4.1708 oder höher
- FreeBSD 11.1 oder höher
- Debian GNU/Linux 9 oder höher

Um zu testen, ob Enhanced Networking bereits aktiviert ist, stellen Sie sicher, dass das `ena` Modul auf Ihrer Instance installiert ist und ob das `enaSupport` Attribut gesetzt ist. Wenn ja, ethtool -i eth*n* sollte der Befehl anzeigen, dass das Modul auf der Netzwerkschnittstelle verwendet wird.

Kernel-Modul (ena)

Verifizieren Sie, dass das `ena`-Modul installiert ist. Verwenden Sie dazu den Befehl modinfo, wie im folgenden Beispiel dargestellt.

```
[ec2-user ~]$ modinfo ena
filename:    /lib/modules/4.14.33-59.37.amzn2.x86_64/kernel/drivers/amazon/net/ena/
ena.ko
version:  1.5.0g
license:  GPL
description: Elastic Network Adapter (ENA)
author:   Amazon.com, Inc. or its affiliates
srcversion:  692C7C68B8A9001CB3F31D0
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
retpoline:   Y
intree:   Y
name:     ena
...
```

In der Amazon Linux-Instance ist das `ena` Modul installiert.

```
ubuntu:~$ modinfo ena
ERROR: modinfo: could not find module ena
```

In der Ubuntu-Instanz ist das Modul nicht installiert, sodass Sie es zuerst installieren müssen. Weitere Informationen finden Sie unter Ubuntu.

Testen, ob Enhanced Networking aktiviert ist

Sie können testen, ob Enhanced Networking in Ihren Instances oder Ihren AMIs aktiviert ist.

Instance-Attribut

Sie prüfen, ob in einer Instance das `enaSupport`-Attribut für Enhanced Networking gesetzt wurde, indem Sie einen der folgenden Befehle verwenden. Wenn das Attribut gesetzt wurde, wird als Antwort „true” ausgegeben.

- describe-instances (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instances --instance-ids instance_id --query
 "Reservations[].Instances[].EnaSupport"
```

- Get-EC2Instance(Tools für Windows PowerShell)

```
(Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
```

Bildattribut

Sie prüfen, ob in einem AMI das `enaSupport`-Attribut für Enhanced Networking bereits gesetzt wurde, indem Sie einen der folgenden Befehle verwenden. Wenn das Attribut gesetzt wurde, wird als Antwort „true” ausgegeben.

- describe-images (AWS CLI/AWS CloudShell)

```
aws ec2 describe-images --image-id ami_id --query "Images[].EnaSupport"
```

- Get-EC2Image(Tools für Windows PowerShell)

```
(Get-EC2Image -ImageId ami_id).EnaSupport
```

Treiber für die Linux-Netzwerkschnittstelle

Prüfen Sie mit dem folgenden Befehl, ob das Modul `ena` aktuell an einer bestimmten Schnittstelle verwendet wird; setzen Sie dabei den Namen der Schnittstelle ein, die Sie überprüfen möchten. Wenn Sie eine einzige Schnittstelle verwenden (der Standard), lautet der Name `eth0`. Wenn das Betriebssystem vorhersagbare Netzwerknamen unterstützt, könnte der Name `ens5` lauten.

Im folgenden Beispiel wird das `ena`-Modul nicht geladen, da als Treiber `vif` angezeigt wird.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

In diesem Beispiel wurde das `ena`-Modul bereits geladen und liegt in der empfohlenen Mindestversion vor. In dieser Instance wurde Enhanced Networking richtig konfiguriert.

```
[ec2-user ~]$ ethtool -i eth0
driver: ena
version: 1.5.0g
firmware-version:
expansion-rom-version:
bus-info: 0000:00:05.0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

Aktivieren von Enhanced Networking auf Ihrer Instance

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instanz ab.

Amazon Linux

Amazon Linux 2 und die neuesten Versionen von Amazon Linux AMI enthalten das Modul, das für Enhanced Networking erforderlich ist, wenn ENA installiert und die ENA-Unterstützung aktiviert ist. Wenn Sie eine Instance mit einer HVM-Version von Amazon Linux auf einem unterstützten Instance-Typ starten, ist Enhanced Networking für Ihre Instance bereits aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist.

Wenn Sie Ihre Instance aus einem älteren Amazon Linux AMI gestartet haben und Enhanced Networking noch nicht aktiviert wurde, gehen Sie wie folgt vor, um die optimierte Netzwerkleistung zu aktivieren.

Aktivieren von Enhanced Networking im Amazon Linux AMI

1. Verbinden Sie sich mit der Instance.
2. Führen Sie den folgenden Befehl in der Instance aus, um die Instance mit dem aktuellen Kernel und den aktuellen Kernel-Modulen einschließlich `ena` zu aktualisieren:

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. Starten Sie die Instance von Ihrem lokalen Computer aus neu, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: reboot-instances (AWS CLI), Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Stellen Sie erneut eine Verbindung mit der Instance her und prüfen Sie, ob das `ena`-Modul installiert wurde und in der empfohlenen Mindestversion vorliegt, indem Sie den Befehl modinfo ena aus dem Abschnitt Testen, ob Enhanced Networking aktiviert ist verwenden.
5. [EBS-gestützte Instance] Halten Sie die Instance von Ihrem lokalen Computer aus an, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instanz von verwaltet wird AWS OpsWorks, sollten Sie die Instanz in der AWS OpsWorks Konsole beenden, damit der Instanzstatus synchron bleibt.

   [In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Gehen Sie stattdessen wie folgt vor: So aktivieren Sie Enhanced Networking im Amazon Linux AMI (Instance Store-Backed Instances).
6. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

- modify-instance-attribute (AWS CLI)

```
aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
```

- Edit-EC2InstanceAttribute(Tools für Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
```

7. (Optional) Erstellen Sie ein AMI von der Instance, wie unter Erstellen Sie ein Amazon EBS-backed AMI beschrieben. Das AMI erbt das Enhanced Networking-Attribut `enaSupport` von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.
8. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instanz von verwaltet wird AWS OpsWorks, sollten Sie die Instanz in der AWS OpsWorks Konsole starten, damit der Instanzstatus synchron bleibt.
9. Stellen Sie eine Verbindung mit der Instance her und prüfen Sie, ob das `ena`-Modul installiert und in der Netzwerkschnittstelle geladen wurde, indem Sie den Befehl ethtool -i eth*n* aus dem Abschnitt Testen, ob Enhanced Networking aktiviert ist verwenden.

   Wenn Sie nach der Aktivierung von Enhanced Networking keine Verbindung zu Ihrer Instance herstellen können, informieren Sie sich unter Beheben Sie Fehler beim Elastic Network Adapter unter Linux.

So aktivieren Sie Enhanced Networking im Amazon Linux AMI (Instance Store-Backed Instances)

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Erstellen einer Instance-Speicher-Backed Linux-AMI beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

Ubuntu

Die neuesten Ubuntu-HVM-AMIs enthalten das Modul, das für Enhanced Networking mit installierter ENA und aktivierter ENA-Unterstützung erforderlich ist. Wenn Sie also eine Instance mit dem aktuellen Ubuntu HVM-AMI auf einem unterstützten Instance-Typ starten, ist Enhanced Networking bereits für Ihre Instance aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist.

Wenn Sie Ihre Instance aus einem älteren AMI gestartet haben und Enhanced Networking noch nicht aktiviert wurde, können Sie das Kernel-Paket `linux-aws` installieren, um die aktuellen Enhanced Networking-Treiber zu erhalten und das erforderliche Attribut zu aktualisieren.

`linux-aws`-Kernel-Paket (Ubuntu 16.04 oder höher) installieren

Ubuntu 16.04 und 18.04 werden mit dem benutzerdefinierten Ubuntu-Kernel geliefert (`linux-aws`-Kernel-Paket). Um einen anderen Kernel zu verwenden, wenden Sie sich an AWS Support.

`linux-aws`-Kernel-Paket (Ubuntu Trusty 14.04) installieren

1. Verbinden Sie sich mit der Instance.
2. Aktualisieren Sie den Cache der Paketverwaltung und die einzelnen Pakete.

   ```
   ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
   ```

   > **Important**
   >
   > Wenn Sie während des Aktualisierungsvorgangs aufgefordert werden, `grub` zu installieren, verwenden Sie `/dev/xvda` für die Installation von `grub` und wählen Sie anschließend aus, dass die aktuelle Version von `/boot/grub/menu.lst` beibehalten werden soll.

3. [EBS-gestützte Instance] Halten Sie die Instance von Ihrem lokalen Computer aus an, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instance von verwaltet

wird AWS OpsWorks, sollten Sie die Instance in der AWS OpsWorks Konsole beenden, damit der Instanzstatus synchron bleibt.

[In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Gehen Sie stattdessen wie folgt vor: So aktivieren Sie Enhanced Networking unter Ubuntu (Instance Store-Backed Instances).

4. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute(Tools für Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
     ```

5. (Optional) Erstellen Sie ein AMI von der Instance, wie unter Erstellen Sie ein Amazon EBS-backed AMI beschrieben. Das AMI erbt das Enhanced Networking-Attribut `enaSupport` von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.
6. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instanz von verwaltet wird AWS OpsWorks, sollten Sie die Instanz in der AWS OpsWorks Konsole starten, damit der Instanzstatus synchron bleibt.

So aktivieren Sie Enhanced Networking unter Ubuntu (Instance Store-Backed Instances)

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Erstellen einer Instance-Speicher-Backed Linux-AMI beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

- register-image (AWS CLI)

  ```
  aws ec2 register-image --ena-support ...
  ```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport $true ...
```

RHEL, SUSE, CentOS

Die neuesten AMIs für Red Hat Enterprise Linux, SUSE Linux Enterprise Server und CentOS enthalten das Modul, das für Enhanced Networking mit ENA und aktivierter ENA-Unterstützung erforderlich ist. Wenn Sie also eine Instance mit dem aktuellen AMI auf einem unterstützten Instance-Typ starten, ist Enhanced Networking bereits für Ihre Instance aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist.

In der folgenden Anleitung werden die Schritte beschrieben, die Sie für die Aktivierung von Enhanced Networking unter einer anderen Linux-Distribution als Amazon Linux AMI oder Ubuntu ausführen müssen. Weitere Informationen, z. B. hinsichtlich der genauen Syntax für Befehle, der Speicherorte von Dateien oder der Unterstützung von einzelnen Paketen bzw. Tools, finden Sie in der Dokumentation zu der jeweiligen Linux-Distribution.

Aktivieren von Enhanced Networking in Linux

1. Verbinden Sie sich mit der Instance.
2. Klonen Sie den Quellcode für das `ena` Modul auf Ihrer Instanz von at. GitHub https://github.com/amzn/amzn-drivers (SUSE Linux Enterprise Server 12 SP2 und höher enthalten standardmäßig ENA 2.02, sodass Sie den ENA-Treiber nicht herunterladen und kompilieren müssen. Bei SUSE Linux Enterprise Server 12 SP2 und höher sollten Sie eine Anforderung übermitteln, um die von Ihnen gewünschte Treiberversion zum Bestands-Kernel hinzuzufügen).

   ```
   git clone https://github.com/amzn/amzn-drivers
   ```

3. Kompilieren und installieren Sie das `ena`-Module in Ihrer Instance. Diese Schritte hängen von der Linux-Distribution ab. Weitere Informationen zur Kompilierung des Moduls auf Red Hat Enterprise Linux finden Sie unter Wie installiere ich den neuesten ENS-Treiber für erweiterte Netzwerkunterstützung auf einer Amazon EC2 EC2-Instance, auf der RHEL ausgeführt wird?
4. Führen Sie den Befehl sudo depmod aus, um die Abhängigkeiten für das Modul zu aktualisieren.
5. Aktualisieren Sie `initramfs` in Ihrer Instance, um sicherzustellen, dass das neue Modul während des Bootvorgangs geladen wird. Wenn die Verteilung beispielsweise dracut unterstützt, können Sie den folgenden Befehl verwenden.

```
dracut -f -v
```

6. Ermitteln Sie, ob Ihr System standardmäßig transparente Netzwerkschnittstellennamen verwendet. Systeme, die systemd- oder udev-Versionen ab 197 verwenden, können Ethernet-Geräte umbenennen, d. h. die einzige Netzwerkschnittstelle in einem solchen System wird nicht zwingend als `eth0` bezeichnet. Dieses Verhalten kann Probleme bei der Verbindung mit Ihrer Instance verursachen. Weitere Informationen und andere Konfigurationsoptionen finden Sie unter Predictable Network Interface Names auf der freedesktop.org-Website.

   a. Sie können die systemd- und udev-Versionen auf RPM-basierten Systemen mit dem folgenden Befehl überprüfen.

   ```
   rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
   systemd-208-11.el7_0.2.x86_64
   ```

   In dem Red Hat Enterprise Linux 7-Beispiel oben lautet die systemd-Version 208, d. h. transparente Netzwerkschnittstellennamen müssen deaktiviert werden.

   b. Sie können transparente Netzwerkschnittstellennamen deaktivieren, indem Sie in der Zeile `net.ifnames=0` in der Datei `GRUB_CMDLINE_LINUX` die Option `/etc/default/grub` hinzufügen.

   ```
   sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /etc/default/
   grub
   ```

   c. Erstellen Sie die neue Grub-Konfigurationsdatei.

   ```
   sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

7. [EBS-gestützte Instance] Halten Sie die Instance von Ihrem lokalen Computer aus an, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instance in der AWS OpsWorks Konsole beenden, damit der Instance-Status synchron bleibt.

   [In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Gehen Sie stattdessen wie folgt vor: So aktivieren Sie Enhanced Networking unter Linux (Instance-Speicher-gestützte Instances):.

8. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut `enaSupport` mit einem der folgenden Befehle:

   - modify-instance-attribute (AWS CLI)

     ```
     aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
     ```

   - Edit-EC2InstanceAttribute(Tools für Windows PowerShell)

     ```
     Edit-EC2InstanceAttribute -InstanceId instance-id -EnaSupport $true
     ```

9. (Optional) Erstellen Sie ein AMI von der Instance, wie unter Erstellen Sie ein Amazon EBS-backed AMI beschrieben. Das AMI erbt das Enhanced Networking-Attribut `enaSupport` von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.

   Wenn Ihr Instance-Betriebssystem eine `/etc/udev/rules.d/70-persistent-net.rules`-Datei enthält, müssen Sie diese vor der Erstellung des AMI löschen. Diese Datei enthält die MAC-Adresse des Ethernet-Adapters in der ursprünglichen Instance. Wenn eine andere Instance mit dieser Datei gestartet wird, kann das Betriebssystem das Gerät nicht finden und von `eth0` schlägt möglicherweise fehl, was zu Problemen beim Start führt. Diese Datei wird während des nächsten Bootvorgangs neu generiert, und jede aus dem AMI gestartete Instance erstellt eine eigene Version der Datei.

10. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instanz von verwaltet wird AWS OpsWorks, sollten Sie die Instanz in der AWS OpsWorks Konsole starten, damit der Instanzstatus synchron bleibt.

11. (Optional) Stellen Sie eine Verbindung mit Ihrer Instance her und überprüfen Sie, ob das Modul installiert wurde.

    Wenn Sie nach der Aktivierung von Enhanced Networking keine Verbindung zu Ihrer Instance herstellen können, informieren Sie sich unter Beheben Sie Fehler beim Elastic Network Adapter unter Linux.

So aktivieren Sie Enhanced Networking unter Linux (Instance-Speicher-gestützte Instances):

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Erstellen einer Instance-Speicher-Backed Linux-AMI beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

- register-image (AWS CLI)

```
aws ec2 register-image --ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -EnaSupport ...
```

Ubuntu mit DKMS

Diese Methode ist nur für Test- und Feedbackzwecke. Sie ist nicht für die Nutzung mit Produktionsbereitstellungen gedacht. Für Produktionsbereitstellungen siehe Ubuntu.

> **Important**
>
> Bei Verwendung von DKMS wird die Supportvereinbarung für Ihr Abonnement unwirksam. Es sollte nicht für Produktionsbereitstellungen verwendet werden.

So aktivieren Sie Enhanced Networking mit ENA unter Ubuntu (EBS-gestützte Instances)

1. Führen Sie die Schritte 1 und 2 unter Ubuntu aus.
2. Installieren Sie die `build-essential`-Pakete zum Kompilieren des Kernel-Moduls und das `dkms`-Paket, damit Ihr `ena`-Modul bei jeder Aktualisierung von Kernel neu erstellt wird.

```
ubuntu:~$ sudo apt-get install -y build-essential dkms
```

3. Klonen Sie die Quelle für das `ena` Modul auf Ihrer Instanz von GitHub athttps://github.com/amzn/amzn-drivers.

```
ubuntu:~$ git clone https://github.com/amzn/amzn-drivers
```

4. Verschieben Sie das `amzn-drivers`-Paket in das Verzeichnis `/usr/src/`, sodass es von DKMS gefunden und bei jedem Kernel-Update neu erstellt wird. Fügen Sie die Versionsnummer des Quellcodes an den Verzeichnisnamen an (Sie finden die aktuelle Versionsnummer in den Versionshinweisen). Im folgenden Beispiel wird Version `1.0.0` angezeigt.

```
ubuntu:~$ sudo mv amzn-drivers /usr/src/amzn-drivers-1.0.0
```

5. Erstellen Sie eine DKMS-Konfigurationsdatei mit den folgenden Werten. Geben Sie dabei Ihre `ena`-Version an.

   Erstellen Sie die Datei.

```
ubuntu:~$ sudo touch /usr/src/amzn-drivers-1.0.0/dkms.conf
```

   Öffnen Sie die Datei und fügen Sie die folgenden Werte hinzu.

```
ubuntu:~$ sudo vim /usr/src/amzn-drivers-1.0.0/dkms.conf
PACKAGE_NAME="ena"
PACKAGE_VERSION="1.0.0"
CLEAN="make -C kernel/linux/ena clean"
MAKE="make -C kernel/linux/ena/ BUILD_KERNEL=${kernelver}"
BUILT_MODULE_NAME[0]="ena"
BUILT_MODULE_LOCATION="kernel/linux/ena"
DEST_MODULE_LOCATION[0]="/updates"
DEST_MODULE_NAME[0]="ena"
AUTOINSTALL="yes"
```

6. Verwenden Sie DKMS, um das `ena`-Modul in der Instance hinzuzufügen, zu erstellen und zu installieren.

   Fügen Sie das Modul DKMS hinzu.

```
ubuntu:~$ sudo dkms add -m amzn-drivers -v 1.0.0
```

   Erstellen Sie das Modul mit dem Befehl dkms.

```
ubuntu:~$ sudo dkms build -m amzn-drivers -v 1.0.0
```

   Installieren Sie das Modul mit dkms.

```
ubuntu:~$ sudo dkms install -m amzn-drivers -v 1.0.0
```

7. Erstellen Sie die Datei `initramfs` neu, damit das richtige Modul während des Bootvorgangs geladen wird.

```
ubuntu:~$ sudo update-initramfs -u -k all
```

8. Stellen Sie sicher, dass das `ena`-Modul installiert ist. Verwenden Sie dafür den Befehl modinfo ena aus Testen, ob Enhanced Networking aktiviert ist.

```
ubuntu:~$ modinfo ena
filename:    /lib/modules/3.13.0-74-generic/updates/dkms/ena.ko
version:  1.0.0
license:  GPL
description: Elastic Network Adapter (ENA)
author:   Amazon.com, Inc. or its affiliates
srcversion:  9693C876C54CA64AE48F0CA
alias:    pci:v00001D0Fd0000EC21sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd0000EC20sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00001EC2sv*sd*bc*sc*i*
alias:    pci:v00001D0Fd00000EC2sv*sd*bc*sc*i*
depends:
vermagic:    3.13.0-74-generic SMP mod_unload modversions
parm:     debug:Debug level (0=none,...,16=all) (int)
parm:     push_mode:Descriptor / header push mode (0=automatic,1=disable,3=enable)
     0 - Automatically choose according to device capability (default)
     1 - Don't push anything to device memory
     3 - Push descriptors and header buffer to device memory (int)
parm:     enable_wd:Enable keepalive watchdog (0=disable,1=enable,default=1) (int)
parm:     enable_missing_tx_detection:Enable missing Tx completions. (default=1)
 (int)
parm:     numa_node_override_array:Numa node override map
 (array of int)
parm:     numa_node_override:Enable/Disable numa node override (0=disable)
 (int)
```

9. Fahren Sie mit Schritt 3 in Ubuntu fort.

Aktivieren von Enhanced Networking unter Windows

Wenn Sie Ihre Instance gestartet haben und Enhanced Networking noch nicht aktiviert wurde, müssen Sie den erforderlichen Netzwerkadaptertreiber herunterladen und in der Instance installieren sowie anschließend das `enaSupport`-Instance-Attribut setzen, um die optimierte Netzwerkleistung zu erzielen. Sie können dieses Attribut nur aus unterstützten Instance-Typen und nur bei installiertem ENA-Treiber aktivieren. Weitere Informationen finden Sie unter Unterstützung von Enhanced Networking.

Aktivieren von Enhanced Networking

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. [Nur Windows Server 2016 und 2019] Führen Sie das folgende PowerShell EC2Launch-Skript aus, um die Instanz zu konfigurieren, nachdem der Treiber installiert wurde.

   ```
   PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
   ```

3. Installieren Sie den Treiber in der Instance, indem Sie wie folgt vorgehen:

   a. Laden Sie den aktuellen Treiber in die Instance herunter.

   b. Extrahieren Sie die ZIP-Datei.

   c. Installieren Sie den Treiber, indem Sie das `install.ps1` PowerShell Skript ausführen.

   > **Note**
   >
   > Wenn ein Fehler der Ausführungsrichtlinie gemeldet wird, weisen Sie der Richtlinie `Unrestricted` zu (standardmäßig ist `Restricted` oder `RemoteSigned` zugewiesen). Führen Sie das `install.ps1` PowerShell Skript in einer Befehlszeile aus`Set-ExecutionPolicy -ExecutionPolicy Unrestricted`, und führen Sie es dann erneut aus.

4. Halten Sie die Instance von Ihrem lokalen Computer aus an, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instanz in der AWS OpsWorks Konsole beenden, damit der Instanzstatus synchron bleibt.

5. Aktivieren Sie die ENA-Unterstützung in Ihrer Instance wie folgt:

   a. Prüfen Sie auf Ihrem lokalen Computer das ENA-Support-Attribut auf Ihrer EC2-Instance, indem Sie einen der folgenden Befehle ausführen. Wenn das Attribut nicht aktiviert ist, wird „[]" oder ein leeres Feld zurückgegeben. `EnaSupport` ist standardmäßig auf `false` festgelegt.

      - describe-instances (AWS CLI/AWS CloudShell)

      ```
      aws ec2 describe-instances --instance-ids instance_id --query
       "Reservations[].Instances[].EnaSupport"
      ```

      - Get-EC2Instance(Tools für Windows PowerShell)

      ```
      (Get-EC2Instance -InstanceId instance-id).Instances.EnaSupport
      ```

   b. Führen Sie zur Aktivierung der ENA-Unterstützung einen der folgenden Befehle aus:

      - modify-instance-attribute (AWS CLI/AWS CloudShell)

      ```
      aws ec2 modify-instance-attribute --instance-id instance_id --ena-support
      ```

      - Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

      ```
      Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $true
      ```

      Wenn beim Neustarten der Instance Probleme auftreten, können Sie die ENA-Unterstützung auch über einen der folgenden Befehle deaktivieren:

      - modify-instance-attribute (AWS CLI/AWS CloudShell)

      ```
      aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
      ```

      - Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

      ```
      Edit-EC2InstanceAttribute -InstanceId instance_id -EnaSupport $false
      ```

   c. Stellen Sie sicher, dass das Attribut auf `true` gesetzt wurde, indem Sie den Befehl describe-instances oder Get-EC2Instance wie oben gezeigt ausführen. Die Ausgabe sollte hetzt folgendermaßen aussehen:

```
[
 true
]
```

6. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI/AWS CloudShell), Start-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instance über die AWS OpsWorks Konsole starten, damit der Instanzstatus synchron bleibt.
7. Prüfen Sie auf der Instance, wie folgt ob der ENA-Treiber installiert und aktiviert ist:
   a. Klicken Sie mit der rechten Maustaste auf das Netzwerksymbol und wählen Sie Open Network and Sharing Center aus.
   b. Wählen Sie den Ethernet-Adapter aus (z. B. Ethernet 2).
   c. Wählen Sie Details aus. Prüfen Sie unter Network Connection Details, ob Description den Wert Amazon Elastic Network Adapter hat.
8. (Optional) Erstellen Sie aus der Instance ein AMI. Das AMI übernimmt das `enaSupport`-Attribute von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der ENA standardmäßig aktiviert ist.

Versionsinformationen für Treiber

Linux-ENA-Treiber

Informationen zu den Versionen des Linux-ENA-Treibers finden Sie in den Versionshinweisen des ENA-Linux-Treibers.

Windows-ENA-Treiber

Windows AMIs umfassen den Amazon ENA-Treiber zum Aktivieren von Enhanced Networking.

Die folgende Tabelle enthält die entsprechende ENA-Treiberversion, die für jede Windows-Server-Version heruntergeladen werden sollte.

Windows Server Version	ENA-Treiberversion
Windows Server 2022	2.4.0 und höher

Windows Server Version	ENA-Treiberversion
Windows Server 2019	brandneue
Windows Server 2016	brandneue
Windows Server 2012 R2	2.6.0 und niedriger
Windows Server 2012	2.6.0 und niedriger
Windows Server 2008 R2	2.2.3 und niedriger

Die folgende Tabelle fasst die Änderungen für jede Version zusammen.

Treiberversion	Details	Datum der Veröffentlichung
2.7.0	Neue Features • Die Unterstützung für Windows Server 2012 (Windows 8) und Windows Server 2012 R2 (Windows 8.1) wurde entfernt. Für diese Betriebssystemversionen wurde der Support von eingestellt AWS. Die Treiberinstallation schlägt unter Windows Server 2012 und früheren Versionen fehl. • Unterstützung für die Übertragung der IPv6-Tx-Prüfsummenberechnung auf das Gerät wurde hinzugefügt. • Umfassende Unterstützung für Low Latency Queuing (LLQ) hinzugefügt. Dies wird basierend auf der Geräteempfehlung dynamisch aktiviert. Sie können diese Einstellung mit dem neuen Registrierungsschlüssel „WidellQ“ überschreiben. •	1. Mai 2024

Treiberversion	Details	Datum der Veröffentlichung
	Es wurde eine Meldung für Paketverluste hinzugefügt, die auf einen Rx-Überlauf zurückzuführen sind, was darauf hindeutet, dass im Rx-Ring nicht genügend Speicherplatz für eingehende Pakete verfügbar ist. • Unterstützung für suboptimale Konfigurationsbena chrichtigungen vom Gerät wurde hinzugefügt. Sehen Sie sich die Ereignis-ID `59000` in der Windows-E reignisanzeige an. Fehlerbehebungen • Vermeiden Sie unnötiges Zurücksetzen von Geräten, die durch Tx-Pakete verursacht werden, deren Header die maximale Low Latency Queuing (LLQ) -Header-G röße überschreiten.	

Treiberversion	Details	Datum der Veröffentlichung

2.6.0	Neue Features
	• Fügt die folgenden Netzwerkleistungsmetriken für Instance-Typen hinzu, die ENA Express unterstützen.
	  • `ena_srd_mode`
	  • `ena_srd_tx_pkts`
	  • `ena_srd_eligible_tx_pkts`
	  • `ena_srd_rx_pkts`
	  • `ena_srd_resource_utilization`
	• Fügt die Netzwerkleistungsmetrik `conntrack_allowance_available` für Nitro-basierte Instance-Typen hinzu.
	• Fügt einen neuen Grund für das Zurücksetzen des Adapters hinzu, weil eine Beschädigung der RX-Daten erkannt wurde.
	• Aktualisiert die Infrastruktur zur Treiberprotokollierung.
	
	Fehlerbehebungen
	• Verhindert das Zurücksetzen des Adapters für den Fall, dass ein Update der Netzwerkleistungsmetriken aufgrund von CPU-Mangel fehlschlägt.
	•
		20. Juni 2023

Treiberversion	Details	Datum der Veröffentlichung
	Verhindert die falsche Erkennung einer Unterbrechung des Geräte-Heartbeats. • Korrigiert das Treiberinstallationsskript, um den Downgrade-Vorgang zu unterstützen. • Korrigiert die Statistik zur Anzahl der Empfangsfehler.	
2.5.0	Ankündigung Die ENA-Windows-Treiberversion 2.5.0 wurde zurückgesetzt, da die Initialisierung auf dem Windows-Domain-Controller fehlgeschlagen ist. Windows Client und Windows Server sind nicht betroffen.	17. Februar 2023

Treiberversion	Details	Datum der Veröffentlichung
2.4.0	Neue Features • Fügt Unterstützung für Windows Server 2022 hinzu. • Entfernt Unterstützung für Windows Server 2008 R2. • Setzt Low Latency Queuing (LLQ) auf immer aktiviert , um die Leistung bei Amazon-EC2-Instances der sechsten Generation zu verbessern. Fehlerbehebung • Behebt ein Problem, durch das die Weitergabe von Netzwerkleistungsmetriken an die Leistungsindikatoren für Windows (PCW) fehlschlug. • Behebt ein Speicherleck während des Lesevorgangs des Registrierungsschlüssels. • Verhindert eine unendliche Reset-Schleife im Falle eines nicht behebbaren Fehlers während der Adapterrü cksetzung.	28. April 2022

Treiberversion	Details	Datum der Veröffentlichung
2.2.4	Ankündigung Die ENA-Windows-Treiberversion 2.2.4 wurde aufgrund einer möglichen Leistungsverschlechterung bei EC2-Instances der sechsten Generation zurückgesetzt. Es wird empfohlen, dass Sie ein Downgrade des Treibers mit einer der folgenden Methoden durchführen: • Installieren der vorherigen Version 1. Laden Sie das vorherige Versionspaket über den Link in dieser Tabelle herunter (Version 2.2.3). 2. Führen Sie das install.ps1 PowerShell Installationsskript aus. Weitere Informationen zu Schritten vor und nach der Installation finden Sie unter Aktivieren von Enhanced Networking unter Windows. Verwenden von Amazon EC2 Systems Manager für ein Massenupdate • Führen Sie eine Massenaktualisierung über ein SSM-Dokument `AWS-ConfigureAWSPackage` mit folgenden Parametern durch: • Name: AwsEnaNetworkDriver • Version: 2.2.3	26. Oktober 2021

Treiberversion	Details	Datum der Veröffentlichung
2.2.3	Neues Feature • Integriert Unterstützung für neue Nitro-Karten mit bis zu 400 Gbit/s Instance-Netzwerken. Fehlerbehebung • Behebt die Race-Bedingung zwischen der Änderung der Systemzeit und der Abfrage der Systemzeit durch den ENA-Treiber, was zu einer fälschlicherweise positiven Erkennung von HW-Nichtreaktionen führt. Die Windows-ENA-Treiberversion 2.2.3 ist die letzte Version, die Unterstützung für Windows Server 2008 R2 bietet. Derzeit verfügbare Instance-Typen, die ENA verwenden, werden unter Windows Server 2008 R2 weiterhin unterstützt. Die Treiber sind per Download verfügbar. Künftige Instance-Typen bieten keine Unterstützung für Windows Server 2008 R2 und Sie können Images mit Windows Server 2008 R2 nicht auf künftige Instance-Typen importieren, migrieren oder auf diesen starten.	25. März 2021

Treiberversion	Details	Datum der Veröffentlichung
2.2.2	Neues Feature • Integriert die Unterstützung für die Abfrage von Netzwerkadapter-Leistungsmetriken mit CloudWatch und die Leistungsindikatoren für Windows-Verbraucher. Fehlerbehebung • Behebt Leistungsprobleme bei Bare-Metal-Instances.	21. Dezember 2020
2.2.1	Neues Feature • Fügt eine Methode hinzu, mit der der Host den Elastic-Network-Adapter nach Netzwerkleistungsmetriken abfragen kann.	1. Oktober 2020

Treiberversion	Details	Datum der Veröffentlichung
2.2.0	Neue Features • Fügt Unterstützung für Hardwaretypen der nächsten Generation hinzu. • Verbessert die Startzeit der Instance nach der Wiederaufnahme aus dem Stop-Ruhezustand und eliminiert falsch positive ENA-Fehlermeldungen. Leistungsoptimierungen • Optimiert die Verarbeitung des eingehenden Datenverkehrs. • Verbessert die Verwaltung des gemeinsam genutzten Speichers in einer Umgebung mit geringen Ressourcen. Fehlerbehebung • Vermeidet Systemabsturz beim Entfernen von ENA-Geräten in seltenen Fällen, in denen der Treiber nicht zurückgesetzt werden kann.	12. August 2020
2.1.5	Fehlerbehebung • Behebt gelegentliche Netzwerkadapter-Initialisierungsfehler auf Bare-Metal-Instances.	23. Juni 2020

Treiberversion	Details	Datum der Veröffentlichung
2.1.4	Fehlerbehebungen • Verhindern Sie Verbindungsprobleme durch vom Netzwerk-Stack eingehende beschädigte LSO-Paket metadaten. • Verhindern Sie einen Systemabsturz durch eine seltene Race-Condition, die zum Zugriff auf einen bereits freigegebenen Paketspeicher führt.	25. November 2019
2.1.2	Neues Feature • Unterstützung für den Vendor-ID-Bericht hinzugefügt, um dem Betriebssystem das Generieren MAC-basierter UUIDs zu ermöglichen. Fehlerbehebungen • Verbesserte DHCP-Netzwerkkonfigurationsleistung während der Initialisierung. • Korrekte Berechnung der L4-Prüfsumme für eingehend en IPv6-Datenverkehr, wenn die maximale Übertragu ngseinheit (MTU) 4 K überschreitet. • Allgemeine Verbesserungen der Treiberstabilität und kleinere Fehlerbehebungen.	4. November 2019

Treiberversion	Details	Datum der Veröffentlichung
2.1.1	Fehlerbehebungen • Verhinderung von Drops hoch fragmentierter TCP-LSO-Pakete, die aus dem Betriebssystem eingehen. • Ordnungsgemäße Verarbeitung des Encapsulating Security Payload (ESP)-Protokolls innerhalb von IPSec in IPv6-Netzwerken.	16. September 2019

Treiberversion	Details	Datum der Veröffentlichung

2.1.0	ENA Windows-Treiber v2.1 führt neue ENA-Gerät efunktionalitäten ein. Die Leistung wird gesteigert, es werden neue Features hinzugefügt und mehrere Stabilitä tsverbesserungen vorgenommen.
	• Neue Features
	  • Verwenden Sie den standardisierten Windows-R egistrierungsschlüssel für Jumbo-Rahmenkonfig urationen.
	  • Erlauben Sie die VLAN-ID-Einstellung über die ENA-Treibereigenschaften-GUI.
	  • Verbesserte Wiederherstellungsflüsse
	  • Verbesserte Mechanismen zur Ausfallidentifikation.
	  • Zusätzliche Unterstützung für einstellbare Wiederherstellungsparameter.
	  • Unterstützung für bis zu 32 I/O-Warteschlangen für neuere EC2-Instances, die mehr als 8 vCPUs haben.
	  • ~90 % Verringerung des Treiber-Arbeitsspeicherplat zes.
	• Leistungsoptimierungen
	  • Geringere Latenz des Übertragungspfads.
	  • Unterstützung für den Empfang des Checksum Offload.
	  •
		1. Juli 2019

Treiberversion	Details	Datum der Veröffentlichung
	Leistungsoptimierung für schwer geladenes System (optimierte Nutzung der Sperrmechanismen). • Weitere Verbesserungen, um die CPU-Nutzung zu verringern und die Reaktionsfähigkeit des Systems unter Last zu verbessern. • Fehlerbehebungen • Absturz während ungültigem Parsing nicht fortlaufe nder Tx-Header behoben. • Absturz des Treibers v1.5 während Trennung der Elastic-Network-Schnittstelle auf Bare-Metal-Instanc es behoben. • Berechungsfehler über IPv6 der LSO-Pseudo-Header-Prüfsumme behoben • Potenzielles Leck der Arbeitsspeicherressource bei fehlgeschlagener Initialisierung behoben. • TCP/UDP Checksum Offload für IPv4-Fragmente deaktiviert. • Fix für VLAN-Konfiguration. VLAN wurde falsch deaktiviert, als nur die VLAN-Priorität hätte deaktivie rt werden sollen. • Korrektes Parsing der Kunden-Treibermeldungen durch die Ereignisanzeige aktiviert. • Fehler beim Initialisieren des Treibers aufgrund ungültiger Zeitstempel-Bearbeitung behoben.	

Treiberversion	Details	Datum der Veröffentlichung
	• Laufbedingung zwischen Datenverarbeitung und ENA-Gerätedeaktivierung behoben.	
1.5.0	• Stabilitäts- und Leistungsverbesserungen. • Empfangspuffer können jetzt mit einem Wert bis zu 8192 in den erweiterten Eigenschaften der ENA NIC konfiguriert werden. • Standardempfangspuffer 1k.	4. Oktober 2018
1.2.3	Enthält Zuverlässigkeitskorrekturen und vereinheitlicht die Unterstützung für Windows Server 2008 R2 bis Windows Server 2016.	13. Februar 2018
1.0.8	Die Erstversion. Enthalten in AMIs für Windows Server 2008 R2, Windows Server 2012 RTM, Windows Server 2012 R2 und Windows Server 2016.	. Juli 2016

Amazon SNS kann Sie benachrichtigen, wenn neue Versionen von EC2-Windows-Treibern veröffentlicht werden. Führen Sie die folgenden Schritte durch, um diese Benachrichtigungen zu abonnieren.

So abonnieren Sie EC2-Benachrichtigungen

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Ändern Sie, falls erforderlich, die Region in der Navigationsleiste zu US East (N. Virginia). Sie müssen diese Region auswählen, weil sich die SNS-Benachrichtigungen, die Sie abonnieren, in dieser Region befinden.
3. Wählen Sie im Navigationsbereich Subscriptions aus.
4. Wählen Sie Create subscription.

5. Führen Sie im Dialogfeld Create subscription Folgendes aus:

   a. Kopieren Sie den folgenden Amazon-Ressourcennamen (ARN) unter TopicARN:

      arn:aws:sns:us-east-1:801119661308:ec2-windows-drivers

   b. Wählen Sie unter Protocol die Option `Email` aus.

   c. Geben Sie unter Endpoint (Endpunkt) eine E-Mail-Adresse ein, um die Benachrichtigungen zu empfangen.

   d. Wählen Sie Create subscription.

6. Sie erhalten eine Bestätigungs-E-Mail. Öffnen Sie die E-Mail und befolgen Sie die Anweisungen, um Ihr Abonnement abzuschließen.

Jedes Mal wenn neue EC2-Treiber für Windows veröffentlicht werden, senden wir ein Benachrichtigung an die Abonnenten. Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

So kündigen Sie ein Abonnement der Benachrichtigungen zu Amazon EC2-Treibern für Windows

1. Öffnen Sie die Amazon SNS-Konsole unter https://console.aws.amazon.com/sns/v3/home.
2. Wählen Sie im Navigationsbereich Subscriptions aus.
3. Aktivieren Sie das Kontrollkästchen für das Abonnement und wählen Sie dann Actions (Aktionen) und Delete subscriptions (Abonnements löschen) aus. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Verbessern Sie die Netzwerkleistung mit ENA Express auf Ihren EC2-Instances

ENA Express basiert auf der SRD-Technologie (AWS Scalable Reliable Datagram). SRD ist ein leistungsstarkes Netzwerktransportprotokoll, das dynamisches Routing verwendet, um den Durchsatz zu erhöhen und die Tail-Latenz zu minimieren. Mit ENA Express können Sie zwischen zwei EC2-Instances in derselben Availability Zone kommunizieren.

Vorteile von ENA Express

- Erhöht die maximale Bandbreite, die ein einzelner Datenfluss nutzen kann, von 5 Gbit/s auf 25 Gbit/s innerhalb des Subnetzes bis zum aggregierten Instance-Limit.

- Reduziert die Latenz des Netzwerkverkehrs zwischen EC2-Instances, insbesondere in Zeiten hoher Netzwerkauslastung.
- Erkennt und vermeidet überlastete Netzwerkpfade.
- Führt einige Aufgaben direkt auf der Netzwerkebene aus, z. B. die Neuordnung von Paketen auf der Empfängerseite und die meisten erforderlichen Neuübertragungen. Dadurch wird die Anwendungsebene für andere Arbeiten freigegeben.

> **Note**
>
> Wenn Ihre Anwendung ein hohes Volumen an Paketen pro Sekunde sendet oder empfängt und die meiste Zeit auf Latenz optimiert werden muss, insbesondere in Zeiten ohne Überlastung des Netzwerks, ist Enhanced Networking möglicherweise besser für Ihr Netzwerk geeignet.

In Zeiträumen mit geringem Netzwerkverkehr bemerken Sie möglicherweise eine leichte Erhöhung der Paketlatenz (mehrere zehn Mikrosekunden), wenn das Paket ENA Express verwendet. Während dieser Zeiten können Anwendungen, die bestimmte Netzwerkleistungsmerkmale priorisieren, von ENA Express wie folgt profitieren:

- Prozesse können von einer erhöhten maximalen Single-Flow-Bandbreite von 5 Gbit/s auf 25 Gbit/s innerhalb derselben Availability Zone bis hin zum aggregierten Instance-Limit profitieren. Wenn ein bestimmter Instance-Typ beispielsweise bis zu 12,5 Gbit/s unterstützt, ist die Single-Flow-Bandbreite ebenfalls auf 12,5 Gbit/s begrenzt.
- Länger ausgeführte Prozesse sollten in Zeiten der Netzwerküberlastung eine geringere Latenz aufweisen.
- Prozesse können von einer gleichmäßigeren und einheitlicheren Verteilung der Reaktionszeiten des Netzwerks profitieren.

Voraussetzungen für Linux-Instances

Um sicherzustellen, dass ENA Express effektiv arbeiten kann, aktualisieren Sie die Einstellungen für Ihre Instance wie folgt.

- Wenn Ihre Instance Jumbo-Frames verwendet, führen Sie den folgenden Befehl aus, um Ihre maximale Übertragungseinheit (MTU) auf `8900` festzulegen.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 8900
```

- Erhöhen Sie die Ringgröße des Empfängers (Rx) wie folgt:

```
[ec2-user ~]$ ethtool -G device rx 8192
```

- Um die ENA-Express-Bandbreite zu maximieren, konfigurieren Sie Ihre TCP-Warteschlangenlimits wie folgt:

  1. Legen Sie den Grenzwert für die kleine TCP-Warteschlange auf 1 MB oder höher fest. Dadurch erhöht sich die Datenmenge, die für die Übertragung auf einem Socket in der Warteschlange steht.

     ```
     sudo sh -c 'echo 1048576 > /proc/sys/net/ipv4/tcp_limit_output_bytes'
     ```

  2. Deaktivieren Sie Byte-Warteschlangenlimits auf dem ETH-Gerät, wenn diese für Ihre Linux-Distribution aktiviert sind. Dadurch erhöht sich die Anzahl der für die Übertragung in der Gerätewarteschlange anstehenden Daten.

     ```
     sudo sh -c 'for txq in /sys/class/net/eth0/queues/tx-*; do echo max > ${txq}/
     byte_queue_limits/limit_min; done'
     ```

     > **Note**
     >
     > Der ENA-Treiber für die Amazon-Linux-Distribution deaktiviert standardmäßig die Byte-Warteschlangenlimits.

So funktioniert ENA Express

ENA Express basiert auf der SRD-Technologie (AWS Scalable Reliable Datagram). Es verteilt Pakete für jeden Netzwerkfluss auf verschiedene AWS Netzwerkpfade und passt die Verteilung dynamisch an, wenn Anzeichen einer Überlastung erkannt werden. Sie verwaltet auch die Neuordnung von Paketen auf der Empfängerseite.

Um sicherzustellen, dass ENA Express den Netzwerkverkehr wie vorgesehen verwalten kann, müssen sendende und empfangende Instances, sowie die Kommunikation zwischen ihnen, alle nachstehenden Anforderungen erfüllen:

- Sowohl sendende als auch empfangende Instance-Typen werden unterstützt. Weitere Informationen finden Sie in der Unterstützte Instance-Typen für ENA Express-Tabelle.
- Sowohl die sendenden als auch die empfangenden Instances müssen ENA Express konfiguriert haben. Wenn es Unterschiede in der Konfiguration gibt, kann es zu Situationen kommen, in denen der Datenverkehr standardmäßig auf die ENA-Standardübertragung umgestellt wird. Das folgende Szenario zeigt, was in diesem Fall passieren kann.

  Szenario: Unterschiede in der Konfiguration

Instance	ENA Express aktiviert	UDP verwendet ENA Express
Instance 1	Ja	Ja
Instance 2	Ja	Nein

  In diesem Fall kann für den TCP-Verkehr zwischen den beiden Instances ENA Express verwendet werden, da beide Instances dies aktiviert haben. Da jedoch eine der Instances ENA Express nicht für den UDP-Verkehr verwendet, verwendet die Kommunikation zwischen diesen beiden Instances via UDP die ENA-Standardübertragung.
- Die sendenden und empfangenden Instances müssen in derselben Availability Zone ausgeführt werden.
- Der Netzwerkpfad zwischen den Instances darf keine Middleware-Boxen enthalten. ENA Express unterstützt derzeit keine Middleware-Boxen.
- (Nur Linux-Instances) Verwenden Sie die Treiberversion 2.2.9 oder höher, um das volle Bandbreitenpotenzial auszuschöpfen.
- (Nur Linux-Instances) Verwenden Sie die Treiberversion 2.8 oder höher, um Metriken zu erstellen.

Wenn eine Anforderung nicht erfüllt ist, verwenden die Instances zur Kommunikation das Standard-TCP/UDP-Protokoll, jedoch ohne SRD.

Um sicherzustellen, dass Ihr Instance-Netzwerktreiber für eine optimale Leistung konfiguriert ist, lesen Sie sich die empfohlenen bewährten Methoden für ENA-Treiber durch. Diese bewährten Methoden gelten auch für ENA Express. Weitere Informationen finden Sie im ENA Linux Driver Best Practices and Performance Optimization Guide auf der GitHub Website.

> **Note**
>
> Amazon EC2 bezieht sich auf die Beziehung zwischen einer Instance und einer Netzwerkschnittstelle, die als Anhang an sie angehängt ist. Die ENA-Express-Einstellungen gelten für den Anhang. Wenn die Netzwerkschnittstelle von der Instance getrennt ist, existiert der Anhang nicht mehr und die ENA-Express-Einstellungen, die für ihn galten, sind nicht mehr gültig. Das Gleiche gilt, wenn eine Instance beendet wird, auch wenn die Netzwerkschnittstelle erhalten bleibt.

Unterstützte Instance-Typen für ENA Express

Die folgenden Tabs zeigen Instance-Typen, die ENA Express unterstützen.

General purpose

Instance-Typ	Architektur
m6a.12xlarge	x86_64
m6a.16xlarge	x86_64
m6a.24xlarge	x86_64
m6a.32xlarge	x86_64
m6a.48xlarge	x86_64
m6a.metal	x86_64
m6i.8xlarge	x86_64
m6i.12xlarge	x86_64
m6i.16xlarge	x86_64
m6i.24xlarge	x86_64
m6i.32xlarge	x86_64

Instance-Typ	Architektur
m6i.metal	x86_64
m6id.8xlarge	x86_64
m6id.12xlarge	x86_64
m6id.16xlarge	x86_64
m6id.24xlarge	x86_64
m6id.32xlarge	x86_64
m6id.metal	x86_64
m7g.12xlarge	arm64
m7g.16xlarge	arm64
m7g.metal	arm64
m7gd.12xlarge	arm64
m7gd.16xlarge	arm64
m7gd.metal	arm64
m7i.12xlarge	x86_64
m7i.16xlarge	x86_64
m7i.24xlarge	x86_64
m7i.48xlarge	x86_64
m7i.metal-24xl	x86_64
m7i.metal-48xl	x86_64

Compute optimized

Instance-Typ	Architektur
c6a.12xlarge	x86_64
c6a.16xlarge	x86_64
c6a.24xlarge	x86_64
c6a.32xlarge	x86_64
c6a.48xlarge	x86_64
c6a.metal	x86_64
c6gn.16xlarge	arm64
c6i.8xlarge	x86_64
c6i.12xlarge	x86_64
c6i.16xlarge	x86_64
c6i.24xlarge	x86_64
c6i.32xlarge	x86_64
c6i.metal	x86_64
c6id.8xlarge	x86_64
c6id.12xlarge	x86_64
c6id.16xlarge	x86_64
c6id.24xlarge	x86_64
c6id.32xlarge	x86_64
c6id.metal	x86_64

Instance-Typ	Architektur
c7g.12xlarge	arm64
c7g.16xlarge	arm64
c7g.metal	arm64
c7gd.12xlarge	arm64
c7gd.16xlarge	arm64
c7gd.metal	arm64
c7i.12xlarge	x86_64
c7i.16xlarge	x86_64
c7i.24xlarge	x86_64
c7i.48xlarge	x86_64
c7i.metal-24xl	x86_64
c7i.metal-48xl	x86_64

Memory optimized

Instance-Typ	Architektur
r6a.12xlarge	x86_64
r6a.16xlarge	x86_64
r6a.24xlarge	x86_64
r6a.32xlarge	x86_64
r6a.48xlarge	x86_64

Instance-Typ	Architektur
r6a.metal	x86_64
r6i.8xlarge	x86_64
r6i.12xlarge	x86_64
r6i.16xlarge	x86_64
r6i.24xlarge	x86_64
r6i.32xlarge	x86_64
r6i.metal	x86_64
r6id.8xlarge	x86_64
r6id.12xlarge	x86_64
r6id.16xlarge	x86_64
r6id.24xlarge	x86_64
r6id.32xlarge	x86_64
r6id.metal	x86_64
r7g.12xlarge	arm64
r7g.16xlarge	arm64
r7g.metal	arm64
r7gd.12xlarge	arm64
r7gd.16xlarge	arm64
r7gd.metal	arm64
r7i.12xlarge	x86_64

Instance-Typ	Architektur
r7i.16xlarge	x86_64
r7i.24xlarge	x86_64
r7i.48xlarge	x86_64
r7i.metal-24xl	x86_64
r7i.metal-48xl	x86_64
u7i-12tb.224xlarge	x86_64
u7in-16tb.224xlarge	x86_64
u7in-24tb.224xlarge	x86_64
u7in-32tb.224xlarge	x86_64
x2idn.16xlarge	x86_64
x2idn.24xlarge	x86_64
x2idn.32xlarge	x86_64
x2idn.metal	x86_64
x2iedn.8xlarge	x86_64
x2iedn.16xlarge	x86_64
x2iedn.24xlarge	x86_64
x2iedn.32xlarge	x86_64
x2iedn.metal	x86_64

Accelerated computing

Instance-Typ	Architektur
g6.48xlarge	x86_64

Storage optimized

Instance-Typ	Architektur
i4g.4xlarge	arm64
i4g.8xlarge	arm64
i4g.16xlarge	arm64
i4i.8xlarge	x86_64
i4i.12xlarge	x86_64
i4i.16xlarge	x86_64
i4i.24xlarge	x86_64
i4i.32xlarge	x86_64
i4i.metal	x86_64
im4gn.4xlarge	arm64
im4gn.8xlarge	arm64
im4gn.16xlarge	arm64

Auflisten und Anzeigen von ENA-Express-Einstellungen

In diesem Abschnitt wird beschrieben, wie Sie ENA-Express-Informationen aus AWS Management Console oder AWS CLI auflisten und anzeigen. Für weitere Informationen wählen Sie die Registerkarte aus, die der Methode entspricht, die Sie verwenden werden.

Console

Auf dieser Registerkarte erfahren Sie, wie Sie Informationen zu Ihren aktuellen ENA-Express-Einstellungen finden und die Unterstützung für Instance-Typen in der AWS Management Console anzeigen lassen.

Anzeigen von unterstützten Instance-Typen

1. Öffnen Sie die Amazon-EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Instance Types (Instance-Typen) aus.
3. Wählen Sie einen Instance-Typ aus, um die Details der Instance anzuzeigen. Sie können den Link Instance type (Instance-Typ) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste aktivieren, um Details im Detailbereich unten auf der Seite anzuzeigen.
4. Auf der Registerkarte Networking (Vernetzung) oder dem entsprechenden Abschnitt auf der Detailseite zeigt der ENA Express support (ENA-Express-Unterstützung) die Werte „wahr“ oder „falsch“ an, um anzugeben, ob der Instance-Typ dieses Feature unterstützt.

Anzeigen der Einstellungen aus der Liste der Netzwerkschnittstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Network interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie eine Netzwerkschnittstelle aus, um Details für diese Instance zu sehen. Sie können den Link Network interface ID (Netzwerkschnittstellen-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste aktivieren, um Details im Detailbereich unten auf der Seite anzuzeigen.
4. Überprüfen Sie im Abschnitt Network interface attachment (Netzwerkschnittstellenanhang) auf der Registerkarte Details oder auf der Detailseite die Einstellungen für ENA Express und ENA Express UDP.

Anzeigen der Einstellungen von Instances

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie eine Instance aus, um die Details der Instance anzuzeigen. Sie können den Link Instance ID (Instance-ID) wählen, um die Detailseite zu öffnen oder Sie können das

Kontrollkästchen auf der linken Seite der Liste aktivieren, um Details im Detailbereich unten auf der Seite anzuzeigen.

4. Scrollen Sie im Abschnitt Network interfaces (Netzwerkschnittstellen) auf der Registerkarte Networking (Vernetzung) nach rechts, um die Einstellungen für ENA Express und ENA Express UDP zu überprüfen.

AWS CLI

Auf dieser Registerkarte erfahren Sie, wie Sie Informationen zu Ihren aktuellen ENA-Express-Einstellungen finden und die Unterstützung für Instance-Typen in der AWS CLI anzeigen lassen.

Beschreiben von Instance-Typen

Um Informationen zu den Instance-Typ-Einstellungen für einen bestimmten Instance-Typ zu erhalten, führen Sie den describe-instance-types AWS CLI Befehl im aus und ersetzen Sie den Instance-Typ wie folgt:

```
[ec2-user ~]$ aws ec2 describe-instance-types --instance-types m6i.metal
{
"InstanceTypes": [
{
 "InstanceType": "m6i.metal",
 "CurrentGeneration": true,
 ...
 },
 "NetworkInfo": {
  ...
  "EnaSrdSupported": true
 },
 ...
}
]
}
```

Beschreiben von Instances

Informationen zur ENA Express-Konfiguration für bestimmte Instances erhalten Sie, indem Sie den describe-instancesBefehl in der AWS CLI wie folgt ausführen. Dieses Befehlsbeispiel gibt eine Liste der ENA Express-Konfigurationen für die Netzwerkschnittstellen zurück, die an jede der laufenden Instances angeschlossen sind, die durch den `--instance-ids` Parameter angegeben sind.

```
[ec2-user ~]$ aws ec2 describe-instances --instance-
ids i-1234567890abcdef0 i-0598c7d356eba48d7 --query 'Reservations[*].Instances[*].
[InstanceId, NetworkInterfaces[*].Attachment.EnaSrdSpecification]'[
 [
  [
   "i-1234567890abcdef0",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ],
 [
  [
   "i-0598c7d356eba48d7",
   [
    {
     "EnaSrdEnabled": true,
     "EnaSrdUdpSpecification": {
      "EnaSrdUdpEnabled": false
     }
    }
   ]
  ]
 ]
]
```

Beschreiben von Netzwerkschnittstellen

Um Informationen zu den ENA Express-Einstellungen für eine Netzwerkschnittstelle zu erhalten, führen Sie den describe-network-interfacesBefehl AWS CLI wie folgt aus:

```
[ec2-user ~]$ aws ec2 describe-network-interfaces
{
"NetworkInterfaces": [
{
 "Association": {
  ....IPs, DNS...
 },
```

```
 "Attachment": {
  "AttachTime": "2022-11-17T09:04:28+00:00",
  "AttachmentId": "eni-attach-0ab1c23456d78e9f0",
  "DeleteOnTermination": true,
  "DeviceIndex": 0,
  "NetworkCardIndex": 0,
  "InstanceId": "i-1234567890abcdef0",
  "InstanceOwnerId": "111122223333",
  "Status": "attached",
  "EnaSrdSpecification": {
   "EnaSrdEnabled": true,
   "EnaSrdUdpSpecification": {
    "EnaSrdUdpEnabled": true
   }
  }
 },
 ...
 "NetworkInterfaceId": "eni-1234567890abcdef0",
 "OwnerId": "111122223333",
 ...
}
]
}
```

PowerShell

Auf dieser Registerkarte erfahren Sie, wie Sie Informationen zu Ihren aktuellen ENA Express-Einstellungen finden und sich die Unterstützung für Instance-Typen anzeigen lassen können PowerShell.

Beschreiben von Instance-Typen

Informationen zu den Instance-Typ-Einstellungen für einen bestimmten Instance-Typ erhalten Sie, indem Sie das Get-EC2InstanceType Cmdletmit den Tools für PowerShell ausführen und den Instance-Typ wie folgt ersetzen:

```
PS C:\> Get-EC2InstanceType -InstanceType m6i.metal | `
Select-Object `
    InstanceType,
    CurrentGeneration,
    @{Name = 'EnaSrdSupported'; Expression = { $_.NetworkInfo.EnaSrdSupported } } |
 `
Format-List
```

```
InstanceType      : m6i.metal
CurrentGeneration : True
EnaSrdSupported   : True
```

Wenn ENA Express aktiviert ist, wird ein Wert von `True` zurückgegeben.

Beschreiben von Netzwerkschnittstellen

Informationen zu den ENA Express-Einstellungen für eine Netzwerkschnittstelle erhalten Sie, indem Sie den Get-EC2NetworkInterface Cmdletmit den Tools für PowerShell wie folgt ausführen:

```
PS C:\> Get-EC2NetworkInterface -NetworkInterfaceId eni-0d1234e5f6a78901b | `
Select-Object `
    Association,
    NetworkInterfaceId,
    OwnerId,
    @{Name = 'AttachTime'; Expression = { $_.Attachment.AttachTime } },
    @{Name = 'AttachmentId'; Expression = { $_.Attachment.AttachmentId } },
    @{Name = 'DeleteOnTermination'; Expression =
 { $_.Attachment.DeleteOnTermination } },
    @{Name = 'NetworkCardIndex'; Expression = { $_.Attachment.NetworkCardIndex } },
    @{Name = 'InstanceId'; Expression = { $_.Attachment.InstanceId } },
    @{Name = 'InstanceOwnerId'; Expression = { $_.Attachment.InstanceOwnerId } },
    @{Name = 'Status'; Expression = { $_.Attachment.Status } },
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled } },
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled } }

Association         :
NetworkInterfaceId  : eni-0d1234e5f6a78901b
OwnerId             : 111122223333
AttachTime          : 6/11/2022 1:13:11 AM
AttachmentId        : eni-attach-0d1234e5f6a78901b
DeleteOnTermination : True
NetworkCardIndex    : 0
InstanceId          : i-0d1234e5f6a78901b
InstanceOwnerId     : 111122223333
Status              : attached
EnaSrdEnabled       : True
EnaSrdUdpEnabled    : False
```

Konfigurieren der ENA-Express-Einstellungen

Sie können ENA Express für unterstützte EC2-Instance-Typen konfigurieren, ohne zusätzliche Software installieren zu müssen.

In diesem Abschnitt wird beschrieben, wie Sie ENA Express vom AWS Management Console oder vom aus konfigurieren AWS CLI. Für weitere Informationen wählen Sie die Registerkarte aus, die der Methode entspricht, die Sie verwenden werden.

Console

Auf dieser Registerkarte wird beschrieben, wie Sie ENA-Express-Einstellungen für Netzwerkschnittstellen verwalten, die an eine Instance angehängt sind.

Verwalten von ENA Express über die Liste der Netzwerkschnittstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Network interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie eine Netzwerkschnittstelle aus, die an eine Instance angehängt ist. Sie können den Link Network interface ID (Netzwerkschnittstellen-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste auswählen.
4. Wählen Sie im Menü Action (Aktion) oben rechts auf der Seite die Option Manage ENA Express (ENA Express verwalten) aus. Dadurch wird das Dialogfeld Manage ENA Express (ENA Express verwalten) geöffnet, in dem die ausgewählte Netzwerkschnittstellen-ID und die aktuellen Einstellungen angezeigt werden.

   > **Note**
   >
   > Wenn die von Ihnen gewählte Netzwerkschnittstelle nicht mit einer Instance verbunden ist, wird diese Aktion nicht im Menü angezeigt.

5. Um ENA Express zu verwenden, wählen Sie das Kontrollkästchen Enable (Aktivieren) aus.
6. Wenn ENA Express aktiviert ist, können Sie die UDP-Einstellungen konfigurieren. Um ENA Express UDP zu verwenden, wählen Sie das Kontrollkästchen Enable (Aktivieren) aus.
7. Um Ihre Einstellungen zu speichern, wählen Sie Save (Speichern).

Verwalten von ENA Express über die Instance-Liste

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus, die Sie verwalten möchten. Sie können den Link Instance ID (Instance-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste auswählen.
4. Wählen Sie die Network interface (Netzwerkschnittstelle) aus, die Sie für Ihre Instance konfigurieren möchten.
5. Wählen Sie im Menü Action (Aktion) oben rechts auf der Seite die Option Manage ENA Express (ENA Express verwalten) aus.
6. Um ENA Express für eine Netzwerkschnittstelle zu konfigurieren, die an Ihre Instance angeschlossen ist, wählen Sie sie aus der Liste der Network interface (Netzwerkschnittstelle) aus.
7. Um ENA Express für den ausgewählten Netzwerkschnittstellenanhang zu verwenden, aktivieren Sie das Kontrollkästchen Enable (Aktivieren).
8. Wenn ENA Express aktiviert ist, können Sie die UDP-Einstellungen konfigurieren. Um ENA Express UDP zu verwenden, wählen Sie das Kontrollkästchen Enable (Aktivieren) aus.
9. Um Ihre Einstellungen zu speichern, wählen Sie Save (Speichern).

Konfigurieren Sie ENA Express, wenn Sie eine Netzwerkschnittstelle an eine EC2-Instance anfügen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Network interfaces (Netzwerkschnittstellen) aus.
3. Wählen Sie eine Netzwerkschnittstelle aus, die nicht an eine Instance angeschlossen ist (Status ist Available (Verfügbar)). Sie können den Link Network interface ID (Netzwerkschnittstellen-ID) wählen, um die Detailseite zu öffnen oder Sie können das Kontrollkästchen auf der linken Seite der Liste auswählen.
4. Wählen Sie die Instance aus, an die Sie anhängen möchten.
5. Um ENA Express zu verwenden, nachdem Sie die Netzwerkschnittstelle an die Instance angefügt haben, aktivieren Sie das Kontrollkästchen Enable (Aktivieren).
6. Wenn ENA Express aktiviert ist, können Sie die UDP-Einstellungen konfigurieren. Um ENA Express UDP zu verwenden, wählen Sie das Kontrollkästchen Enable (Aktivieren) aus.

7. Um die Netzwerkschnittstelle an die Instance anzuschließen und Ihre ENA Express-Einstellungen zu speichern, wählen Sie Attach (Anhängen).

AWS CLI

Auf dieser Registerkarte erfahren Sie, wie Sie die ENA-Express-Einstellungen in der AWS CLI konfigurieren.

Konfigurieren von ENA Express, wenn Sie eine Netzwerkschnittstelle anfügen

Um ENA Express zu konfigurieren, wenn Sie eine Netzwerkschnittstelle an eine Instanz anschließen, führen Sie den attach-network-interfaceBefehl in der aus AWS CLI, wie in den folgenden Beispielen gezeigt:

Beispiel 1: Verwenden von ENA Express für den TCP-Verkehr, aber nicht für den UDP-Verkehr

In diesem Beispiel konfigurieren wir `EnaSrdEnabled` als wahr und erlauben `EnaSrdUdpEnabled`, standardmäßig als falsch zu gelten.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification 'EnaSrdEnabled=true'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Beispiel 2: Verwenden von ENA Express sowohl für den TCP-Verkehr als auch für den UDP-Verkehr

In diesem Beispiel konfigurieren wir sowohl `EnaSrdEnabled` und `EnaSrdUdpEnabled` als wahr.

```
[ec2-user ~]$ aws ec2 attach-network-interface --network-interface-
id eni-0123f4567890a1b23 --instance-id i-0f1a234b5cd67e890 --device-index 1 --ena-
srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
{
"AttachmentId": "eni-attach-012c3d45e678f9012"
}
```

Aktualisieren der ENA-Express-Einstellungen für Ihren Netzwerkschnittstellenanhang

Um die ENA Express-Einstellungen für eine Netzwerkschnittstelle zu aktualisieren, die mit einer Instance verbunden ist, führen Sie den modify-network-interface-attributeBefehl in der aus AWS CLI, wie in den folgenden Beispielen gezeigt:

Beispiel 1: Verwenden von ENA Express für den TCP-Verkehr, aber nicht für den UDP-Verkehr

In diesem Beispiel konfigurieren wir `EnaSrdEnabled` als wahr und erlauben `EnaSrdUdpEnabled`, standardmäßig als falsch zu gelten, wenn es nicht zuvor schon eingestellt wurde.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --network-interface-
id eni-0123f4567890a1b23 --ena-srd-specification 'EnaSrdEnabled=true'
```

Beispiel 2: Verwenden von ENA Express sowohl für den TCP-Verkehr als auch für den UDP-Verkehr

In diesem Beispiel konfigurieren wir sowohl `EnaSrdEnabled` und `EnaSrdUdpEnabled` als wahr.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdEnabled=true,EnaSrdUdpSpecification={EnaSrdUdpEnabled=true}'
```

Beispiel 3: Beenden der Verwendung von ENA Express für den UDP-Verkehr

In diesem Beispiel konfigurieren wir `EnaSrdUdpEnabled` als falsch.

```
[ec2-user ~]$ aws ec2 modify-network-interface-attribute --
network-interface-id eni-0123f4567890a1b23 --ena-srd-specification
 'EnaSrdUdpSpecification={EnaSrdUdpEnabled=false}'
```

PowerShell

Auf dieser Registerkarte erfahren Sie, wie Sie die ENA Express-Einstellungen mithilfe von konfigurieren PowerShell.

Konfigurieren von ENA Express, wenn Sie eine Netzwerkschnittstelle anfügen

Um die ENA Express-Einstellungen für eine Netzwerkschnittstelle zu konfigurieren, führen Sie den Add-EC2NetworkInterface Cmdletmit den Tools für aus, PowerShell wie in den folgenden Beispielen gezeigt:

Beispiel 1: Verwenden von ENA Express für den TCP-Verkehr, aber nicht für den UDP-Verkehr

In diesem Beispiel konfigurieren wir `EnaSrdEnabled` als wahr und erlauben `EnaSrdUdpEnabled`, standardmäßig als falsch zu gelten.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true

eni-attach-012c3d45e678f9012
```

Beispiel 2: Verwenden von ENA Express sowohl für den TCP-Verkehr als auch für den UDP-Verkehr

In diesem Beispiel konfigurieren wir sowohl `EnaSrdEnabled` und `EnaSrdUdpEnabled` als wahr.

```
PS C:\> Add-EC2NetworkInterface `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-InstanceId i-0f1a234b5cd67e890 `
-DeviceIndex 1 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdUdpSpecification_EnaSrdUdpEnabled $true

eni-attach-012c3d45e678f9012
```

Aktualisieren der ENA-Express-Einstellungen für Ihren Netzwerkschnittstellenanhang

Um die ENA Express-Einstellungen für eine Netzwerkschnittstelle zu aktualisieren, die mit einer Instance verbunden ist, führen Sie den Add-EC2NetworkInterface CmdletBefehl in den Tools für aus PowerShell, wie in den folgenden Beispielen gezeigt:

Beispiel 1: Verwenden von ENA Express für den TCP-Verkehr, aber nicht für den UDP-Verkehr

In diesem Beispiel konfigurieren wir `EnaSrdEnabled` als wahr und erlauben `EnaSrdUdpEnabled`, standardmäßig als falsch zu gelten, wenn es nicht zuvor schon eingestellt wurde.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
```

```
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Beispiel 2: Verwenden von ENA Express sowohl für den TCP-Verkehr als auch für den UDP-Verkehr

In diesem Beispiel konfigurieren wir sowohl `EnaSrdEnabled` und `EnaSrdUdpEnabled` als wahr.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdEnabled $true `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $true ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : True
```

Beispiel 3: Beenden der Verwendung von ENA Express für den UDP-Verkehr

In diesem Beispiel konfigurieren wir `EnaSrdUdpEnabled` als falsch.

```
PS C:\> Edit-EC2NetworkInterfaceAttribute `
-NetworkInterfaceId eni-0123f4567890a1b23 `
-EnaSrdSpecification_EnaSrdUdpSpecification_EnaSrdUdpEnabled $false ;
Get-EC2NetworkInterface -NetworkInterfaceId eni-0123f4567890a1b23 | `
Select-Object `
    NetworkInterfaceId,
```

```
    @{Name = 'EnaSrdEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdEnabled }},
    @{Name = 'EnaSrdUdpEnabled'; Expression =
 { $_.Attachment.EnaSrdSpecification.EnaSrdUdpSpecification.EnaSrdUdpEnabled }} | `
Format-List

NetworkInterfaceId : eni-0123f4567890a1b23
EnaSrdEnabled      : True
EnaSrdUdpEnabled   : False
```

Konfigurieren Sie ENA Express beim Start

Sie können eine der folgenden Methoden verwenden, um ENA Express für ein AMI zu konfigurieren, wenn Sie eine Instance über die AWS Management Console starten.

- Sie können ENA Express für Ihr AMI konfigurieren, wenn Sie eine Instance mit dem Launch Instance Wizard starten. Ausführliche Informationen zur Konfiguration finden Sie unter Erweiterte Netzwerkkonfiguration in den Network settings (Netzwerkeinstellungen) für den Launch Instance Wizard.
- Sie können ENA Express für Ihr AMI konfigurieren, wenn Sie eine Startvorlage verwenden. Weitere Informationen zur Konfiguration von Startvorlagen finden Sie unter Erweiterte Netzwerkkonfiguration in den Network settings (Netzwerkeinstellungen) für Startvorlagen.

Überwachen der Leistung von ENA Express

Nachdem Sie ENA Express für die Netzwerkschnittstellenanhänge sowohl auf der sendenden als auch auf der empfangenden Instance aktiviert haben, können Sie ENA-Express-Metriken verwenden, um sicherzustellen, dass Ihre Instances die Leistungsverbesserungen der SRD-Technologie voll ausschöpfen.

Um eine Liste der Metriken anzuzeigen, die nach ENA Express gefiltert wurden, führen Sie den folgenden ethtool-Befehl für Ihre Netzwerkschnittstelle aus (hier dargestellt als `eth0`):

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
```

```
ena_srd_resource_utilization: 0
```

Überprüfen der ENA-Express-Einstellungen für eine Instance

Um die aktuellen ENA-Express-Einstellungen für den Netzwerkschnittstellenanhang auf Ihrer Instance zu überprüfen, führen Sie den`ethtool`-Befehl zum Auflisten der ENA-Express-Metriken aus und notieren Sie sich den Wert der `ena_srd_mode`-Metrik. Werte sind wie folgt:

- `0` = ENA Express aus, UDP aus
- `1` = ENA Express ein, UDP aus
- `2` = ENA Express aus, UDP ein

> **Note**
>
> Dies passiert nur, wenn ENA Express ursprünglich aktiviert war und UDP für dessen Verwendung konfiguriert wurde. Der vorherige Wert wird für UDP-Verkehr beibehalten.

- `3` = ENA Express ein, UDP ein

Nachdem Sie ENA Express für den Netzwerkschnittstellenanhang auf einer Instance aktiviert haben, initiiert die sendende Instance die Kommunikation mit der empfangenden Instance und SRD erkennt, ob ENA Express sowohl auf der sendenden als auch auf der empfangenden Instance ausgeführt wird. Wenn ENA Express in Betrieb ist, kann die Kommunikation eine SRD-Übertragung verwenden. Wenn ENA Express nicht funktioniert, fällt die Kommunikation auf die standardmäßige ENA-Übertragung zurück. Um zu überprüfen, ob die Paketübertragung SRD verwendet, können Sie die Anzahl der zulässigen Pakete (`ena_srd_eligible_tx_pkts`-Metrik) mit der Anzahl der übertragenen SRD-Pakete (`ena_srd_tx_pkts`-Metrik) während eines bestimmten Zeitraums vergleichen.

Mithilfe der `ena_srd_resource_utilization`-Metrik können Sie Ihre SRD-Ressourcenauslastung überwachen. Wenn Ihre Instance kurz davor ist, ihre SRD-Ressourcen zu erschöpfen, wissen Sie, dass es an der Zeit ist, die Instance aufzuskalieren.

Weitere Informationen zu ENA-Express-Metriken finden Sie unter Metriken für ENA Express.

Optimieren Sie die Leistung der ENA Express-Einstellungen

Um Ihre Linux-Instance-Konfiguration auf optimale ENA Express-Leistung zu überprüfen, können Sie das folgende Skript ausführen, das im GitHub Amazon-Repository verfügbar ist:

https://github.com/amzn/amzn-ec2-ena-utilities/blob/main/ena-express/check-ena-express-settings.sh

Das Skript führt eine Reihe von Tests durch und schlägt sowohl empfohlene als auch erforderliche Konfigurationsänderungen vor.

Aktivieren Sie Enhanced Networking mit der Intel 82599 VF-Schnittstelle auf Ihren EC2-Instances

Amazon EC2 stellt Enhanced Networking-Funktionen über die Intel 82599 VF-Schnittstelle bereit, die den Intel-Treiber `ixgbevf` verwendet.

Inhalt

Voraussetzungen

Zur Vorbereitung für Enhanced Networking mit der Intel 82599 VF-Schnittstelle sollten Sie Ihre Instance wie folgt einrichten:

- Wählen Sie einen der folgenden unterstützten Instance-Typen aus: C3, C4, D2, I2, M4 (außer `m4.16xlarge`) und R3.
- Überprüfen Sie, ob der Instance eine Verbindung zum Internet fehlt.
- Wenn Sie wichtige Daten auf der Instance gespeichert haben, die Sie erhalten möchten, sollten Sie diese Daten jetzt sichern, indem Sie ein AMI von Ihrer Instance erstellen. Die Aktualisierung von Kernels und Kernel-Modulen sowie die Aktivierung des Attributs `sriovNetSupport` kann dazu führen, dass Instances inkompatibel oder Betriebssysteme unerreichbar werden. Wenn Sie über ein aktuelles Backup verfügen, gehen die Daten nicht verloren, falls das geschieht.
- Linux-Instances — Starten Sie die Instance von einem HVM-AMI aus mit der Linux-Kernel-Version 2.6.32 oder höher. In den aktuellen Amazon Linux HVM-AMIs sind die für Enhanced Networking erforderlichen Module bereits installiert und die entsprechenden Attribute gesetzt. D. h., wenn Sie eine Amazon-EBS-gestützte Instance mit Enhanced-Networking-Unterstützung mithilfe eines

aktuellen Amazon Linux HVM-AMI starten, ist Enhanced Networking für Ihre Instance bereits aktiviert.

> **Warning**
>
> Enhanced Networking wird ausschließlich für HVM-Instances unterstützt. Die Aktivierung von Enhanced Networking in einer PV-Instance kann dazu führen, dass diese nicht mehr erreichbar ist. Das Setzen dieses Attributs, ohne dass das richtige Modul bzw. die richtige Modulversion vorhanden ist, kann ebenso dazu führen, dass die Instance nicht mehr erreichbar ist.

- Windows-Instances — Starten Sie die Instance von einem 64-Bit-HVM-AMI aus. Sie können Enhanced Networking unter Windows Server 2008 nicht aktivieren. Enhanced Networking ist in AMIs für Windows Server 2012 R2 sowie Windows Server 2016 und höher bereits aktiviert. Windows Server 2012 R2 enthält den Intel-Treiber 1.0.15.3; wir empfehlen, ein Upgrade dieses Treibers auf die aktuelle Version mithilfe des Dienstprogramms Pnputil.exe durchzuführen.
- Verwenden Sie AWS CloudShelldas AWS Management Console oder installieren und konfigurieren Sie das AWS CLIoder AWS Tools for Windows PowerShellauf einem beliebigen Computer Ihrer Wahl, vorzugsweise auf Ihrem lokalen Desktop oder Laptop. Weitere Informationen finden Sie unter Zugriff auf Amazon EC2 oder im AWS CloudShell -Benutzerhandbuch. Enhanced Networking kann nicht über die Amazon EC2-Konsole verwaltet werden.

Stellen Sie sicher, dass der Treiber installiert ist

Stellen Sie sicher, dass der Treiber auf Ihrer Instanz installiert ist.

Treiber für die Linux-Netzwerkschnittstelle

Prüfen Sie mit dem folgenden Befehl, ob das Modul aktuell an einer bestimmten Schnittstelle verwendet wird; setzen Sie dabei den Namen der Schnittstelle ein, die Sie überprüfen möchten. Wenn Sie eine einzige Schnittstelle verwenden (der Standard), lautet der Name `eth0`. Wenn das Betriebssystem vorhersagbare Netzwerknamen unterstützt, könnte der Name `ens5` lauten.

Im folgenden Beispiel wird das `ixgbevf`-Modul nicht geladen, da als Treiber `vif` angezeigt wird.

```
[ec2-user ~]$ ethtool -i eth0
driver: vif
version:
firmware-version:
```

```
bus-info: vif-0
supports-statistics: yes
supports-test: no
supports-eeprom-access: no
supports-register-dump: no
supports-priv-flags: no
```

In diesem Beispiel wird das Modul `ixgbevf` geladen. In dieser Instance wurde Enhanced Networking richtig konfiguriert.

```
[ec2-user ~]$ ethtool -i eth0
driver: ixgbevf
version: 4.0.3
firmware-version: N/A
bus-info: 0000:00:03.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: no
supports-register-dump: yes
supports-priv-flags: no
```

Windows-Netzwerkadapter

Sie überprüfen, ob der Treiber installiert wurde, indem Sie sich bei der Instance anmelden und den Geräte-Manager öffnen. Unter Network adapters sollte „Intel(R) 82599 Virtual Function” aufgeführt werden.

Testen, ob Enhanced Networking aktiviert ist

Stellen Sie sicher, dass das `sriovNetSupport` Attribut gesetzt ist.

Instanzattribut (sriovNetSupport)

Sie prüfen, ob in einer Instance das `sriovNetSupport`-Attribut für Enhanced Networking gesetzt wurde, indem Sie einen der folgenden Befehle verwenden. Wenn das Attribut gesetzt ist, ist der Wert. `simple`

- describe-instance-attribute (AWS CLI) (AWS CLI/AWS CloudShell)

```
aws ec2 describe-instance-attribute --instance-id instance_id --attribute
 sriovNetSupport
```

- Get-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Get-EC2InstanceAttribute -InstanceId instance-id -Attribute sriovNetSupport
```

Bildattribut (sriovNetSupport)

Verwenden Sie einen der folgenden Befehle, um zu überprüfen, ob für ein AMI bereits das erweiterte `sriovNetSupport` Netzwerkattribut festgelegt ist. Wenn das Attribut gesetzt ist, lautet der Wert`simple`.

- describe-images (AWS CLI)

```
aws ec2 describe-images --image-id ami_id --query "Images[].SriovNetSupport"
```

- Get-EC2Image (AWS Tools for Windows PowerShell)

```
(Get-EC2Image -ImageId ami-id).SriovNetSupport
```

Aktivieren von Enhanced Networking auf Ihrer Instance

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instanz ab.

> **Warning**
>
> Es ist nicht möglich, das Enhanced Networking-Attribut zu deaktivieren, wenn Sie es einmal aktiviert haben.

Amazon Linux

In den aktuellen Amazon Linux HVM-AMIs ist das für Enhanced Networking erforderliche `ixgbevf`-Modul bereits installiert und das `sriovNetSupport`-Attribute gesetzt. Wenn Sie also einen Instance-Typ mit einem aktuellen Amazon Linux-HVM-AMI starten, ist die optimierte Netzwerkfunktionalität bereits für die Instance aktiviert. Weitere Informationen finden Sie unter Testen, ob Enhanced Networking aktiviert ist.

Wenn Sie Ihre Instance aus einem älteren Amazon Linux AMI gestartet haben und Enhanced Networking noch nicht aktiviert wurde, gehen Sie wie folgt vor, um die optimierte Netzwerkleistung zu aktivieren.

Aktivieren von Enhanced Networking

1. Verbinden Sie sich mit der Instance.
2. Führen Sie den folgenden Befehl in der Instance aus, um die Instance mit dem aktuellen Kernel und den aktuellen Kernel-Modulen einschließlich `ixgbevf` zu aktualisieren:

   ```
   [ec2-user ~]$ sudo yum update
   ```

3. Starten Sie die Instance von Ihrem lokalen Computer aus neu, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: reboot-instances (AWS CLI), Restart-EC2Instance (AWS Tools for Windows PowerShell).
4. Stellen Sie erneut eine Verbindung mit der Instance her und prüfen Sie, ob das `ixgbevf`-Modul installiert wurde und in der empfohlenen Mindestversion vorliegt, indem Sie den Befehl modinfo ixgbevf aus dem Abschnitt Testen, ob Enhanced Networking aktiviert ist verwenden.
5. [EBS-gestützte Instance] Halten Sie die Instance von Ihrem lokalen Computer aus an, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: stop-instances (AWS CLI), Stop-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instanz von verwaltet wird AWS OpsWorks, sollten Sie die Instanz in der AWS OpsWorks Konsole beenden, damit der Instanzstatus synchron bleibt.

   [In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Gehen Sie stattdessen wie folgt vor: So aktivieren Sie Enhanced Networking (Instance Store-Backed Instances).
6. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

   AWS CLI

   modify-instance-attribute (AWS CLI)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

PowerShell

Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

7. (Optional) Erstellen Sie ein AMI von der Instance, wie unter Erstellen Sie ein Amazon EBS-backed AMI beschrieben. Das AMI erbt das Enhanced Networking-Attribut von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.
8. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instance in der AWS OpsWorks Konsole starten, damit der Instanzstatus synchron bleibt.
9. Stellen Sie eine Verbindung mit der Instance her und prüfen Sie, ob das `ixgbevf`-Modul installiert und in der Netzwerkschnittstelle geladen wurde, indem Sie den Befehl ethtool -i eth***n*** aus dem Abschnitt Testen, ob Enhanced Networking aktiviert ist verwenden.

So aktivieren Sie Enhanced Networking (Instance Store-Backed Instances)

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Erstellen einer Instance-Speicher-Backed Linux-AMI beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Ubuntu

Bevor Sie anfangen, überprüfen Sie, ob das Enhanced Networking bereits auf Ihrer Instance aktiviert ist.

Die Quick Start Ubuntu HVM AMIs enthalten die erforderlichen Treiber für Enhanced Networking. Bei einer Version von `ixgbevf` vor 2.16.4 können Sie das Kernel-Paket `linux-aws` installieren, um die neuesten Enhanced Networking-Treiber zu erhalten.

In der folgenden Anleitung sind die allgemeinen Schritte für die Kompilierung des `ixgbevf`-Moduls auf einer Ubuntu-Instance.

`linux-aws`-Kernel-Paket installieren

1. Verbinden Sie sich mit der Instance.
2. Aktualisieren Sie den Cache der Paketverwaltung und die einzelnen Pakete.

```
ubuntu:~$ sudo apt-get update && sudo apt-get upgrade -y linux-aws
```

> **Important**
>
> Wenn Sie während des Aktualisierungsvorgangs aufgefordert werden, `grub` zu installieren, verwenden Sie `/dev/xvda` für die Installation von `grub` und wählen Sie anschließend aus, dass die aktuelle Version von `/boot/grub/menu.lst` beibehalten werden soll.

Andere Linux-Distributionen

Bevor Sie anfangen, überprüfen Sie, ob das Enhanced Networking bereits auf Ihrer Instance aktiviert ist. Die neuesten Quick Start HVM AMIs enthalten die erforderlichen Treiber für Enhanced Networking, Sie müssen deshalb keine weiteren Schritte ausführen.

In der folgenden Anleitung werden die Schritte beschrieben, die Sie für die Aktivierung von Enhanced Networking für die Intel 82599 VF-Schnittstelle unter einer anderen Linux-Distributionen als Amazon Linux oder Ubuntu ausführen müssen. Weitere Informationen z. B. hinsichtlich der genauen Syntax für Befehle, der Speicherorte von Dateien oder der Unterstützung von einzelnen Paketen bzw. Tools finden Sie in der Dokumentation zu der jeweiligen Linux-Distribution.

Aktivieren von Enhanced Networking in Linux

1. Verbinden Sie sich mit der Instance.
2. Laden Sie die Quelldatei für das `ixgbevf`-Modul in Ihrer Instance herunter. Sie finden diese auf der Sourceforge-Website unter https://sourceforge.net/projects/e1000/files/ixgbevf%20stable/.

   Mit früheren Versionen von `ixgbevf` als 2.16.4 – einschließlich Version 2.14.2 – werden die Builds unter manchen Linux-Distributionen nicht richtig erstellt, einschließlich bestimmter Versionen von Ubuntu.
3. Kompilieren und installieren Sie das `ixgbevf`-Module in Ihrer Instance.

   > **Warning**
   >
   > Wenn Sie das `ixgbevf`-Modul für den aktuellen Kernel kompilieren und anschließend ein Upgrade des Kernels durchführen, ohne einen neuen Build des Treibers für den neuen Kernel zu erstellen, wechselt das System beim nächsten Neustart möglicherweise zum ursprünglichen `ixgbevf`-Modul der Verteilung zurück. Dies kann den Zugriff auf das System verhindern, wenn die verteilungsspezifische Version mit Enhanced Networking nicht kompatibel ist.
4. Führen Sie den Befehl sudo depmod aus, um die Abhängigkeiten für das Modul zu aktualisieren.
5. Aktualisieren Sie `initramfs` in Ihrer Instance, um sicherzustellen, dass das neue Modul während des Bootvorgangs geladen wird.
6. Ermitteln Sie, ob Ihr System standardmäßig transparente Netzwerkschnittstellennamen verwendet. Systeme, die systemd- oder udev-Versionen ab 197 verwenden, können Ethernet-Geräte umbenennen, d. h. die einzige Netzwerkschnittstelle in einem solchen System wird nicht zwingend als `eth0` bezeichnet. Dieses Verhalten kann Probleme bei der Verbindung mit Ihrer Instance verursachen. Weitere Informationen und andere Konfigurationsoptionen finden Sie unter Predictable Network Interface Names auf der freedesktop.org-Website.

   a. Sie können die systemd- und udev-Versionen auf RPM-basierten Systemen mit den folgenden Befehl überprüfen:

      ```
      [ec2-user ~]$ rpm -qa | grep -e '^systemd-[0-9]\+\|^udev-[0-9]\+'
      systemd-208-11.el7_0.2.x86_64
      ```

In dem Red Hat Enterprise Linux 7-Beispiel oben lautet die systemd-Version 208, d. h. transparente Netzwerkschnittstellennamen müssen deaktiviert werden.

b. Sie können transparente Netzwerkschnittstellennamen deaktivieren, indem Sie in der Zeile `net.ifnames=0` in der Datei `GRUB_CMDLINE_LINUX` die Option `/etc/default/grub` hinzufügen.

```
[ec2-user ~]$ sudo sed -i '/^GRUB\_CMDLINE\_LINUX/s/\"$/\ net\.ifnames\=0\"/' /
etc/default/grub
```

c. Erstellen Sie die neue Grub-Konfigurationsdatei.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. [EBS-gestützte Instance] Halten Sie die Instance von Ihrem lokalen Computer aus an, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: stop-instances (AWS CLI/AWS CloudShell), Stop-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instance in der AWS OpsWorks Konsole beenden, damit der Instanzstatus synchron bleibt.

   [In einem Instance-Speicher gesicherte Instance] Sie können die Instance nicht anhalten, um das Attribut zu ändern. Gehen Sie stattdessen wie folgt vor: So aktivieren Sie Enhanced Networking (Instance-Speicher-gestützte Instances):.

8. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

   ```
   Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
   ```

9. (Optional) Erstellen Sie ein AMI von der Instance, wie unter Erstellen Sie ein Amazon EBS-backed AMI beschrieben. Das AMI erbt das Enhanced Networking-Attribut von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.

   Wenn Ihr Instance-Betriebssystem eine `/etc/udev/rules.d/70-persistent-net.rules`-Datei enthält, müssen Sie diese vor der Erstellung des AMI löschen. Diese Datei enthält die MAC-Adresse des Ethernet-Adapters in der ursprünglichen Instance. Wenn eine andere Instance mit dieser Datei gestartet wird, kann das Betriebssystem das Gerät nicht finden und von `eth0` schlägt möglicherweise fehl, was zu Problemen beim Start führt. Diese Datei wird während des nächsten Bootvorgangs neu generiert, und jede aus dem AMI gestartete Instance erstellt eine eigene Version der Datei.
10. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instance in der AWS OpsWorks Konsole starten, damit der Instanzstatus synchron bleibt.
11. (Optional) Stellen Sie eine Verbindung mit Ihrer Instance her und überprüfen Sie, ob das Modul installiert wurde.

So aktivieren Sie Enhanced Networking (Instance-Speicher-gestützte Instances):

Führen Sie die Schritte aus dem vorherigen Verfahren durch bis zu dem Schritt, in dem die Instance angehalten wird. Erstellen Sie ein neues AMI, wie in Erstellen einer Instance-Speicher-Backed Linux-AMI beschreiben, um sicherzustellen, dass Sie das Enhanced Networking-Attribut aktivieren, wenn Sie das AMI registrieren.

AWS CLI

register-image (AWS CLI/AWS CloudShell)

```
aws ec2 register-image --sriov-net-support simple ...
```

PowerShell

Register-EC2Image (AWS Tools for Windows PowerShell)

```
Register-EC2Image -SriovNetSupport "simple" ...
```

Windows

Wenn Sie Ihre Instance gestartet haben und Enhanced Networking noch nicht aktiviert wurde, müssen Sie den erforderlichen Netzwerkadaptertreiber herunterladen und in der Instance installieren sowie anschließend das `sriovNetSupport`-Instance-Attribut setzen, um die optimierte Netzwerkleistung zu erzielen. Sie können dieses Attribut nur in unterstützten Instance-Typen aktivieren. Weitere Informationen finden Sie unter Unterstützung von Enhanced Networking.

> **Important**
>
> Die neuesten Treiberupdates in den Windows-AMIs finden Sie im Windows AMI-Versionsverlauf in der AWS Windows AMI-Referenz.

Aktivieren von Enhanced Networking

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. [Windows Server 2016 und höher] Führen Sie das folgende PowerShell EC2-Startskript aus, um die Instanz zu konfigurieren, nachdem der Treiber installiert wurde.

   ```
   PS C:\> C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeInstance.ps1 -Schedule
   ```

   > **Important**
   >
   > Das Administratorpasswort wird zurückgesetzt, wenn Sie das EC2-Launch-Skript zum Initialisieren der Instance aktivieren. Sie können die Konfigurationsdatei bearbeiten, um das Zurücksetzen des Administratorpassworts zu deaktivieren, indem Sie es in den Einstellungen für die Initialisierungsaufgaben festlegen.

3. Laden Sie von der Instance den Intel-Netzwerkadaptertreiber für Ihr Betriebssystem herunter:

   - Windows Server 2022

     Besuchen Sie die Download-Seite und laden Sie `Wired_driver_`*`version`*`_x64.zip` herunter.

   - Windows Server 2019, einschließlich Server-Version 1809 und neuer*

Besuchen Sie die Download-Seite und laden Sie `Wired_driver_version_x64.zip` herunter.

- Windows Server 2016, einschließlich Server-Version 1803 und früher*

  Besuchen Sie die Download-Seite und laden Sie `Wired_driver_version_x64.zip` herunter.

- Windows Server 2012 R2

  Besuchen Sie die Download-Seite und laden Sie `Wired_driver_version_x64.zip` herunter.

- Windows Server 2012

  Besuchen Sie die Download-Seite und laden Sie `Wired_driver_version_x64.zip` herunter.

- Windows Server 2008 R2

  Besuchen Sie die Download-Seite und laden Sie `PROWinx64Legacy.exe` herunter.

*Die Serverversionen 1803 und früher sowie 1809 und später werden auf den Intel-Seiten für Treiber und Software nicht ausdrücklich genannt.

4. Installieren Sie den Intel-Netzwerkadaptertreiber für Ihr Betriebssystem.

   - Windows Server 2008 R2

     1. Suchen Sie im Downloads-Ordner die Datei `PROWinx64Legacy.exe` und benennen Sie sie in `PROWinx64Legacy.zip` um.
     2. Extrahieren Sie den Inhalt der Datei `PROWinx64Legacy.zip`.
     3. Öffnen Sie die Befehlszeile, navigieren Sie zum extrahierten Ordner und führen Sie den folgenden Befehl aus, um das Dienstprogramm `pnputil` zum Hinzufügen und Installieren der INF-Datei im Treiberspeicher zu verwenden.

        ```
        C:\> pnputil -a PROXGB\Winx64\NDIS62\vxn62x64.inf
        ```

   - Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 und Windows Server 2012

     1. Extrahieren Sie im Downloads-Ordner den Inhalt der Datei `Wired_driver_version_x64.zip`.

2. Suchen Sie im extrahierten Ordner die Datei `Wired_driver_version_x64.exe` und benennen Sie sie in `Wired_driver_version_x64.zip` um.
3. Extrahieren Sie den Inhalt der Datei `Wired_driver_version_x64.zip`.
4. Öffnen Sie die Befehlszeile, navigieren Sie zum extrahierten Ordner und führen Sie einen der folgenden Befehle aus, um das Dienstprogramm `pnputil` zum Hinzufügen und Installieren der INF-Datei im Treiberspeicher zu verwenden.
   - Windows Server 2022

     ```
     C:\> pnputil -i -a PROXGB\Winx64\WS2022\vxs.inf
     ```

   - Windows Server 2019

     ```
     C:\> pnputil -i -a PROXGB\Winx64\NDIS68\vxn68x64.inf
     ```

   - Windows Server 2016

     ```
     C:\> pnputil -i -a PROXGB\Winx64\NDIS65\vxn65x64.inf
     ```

   - Windows Server 2012 R2

     ```
     C:\> pnputil -i -a PROXGB\Winx64\NDIS64\vxn64x64.inf
     ```

   - Windows Server 2012

     ```
     C:\> pnputil -i -a PROXGB\Winx64\NDIS63\vxn63x64.inf
     ```

5. Aktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mit einem der folgenden Befehle:

   AWS CLI

   modify-instance-attribute (AWS CLI/AWS CloudShell)

   ```
   aws ec2 modify-instance-attribute --instance-id instance_id --sriov-net-support
    simple
   ```

   PowerShell

   Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

```
Edit-EC2InstanceAttribute -InstanceId instance_id -SriovNetSupport "simple"
```

6. (Optional) Erstellen Sie ein AMI von der Instance, wie unter Erstellen Sie ein Amazon EBS-backed AMI beschrieben. Das AMI erbt das Enhanced Networking-Attribut von der Instance. D. h. Sie können mit diesem AMI eine andere Instance starten, in der Enhanced Networking standardmäßig aktiviert ist.
7. Starten Sie die Instance von Ihrem lokalen Computer aus, indem Sie die Amazon-EC2-Konsole oder einen der folgenden Befehle verwenden: start-instances (AWS CLI), Start-EC2Instance (AWS Tools for Windows PowerShell). Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instance in der AWS OpsWorks Konsole starten, damit der Instanzstatus synchron bleibt.

Fehlerbehebung bei Verbindungsproblemen

Wenn die Verbindung bei der Aktivierung von Enhanced Networkings verloren geht, ist das `ixgbevf`-Modul u. U. nicht mit dem Kernel kompatibel. Versuchen Sie, die Version des `ixgbevf`-Moduls zu installieren, die in der Linux-Distribution Ihrer Instance enthalten war.

Wenn Sie Enhanced Networking für eine PV-Instance oder -AMI aktivieren, ist Ihre Instance möglicherweise nicht mehr erreichbar.

Weitere Informationen finden Sie unter Wie aktiviere und konfiguriere ich Enhanced Networking auf meinen EC2-Instances?

Überwachen der Netzwerkleistung für Ihre EC2-Instance

Der Elastic Network Adapter (ENA)-Treiber veröffentlicht Netzwerkleistungsmetriken aus den Instances, in denen sie aktiviert sind. Sie können diese Metriken verwenden, um Probleme mit der Instance-Performance zu beheben, die richtige Instance-Größe für eine Workload auszuwählen, Skalierungsaktivitäten proaktiv zu planen und Anwendungen zu vergleichen, um zu bestimmen, ob sie die auf einer Instance verfügbare Leistung maximieren.

Amazon EC2 definiert Netzwerkmaxima auf Instance-Ebene, um ein qualitativ hochwertiges Netzwerkerlebnis zu gewährleisten, einschließlich einer konsistenten Netzwerkleistung für alle Instance-Größen. AWS bietet für jede Instance Höchstwerte für die folgenden Werte:

- Bandwidth capability (Bandbreitenfähigkeit) – Jede EC2-Instance verfügt über eine maximale Bandbreite für aggregierten ein- und ausgehenden Datenverkehr, basierend auf Instance-Typ

und -Größe. Manche Instances nutzen einen Netzwerk-I/O-Guthabenmechanismus, bei dem die Netzwerkbandbreite anhand der durchschnittlichen Bandbreitenauslastung zugewiesen wird. Amazon EC2 bietet außerdem eine maximale Bandbreite für den Datenverkehr zum AWS Direct Connect und zum Internet. Weitere Informationen finden Sie unter Netzwerkbandbreite für Amazon EC2-Instances.

- P acket-per-second (PPS) -Leistung — Jede EC2-Instance hat je nach Instance-Typ und Größe eine maximale PPS-Leistung.
- Connections tracked (Nachverfolgte Verbindungen) – Die Sicherheitsgruppe verfolgt jede aufgebaute Verbindung, um sicherzustellen, dass die Rückpakete wie erwartet übertragen werden. Es gibt eine maximale Anzahl von Verbindungen, die pro Instance verfolgt werden können. Weitere Informationen finden Sie unter Verbindungsverfolgung von Sicherheitsgruppen
- Link-local service access (Verbindungslokaler Servicezugriff) – Amazon EC2 bietet eine Schnittstelle für maximale PPS pro Netzwerk für Datenverkehr zu Services wie dem DNS-Service, dem Instance Metadata Service und dem Amazon Time Sync Service.

Wenn der Netzwerkverkehr für eine Instance einen Höchstwert überschreitet, wird der Datenverkehr, AWS der das Maximum überschreitet, geformt, indem Netzwerkpakete in eine Warteschlange gestellt und anschließend verworfen werden. Mithilfe der Metriken zur Netzwerkleistung können Sie überwachen, wann der Datenverkehr ein Maximum überschreitet. Diese Metriken informieren Sie in Echtzeit über Auswirkungen auf den Netzwerkverkehr und mögliche Probleme mit der Netzwerkleistung.

Inhalt

Voraussetzungen

Linux-Instances

- Installieren Sie ENA-Treiberversion 2.2.10 oder höher. Verwenden Sie den ethtool-Befehl, um die installierte Version zu überprüfen. Im folgenden Beispiel erfüllt die Version die Mindestanforderung.

```
[ec2-user ~]$ ethtool -i eth0 | grep version
version: 2.2.10
```

  Informationen zum Upgrade Ihres ENA-Treibers finden Sie unter Enhanced networking (Verbessertes Networking).
- Um diese Metriken in Amazon zu importieren CloudWatch, installieren Sie den CloudWatch Agenten. Weitere Informationen finden Sie unter Erfassung von Netzwerkleistungskennzahlen im CloudWatch Amazon-Benutzerhandbuch.
- Um `conntrack_allowance_available` Metric zu unterstützen, installieren Sie die ENA-Treiberversion 2.8.1.

Windows-Instances

- Installieren Sie ENA-Treiberversion 2.2.2 oder höher. Verwenden Sie den Geräte-Manager, um die installierte Version zu überprüfen.
  1. Öffnen Sie den Geräte-Manager, indem Sie `devmgmt.msc` ausführen.
  2. Erweitern Sie Network Adapters (Netzwerkadapter).
  3. Wählen Sie Amazon Elastic Network Adapter (Amazon-Elastic-Netzwerkadapter), Properties (Eigenschaften).
  4. Suchen Sie auf der Registerkarte Driver (Treiber) nach Driver Version (Treiberversion).

  Informationen zum Upgrade Ihres ENA-Treibers finden Sie unter Enhanced networking (Verbessertes Networking).
- Um diese Metriken in Amazon zu importieren CloudWatch, installieren Sie den CloudWatch Agenten. Weitere Informationen finden Sie unter Erfassung erweiterter Netzwerkmetriken im CloudWatch Amazon-Benutzerhandbuch.

Metriken für den ENA-Treiber

Der ENA-Treiber liefert die folgenden Metriken in Echtzeit an die Instance. Sie liefern die kumulative Anzahl von Paketen, die seit dem letzten Zurücksetzen des Treibers in jeder Netzwerkschnittstelle in die Warteschlange gestellt oder verworfen wurden.

Metrik	Beschreibung	Unterstützt auf
`bw_in_allowance_exceeded`	Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, da die eingehende aggregierte Bandbreite das Maximum für die Instance überschritten hat.	Allen Instance-Typen
`bw_out_allowance_exceeded`	Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, weil die ausgehende aggregierte Bandbreite das Maximum für die Instance überschritten hat.	Allen Instance-Typen
`conntrack_allowance_exceeded`	Die Anzahl der verworfenen Pakete, weil die Verbindungsverfolgung das Maximum für die Instance überschritten hat und keine neuen Verbindungen hergestellt werden konnten. Dies kann zu einem Paketverlust für den Datenverkehr zur oder von der Instance führen.	Allen Instance-Typen
`conntrack_allowance_available`	Die Anzahl der nachverfolgten Verbindungen, die von der Instance hergestellt werden können, bevor die zulässige Anzahl nachverfolgter Verbindun	Nur auf dem AWS Nitro-System aufgebaute Instances

Metrik	Beschreibung	Unterstützt auf
	gen dieses Instance-Typs erreicht wird.	
`linklocal_allowance_exceeded`	Die Anzahl der verworfenen Pakete, weil das PPS des Datenverkehrs zu lokalen Proxy-Diensten das Maximum für die Netzwerkschnittstelle überschritten hat. Dies wirkt sich auf den Datenverkehr zum DNS-Dienst, zum Instance Metadata Service und zum Amazon Time Sync Service aus.	Allen Instance-Typen
`pps_allowance_exceeded`	Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, weil die bidirektionale PPS das Maximum für die Instance überschritten hat.	Allen Instance-Typen

Anzeigen der Netzwerkleistungsmetriken für Ihre -Instance

Das Verfahren, das Sie verwenden, hängt vom Betriebssystem der Instanz ab.

Linux-Instances

Sie können Metriken in Ihren bevorzugten Tools veröffentlichen, um die Metrikdaten zu visualisieren. Sie können die Metriken beispielsweise CloudWatch mithilfe des CloudWatch Agenten auf Amazon veröffentlichen. Der Agent ermöglicht es Ihnen, einzelne Metriken auszuwählen und die Veröffentlichung zu steuern.

Sie können auch den ethtool verwenden, um die Metriken für jede Netzwerkschnittstelle wie eth0 wie folgt abzurufen.

```
[ec2-user ~]$ ethtool -S eth0
```

```
    bw_in_allowance_exceeded: 0
    bw_out_allowance_exceeded: 0
    pps_allowance_exceeded: 0
    conntrack_allowance_exceeded: 0
    linklocal_allowance_exceeded: 0
    conntrack_allowance_available: 136812
```

Windows-Instances

Sie können die Metriken mit jedem Verbraucher von Windows-Leistungsindikatoren anzeigen. Die Daten können gemäß dem EnaPerfCounters Manifest analysiert werden. Dies ist eine XML-Datei, die den Leistungsindikatoranbieter und seine Leistungsindikatoren definiert.

Um das Manifest zu installieren

Wenn Sie die Instance mit einem AMI gestartet haben, das ENA-Treiber 2.2.2 oder höher enthält oder das Installationsskript im Treiberpaket für ENA-Treiber 2.2.2 verwendet hat, ist das Manifest bereits installiert. Gehen Sie folgendermaßen vor, um das Manifest manuell zu installieren:

1. Entfernen Sie das vorhandene Manifest mit dem folgenden Befehl:

   ```
   unlodctr /m:EnaPerfCounters.man
   ```

2. Kopieren Sie die Manifestdatei `EnaPerfCounters.man` aus dem Treiberinstallationspaket nach `%SystemRoot%\System32\drivers`.
3. Installieren Sie das neue Manifest mit dem folgenden Befehl:

   ```
   lodctr /m:EnaPerfCounters.man
   ```

Um Metriken mit Performance Monitor anzuzeigen

1. Öffnen Sie Performance Monitor.
2. Drücken Sie Strg+N, um neue Leistungsindikatoren hinzuzufügen.
3. Wählen Sie ENA Packets Shaping (ENA-Paketformung) aus der Liste aus.
4. Wählen Sie die zu überwachenden Instances aus und wählen Sie Add (Hinzufügen).
5. Klicken Sie auf OK.

Metriken für ENA Express

ENA Express basiert auf der SRD-Technologie (AWS Scalable Reliable Datagram). SRD ist ein leistungsstarkes Netzwerktransportprotokoll, das dynamisches Routing verwendet, um den Durchsatz zu erhöhen und die Tail-Latenz zu minimieren. Sie können ENA-Express-Metriken verwenden, um sicherzustellen, dass Ihre Instances die Leistungsverbesserungen, die die SRD-Technologie bietet, voll ausschöpfen, zum Beispiel:

- Bewerten Sie Ihre Ressourcen, um sicherzustellen, dass sie über ausreichende Kapazitäten verfügen, um mehr SRD-Verbindungen herzustellen.
- Identifizieren Sie, wo potenzielle Probleme bestehen, die verhindern, dass berechtigte ausgehende Pakete SRD verwenden.
- Berechnen Sie den Prozentsatz des ausgehenden Datenverkehrs, welcher SRD für die Instance verwendet.
- Berechnen Sie den Prozentsatz des eingehenden Datenverkehrs, welcher SRD für die Instance verwendet.

> **Note**
>
> Verwenden Sie zum Erstellen von Metriken die Treiberversion 2.8 oder höher.

Die folgenden ENA-Express-Metriken sind mit dem ethtool-Befehl für Linux-basierte Instances verfügbar.

- `ena_srd_mode` – Beschreibt, welche ENA-Express-Features aktiviert sind. Werte sind wie folgt:
  - `0` = ENA Express aus, UDP aus
  - `1` = ENA Express ein, UDP aus
  - `2` = ENA Express aus, UDP ein

    > **Note**
    >
    > Dies passiert nur, wenn ENA Express ursprünglich aktiviert war und UDP für dessen Verwendung konfiguriert wurde. Der vorherige Wert wird für UDP-Verkehr beibehalten.

  - `3` = ENA Express ein, UDP ein

- `ena_srd_eligible_tx_pkts` – Die Anzahl der innerhalb eines bestimmten Zeitraums gesendeten Netzwerkpakete, die die SRD-Anforderungen für die Zulassung erfüllen, wie folgt:
  - Sowohl sendende als auch empfangende Instance-Typen werden unterstützt. Weitere Informationen finden Sie in der Unterstützte Instance-Typen für ENA Express-Tabelle.
  - Sowohl die sendenden als auch die empfangenden Instances müssen ENA Express konfiguriert haben.
  - Die sendenden und empfangenden Instances müssen in derselben Availability Zone ausgeführt werden.
  - Der Netzwerkpfad zwischen den Instances darf keine Middleware-Boxen enthalten. ENA Express unterstützt derzeit keine Middleware-Boxen.

  > **Note**
  >
  > Die ENA-Express-Zulassungsmetrik deckt die Quell- und Zielanforderungen sowie das Netzwerk zwischen den beiden Endpunkten ab. Zugelassene Pakete können immer noch disqualifiziert werden, nachdem sie bereits gezählt wurden. Wenn beispielsweise ein berechtigtes Paket das Maximum Transmission Unit (MTU)-Limit überschreitet, wird auf die standardmäßige ENA-Übertragung zurückgegriffen, obwohl das Paket im Zähler immer noch als geeignet angezeigt wird.

- `ena_srd_tx_pkts` – Die Anzahl der SRD-Pakete, die innerhalb eines bestimmten Zeitraums übertragen wurden.
- `ena_srd_rx_pkts` – Die Anzahl der SRD-Pakete, die innerhalb eines bestimmten Zeitraums empfangen wurden.
- `ena_srd_resource_utilization` – Der Prozentsatz der maximal zulässigen Speichernutzung für gleichzeitige SRD-Verbindungen, den die Instance verbraucht hat.

Um eine Liste der Metriken anzuzeigen, die nach ENA Express gefiltert wurden, führen Sie den folgenden ethtool-Befehl für Ihre Netzwerkschnittstelle aus (hier dargestellt als `eth0`):

```
[ec2-user ~]$ ethtool -S eth0 | grep ena_srd
NIC statistics:
 ena_srd_mode: 0
 ena_srd_tx_pkts: 0
 ena_srd_eligible_tx_pkts: 0
 ena_srd_rx_pkts: 0
```

```
ena_srd_resource_utilization: 0
```

Ausgehender Verkehr (ausgehende Pakete)

Um sicherzustellen, dass Ihr ausgehender Verkehr SRD wie erwartet verwendet, vergleichen Sie die Anzahl der SRD-fähigen Pakete (`ena_srd_eligible_tx_pkts`) mit der Anzahl der gesendeten SRD-Pakete (`ena_srd_tx_pkts`) über einen bestimmten Zeitraum.

Signifikante Unterschiede zwischen der Anzahl der berechtigten Pakete und der Anzahl der gesendeten SRD-Pakete werden häufig durch Probleme mit der Ressourcenauslastung verursacht. Wenn die an die Instance angeschlossene Netzwerkkarte ihre maximalen Ressourcen aufgebraucht hat oder wenn die Pakete das MTU-Limit überschreiten, können berechtigte Pakete nicht über SRD übertragen werden und müssen auf die standardmäßige ENA-Übertragung zurückgreifen. Pakete können auch bei Live-Migrationen oder Live-Server-Updates in diese Lücke fallen. Eine zusätzliche Fehlerbehebung ist erforderlich, um die Grundursache zu ermitteln.

> **Note**
>
> Sie können gelegentliche geringfügige Unterschiede zwischen der Anzahl der berechtigten Pakete und der Anzahl der SRD-Pakete ignorieren. Dies kann beispielsweise passieren, wenn Ihre Instance eine Verbindung zu einer anderen Instance für SRD-Traffic herstellt.

Um herauszufinden, welcher Prozentsatz Ihres gesamten ausgehenden Datenverkehrs in einem bestimmten Zeitraum SRD verwendet, vergleichen Sie die Anzahl der gesendeten SRD-Pakete (`ena_srd_tx_pkts`) mit der Gesamtzahl der Pakete, die während dieser Zeit für die Instance (`NetworkPacketOut`) gesendet wurden.

Eingehender Verkehr (eingehende Pakete)

Um herauszufinden, welcher Prozentsatz Ihres gesamten eingehenden Datenverkehrs in einem bestimmten Zeitraum SRD verwendet, vergleichen Sie die Anzahl der empfangenen SRD-Pakete (`ena_srd_rx_pkts`) mit der Gesamtzahl der Pakete, die während dieser Zeit von der Instance (`NetworkPacketIn`) erhalten wurden.

Ressourcenauslastung

Die Ressourcenauslastung basiert auf der Anzahl der gleichzeitigen SRD-Verbindungen, die eine einzelne Instance zu einem bestimmten Zeitpunkt unterhalten kann. Die Metrik zur Ressourcenauslastung (`ena_srd_resource_utilization`) verfolgt Ihre aktuelle Auslastung für

die Instance. Wenn sich die Auslastung 100 % nähert, können Sie Leistungsproblemen erwarten. ENA Express greift von der SRD auf die standardmäßige ENA-Übertragung zurück und die Wahrscheinlichkeit, dass Pakete verworfen werden, steigt. Eine hohe Ressourcenauslastung ist ein Zeichen dafür, dass es an der Zeit ist, die Instance aufzuskalieren, um die Netzwerkleistung zu verbessern.

> **Note**
>
> Wenn der Netzwerkverkehr für eine Instance ein Maximum überschreitet, wird der Datenverkehr, AWS der das Maximum überschreitet, geformt, indem Netzwerkpakete in eine Warteschlange gestellt und anschließend gelöscht werden.

Persistenz

Ausgangs- und Eingangsmetriken fallen an, solange ENA Express für die Instance aktiviert ist. Metriken fallen nicht mehr an, wenn ENA Express deaktiviert ist, aber sie bleiben bestehen, solange die Instance noch läuft. Die Metriken werden zurückgesetzt, wenn die Instance neu gestartet oder beendet wird oder wenn die Netzwerkschnittstelle von der Instance getrennt ist.

Metriken zur Netzwerkleistung mit dem DPDK-Treiber für ENA

Die ENA-Treiberversion 2.2.0 und höher unterstützt die Berichterstellung von Netzwerkmetriken. DPDK 20.11 enthält den ENA-Treiber 2.2.0 und ist die erste DPDK-Version, die dieses Feature unterstützt.

Sie können eine Beispielanwendung verwenden, um DPDK-Statistiken anzuzeigen. Um eine interaktive Version der Beispielanwendung zu starten, führen Sie den folgenden Befehl aus.

```
./app/dpdk-testpmd -- -i
```

In dieser interaktiven Sitzung können Sie einen Befehl eingeben, um erweiterte Statistiken für einen Port abzurufen. Der folgende Beispielbefehl ruft die Statistiken für Port 0 ab.

```
show port xstats 0
```

Das Folgende ist ein Beispiel für eine interaktive Sitzung mit der DPDK-Beispielanwendung.

```
[root@ip-192.0.2.0 build]# ./app/dpdk-testpmd -- -i
        EAL: Detected 4 lcore(s)
```

```
        EAL: Detected 1 NUMA nodes
        EAL: Multi-process socket /var/run/dpdk/rte/mp_socket
        EAL: Selected IOVA mode 'PA'
        EAL: Probing VFIO support...
        EAL:   Invalid NUMA socket, default to 0
        EAL:   Invalid NUMA socket, default to 0
        EAL: Probe PCI driver: net_ena (1d0f:ec20) device: 0000:00:06.0
(socket 0)
        EAL: No legacy callbacks, legacy socket not created
        Interactive-mode selected

        Port 0: link state change event
        testpmd: create a new mbuf pool <mb_pool_0>: n=171456,
size=2176, socket=0
        testpmd: preferred mempool ops selected: ring_mp_mc

        Warning! port-topology=paired and odd forward ports number, the
last port will pair with itself.

        Configuring Port 0 (socket 0)
        Port 0: 02:C7:17:A2:60:B1
        Checking link statuses...
        Done
        Error during enabling promiscuous mode for port 0: Operation
not supported - ignore
        testpmd> show port xstats 0
        ###### NIC extended statistics for port 0
        rx_good_packets: 0
        tx_good_packets: 0
        rx_good_bytes: 0
        tx_good_bytes: 0
        rx_missed_errors: 0
        rx_errors: 0
        tx_errors: 0
        rx_mbuf_allocation_errors: 0
        rx_q0_packets: 0
        rx_q0_bytes: 0
        rx_q0_errors: 0
        tx_q0_packets: 0
        tx_q0_bytes: 0
        wd_expired: 0
        dev_start: 1
        dev_stop: 0
        tx_drops: 0
```

```
        bw_in_allowance_exceeded: 0
        bw_out_allowance_exceeded: 0
        pps_allowance_exceeded: 0
        conntrack_allowance_exceeded: 0
        linklocal_allowance_exceeded: 0
        rx_q0_cnt: 0
        rx_q0_bytes: 0
        rx_q0_refill_partial: 0
        rx_q0_bad_csum: 0
        rx_q0_mbuf_alloc_fail: 0
        rx_q0_bad_desc_num: 0
        rx_q0_bad_req_id: 0
        tx_q0_cnt: 0
        tx_q0_bytes: 0
        tx_q0_prepare_ctx_err: 0
        tx_q0_linearize: 0
        tx_q0_linearize_failed: 0
        tx_q0_tx_poll: 0
        tx_q0_doorbells: 0
        tx_q0_bad_req_id: 0
        tx_q0_available_desc: 1023
        testpmd>
```

Weitere Informationen über die Beispielanwendung und deren Verwendung zum Abrufen erweiterter Statistiken. Siehe Testpmd Application User Guide (Testpmd-Anwendungs-Benutzerhandbuch) in der DPDK-Dokumentation.

Metriken für Instances, auf denen FreeBSD läuft

Ab Version 2.3.0 unterstützt der ENA-FreeBSD-Treiber das Sammeln von Netzwerkleistungsmetriken auf Instances, auf denen FreeBSD ausgeführt wird. Um die Erfassung von FreeBSD-Metriken zu aktivieren, geben Sie den folgenden Befehl ein und legen Sie das *Intervall* auf einen Wert zwischen 1 und 3600 fest. Dies gibt an, wie oft in Sekundenschnelle FreeBSD-Metriken gesammelt werden.

```
sysctl dev.ena.network_interface.eni_metrics.sample_interval=interval
```

Mit dem folgenden Befehl wird beispielsweise festgelegt, dass der Treiber alle 10 Sekunden FreeBSD-Metriken auf der Netzwerkschnittstelle 1 sammelt:

```
sysctl dev.ena.1.eni_metrics.sample_interval=10
```

Um die Sammlung von FreeBSD-Metriken zu deaktivieren, können Sie den vorhergehenden Befehl ausführen und `0` als das *`Intervall`* angeben.

Nachdem Sie das Sammeln von FreeBSD-Metriken aktiviert haben, können Sie die neuesten gesammelten Metriken abrufen, indem Sie den folgenden Befehl ausführen.

```
sysctl dev.ena.network_interface.eni_metrics
```

Beheben Sie Fehler beim Elastic Network Adapter unter Linux

Der Elastic Network Adapter (ENA) soll die Integrität des Betriebssystems verbessern und mögliche langfristige Störungen aufgrund von unerwartetem Hardwareverhalten oder Fehlern verringern. In der ENA-Architektur bleiben Geräte- oder Treiberfehler für das System weitestgehend transparent. Dieses Thema enthält Informationen zur Fehlerbehebung für ENA.

Beginnen Sie mit Abschnitt Fehlerbehebung bei Verbindungsproblemen, wenn Sie keine Verbindung mit Ihrer Instance herstellen können.

Wenn nach der Migration zu einem Instance-Typ der sechsten Generation Leistungseinbußen auftreten, lesen Sie den Artikel Was muss ich tun, bevor ich meine EC2-Instance auf eine Instance der sechsten Generation migriere, um sicherzustellen, dass ich die maximale Netzwerkleistung erhalte?

Wenn Sie eine Verbindung mit Ihrer Instance herstellen können, können Sie mithilfe der Fehlererkennungs- und Wiederherstellungsmechanismen Diagnose-Informationen sammeln. Ausführliche Informationen zu diesen Mechanismen finden Sie in den weiteren Abschnitten dieses Themas.

Inhalt

Fehlerbehebung bei Verbindungsproblemen

Wenn die Verbindung bei der Aktivierung des Enhanced Networking verloren geht, ist das `ena`-Modul u. U. nicht mit der Kernelversion Ihrer Instance kompatibel. Dies geschieht z .B. dann, wenn Sie das Modul für eine bestimmte Kernelversion (ohne Befehl dkms oder mit einer falsch konfigurierten dkms.conf-Datei) installieren und Ihr Instance-Kernel anschließend aktualisiert wird. Wenn der beim Start geladene Instance-Kernel nicht über ein richtig installiertes `ena`-Modul verfügt, erkennt Ihre Instance den Netzwerkadapter nicht und Ihre Instance ist nicht erreichbar.

Wenn Sie Enhanced Networking für eine PV-Instance oder ein AMI aktivieren, kann es ebenfalls vorkommen, dass Ihre Instance nicht erreichbar ist.

Wenn Ihre Instance nach dem Aktivieren von Enhanced Networking mit ENA nicht erreichbar ist, können Sie das Attribut `enaSupport` für Ihre Instance deaktivieren, damit diese wieder den üblichen Netzwerkadapter nutzt.

So deaktivieren Sie Enhanced Networking mit ENA (EBS-gestützte Instances)

1. Stoppen Sie die Instance von Ihrem lokalen Computer aus mithilfe der Amazon EC2 EC2-Konsole oder mit einem der folgenden Befehle: stop-instances (AWS CLI), Stop-EC2Instance().AWS Tools for Windows PowerShell Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instance in der AWS OpsWorks Konsole beenden, damit der Instance-Status synchron bleibt.

   > **Important**
   >
   > Wenn Sie eine Instance Store-Backed Instance verwenden, können Sie die Instance nicht anhalten. Fahren Sie stattdessen mit So deaktivieren Sie Enhanced Networking mit ENA (Instance Store-Backed Instances) fort.

2. Deaktivieren Sie auf Ihrem lokalen Computer das Enhanced Networking-Attribut mithilfe des folgenden Befehls:

   - modify-instance-attribute (AWS CLI)

     ```
     $ C:\> aws ec2 modify-instance-attribute --instance-id instance_id --no-ena-support
     ```

3. Starten Sie die Instance von Ihrem lokalen Computer aus mit der Amazon EC2 EC2-Konsole oder mit einem der folgenden Befehle: start-instances (AWS CLI), Start-EC2Instance().AWS

Tools for Windows PowerShell Wenn Ihre Instance von verwaltet wird AWS OpsWorks, sollten Sie die Instance in der AWS OpsWorks Konsole starten, damit der Instance-Status synchron bleibt.

4. (Optional) Stellen Sie eine Verbindung mit Ihrer Instance her und versuchen Sie, das Modul `ena` erneut mit Ihrer aktuellen Kernelversion zu installieren, indem Sie die entsprechenden Schritte unter Aktivieren Sie Enhanced Networking mit dem Elastic Network Adapter (ENA) auf Ihren EC2-Instances ausführen.

So deaktivieren Sie Enhanced Networking mit ENA (Instance Store-Backed Instances)

Wenn es sich bei Ihrer Instance um eine Instance Store-Backed Instance handelt, müssen Sie ein neues AMI wie unter Erstellen einer Instance-Speicher-Backed Linux-AMI beschrieben erstellen. Vergewissern Sie sich, dass Sie das Enhanced Networking-Attribut `enaSupport` deaktivieren, wenn Sie das AMI registrieren.

- register-image (AWS CLI)

```
$ C:\> aws ec2 register-image --no-ena-support ...
```

- Register-EC2Image (AWS Tools for Windows PowerShell)

```
C:\> Register-EC2Image -EnaSupport $false ...
```

Keep-Alive-Mechanismus

Das ENA-Gerät sendet Keep-Alive-Ereignisse in einem bestimmten Zeitintervall (i. d. R. einmal pro Sekunde). Der ENA-Treiber implementiert einen Überwachungsmechanismus, der regelmäßig nach allen Keep-Alive-Nachrichten sucht. Wenn eine oder mehrere Nachrichten vorhanden sind, wird der Überwachungsmechanismus wieder aktiviert. Andernfalls geht der Treiber davon aus, dass ein Gerätefehler vorliegt, und ergreift folgende Maßnahmen:

- Er legt seine aktuellen Statistiken unter syslog ab.
- Er setzt das ENA-Gerät zurück.
- Er setzt den ENA-Treiberstatus zurück.

Der obige Zurücksetzungsvorgang kann kurzzeitig zu einem Traffic-Verlust führen (TCP-Verbindungen können i. d. R. wiederhergestellt werden), der aber keine weiteren Auswirkungen für den Benutzer haben sollte.

Das ENA-Gerät fordert u. U. indirekt eine Gerätezurücksetzung an, indem keine Keep-Alive-Benachrichtigung gesendet wird, z. B. wenn das ENA-Gerät nach dem Laden einer nicht wiederherstellbaren Konfiguration in einen unbekannten Status versetzt wird.

Im Folgenden finden Sie ein Beispiel für das Reset-Verfahren:

```
[18509.800135] ena 0000:00:07.0 eth1: Keep alive watchdog timeout. // The watchdog
 process initiates a reset
[18509.815244] ena 0000:00:07.0 eth1: Trigger reset is on
[18509.825589] ena 0000:00:07.0 eth1: tx_timeout: 0 // The driver logs the current
 statistics
[18509.834253] ena 0000:00:07.0 eth1: io_suspend: 0
[18509.842674] ena 0000:00:07.0 eth1: io_resume: 0
[18509.850275] ena 0000:00:07.0 eth1: wd_expired: 1
[18509.857855] ena 0000:00:07.0 eth1: interface_up: 1
[18509.865415] ena 0000:00:07.0 eth1: interface_down: 0
[18509.873468] ena 0000:00:07.0 eth1: admin_q_pause: 0
[18509.881075] ena 0000:00:07.0 eth1: queue_0_tx_cnt: 0
[18509.888629] ena 0000:00:07.0 eth1: queue_0_tx_bytes: 0
[18509.895286] ena 0000:00:07.0 eth1: queue_0_tx_queue_stop: 0
.......
........
[18511.280972] ena 0000:00:07.0 eth1: free uncompleted tx skb qid 3 idx 0x7 // At the
 end of the down process, the driver discards incomplete packets.
[18511.420112] [ENA_COM: ena_com_validate_version] ena device version: 0.10 //The
 driver begins its up process
[18511.420119] [ENA_COM: ena_com_validate_version] ena controller version: 0.0.1
 implementation version 1
[18511.420127] [ENA_COM: ena_com_admin_init] ena_defs : Version:[b9692e8] Build date
 [Wed Apr  6 09:54:21 IDT 2016]
[18512.252108] ena 0000:00:07.0: Device watchdog is Enabled
[18512.674877] ena 0000:00:07.0: irq 46 for MSI/MSI-X
[18512.674933] ena 0000:00:07.0: irq 47 for MSI/MSI-X
[18512.674990] ena 0000:00:07.0: irq 48 for MSI/MSI-X
[18512.675037] ena 0000:00:07.0: irq 49 for MSI/MSI-X
[18512.675085] ena 0000:00:07.0: irq 50 for MSI/MSI-X
[18512.675141] ena 0000:00:07.0: irq 51 for MSI/MSI-X
[18512.675188] ena 0000:00:07.0: irq 52 for MSI/MSI-X
[18512.675233] ena 0000:00:07.0: irq 53 for MSI/MSI-X
```

```
[18512.675279] ena 0000:00:07.0: irq 54 for MSI/MSI-X
[18512.772641] [ENA_COM: ena_com_set_hash_function] Feature 10 isn't supported
[18512.772647] [ENA_COM: ena_com_set_hash_ctrl] Feature 18 isn't supported
[18512.775945] ena 0000:00:07.0: Device reset completed successfully // The reset
 process is complete
```

Timeout für Registerlesevorgänge

Bei der ENA-Architektur kommt es nur zu einer begrenzten Nutzung von im Speicher abgebildeten I/O-Lesevorgängen (MMIO). Der ENA-Treiber greift nur während seines Initialisierungsvorgangs auf MMIO-Register zu.

Wenn die Treiberprotokolle (verfügbar in der dmesg-Ausgabe) Fehler bei Lesevorgängen ausgeben, kann die Ursache ein nicht kompatibler oder falsch kompilierter Treiber, ein ausgelastetes Hardwaregerät oder einen Hardwarefehler sein.

Intermittierende Protokolleinträge, die auf Fehler bei Lesevorgängen hinweisen, stellen i. d. R. kein Problem dar. Der Treiber führt dafür in diesem Fall einen neuen Versuch durch. Eine Reihe von Protokolleinträgen mit Lesefehlern deuten jedoch auf ein Treiber- oder Hardwareproblem hin.

Nachfolgend finden Sie ein Beispiel für einen Treiber-Protokolleintrag, der auf einen Lesevorgangsfehler aufgrund eines Timeouts hindeutet:

```
[ 47.113698] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[1] offset[88] actual: req id[57006] offset[0]
[ 47.333715] [ENA_COM: ena_com_reg_bar_read32] reading reg failed for timeout.
 expected: req id[2] offset[8] actual: req id[57007] offset[0]
[ 47.346221] [ENA_COM: ena_com_dev_reset] Reg read32 timeout occurred
```

Statistiken

Falls eine unzureichende Netzwerkleistung oder Latenzprobleme auftreten, sollten Sie die Gerätestatistiken aufrufen und überprüfen. Diese Statistiken können Sie mithilfe von ethtool wie folgt aufrufen.

```
[ec2-user ~]$ ethtool -S ethN
NIC statistics:
 tx_timeout: 0
 suspend: 0
 resume: 0
 wd_expired: 0
```

```
  interface_up: 1
  interface_down: 0
  admin_q_pause: 0
  bw_in_allowance_exceeded: 0
  bw_out_allowance_exceeded: 0
  pps_allowance_exceeded: 0
  conntrack_allowance_available: 450878
  conntrack_allowance_exceeded: 0
  linklocal_allowance_exceeded: 0
  queue_0_tx_cnt: 4329
  queue_0_tx_bytes: 1075749
  queue_0_tx_queue_stop: 0
  ...
```

Unten sind die folgenden Befehlsausgabeparameter beschrieben:

`tx_timeout`: *N*

Gibt an, wie oft der Netdev-Überwachungsmechanismus aktiviert wurde.

`suspend`: *N*

Gibt an, wie oft der Treiber eine Aussetzung durchgeführt hat.

`resume`: *N*

Gibt an, wie oft der Treiber eine Wiederaufnahme durchgeführt hat.

`wd_expired`: *N*

Gibt an, wie oft der Treiber in den letzten drei Sekunden kein Keep-Alive-Ereignis empfangen hat.

`interface_up`: *N*

Gibt an, wie oft die ENA-Schnittstelle aufgerufen wurde.

`interface_down`: *N*

Gibt an, wie oft die ENA-Schnittstelle heruntergefahren wurde.

`admin_q_pause`: *N*

Gibt an, wie oft die Admin-Warteschlange nicht in einem laufenden Zustand gefunden wurde.

`bw_in_allowance_exceeded`: *N*

Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, da die eingehende aggregierte Bandbreite das Maximum für die Instance überschritten hat.

`bw_out_allowance_exceeded`: *N*

Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, weil die ausgehende aggregierte Bandbreite das Maximum für die Instance überschritten hat.

`pps_allowance_exceeded`: *N*

Die Anzahl der Pakete, die in die Warteschlange gestellt oder verworfen wurden, weil die bidirektionale PPS das Maximum für die Instance überschritten hat.

`conntrack_allowance_available`: *N*

Die Anzahl der nachverfolgten Verbindungen, die von der Instance hergestellt werden können, bevor die zulässige Anzahl nachverfolgter Verbindungen dieses Instance-Typs erreicht wird. Nur für Nitro-basierte Instances verfügbar. Wird mit FreeBSD-Instances oder DPDK-Umgebungen nicht unterstützt.

`conntrack_allowance_exceeded`: *N*

Die Anzahl der verworfenen Pakete, weil die Verbindungsverfolgung das Maximum für die Instance überschritten hat und keine neuen Verbindungen hergestellt werden konnten. Dies kann zu einem Paketverlust für den Datenverkehr zur oder von der Instance führen.

`linklocal_allowance_exceeded`: *N*

Die Anzahl der verworfenen Pakete, weil das PPS des Datenverkehrs zu lokalen Proxy-Diensten das Maximum für die Netzwerkschnittstelle überschritten hat. Dies wirkt sich auf den Datenverkehr zum DNS-Dienst, zum Instance Metadata Service und zum Amazon Time Sync Service aus.

`queue_`*N*`_tx_cnt`: *N*

Gibt die Anzahl der übertragenen Pakete für diese Warteschlange an.

`queue_`*N*`_tx_bytes`: *N*

Gibt die Anzahl von übertragenen Bytes für diese Warteschlange an.

`queue_`*N*`_tx_queue_stop`: *N*

Gibt an, wie oft die Warteschlange *N* vollständig gefüllt war und angehalten wurde.

`queue_`*N*`_tx_queue_wakeup`: *N*

Gibt an, wie oft die Warteschlange *N* nach dem Anhalten wieder gestartet wurde.

`queue_N_tx_dma_mapping_err`: *N*

Fehleranzahl für direkten Speicherzugriff. Wenn dieser Wert nicht 0 ist, weist dies auf einen niedrigen Stand der Systemressourcen hin.

`queue_N_tx_linearize`: *N*

Gibt an, wie oft die SKB-Linearisierung für diese Warteschlange versucht wurde.

`queue_N_tx_linearize_failed`: *N*

Gibt an, wie oft die SKB-Linearisierung für diese Warteschlange fehlgeschlagen ist.

`queue_N_tx_napi_comp`: *N*

Gibt an, wie oft der `napi`-Handler `napi_complete` für diese Warteschlange aufgerufen hat.

`queue_N_tx_tx_poll`: *N*

Gibt an, wie oft der `napi`-Handler für diese Warteschlange geplant war.

`queue_N_tx_doorbells`: *N*

Gibt die Anzahl der Übertragungs-Doorbells für diese Warteschlange an.

`queue_N_tx_prepare_ctx_err`: *N*

Gibt an, wie oft `ena_com_prepare_tx` für diese Warteschlange fehlgeschlagen ist.

`queue_N_tx_bad_req_id`: *N*

Ungültige `req_id` für diese Warteschlange. Die gültige `req_id` ist 0, minus `queue_size` und minus 1.

`queue_N_tx_llq_buffer_copy`: *N*

Die Anzahl der Pakete, deren Header-Größe größer ist als der llq-Eintrag für diese Warteschlange.

`queue_N_tx_missed_tx`: *N*

Gibt die Anzahl der nicht abgeschlossenen Pakete für diese Warteschlange an.

`queue_N_tx_unmask_interrupt`: *N*

Gibt an, wie oft der tx-Interrupt für diese Warteschlange entlarvt wurde.

`queue_N_rx_cnt`: *N*

Anzahl der empfangenen Pakete für diese Warteschlange.

`queue_N_rx_bytes`: *N*

Anzahl der empfangenen Bytes für diese Warteschlange.

`queue_N_rx_rx_copybreak_pkt`: *N*

Gibt an, wie oft die rx-Warteschlange ein Paket erhalten hat, das kleiner als die rx_copybreak-Paketgröße für diese Warteschlange ist.

`queue_N_rx_csum_good`: *N*

Gibt an, wie oft die rx-Warteschlange ein Paket erhalten hat, in dem die Prüfsumme überprüft wurde und für diese Warteschlange korrekt war.

`queue_N_rx_refil_partial`: *N*

Gibt an, wie oft der Treiber erfolglos versucht hat, den leeren Teil der rx-Warteschlange mit den Puffern für diese Warteschlange wieder aufzufüllen. Ist dieser Wert nicht 0, weist dies auf einen niedrigen Stand der Speicherressourcen hin.

`queue_N_rx_bad_csum`: *N*

Gibt an, wie oft die Warteschlange `rx` eine fehlerhafte Prüfsumme für diese Warteschlange ermittelt hat (nur wenn rx-Prüfsummenabladung unterstützt wird).

`queue_N_rx_page_alloc_fail`: *N*

Gibt an, wie oft die Seitenzuordnung für diese Warteschlange fehlgeschlagen ist. Ist dieser Wert nicht 0, weist dies auf einen niedrigen Stand der Speicherressourcen hin.

`queue_N_rx_skb_alloc_fail`: *N*

Gibt an, wie oft die SKB-Zuordnung für diese Warteschlange fehlgeschlagen ist. Wenn dieser Wert nicht 0 ist, weist dies auf einen niedrigen Stand der Systemressourcen hin.

`queue_N_rx_dma_mapping_err`: *N*

Fehleranzahl für direkten Speicherzugriff. Wenn dieser Wert nicht 0 ist, weist dies auf einen niedrigen Stand der Systemressourcen hin.

`queue_N_rx_bad_desc_num`: *N*

Zu viele Puffer pro Paket. Wenn dieser Wert nicht 0 ist, weist dies auf die Verwendung von sehr kleinen Puffern hin.

`queue_N_rx_bad_req_id: N`

Die req_id für diese Warteschlange ist nicht gültig. Die gültige req_id stammt von [0, queue_size - 1].

`queue_N_rx_empty_rx_ring: N`

Gibt an, wie oft die rx-Warteschlange für diese Warteschlange leer war.

`queue_N_rx_csum_unchecked: N`

Gibt an, wie oft die rx-Warteschlange ein Paket erhalten hat, dessen Prüfsumme nicht für diese Warteschlange überprüft wurde.

`queue_N_rx_xdp_aborted: N`

Gibt an, wie oft ein XDP-Paket als XDP_ABORT klassifiziert wurde.

`queue_N_rx_xdp_drop: N`

Gibt an, wie oft ein XDP-Paket als XDP_DROP klassifiziert wurde.

`queue_N_rx_xdp_pass: N`

Gibt an, wie oft ein XDP-Paket als XDP_PASS klassifiziert wurde.

`queue_N_rx_xdp_tx: N`

Gibt an, wie oft ein XDP-Paket als XDP_TX klassifiziert wurde.

`queue_N_rx_xdp_invalid: N`

Gibt an, wie oft der XDP-Rückgabecode für das Paket ungültig war.

`queue_N_rx_xdp_redirect: N`

Gibt an, wie oft ein XDP-Paket als XDP_REDIRECT klassifiziert wurde.

`queue_N_xdp_tx_cnt: N`

Gibt die Anzahl der übertragenen Pakete für diese Warteschlange an.

`queue_N_xdp_tx_bytes: N`

Gibt die Anzahl von übertragenen Bytes für diese Warteschlange an.

`queue_N_xdp_tx_queue_stop: N`

Gibt an, wie oft diese Warteschlange vollständig gefüllt war und angehalten wurde.

`queue_N_xdp_tx_queue_wakeup: N`

Gibt an, wie oft diese Warteschlange nach dem Anhalten wieder gestartet wurde.

`queue_N_xdp_tx_dma_mapping_err: N`

Fehleranzahl für direkten Speicherzugriff. Wenn dieser Wert nicht 0 ist, weist dies auf einen niedrigen Stand der Systemressourcen hin.

`queue_N_xdp_tx_linearize: N`

Gibt an, wie oft die XDP-Puffer-Linearisierung für diese Warteschlange versucht wurde.

`queue_N_xdp_tx_linearize_failed: N`

Gibt an, wie oft die XDP-Puffer-Linearisierung für diese Warteschlange fehlgeschlagen ist.

`queue_N_xdp_tx_napi_comp: N`

Gibt an, wie oft der Napi-Handler napi_complete für diese Warteschlange aufgerufen hat.

`queue_N_xdp_tx_tx_poll: N`

Gibt an, wie oft der Napi-Handler für diese Warteschlange geplant war.

`queue_N_xdp_tx_doorbells: N`

Gibt die Anzahl der Übertragungs-Doorbells für diese Warteschlange an.

`queue_N_xdp_tx_prepare_ctx_err: N`

Gibt an, wie oft der ena_com_prepare_tx für diese Warteschlange fehlgeschlagen ist. Dieser Wert sollte immer 0 sein. Überprüfen Sie die Treiberprotokolle, wenn dies nicht der Fall ist.

`queue_N_xdp_tx_bad_req_id: N`

Die req_id für diese Warteschlange ist nicht gültig. Die gültige req_id stammt von [0, queue_size - 1].

`queue_N_xdp_tx_llq_buffer_copy: N`

Die Anzahl der Pakete, deren Header mit LLQ-Pufferkopie für diese Warteschlange kopiert wurden.

`queue_N_xdp_tx_missed_tx: N`

Gibt an, wie oft ein tx-Warteschlangeneintrag ein Abschluss-Timeout für diese Warteschlange verpasst hat.

`queue_N_xdp_tx_unmask_interrupt: N`

Gibt an, wie oft der tx-Interrupt für diese Warteschlange entlarvt wurde.

`ena_admin_q_aborted_cmd: N`

Gibt die Anzahl der abgebrochenen Admin-Befehle an. Dies passiert normalerweise während des automatischen Wiederherstellungsverfahrens.

`ena_admin_q_submitted_cmd: N`

Gibt die Anzahl der Doorbells für die Admin-Warteschlange an.

`ena_admin_q_completed_cmd: N`

Gibt die Anzahl der Abschlüsse für die Admin-Warteschlange an.

`ena_admin_q_out_of_space: N`

Gibt an, wie oft der Treiber versucht hat, einen neuen Admin-Befehl zu senden, während die Warteschlange ausgelastet war.

`ena_admin_q_no_completion: N`

Gibt an, wie oft der Treiber für einen Befehl keinen Admin-Abschluss erhalten hat.

Treiberfehlerprotokolle im syslog

Der ENA-Treiber schreibt während des Systemstarts Protokollnachrichten in das syslog. Wenn Sie entsprechende Probleme feststellen, können Sie diese Protokolle auf Fehler überprüfen. Nachfolgend finden Sie ein Beispiel für Informationen, die vom ENA-Treiber während des Systemstarts im syslog protokolliert wurden, sowie einige Anmerkungen zu ausgewählten Nachrichten.

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.416939] [ENA_COM:
 ena_com_validate_version] ena device version: 0.10
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  478.420915] [ENA_COM:
 ena_com_validate_version] ena controller version: 0.0.1 implementation version 1
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.256831] ena 0000:00:03.0: Device
 watchdog is Enabled
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.672947] ena 0000:00:03.0: creating 8 io
 queues. queue size: 1024
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.680885] [ENA_COM:
 ena_com_init_interrupt_moderation] Feature 20 isn't supported  // Interrupt moderation
 is not supported by the device
```

```
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.691609] [ENA_COM:
 ena_com_get_feature_ex] Feature 10 isn't supported // RSS HASH function configuration
 is not supported by the
 device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.694583] [ENA_COM:
 ena_com_get_feature_ex] Feature 18 isn't supported //RSS HASH input source
 configuration is not supported by the device
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.697433] [ENA_COM:
 ena_com_set_host_attributes] Set host attribute isn't supported
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.701064] ena 0000:00:03.0 (unnamed
 net_device) (uninitialized): Cannot set host attributes
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  479.704917] ena 0000:00:03.0: Elastic
 Network Adapter (ENA) found at mem f3000000, mac addr 02:8a:3c:1e:13:b5 Queues 8
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  480.805037] EXT4-fs (xvda1): re-mounted.
 Opts: (null)
Jun  3 22:37:46 ip-172-31-2-186 kernel: [  481.025842] NET: Registered protocol family
 10
```

Welche Fehler kann ich ignorieren?

Folgende Warnungen, die u. U. in den Fehlerprotokollen Ihres Systems auftauchen, können für den Elastic Network Adapter ignoriert werden:

Das Festlegen des Hostattributs wird nicht unterstützt

Host-Attribute werden für dieses Gerät nicht unterstützt.

Es konnte kein Puffer für die Empfangswarteschlange reserviert werden

Dies ist ein umkehrbarer Fehler, der darauf hinweist, dass beim Auslösen des Fehlers eine starke Speicherbelastung vorgelegen hat.

Feature *X* wird nicht unterstützt

Das angegebene Feature wird vom Elastic Network Adapter nicht unterstützt. Mögliche Werte für *X* sind:

- **10**: Konfiguration der RSS Hash-Funktion wird für dieses Gerät nicht unterstützt.
- **12**: Konfiguration der RSS Indirection-Tabelle wird für dieses Gerät nicht unterstützt.
- **18**: RSS Hash Input-Konfiguration wird für dieses Gerät nicht unterstützt.
- **20**: Interrupt Moderation wird für dieses Gerät nicht unterstützt.
- **27**: Der Elastic Network Adapter-Treiber unterstützt keine Abfrage der Ethernet-Kapazitäten von snmpd.

AENQ konnte nicht konfiguriert werden

Der Elastic Network Adapter unterstützt keine AENQ-Konfiguration.

Es wird versucht, nicht unterstützte AENQ-Ereignisse festzulegen

Dieser Fehler weist darauf hin, dass versucht wurde, eine AENQ-Ereignisgruppe festzulegen, die vom Elastic Network Adapter nicht unterstützt wird.

Benachrichtigungen zur suboptimalen Konfiguration

Das ENA-Gerät erkennt suboptimale Konfigurationseinstellungen im Treiber, die Sie ändern können. Das Gerät benachrichtigt den ENA-Treiber und protokolliert eine Warnung zur Konsole. Das folgende Beispiel zeigt das Format der Warnmeldung.

```
Sub-optimal configuration notification code: 1. Refer to AWS ENA documentation for
 additional details and mitigation options.
```

Die folgende Liste enthält Details zum Benachrichtigungscode und empfohlene Maßnahmen für suboptimale Konfigurationserkenntnisse.

- Code **1**: ENA Express mit umfassender LLQ-Konfiguration wird nicht empfohlen

  ENA Express ENI ist mit umfassenden LLQ konfiguriert. Diese Konfiguration ist suboptimal und könnte die Leistung von ENA Express beeinträchtigen. Wir empfehlen, die umfassenden LLQ-Einstellungen wie folgt zu deaktivieren, wenn Sie ENA Express ENIs verwenden.

  ```
  sudo rmmod ena && sudo modprobe ena force_large_llq_header=0
  ```

  Weitere Informationen zur optimalen Konfiguration für ENA Express finden Sie unter Verbessern Sie die Netzwerkleistung mit ENA Express auf Ihren EC2-Instances.
- Code **2**: ENA Express ENI mit suboptimaler Tx-Warteschlangentiefe wird nicht empfohlen.

  ENA Express ENI ist mit einer suboptimalen Tx-Warteschlangentiefe konfiguriert. Diese Konfiguration beeinträchtigt möglicherweise die Leistung von ENA Express. Wir empfehlen, bei Verwendung von ENA Express alle Tx-Warteschlangen wie folgt auf den maximalen Wert für die Netzwerkschnittstelle zu vergrößern.

  Sie können die folgenden ethtool Befehle ausführen, um die LLQ-Größe anzupassen. Weitere Informationen zur Steuerung, Abfrage und Aktivierung von Wide-LLQ finden Sie im Thema Large

Low-Latency Queue (Large LLQ) der Dokumentation zum Linux-Kernel-Treiber für ENA im Amazon Drivers-Repository. GitHub

```
ethtool -g interface
```

Stellen Sie Ihre Tx-Warteschlangen auf die maximale Tiefe ein:

```
ethtool -G interface tx depth
```

Weitere Informationen zur optimalen Konfiguration für ENA Express finden Sie unter Verbessern Sie die Netzwerkleistung mit ENA Express auf Ihren EC2-Instances.

- Code**3**: ENA mit regulärer LLQ-Größe und Tx-Paketverkehr überschreitet die maximale unterstützte Header-Größe

  Standardmäßig unterstützt ENA LLQ eine Tx-Paket-Header-Größe von bis zu 96 Byte. Wenn die Größe des Paket-Headers mehr als 96 Byte beträgt, wird das Paket verworfen. Um dieses Problem zu beheben, empfehlen wir, Wide-LLQ zu aktivieren, wodurch die unterstützte Tx-Paket-Header-Größe auf maximal 224 Byte erhöht wird.

  Wenn Sie Wide-LLQ aktivieren, wird die maximale Tx-Ringgröße jedoch von 1000 auf 512 Einträge reduziert. Wide-LLQ ist standardmäßig für alle Instance-Typen von Nitro v4 und höher aktiviert.

  - Nitro v4-Instance-Typen haben standardmäßig eine maximale Wide-LLQ-Tx-Ringgröße von 512 Einträgen, die nicht geändert werden kann.
  - Nitro v5-Instance-Typen haben eine standardmäßige Wide-LLQ-Tx-Ringgröße von 512 Einträgen, die Sie auf bis zu 1000 Einträge erhöhen können.

  Sie können die folgenden ethtool Befehle ausführen, um die LLQ-Größe anzupassen. Weitere Informationen zur Steuerung, Abfrage und Aktivierung von Wide-LLQ finden Sie im Thema Large Low-Latency Queue (Large LLQ) der Dokumentation zum Linux-Kernel-Treiber für ENA im Amazon Drivers-Repository. GitHub

  Finden Sie die maximale Tiefe für Ihre Tx-Warteschlangen heraus:

  ```
  ethtool -g interface
  ```

  Stellen Sie Ihre Tx-Warteschlangen auf die maximale Tiefe ein:

```
ethtool -G interface tx depth
```

Beheben Sie Fehler beim Windows-Treiber für den Elastic Network Adapter

Der Elastic Network Adapter (ENA) wurde entwickelt, um den Zustand des Betriebssystems zu verbessern und unerwartetes Hardwareverhalten oder -ausfälle zu reduzieren, die den Betrieb Ihrer Windows-Instance stören können. In der ENA-Architektur bleiben Geräte- oder Treiberfehler für das Betriebssystem weitestgehend transparent.

Installieren Sie den Elastic Network Adapter (ENA) -Treiber

Wenn Ihre Instance nicht auf einem der neuesten Windows Amazon Machine Images (AMIs) basiert, die Amazon bereitstellt, verwenden Sie das folgende Verfahren, um den aktuellen ENA-Treiber auf Ihrer Instance zu installieren. Sie sollten diese Aktualisierung zu einem Zeitpunkt durchführen, zu dem Ihre Instance neu gestartet werden kann. Wenn das Installationsskript Ihre Instance nicht automatisch neu startet, empfehlen wir, die Instance als letzten Schritt neu zu starten.

Wenn Sie ein Instance-Speicher-Volume verwenden, um Daten zu speichern, während die Instance läuft, werden diese Daten gelöscht, wenn Sie die Instance beenden. Stellen Sie vor dem Anhalten Ihrer Instance sicher, dass Sie alle benötigten Daten aus den Instance-Speicher-Volumes in einen persistenten Speicher kopiert haben, z. B. Amazon EBS oder Amazon S3.

Voraussetzungen

Um den ENA-Treiber zu installieren oder zu aktualisieren, muss Ihre Windows-Instance die folgenden Voraussetzungen erfüllen:

- Haben Sie PowerShell Version 3.0 oder höher installiert

Schritt 1: Ihre Daten sichern

Wir empfehlen Ihnen, ein Backup-AMI zu erstellen, falls Sie Ihre Änderungen nicht über den Geräte-Manager rückgängig machen können. Gehen Sie folgendermaßen vor AWS Management Console, um ein Backup-AMI mit dem zu erstellen:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie die Instance, die ein Treiberupgrade benötigt und wählen Sie Instance stoppen aus dem Menü Instance-Status aus.
4. Nachdem die Instance angehalten wurde, wählen Sie die Instance erneut aus. Um Ihr Backup zu erstellen, wählen Sie die Option Image und Vorlagen im Menü Aktionen und dann Image erstellen.
5. Um Ihre Instance neu zu starten, wählen Sie Instance starten aus dem Menü Instance-Status.

Schritt 2: Installieren oder aktualisieren Ihres ENA-Treibers

Sie können Ihren ENA-Treiber mit AWS Systems Manager Distributor oder mit PowerShell Cmdlets installieren oder aktualisieren. Für weitere Anweisungen wählen Sie die Registerkarte aus, die der Methode entspricht, die Sie verwenden möchten.

Systems Manager Distributor

Sie können das Systems-Manager-Distributor-Feature verwenden, um Pakete für Ihre von Systems Manager verwalteten Knoten bereitzustellen. Mit Systems Manager Distributor können Sie das ENA-Treiberpaket einmal oder mit geplanten Aktualisierungen installieren. Weitere Informationen zur Installation des ENA-Treiberpakets (`AwsEnaNetworkDriver`) mit Systems Manager Distributor finden Sie unter Installieren oder Aktualisieren von Paketen im AWS Systems Manager -Benutzerhandbuch.

PowerShell

In diesem Abschnitt wird beschrieben, wie Sie ENA-Treiberpakete mithilfe von Cmdlets herunterladen und auf Ihrer Instanz installieren. PowerShell

Option 1: Die neueste Version herunterladen und extrahieren

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Verwenden Sie das invoke-webrequest cmdlet, um das neueste Treiberpaket herunterzuladen:

```
PS C:\> invoke-webrequest https://ec2-windows-drivers-
downloads.s3.amazonaws.com/ENA/Latest/AwsEnaNetworkDriver.zip -
outfile $env:USERPROFILE\AwsEnaNetworkDriver.zip
```

> **Note**
>
> Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
>
> ```
> [Net.ServicePointManager]::SecurityProtocol =
>  [Net.SecurityProtocolType]::Tls12
> ```
>
> Alternativ können Sie das neueste Treiberpaket aus einem Browserfenster auf Ihrer Instance herunterladen.

3. Verwenden Sie das expand-archive cmdlet, um das ZIP-Archiv zu extrahieren, das Sie auf Ihre Instance heruntergeladen haben:

```
PS C:\> expand-archive $env:userprofile\AwsEnaNetworkDriver.zip -
DestinationPath $env:userprofile\AwsEnaNetworkDriver
```

Option 2: Eine bestimmte Version herunterladen und extrahieren

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Laden Sie das ENA-Treiberpaket für die gewünschte Version über den Versionslink in der Windows-ENA-Treiber-Tabelle herunter.
3. Extrahieren Sie die ZIP-Datei auf Ihre Instance.

Installieren Sie den ENA-Treiber mit PowerShell

Die Installationsschritte sind dieselben, unabhängig davon, ob Sie den neuesten Treiber oder eine bestimmte Version heruntergeladen haben. Um den ENA-Treiber zu installieren, gehen Sie folgendermaßen vor.

1. Um den Treiber zu installieren, führen Sie das `install.ps1` PowerShell Skript aus dem `AwsEnaNetworkDriver` Verzeichnis auf Ihrer Instanz aus. Wenn Sie eine Fehlermeldung erhalten, stellen Sie sicher, dass Sie PowerShell 3.0 oder höher verwenden.
2. Wenn das Installationsprogramm Ihre Instanz nicht automatisch neu startet, führen Sie das Restart-Computer PowerShell Cmdlet aus.

```
PS C:\> Restart-Computer
```

Schritt 3 (optional): Überprüfen Sie die ENA-Treiberversion nach der Installation

Um sicherzustellen, dass das ENA-Treiberpaket erfolgreich auf Ihrer Instance installiert wurde, können Sie die neue Version wie folgt überprüfen:

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.

   > **Note**
   >
   > ENA-Adapter verwenden alle denselben Treiber. Wenn Sie mehrere ENA-Adapter haben, können Sie einen von ihnen auswählen, um den Treiber für alle ENA-Adapter zu aktualisieren.

6. Um zu überprüfen, welche Version aktuell installiert ist, öffnen Sie die Registerkarte Treiber und überprüfen Sie die Treiberversion. Falls die aktuelle Version nicht mit Ihrer Zielversion übereinstimmt, finden Sie weitere Informationen unter Beheben Sie Fehler beim Windows-Treiber für den Elastic Network Adapter.

Eine ENA-Treiberinstallation rückgängig machen

Wenn bei der Installation etwas schiefgeht, müssen Sie möglicherweise den Treiber zurücksetzen. Gehen Sie wie folgt vor, um zur vorherigen Version des ENA-Treibers zurückzukehren, der auf Ihrer Instance installiert war.

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.

   > **Note**
   >
   > ENA-Adapter verwenden alle denselben Treiber. Wenn Sie mehrere ENA-Adapter haben, können Sie einen von ihnen auswählen, um den Treiber für alle ENA-Adapter zu aktualisieren.

6. Um den Treiber zurückzusetzen, öffnen Sie die Registerkarte Treiber und wählen Sie Treiber zurücksetzen. Dadurch wird das Rollback-Fenster für das Treiberpaket geöffnet.

   > **Note**
   >
   > Wenn auf der Registerkarte Treiber die Aktion Treiber zurücksetzen nicht angezeigt wird oder wenn die Aktion nicht verfügbar ist, bedeutet dies, dass der Treiberspeicher auf Ihrer Instance das zuvor installierte Treiberpaket nicht enthält. Um dieses Problem zu beheben, siehe Fehlerbehebungsszenarien und erweitern Sie den Abschnitt Unerwartete ENA-Treiberversion installiert. Weitere Informationen zur Auswahl von Gerätetreiberpaketen finden Sie auf der Microsoft-Dokumentationswebsite unter So wählt Windows ein Treiberpaket für ein Gerät aus.

Sammeln von Diagnoseinformationen über die Instance

Die Schritte zum Öffnen der Tools des Windows-Betriebssystems variieren je nachdem, welche Version des Betriebssystems auf Ihrer Instance installiert ist. In den folgenden Abschnitten verwenden wir das Dialogfeld Run (Ausführen) zum Öffnen der Tools, das in allen Betriebssystemversionen gleich funktioniert. Sie können jedoch mit jeder beliebigen Methode auf diese Tools zugreifen.

Zugriff auf das Dialogfeld „Run“ (Ausführen)

- Mit der Windows-Logo-Tastenkombination: `Windows` + `R`
- Über die Suchleiste:
  - Geben Sie im Suchfeld `run` ein.
  - Wählen Sie die Anwendung Run (Ausführen) aus den Suchergebnissen aus.

Einige Schritte erfordern das Kontextmenü, um auf Eigenschaften oder kontextsensitive Aktionen zuzugreifen. Dazu gibt es je nach Betriebssystemversion und Hardware verschiedene Möglichkeiten.

Zugriff auf das Kontextmenü

- Mit der Maus: Klicken Sie mit der rechten Maustaste auf ein Element, um das Kontextmenü aufzurufen.
- Mit der Tastatur:
  - Verwenden Sie je nach Betriebssystemversion `Shift` + `F10` oder `Ctrl` + `Shift` + `F10`.
  - Wenn Sie die Kontexttaste auf Ihrer Tastatur haben (drei horizontale Linien in einem Feld), wählen Sie das gewünschte Element aus und drücken Sie dann die Kontexttaste.

Wenn Sie eine Verbindung mit Ihrer Instance herstellen können, verwenden Sie die folgenden Techniken, um Diagnoseinformationen zur Fehlerbehebung zu sammeln.

Überprüfen des ENA-Gerätestatus

Gehen Sie folgendermaßen vor, um den Status Ihres ENA-Windows-Treibers mit dem Windows-Geräte-Manager zu überprüfen:

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.

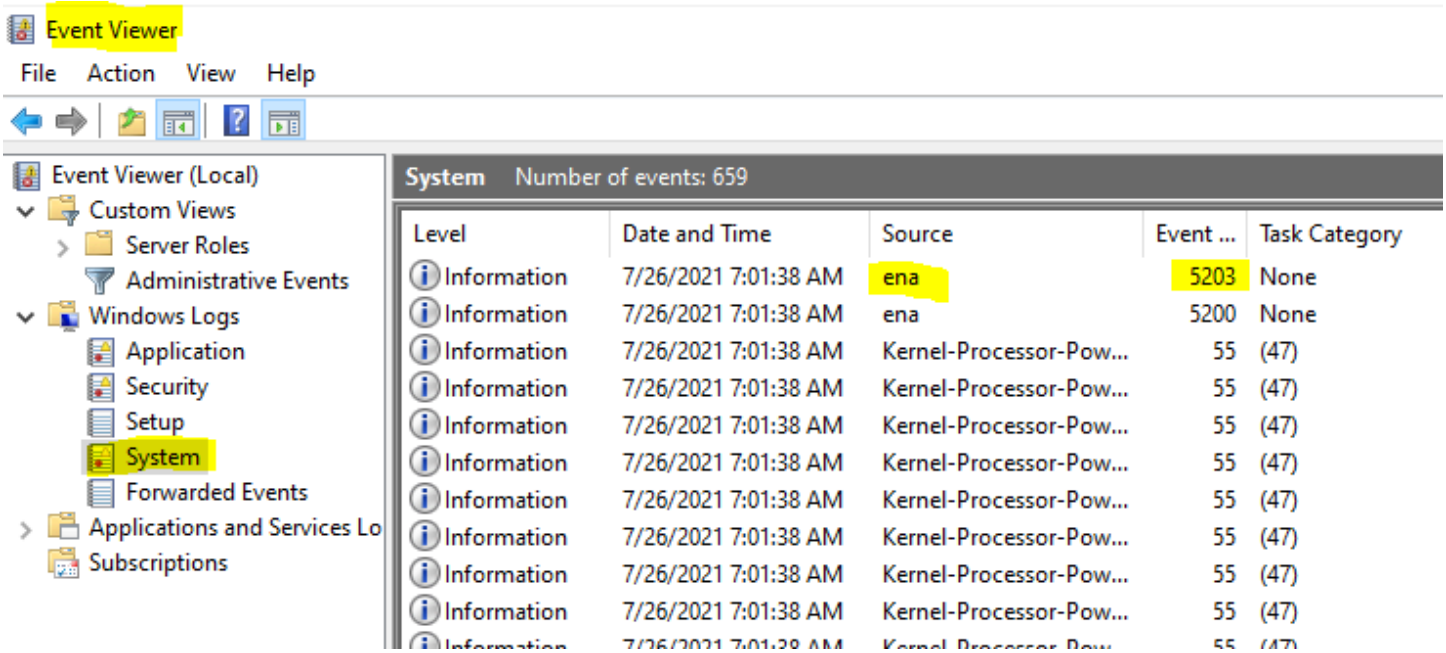
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.
6. Vergewissern Sie sich, dass auf der Registerkarte Allgemein die Meldung „Dieses Gerät funktioniert ordnungsgemäß“ erscheint.

Untersuchen von Treiberereignismeldungen

Gehen Sie folgendermaßen vor, um die Ereignisprotokolle des ENA-Windows-Treibers mit der Windows-Ereignisanzeige zu überprüfen:

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Zum Aufrufen der Windows-Ereignisanzeige geben Sie `eventvwr.msc` im Feld Ausführen ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Ereignisanzeige“ geöffnet.
4. Erweitern Sie das Menü Windows Logs (Windows--Protokolle) und wählen Sie dann System (System) aus.
5. Wählen Sie unter Actions (Aktionen) im oberen rechten Bereich Filter Current Log (Aktuelles Protokoll filtern) aus. Daraufhin wird das Filterdialogfeld angezeigt.
6. Geben Sie im Feld Event sources (Ereignisquellen) `ena` ein. Dies beschränkt die Ergebnisse auf Ereignisse, die vom ENA-Windows-Treiber generiert wurden.
7. Wählen Sie OK aus. Daraufhin werden gefilterte Ereignisprotokollergebnisse in den Detailabschnitten des Fensters angezeigt.
8. Um die Details ausführlicher anzuzeigen, wählen Sie eine Ereignismeldung in der Liste aus.

Das folgende Beispiel zeigt ein ENA-Treiberereignis in der Systemereignisliste der Windows-Ereignisanzeige:



Zusammenfassung der Ereignismeldung

Die folgende Tabelle zeigt Ereignismeldungen, die der ENA-Windows-Treiber generiert.

Eingabe

Ereignis-ID	Beschreibung des ENA-Treibereignisses	Typ
5001	Hardware hat keine Ressourcen mehr.	Fehler
5002	Adapter hat einen Hardwarefehler erkannt.	Fehler
5005	Für den Adapter ist bei einem NDIS-Vorgang, der nicht rechtzeitig abgeschlossen wurde, eine Zeitüberschreitung aufgetreten.	Fehler
5032	Adapter konnte das Gerät nicht zurücksetzen.	Fehler

Ereignis-ID	Beschreibung des ENA-Treibereignisses	Typ
5200	Adapter wurde initialisiert.	Informativ
5201	Adapter wurde unterbrochen.	Informativ
5202	Adapter wurde angehalten.	Informativ
5203	Adapter wurde neu gestartet.	Informativ
5204	Adapter wurde heruntergefahren.	Informativ
5205	Adapter wurde zurückgesetzt.	Fehler
5206	Adapter wurde überraschend entfernt.	Fehler
5208	Initialisierungsroutine des Adapters ist fehlgeschlagen.	Fehler
5210	Adapter ist auf ein internes Problem gestoßen und hat erfolgreich wiederhergestellt.	Fehler

Leistungsmetriken überprüfen

Der ENA-Windows-Treiber veröffentlicht Netzwerkleistungsmetriken der Instances, für die sie aktiviert sind. Sie können Metriken für die Instance mit der nativen Leistungsmonitoranwendung anzeigen und aktivieren. Weitere Informationen zu den Metriken, die der ENA-Windows-Treiber erstellt, finden Sie unter Überwachen der Netzwerkleistung für Ihre EC2-Instance.

Auf Instances, in denen ENA-Metriken aktiviert sind und der CloudWatch Amazon-Agent installiert ist, CloudWatch sammelt er die Metriken, die den Zählern im Windows Performance Monitor zugeordnet sind, sowie einige erweiterte Metriken für ENA. Diese Metriken werden zusätzlich zu den Metriken erfasst, die auf EC2-Instances standardmäßig aktiviert sind. Weitere Informationen zu den Metriken finden Sie unter Vom CloudWatch Agenten gesammelte Metriken im CloudWatch Amazon-Benutzerhandbuch.

> **Note**
>
> Leistungsmetriken stehen ab der ENA-Treiberversion 2.4.0 (sowie für die Version 2.2.3) zur Verfügung. Die ENA-Treiberversion 2.2.4 wurde aufgrund einer möglichen Leistungsverschlechterung bei EC2-Instances der sechsten Generation zurückgesetzt. Wir empfehlen, ein Upgrade auf die aktuelle Version des Treibers durchzuführen, um sicherzustellen, dass Sie über die neuesten Updates verfügen.

Zu den Möglichkeiten, wie Sie Leistungsmetriken verwenden können, gehören:

- Beheben von Problemen mit der Instance-Leistung
- Auswählen der richtigen Instance-Größe für eine Workload
- Proaktives Planen von Skalierungsaktivitäten
- Benchmarking von Anwendungen, um festzustellen, ob sie die auf einer Instance verfügbare Leistung maximieren

Aktualisierungsrate

Standardmäßig aktualisiert der Treiber Metriken in einem Intervall von 1 Sekunde. Die Anwendung, die die Metriken abruft, verwendet jedoch möglicherweise ein anderes Intervall für die Abfrage. Sie können das Aktualisierungsintervall im Geräte-Manager mithilfe der erweiterten Eigenschaften für den Treiber ändern.

Gehen Sie folgendermaßen vor, um das Aktualisierungsintervall für den ENA-Windows-Treiber zu ändern:

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.

5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.
6. Öffnen Sie die Registerkarte Advanced (Erweitert) im Popup-Fenster.
7. Wählen Sie in der Liste Property (Eigenschaft) Metrics Refresh Interval (Aktualisierungsintervall für Metriken) aus, um den Wert zu ändern.
8. Wählen Sie OK aus, wenn Sie damit fertig sind.

Zurücksetzen des ENA-Adapters

Der Zurücksetzungsprozess startet, wenn der ENA-Windows-Treiber einen Fehler an einem Adapter feststellt und den Adapter als fehlerhaft markiert. Der Treiber kann sich nicht selbst zurücksetzen, daher ist es die Aufgabe des Betriebssystems, den Zustand des Adapters zu überprüfen und den Rücksetz-Handle für den ENA-Windows-Treiber aufzurufen. Beim Zurücksetzen kann es zu einer kurzen Zeitspanne kommen, in der der Datenverkehr unterbrochen ist. TCP-Verbindungen sollten jedoch wiederhergestellt werden können.

Der ENA-Adapter fordert möglicherweise auch indirekt eine Prozedur zum Zurücksetzen des Geräts an, indem er keine Keep-Alive-Benachrichtigung sendet. Wenn der ENA-Adapter beispielsweise nach dem Laden einer nicht wiederherstellbaren Konfiguration in einen unbekannten Status versetzt wird, sendet er möglicherweise keine Keep-Alive-Benachrichtigungen mehr.

Häufige Ursachen für das Zurücksetzen des ENA-Adapters

- Keep-Alive-Nachrichten fehlen.

  Der ENA-Adapter sendet Keep-Alive-Ereignisse in einem bestimmten Zeitintervall (i. d. R. einmal pro Sekunde). Der ENA-Windows-Treiber implementiert einen Überwachungsmechanismus, der regelmäßig auf das Vorhandensein von Keep-Alive-Nachrichten überprüft. Wenn er seit der letzten Überprüfung eine oder mehrere neue Nachrichten erkennt, zeichnet er ein erfolgreiches Ergebnis auf. Andernfalls kommt der Treiber zu dem Schluss, dass das Gerät einen Fehler festgestellt hat, und leitet eine Zurücksetzungssequenz ein.
- Pakete stecken in Übertragungswarteschlangen fest.

  Der ENA-Adapter überprüft, ob Pakete wie erwartet durch die Übertragungswarteschlangen fließen. Der ENA-Windows-Treiber erkennt, ob Pakete hängen bleiben, und leitet eine Zurücksetzungssequenz ein, wenn dies der Fall ist.

- Timeout beim Lesen für MMIO-Register (Memory Mapped I/O)

  Um die im Speicher abgebildeten I/O-Lesevorgänge (MMIO) einzuschränken, greift der ENA-Windows-Treiber nur während der Initialisierungs- und Zurücksetzungsprozesse auf MMIO-Register zu. Wenn der Treiber ein Timeout erkennt, führt er je nachdem, welcher Prozess ausgeführt wurde, eine der folgenden Aktionen aus:

  - Wenn während der Initialisierung ein Timeout erkannt wird, schlägt der Datenfluss fehl, was dazu führt, dass der Treiber ein gelbes Ausrufezeichen des ENA-Adapters im Windows-Geräte-Manager anzeigt.
  - Wenn beim Zurücksetzen ein Timeout erkannt wird, schlägt der Datenfluss fehl. Das Betriebssystem leitet dann ein überraschendes Entfernen des ENA-Adapters ein und stellt ihn wieder her, indem es den entfernten Adapter anhält und startet. Weitere Informationen zum überraschenden Entfernen einer Network Interface Card (NIC, Netzwerkschnittstellenkarte) finden Sie unter Behandeln des überraschenden Entfernens einer NIC in der Dokumentation für Microsoft Windows-Hardwareentwickler.

Fehlerbehebungsszenarien

Die folgenden Szenarien können Ihnen bei der Behebung von Problemen helfen, die beim ENA-Windows-Treiber möglicherweise auftreten. Wir empfehlen Ihnen, mit dem Upgrade Ihres ENA-Treibers zu beginnen, wenn Sie nicht über die aktuelle Version verfügen. Den aktuellen Treiber für Ihre Windows-Betriebssystemversion finden Sie unter Windows-ENA-Treiber.

Unerwartete ENA-Treiberversion installiert

Beschreibung

Nachdem Sie die Schritte zur Installation einer bestimmten Version des ENA-Treibers ausgeführt haben, zeigt der Windows-Geräte-Manager an, dass Windows eine andere Version des ENA-Treibers installiert hat.

Ursache

Wenn Sie die Installation für ein Treiberpaket ausführen, ordnet Windows alle Treiberpakete, die für das angegebene Gerät gültig sind, im lokalen Treiberspeicher ein, bevor es beginnt. Dann wird das Paket mit dem niedrigsten Rangwert als das am besten passende Paket ausgewählt. Dies kann sich von dem Paket unterscheiden, das Sie installieren wollten. Weitere Informationen zur Auswahl von Gerätetreiberpaketen finden Sie auf der Microsoft-Dokumentationswebsite unter So wählt Windows ein Treiberpaket für ein Gerät aus.

Lösung

Um sicherzustellen, dass Windows die von Ihnen gewählte Treiberpaketversion installiert, können Sie mit dem PnPUtil-Befehlszeilentool Treiberpakete mit niedrigerem Rang aus dem Treiberspeicher entfernen.

Gehen Sie folgendermaßen vor, um den ENA-Treiber zu aktualisieren:

1. Stellen Sie eine Verbindung mit Ihrer Instance her und melden Sie sich als lokaler Administrator an.
2. Öffnen Sie das Eigenschaftenfenster des Geräte-Managers, wie im Abschnitt Überprüfen des ENA-Gerätestatus beschrieben. Dadurch wird die Registerkarte Allgemein des Fensters Eigenschaften zu Amazon Elastic Network Adapter geöffnet.
3. Öffnen Sie die Registerkarte Driver (Treiber).
4. Wählen Sie Update Driver (Treiber aktualisieren) aus. Dadurch wird das Dialogfeld Treibersoftware aktualisieren – Amazon Elastic Network Adapter geöffnet.
    a. Auf der Seite Wie wollen Sie nach Treibersoftware suchen? wählen Sie Meinen Computer nach Treibersoftware durchsuchen.
    b. Wählen Sie auf der Seite Nach Treibersoftware auf Ihrem Computer suchen die Option Lassen Sie mich aus einer Liste von Gerätetreibern auf meinem Computer auswählen, die sich unter der Suchleiste befindet.
    c. Wählen Sie auf der Seite Wählen Sie den Gerätetreiber aus, den Sie für diese Hardware installieren möchten, die Option Hat Festplatte ... .
    d. Wählen Sie im Fenster Von Festplatte installieren die Option Durchsuchen ... , neben dem Verzeichnis der Datei aus der Dropdown-Liste.
    e. Navigieren Sie zu dem Verzeichnis, in das Sie das ENA-Treiberpaket heruntergeladen haben. Wählen Sie die Datei namens `ena.inf` und dann Öffnen aus.
    f. Um die Installation zu starten, wählen Sie OK und dann Weiter.
5. Wenn das Installationsprogramm Ihre Instance nicht automatisch neu startet, führen Sie das Restart-Computer PowerShell Cmdlet aus.

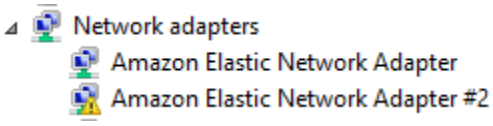
```
PS C:\> Restart-Computer
```

Gerätewarnung für ENA-Treiber

Beschreibung

Das ENA-Adaptersymbol im Abschnitt Network adapters (Netzwerkadapter) des Geräte-Managers zeigt ein Warnzeichen an (ein gelbes Dreieck mit einem Ausrufezeichen darin).

Das folgende Beispiel zeigt einen ENA-Adapter mit dem Warnsymbol im Windows-Geräte-Manager:



Ursache

Diese Gerätewarnung wird in der Regel durch Umgebungsprobleme verursacht, die möglicherweise weitere Nachforschungen und oft einen Eliminierungsprozess erfordern, um die zugrunde liegende Ursache zu ermitteln. Eine vollständige Liste der Gerätefehler finden Sie unter Geräte-Manager: Fehlermeldungen in der Dokumentation für Microsoft Windows-Hardwareentwickler.

Lösung

Die Lösung für diese Gerätewarnung hängt von der Ursache ab. Der hier beschriebene Eliminierungsprozess umfasst einige grundlegende Schritte, um die häufigsten Probleme zu identifizieren und zu beheben, für die es möglicherweise eine einfache Lösung gibt. Eine zusätzliche Ursachenanalyse ist erforderlich, wenn diese Schritte das Problem nicht beheben.

Gehen Sie folgendermaßen vor, um häufige Probleme zu identifizieren und zu beheben:

1. Anhalten und Starten des Geräts

   Öffnen Sie das Eigenschaftenfenster des Geräte-Managers, wie im Abschnitt Überprüfen des ENA-Gerätestatus beschrieben. Damit wird die Registerkarte General (Allgemein) des Fensters Amazon Elastic Network Adapter Properties (Eigenschaften von Amazon Elastic Network Adapter) geöffnet, in dem der Device status (Gerätestatus) den Fehlercode und eine kurze Meldung anzeigt.

   a. Öffnen Sie die Registerkarte Driver (Treiber).
   b. Wählen Sie Disable Device (Gerät deaktivieren) aus und antworten Sie bei der angezeigten Warnmeldung mit Yes (Ja).
   c. Wählen Sie Enable Device (Gerät aktivieren) aus.

2. Stoppen und Starten der EC2-Instance

   Wenn der Adapter weiterhin das Warnsymbol im Geräte-Manager anzeigt, besteht der nächste Schritt darin, die EC2-Instance zu stoppen und zu starten. Dadurch wird die Instance in den meisten Fällen auf unterschiedlicher Hardware neu gestartet.
3. Untersuchen eines möglichen Instance-Ressourcenproblems

   Wenn Sie Ihre EC2-Instance gestoppt und gestartet haben und das Problem weiterhin besteht, kann dies auf ein Ressourcenproblem in Ihrer Instance hinweisen, z. B. auf unzureichenden Speicher.

Verbindungs-Timeout und Adapterzurücksetzung (Fehlercodes 5007, 5205)

Beschreibung

Die Windows-Ereignisanzeige zeigt Adapter-Timeout und Zurücksetzungsereignisse an, die in Kombination für ENA-Adapter auftreten. Die Meldungen können wie die folgenden Beispiele aussehen:

- Ereignis-ID 5007: Amazon Elastic Network Adapter: Timeout während eines Vorgangs.
- Ereignis-ID 5205: Amazon Elastic Network Adapter: Zurücksetzen des Adapters wurde gestartet.

Adapterzurücksetzungen verursachen minimale Datenverkehrsunterbrechungen. Selbst wenn es mehrere Zurücksetzungen gibt, wäre es ungewöhnlich, dass sie zu schwerwiegenden Netzwerkstörungen führen.

Ursache

Diese Ereignissequenz zeigt an, dass der ENA-Windows-Treiber eine Zurücksetzung für einen ENA-Adapter initiiert hat, der nicht reagierte. Der Mechanismus, den der Gerätetreiber verwendet, um dieses Problem zu erkennen, ist jedoch anfällig für Fehlalarme, die durch ein Verhungern von CPU 0 entstehen.

Lösung

Wenn diese Kombination von Fehlern häufig auftritt, überprüfen Sie Ihre Ressourcenzuweisungen, um zu sehen, wo Anpassungen hilfreich sein könnten.

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.

2. Um den Windows-Ressourcenmonitor zu öffnen, geben Sie `resmon` im Feld Ausführen ein.
3. Wählen Sie OK aus. Daraufhin wird das Fenster „Ressourcenmonitor“ geöffnet.
4. Öffnen Sie die Registerkarte CPU. Diagramme der Auslastung pro CPU werden auf der rechten Seite des Ressourcenmonitor-Fensters angezeigt.
5. Überprüfen Sie die Auslastungswerte für CPU 0, um festzustellen, ob sie zu hoch sind.

Es wird empfohlen, RSS so zu konfigurieren, dass CPU 0 für den ENA-Adapter bei größeren Instance-Typen (mehr als 16 vCPU) ausgeschlossen wird. Bei kleineren Instance-Typen kann die Konfiguration von RSS die Erfahrung verbessern, aber aufgrund der geringeren Anzahl verfügbarer Kerne sind Tests erforderlich, um sicherzustellen, dass sich die Einschränkung von CPU-Kernen nicht negativ auf die Leistung auswirkt.

Verwenden Sie den Set-NetAdapterRss-Befehl, um RSS für Ihren ENA-Adapter zu konfigurieren, wie im folgenden Beispiel gezeigt.

```
Set-NetAdapterRss -name (Get-NetAdapter | Where-Object {$_.InterfaceDescription -like
 "*Elastic*"}).Name -Baseprocessorgroup 0 -BaseProcessorNumber 1
```

Die Migration auf eine Instance-Infrastruktur der sechsten Generation wirkt sich auf Leistung oder die Anfügung aus.

Beschreibung

Wenn Sie auf eine EC2-Instance der sechsten Generation migrieren, können eine Leistungsminderung oder Ausfälle von ENA-Anfügungen auftreten, wenn Sie Ihre ENA Windows-Treiberversion nicht aktualisiert haben.

Ursache

Für die EC2-Instance-Typen der sechsten Generation muss die folgende Mindestversion des ENA-Windows-Treibers vorhanden sein – basierend auf dem Instance-Betriebssystem (OS).

Mindestversion

Windows Server Version	ENA-Treiberversion
Windows Server 2008 R2	2.2.3 oder 2.4.0

Windows Server Version	ENA-Treiberversion
Windows Server 2012 und höher	2.2.3 und höher
Windows Workstation	2.2.3 und höher

Lösung

Vergewissern Sie sich vor dem Upgrade auf eine EC2-Instance der sechsten Generation, dass das AMI, von dem aus Sie starten, über kompatible Treiber verfügt (basierend auf dem Instance-OS gemäß der obigen Tabelle). Weitere Informationen finden Sie im AWS re:Post -Wissenszentrum unter Was muss ich tun, bevor ich meine EC2-Instance auf eine Instance der sechsten Generation migriere, um sicherzustellen, dass ich die maximale Netzwerkleistung erhalte?.

Suboptimale Leistung für die Elastic-Network-Schnittstelle

Beschreibung

Die ENA-Schnittstelle funktioniert nicht wie erwartet.

Ursache

Die Ursachenanalyse für Leistungsprobleme ist ein Eliminierungsprozess. Es sind zu viele Variablen beteiligt, um eine gängige Ursache zu nennen.

Lösung

Der erste Schritt bei der Ursachenanalyse besteht darin, die Diagnoseinformationen für die Instance, die nicht wie erwartet funktioniert, zu überprüfen, um festzustellen, ob es Fehler gibt, die das Problem verursachen könnten. Weitere Informationen finden Sie im Abschnitt Sammeln von Diagnoseinformationen über die Instance.

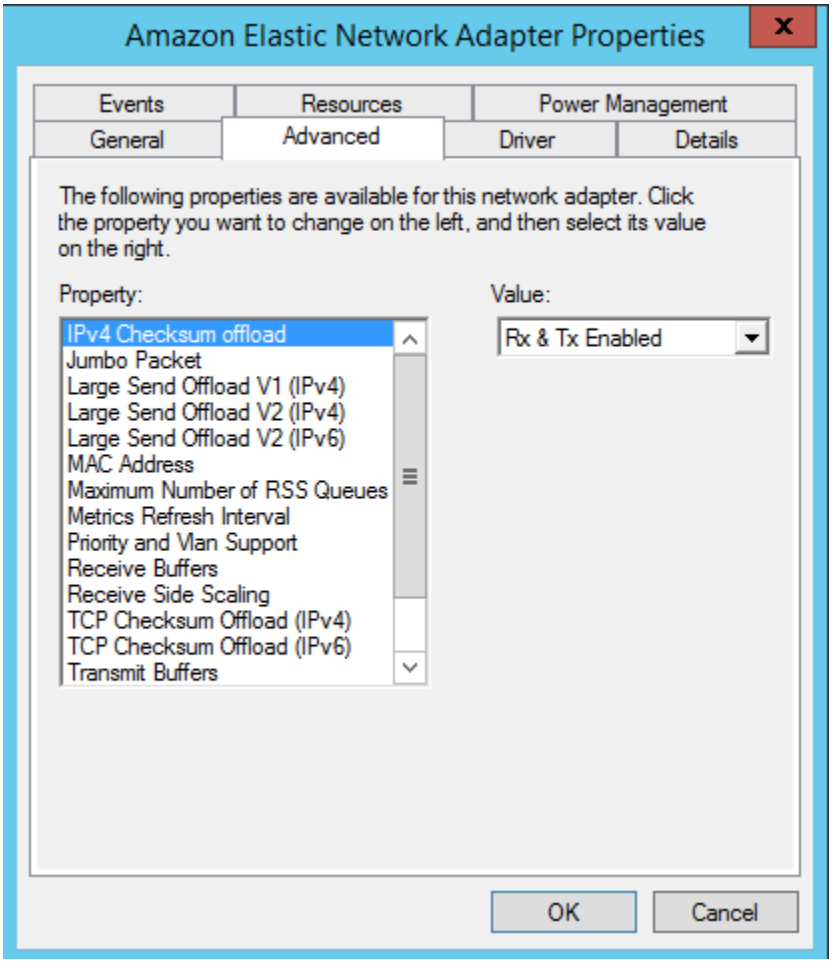
Möglicherweise müssen Sie die Standardkonfiguration des Betriebssystems ändern, um eine maximale Netzwerkleistung auf Instances mit Enhanced Networking zu erreichen. Einige Optimierungen, wie z. B. die Aktivierung des Prüfsummen-Offloads und die Aktivierung von RSS, sind in offiziellen Windows-AMIs standardmäßig konfiguriert. Weitere Optimierungen, die Sie auf den ENA-Adapter anwenden können, finden Sie in den Leistungsanpassungen unter Leistungsanpassungen des ENA-Adapters.

Wir empfehlen, vorsichtig vorzugehen und die Anpassungen der Geräteeigenschaften auf die in diesem Abschnitt aufgeführten Änderungen oder auf bestimmte Änderungen zu beschränken, die vom AWS Support-Team empfohlen werden.

Gehen Sie folgendermaßen vor, um die Eigenschaften des ENA-Adapters zu ändern:

1. Öffnen Sie das Dialogfeld Run (Ausführen) mit einer der im vorherigen Abschnitt beschriebenen Methoden.
2. Zum Aufrufen des Windows-Geräte-Managers geben Sie `devmgmt.msc` im Feld Run (Ausführen) ein.
3. Wählen Sie OK aus. Dadurch wird das Fenster „Device Manager“ (Geräte-Manager) geöffnet.
4. Wählen Sie den Pfeil links neben Network adapters (Netzwerkadapter) aus, um die Liste zu erweitern.
5. Wählen Sie den Namen aus oder öffnen Sie das Kontextmenü für den Amazon Elastic Network Adapter und wählen Sie dann Properties (Eigenschaften) aus. Dadurch wird das Dialogfeld mit den Eigenschaften des Amazon Elastic Network Adapters geöffnet.
6. Um Ihre Änderungen vorzunehmen, öffnen Sie die Registerkarte Erweitert.
7. Wenn Sie fertig sind, wählen Sie OK aus, um Ihre Änderungen zu speichern.

Das folgende Beispiel zeigt eine ENA-Adaptereigenschaft im Windows-Geräte-Manager:



Leistungsanpassungen des ENA-Adapters

Die folgende Tabelle enthält Eigenschaften, die angepasst werden können, um die Leistung für die ENA-Schnittstelle zu verbessern.

Eingabe

Property (Eigenschaft)	Description (Beschreibung)	Standardwert	Anpassung
Empfangspuffer	Steuert die Anzahl der Einträge in den Empfangswarteschlangen der Software.	1024	Kann auf maximal 8 192 erhöht werden.
		Aktiviert	

Property (Eigenschaft)	Description (Beschreibung)	Standardwert	Anpassung
Receive Side Scaling (RSS)	Ermöglicht die effiziente Verteilung der Netzwerkempfangsverarbeitung auf mehrere CPUs in Multiprozessorsystemen.		Sie können die Last auf mehrere Prozessoren verteilen. Weitere Informationen hierzu finden Sie unter Optimieren Sie die Netzwerkleistung auf Windows-Instances.

Property (Eigenschaft)	Description (Beschreibung)	Standardwert	Anpassung
Maximale Anzahl von RSS-Warteschlangen	Legt die maximal zulässige Anzahl von RSS-Warteschlangen fest, wenn RSS aktiviert ist.	32	Die Anzahl der RSS-Warteschlangen wird während der Treiberinitialisierung bestimmt und umfasst (unter anderem) die folgenden Beschränkungen: • Von dieser Eigenschaft festgelegtes RSS-Warteschlangen limit • Instance-Limits (vCPU-Anzahl) • Beschränkungen der Hardwareg enerierung (bis zu 8 RSS-Warteschlangen in ENAv1 und bis zu 32 RSS-Warteschlangen in ENAv2) Sie können einen Wert von 1–32 festlegen, je nach

Property (Eigenschaft)	Description (Beschreibung)	Standardwert	Anpassung
			Ihren Beschränkungen für die Instance und Hardwareg enerierung. Weitere Informationen hierzu finden Sie unter Optimieren Sie die Netzwerkleistung auf Windows-Instances.
Jumbo-Paket	Ermöglicht die Verwendung von Jumbo-Ethernet-Frames (mehr als 1 500 Byte Nutzlast).	Deaktiviert (dies begrenzt die Nutzlast auf höchstens 1 500 Byte).	Ein Wert bis zu 9001 kann festgelegt werden, was auf 9 001 Byte Nutzlast entspricht. Dies ist die maximale Nutzlast für Jumbo-Ethernet-Frames. Siehe Überlegungen zur Verwendung von Jumbo-Ethernet-Frames.

Überlegungen zur Verwendung von Jumbo-Ethernet-Frames

Für Jumbo-Frames sind mehr als 1 500 Byte an Daten zulässig, indem die Nutzlastgröße pro Paket und somit der Prozentsatz des Pakets erhöht wird, bei dem es sich nicht um Paket-Overhead handelt. Es werden weniger Pakete benötigt, um die gleiche Menge an verwendbaren Daten zu übertragen. Der Verkehr ist jedoch in folgenden Fällen auf eine maximale MTU von 1 500 beschränkt:

- Verkehr außerhalb einer bestimmten AWS Region für EC2 Classic.
- Datenverkehr außerhalb einer einzelnen VPC
- Datenverkehr über eine regionsübergreifende VPC-Peering-Verbindung
- Datenverkehr über VPN-Verbindungen

- Datenverkehr über ein Internet-Gateway

> **Note**
>
> Pakete über 1 500 Byte sind fragmentiert. Wenn Sie das `Don't Fragment`-Flag im IP-Header gesetzt haben, werden diese Pakete gelöscht.
> Jumbo-Frames sollten für Internet-Datenverkehr bzw. für Datenverkehr, der eine VPC verlässt, nur mit Vorsicht verwendet werden. Pakete werden durch zwischengeschaltete Systeme fragmentiert, sodass dieser Datenverkehr verlangsamt wird. Um Jumbo-Frames innerhalb einer VPC zu verwenden, ohne den ausgehenden Datenverkehr zu beeinträchtigen, der die VPC verlässt, versuchen Sie es mit einer der folgenden Optionen:
>
> - Konfigurieren Sie die MTU-Größe nach Route.
> - Verwenden Sie mehrere Netzwerkschnittstellen mit unterschiedlichen MTU-Größen und Routen.

Empfohlene Anwendungsfälle für Jumbo-Frames

Jumbo-Frames können für den Datenverkehr innerhalb und zwischen VPCs nützlich sein. Wir empfehlen die Verwendung von Jumbo-Frames für folgende Anwendungsfälle:

- Bei Instances, die sich gemeinsam innerhalb einer Cluster-Placement-Gruppe befinden, helfen Jumbo-Frames dabei, den maximal möglichen Netzwerkdurchsatz zu erzielen. Weitere Informationen finden Sie unter Placement-Gruppen.
- Sie können für Datenverkehr zwischen Ihren VPCs und Ihren On-Premises-Netzwerken über Jumbo-Frames verwende AWS Direct Connect. Weitere Informationen zur Verwendung AWS Direct Connect und Überprüfung der Jumbo-Frame-Fähigkeit finden Sie im Benutzerhandbuch unter Netzwerk-MTU für private virtuelle Schnittstellen oder virtuelle Transitschnittstellen einrichten.AWS Direct Connect
- Weitere Informationen zu unterstützten MTU-Größen für Transit Gateways finden Sie unter Kontingente für Ihre Transit Gateways in Amazon VPC Transit Gateways.

Verbessern Sie die Netzwerklatenz für Amazon-EC2-Instances, die auf Linux ausgeführt werden

Die Netzwerklatenz ist die Zeitspanne, die ein Datenpaket benötigt, um von seiner Quelle zu seinem Ziel zu gelangen. Anwendungen, die Daten über das Netzwerk senden, sind auf zeitnahe Antworten angewiesen, um eine positive Benutzererfahrung zu bieten. Eine hohe Netzwerklatenz kann zu verschiedenen Problemen führen, z. B. zu den folgenden:

- Langsame Ladezeiten für Webseiten
- Verzögerung des Videostreams
- Schwierigkeiten beim Zugriff auf Online-Ressourcen

In diesem Abschnitt werden Schritte beschrieben, die Sie ergreifen können, um die Netzwerklatenz auf Amazon-EC2-Instances zu verbessern, die auf Linux ausgeführt werden. Um eine optimale Latenz zu erreichen, führen Sie die folgenden Schritte aus, um Ihre Instance, den Kernel und die ENA-Treibereinstellungen zu konfigurieren. Weitere Hinweise zur Konfiguration finden Sie im ENA Linux Driver Best Practices and Performance Optimization Guide unter. GitHub

> **Note**
>
> Die Schritte und Einstellungen können je nach Ihrer spezifischen Netzwerkhardware, dem AMI, von dem aus Sie Ihre Instance gestartet haben, und Ihrem Anwendungsfall leicht variieren. Bevor Sie Änderungen vornehmen, testen und überwachen Sie Ihre Netzwerkleistung gründlich, um sicherzustellen, dass Sie die gewünschten Ergebnisse erzielen.

Netzwerksprünge reduzieren

Jeder Sprung, den ein Datenpaket bei der Übertragung von Router zu Router zurücklegt, erhöht die Netzwerklatenz. Üblicherweise muss der Datenverkehr mehrere Sprünge machen, um Ihr Ziel zu erreichen. Es gibt zwei Möglichkeiten, Netzwerksprünge für Ihre Amazon-EC2-Instances zu reduzieren:

- Cluster-Placement-Gruppe – Wenn Sie eine Cluster-Placement-Gruppe angeben, startet Amazon EC2-Instances, die sich in unmittelbarer Nähe zueinander befinden, d. h. physisch in derselben Availability Zone (AZ), mit engerer Packung. Durch die räumliche Nähe der Instances in der

Gruppe können sie die Vorteile einer Hochgeschwindigkeitsverbindung nutzen, was zu niedrigen Latenzzeiten und einem hohen Durchsatz für einzelne Datenströme führt.

- Dedicated Host – Ein Dedicated Host ist ein physischer Server ausschließlich für Ihre Verwendung. Mit einem Dedicated Host können Sie Ihre Instances so starten, dass sie auf demselben physischen Server ausgeführt werden. Kommunikation zwischen Instances, die auf demselben Dedicated Host ausgeführt werden, kann ohne zusätzliche Sprünge erfolgen.

Linux-Kernelkonfiguration

Die Konfiguration des Linux-Kernels kann die Netzwerklatenz erhöhen oder verringern. Um Ihre Ziele zur Latenzoptimierung zu erreichen, ist es wichtig, die Konfiguration des Linux-Kernels an die spezifischen Anforderungen Ihres Workloads anzupassen.

Es gibt viele Konfigurationsoptionen für den Linux-Kernel, die helfen können, die Netzwerklatenz zu verringern. Die wirkungsvollsten Optionen sind folgende.

- Aktivieren des Besetztabfrage-Modus – Der Besetztabfrage-Modus reduziert die Latenzzeit auf dem Netzwerkempfangspfad. Wenn Sie den Besetztabfrage-Modus aktivieren, kann der Socket-Schicht-Code die Empfangswarteschlange eines Netzwerkgeräts direkt abfragen. Der Nachteil des Busy-Polls ist die höhere CPU-Auslastung des Hosts, die durch das Abrufen neuer Daten in einer engen Schleife entsteht. Es gibt zwei globale Einstellungen, welche die Anzahl der Mikrosekunden steuern, die auf Pakete für alle Schnittstellen gewartet wird.

  `busy_read`

  Ein Busy-Poll-Timeout mit geringer Latenz für Socket-Lesevorgänge. Dies steuert die Anzahl der Mikrosekunden, die gewartet wird, bis die Socket-Schicht Pakete in der Geräte-Warteschlange liest. Um das Feature global mit dem Befehl sysctl zu aktivieren, empfiehlt die Linux Kernel-Organisation einen Wert von 50 Mikrosekunden. Weitere Informationen finden Sie unter busy_read im Benutzer- und Administratorenhandbuch für Linux-Kernel.

  ```
  $ C:\> sudo sysctl -w net.core.busy_read=50
  ```

  `busy_poll`

  Ein Busy-Poll-Timeout mit geringer Latenzzeit für die Abfrage und Auswahl. Das steuert die Anzahl der Mikrosekunden, die auf Ereignisse gewartet wird. Der empfohlene Wert liegt

zwischen 50 und 100 Mikrosekunden, abhängig von der Anzahl der abzufragenden Sockets. Je mehr Sockets Sie hinzufügen, desto höher sollte die Zahl sein.

```
$ C:\> sudo sysctl -w net.core.busy_poll=50
```

- Konfigurieren des CPU-Energiestatus (C-Status) – C-Status steuert die Ruhezustände, in denen sich ein Kern in inaktiven Zustand befinden kann. Es kann ratsam sein, die C-Status zu steuern, um Ihr System im Hinblick auf Latenz und Leistung zu optimieren. In tieferen C-Zuständen ist die CPU im Wesentlichen „eingeschlafen“ und kann nicht auf Anfragen reagieren, bis sie aufwacht und wieder in einen aktiven Zustand übergeht. Das Versetzen von Cores in den Ruhezustand benötigt Zeit. Und auch wenn ein Core im Ruhezustand mehr Spielraum zur Nutzung einer höheren Frequenz durch einen anderen Core zulässt, dauert es auch wieder eine gewisse Zeit, bis der Core aus dem Ruhezustand erwacht und Arbeitsschritte ausführen kann.

  Wenn beispielsweise ein Core, der für die Bearbeitung von Interrupts für Netzwerkpakete zuständig ist, schläft, kann es zu einer Verzögerung bei der Bearbeitung des Interrupts kommen. Sie können das System so konfigurieren, dass es keine tieferen C-Zustände verwendet. Diese Konfiguration reduziert zwar die Latenz der Prozessorreaktion, aber gleichzeitig wird auch der Turbo-Boost-Spielraum für andere Cores verringert.

  Um die Reaktionslatenz des Prozessors zu verringern, können Sie tiefere C-Status begrenzen. Weitere Informationen finden Sie unter Hohe Leistung und niedrige Latenz durch Begrenzung tieferer C-States im Amazon Linux 2-Benutzerhandbuch.

ENA-Treiberkonfiguration

Der ENA-Netzwerktreiber ermöglicht die Kommunikation zwischen einer Instance und einem Netzwerk. Der Treiber verarbeitet Netzwerkpakete und leitet sie an den entsprechenden Netzwerkstapel oder die Nitro-Karte weiter. Wenn ein Netzwerkpaket eingeht, generiert die Nitro-Karte eine Unterbrechung für die CPU, um die Software über ein Ereignis zu informieren.

Unterbrechen

Eine Unterbrechung ist ein Signal, das ein Gerät oder eine Anwendung an den Prozessor sendet. Die Unterbrechung teilt dem Prozessor mit, dass ein Ereignis eingetreten ist oder eine Bedingung erfüllt wurde, die sofortige Aufmerksamkeit erfordert. Interrupts können zeitkritische Aufgaben wie den Empfang von Daten von einer Netzwerkschnittstelle, die Bearbeitung von Hardwareereignissen oder die Bearbeitung von Anforderungen von anderen Geräten erledigen.

Moderation unterbrechen

Die Interrupt-Moderation ist eine Technik, die die Anzahl der von einem Gerät generierten Interrupts reduziert, indem sie aggregiert oder verzögert werden. Der Zweck der Interrupt-Moderation besteht darin, die Systemleistung zu verbessern, indem der mit der Bearbeitung einer großen Anzahl von Interrupts verbundene Aufwand reduziert wird. Zu viele Interrupts erhöhen die CPU-Auslastung, was sich negativ auf den Durchsatz auswirkt, während zu wenige Interrupts die Latenz erhöhen.

Dynamische Interrupt-Moderation

Die dynamische Interrupt-Moderation ist eine erweiterte Form der Interrupt-Moderation, bei der die Interrupt-Rate dynamisch an die aktuelle Systemlast und die Verkehrsmuster angepasst wird. Sie zielt darauf ab, ein Gleichgewicht zwischen der Reduzierung des Interrupt-Overheads und der Reduzierung der Pakete pro Sekunde oder Bandbreite zu finden.

> **Note**
>
> Die dynamische Unterbrechungsmoderation ist in einigen AMIs standardmäßig aktiviert (kann aber in allen AMIs aktiviert oder deaktiviert werden).

Um die Netzwerklatenz zu minimieren, ist es eventuell erforderlich, die Unterbrechungsmoderation zu deaktivieren. Dies kann jedoch auch den Aufwand für die Verarbeitung von Unterbrechungen erhöhen. Es ist wichtig, das richtige Gleichgewicht zwischen der Reduzierung der Latenzzeit und der Minimierung des Aufwands zu finden. `ethtool`-Befehle können Sie bei der Konfiguration der Unterbrechungsmoderation unterstützen. `rx-usecs` Ist standardmäßig auf `20` gesetzt und `tx-usecs` ist auf 64 gesetzt.

Verwenden Sie den folgenden Befehl, um die aktuelle Änderungskonfiguration der Unterbrechung abzurufen.

```
$ C:\> ethtool -c interface | egrep "rx-usecs:|tx-usecs:|Adaptive RX"
Adaptive RX: on  TX: off
rx-usecs: 20
tx-usecs: 64
```

Verwenden Sie den folgenden Befehl, um die Unterbrechungsmodifikation und die dynamische Unterbrechungsmoderation zu deaktivieren.

```
$ C:\> sudo ethtool -C interface adaptive-rx off rx-usecs 0 tx-usecs 0
```

Überlegungen zum Nitro-System zur Leistungsoptimierung

Das Nitro-System ist eine von AWS entwickelte Sammlung von Hardware- und Softwarekomponenten, die eine hohe Leistung, Verfügbarkeit und Sicherheit ermöglichen. Das Nitro-System bietet Bare-Metal-ähnliche Funktionen, die den Virtualisierungsaufwand eliminieren und Workloads unterstützen, die vollen Zugriff auf die Host-Hardware erfordern. Ausführlichere Informationen finden Sie unter Nitro System.AWS

Alle EC2-Instance-Typen der aktuellen Generation führen die Netzwerkpaketverarbeitung auf EC2-Nitro-Karten durch. Dieses Thema behandelt die Paketverarbeitung auf hoher Ebene auf der Nitro-Karte, allgemeine Aspekte der Netzwerkarchitektur und -konfiguration, die sich auf die Leistung der Paketverarbeitung auswirken, und welche Maßnahmen Sie ergreifen können, um Spitzenleistung für Ihre Nitro-basierten Instances zu erzielen.

Nitro-Karten verarbeiten alle Eingangs- und Ausgangsschnittstellen (I/O), wie sie beispielsweise für Virtual Private Clouds (VPCs) benötigt werden. Für alle Komponenten, die Informationen über das Netzwerk senden oder empfangen, fungieren die Nitro-Karten als eigenständiges Computergerät für den I/O-Verkehr, das physisch von der Hauptplatine des Systems getrennt ist, auf der die Workloads der Kunden ausgeführt werden.

Netzwerk-Paketfluss auf Nitro-Karten

EC2-Instances, die auf dem Nitro-System basieren, verfügen über Hardwarebeschleunigungsfunktionen, die eine schnellere Paketverarbeitung ermöglichen, gemessen an den Durchsatzraten von Paketen pro Sekunde (PPS). Wenn eine Nitro-Karte die erste Evaluierung für einen neuen Flow durchführt, speichert sie Informationen, die für alle Pakete im Flow identisch sind, wie Sicherheitsgruppen, Zugriffskontrolllisten und Routentabelleneinträge. Wenn sie zusätzliche Pakete für denselben Datenfluss verarbeitet, kann sie die gespeicherten Informationen verwenden, um den Overhead für diese Pakete zu reduzieren.

Ihre Verbindungsrate wird anhand der Metrik Verbindungen pro Sekunde (CPS) gemessen. Jede neue Verbindung erfordert zusätzlichen Verarbeitungsaufwand, der bei den Schätzungen der Workload-Fähigkeit berücksichtigt werden muss. Es ist wichtig, bei der Gestaltung Ihrer Workloads sowohl die CPS- als auch die PPS-Metriken zu berücksichtigen.

Wie wird eine Verbindung hergestellt

Wenn eine Verbindung zwischen einer Nitro-basierten Instanz und einem anderen Endpunkt hergestellt wird, bewertet die Nitro-Karte den gesamten Datenfluss für das erste Paket, das zwischen den beiden Endpunkten gesendet oder empfangen wird. Bei nachfolgenden Paketen desselben Datenflusses ist eine vollständige Neubewertung normalerweise nicht erforderlich. Es gibt jedoch Ausnahmen. Weitere Informationen zu den Ausnahmen finden Sie unterPakete, die keine Hardwarebeschleunigung verwenden.

Die folgenden Eigenschaften definieren die beiden Endpunkte und den Paketfluss zwischen ihnen. Diese fünf Eigenschaften zusammen werden als 5-Tupelfluss bezeichnet.

- Quell-IP
- Quell-Port
- Ziel-IP
- Ziel-Port
- Kommunikationsprotokoll

Die Richtung des Paketflusses wird als Eingang (eingehend) und Ausgang (ausgehend) bezeichnet. Die folgenden allgemeinen Beschreibungen fassen den gesamten Paketfluss im Netzwerk zusammen.

- Eingang — Wenn eine Nitro-Karte ein eingehendes Netzwerkpaket verarbeitet, bewertet sie das Paket anhand von statusbehafteten Firewallregeln und Zugriffskontrolllisten. Sie verfolgt die Verbindung, misst sie und führt gegebenenfalls weitere Aktionen durch. Anschließend leitet es das Paket an sein Ziel auf der Host-CPU weiter.
- Ausgang — Wenn eine Nitro-Karte ein ausgehendes Netzwerkpaket verarbeitet, sucht sie nach dem Remote-Schnittstellenziel, bewertet verschiedene VPC-Funktionen, wendet Ratenbegrenzungen an und führt andere zutreffende Aktionen aus. Dann leitet sie das Paket an ihr nächstes Hop-Ziel im Netzwerk weiter.

Design für optimale Leistung

Um die Leistungsfähigkeit Ihres Nitro-Systems optimal nutzen zu können, müssen Sie Ihre Anforderungen an die Netzwerkverarbeitung kennen und wissen, wie sich diese Anforderungen auf die Arbeitslast Ihrer Nitro-Ressourcen auswirken. Anschließend können Sie die optimale Leistung für Ihre Netzwerklandschaft entwerfen. Ihre Infrastruktureinstellungen sowie der Entwurf und die Konfiguration der Anwendungs-Workloads können sich sowohl auf die Paketverarbeitung

als auch auf die Verbindungsraten auswirken. Wenn Ihre Anwendung beispielsweise eine hohe Verbindungsaufbaurate aufweist, z. B. ein DNS-Dienst, eine Firewall oder ein virtueller Router, hat sie weniger Möglichkeiten, die Hardwarebeschleunigung zu nutzen, die erst nach dem Verbindungsaufbau erfolgt.

Sie können Anwendungs- und Infrastruktureinstellungen konfigurieren, um Workloads zu rationalisieren und die Netzwerkleistung zu verbessern. Allerdings sind nicht alle Pakete für eine Beschleunigung geeignet. Das Nitro-System verwendet den gesamten Netzwerkfluss für neue Verbindungen und für Pakete, die nicht für eine Beschleunigung in Frage kommen.

Der Rest dieses Abschnitts konzentriert sich auf Überlegungen zum Anwendungs- und Infrastrukturdesign, um sicherzustellen, dass Pakete so weit wie möglich innerhalb des beschleunigten Pfads fließen.

Überlegungen

Bei der Konfiguration des Netzwerkverkehrs für Ihre Instance müssen viele Aspekte berücksichtigt werden, die sich auf die PPS-Leistung auswirken können. Sobald ein Datenfluss eingerichtet ist, können die meisten Pakete, die regelmäßig ein- oder ausgehen, beschleunigt werden. Es gibt jedoch Ausnahmen, um sicherzustellen, dass Infrastrukturdesigns und Paketflüsse weiterhin den Protokollstandards entsprechen.

Um die beste Leistung aus Ihrer Nitro-Karte herauszuholen, sollten Sie die Vor- und Nachteile der folgenden Konfigurationsdetails für Ihre Infrastruktur und Anwendungen sorgfältig abwägen.

Überlegungen zur Infrastruktur

Ihre Infrastrukturkonfiguration kann sich auf Ihren Paketfluss und Ihre Verarbeitungseffizienz auswirken. Die folgende Liste enthält einige wichtige Überlegungen.

Netzwerkschnittstellenkonfiguration mit Asymmetrie

Sicherheitsgruppen verwenden die Verbindungsverfolgung, um Informationen über den Datenverkehr zu und von der Instance nachzuverfolgen. Asymmetrisches Routing, bei dem der Datenverkehr über eine Netzwerkschnittstelle in eine Instance eingeht und über eine andere Netzwerkschnittstelle wieder austritt, kann die Spitzenleistung verringern, die eine Instance erzielen kann, wenn Datenflüsse verfolgt werden. Weitere Informationen zur Verbindungsverfolgung von Sicherheitsgruppen, nicht verfolgten Verbindungen und automatisch verfolgten Verbindungen finden Sie unter. Verbindungsverfolgung von Sicherheitsgruppen

Netzwerktreiber

Netzwerktreiber werden regelmäßig aktualisiert und veröffentlicht. Wenn Ihre Treiber veraltet sind, kann dies die Leistung erheblich beeinträchtigen. Halten Sie Ihre Treiber auf dem neuesten Stand, um sicherzustellen, dass Sie über die neuesten Patches verfügen und Leistungsverbesserungen nutzen können, z. B. die Funktion für beschleunigte Pfade, die nur für die neueste Treibergeneration verfügbar ist. Frühere Treiber unterstützen die Funktion für den beschleunigten Pfad nicht.

Um die Vorteile der Funktion für beschleunigte Pfade nutzen zu können, empfehlen wir Ihnen, den neuesten ENA-Treiber auf Ihren Instances zu installieren.

Linux-Instances — ENA-Linux-Treiber 2.2.9 oder höher. Informationen zur Installation oder Aktualisierung des ENA-Linux-Treibers aus dem Amazon GitHub Drivers-Repository finden Sie im Abschnitt Treiberkompilierung der Readme-Datei.

Windows-Instances — ENA Windows-Treiber 2.0.0 oder höher. Informationen zur Installation oder Aktualisierung des ENA-Windows-Treibers finden Sie unterInstallieren Sie den Elastic Network Adapter (ENA) -Treiber.

Entfernung zwischen Endpunkten

Eine Verbindung zwischen zwei Instances in derselben Availability Zone kann mehr Pakete pro Sekunde verarbeiten als eine Verbindung zwischen Regionen. Dies ist auf das TCP-Fenster auf Anwendungsebene zurückzuführen, das bestimmt, wie viele Daten zu einem bestimmten Zeitpunkt übertragen werden können. Große Entfernungen zwischen Instanzen erhöhen die Latenz und verringern die Anzahl der Pakete, die die Endpunkte verarbeiten können.

Überlegungen zum Anwendungsdesign

Es gibt Aspekte des Anwendungsdesigns und der Konfiguration, die sich auf Ihre Verarbeitungseffizienz auswirken können. Die folgende Liste enthält einige wichtige Überlegungen.

Größe des Pakets

Größere Paketgrößen können den Durchsatz für die Daten erhöhen, die eine Instanz im Netzwerk senden und empfangen kann. Kleinere Paketgrößen können die Paketverarbeitungsrate erhöhen, aber dadurch kann die maximal erreichte Bandbreite reduziert werden, wenn die Anzahl der Pakete die PPS-Zulagen überschreitet.

Wenn die Größe eines Pakets die maximale Übertragungseinheit (MTU) eines Netzwerk-Hops überschreitet, wird es möglicherweise von einem Router entlang des Pfads fragmentiert. Die resultierenden Paketfragmente gelten als Ausnahmen und werden mit der Standardrate (nicht beschleunigt) verarbeitet. Dies kann zu Leistungsschwankungen führen. Amazon EC2 unterstützt Jumbo-Frames von 9001 Byte, dies wird jedoch nicht von allen Services unterstützt. Wir empfehlen Ihnen, Ihre Topologie bei der Konfiguration der MTU zu bewerten.

Kompromisse zwischen Protokollen

Zuverlässige Protokolle wie TCP haben mehr Overhead als unzuverlässige Protokolle wie UDP. Der geringere Overhead und die vereinfachte Netzwerkverarbeitung für das UDP-Transportprotokoll können zu einer höheren PPS-Rate führen, allerdings auf Kosten einer zuverlässigen Paketzustellung. Wenn eine zuverlässige Paketzustellung für Ihre Anwendung nicht entscheidend ist, ist UDP möglicherweise eine gute Option.

Mikro-Bursting

Micro-Bursting tritt auf, wenn der Verkehr in kurzen Zeiträumen die zulässigen Grenzwerte überschreitet und nicht gleichmäßig verteilt wird. Dies geschieht in der Regel im Mikrosekundenbereich.

Nehmen wir zum Beispiel an, Sie haben eine Instanz, die bis zu 10 Gbit/s senden kann, und Ihre Anwendung sendet die vollen 10 Gbit/s in einer halben Sekunde. Dieser Micro-Burst überschreitet in der ersten halben Sekunde den zulässigen Wert und für den Rest der Sekunde bleibt nichts übrig. Auch wenn Sie in der ersten Sekunde 10 Gbit gesendet haben, können Freigaben in der ersten halben Sekunde dazu führen, dass Pakete in die Warteschlange gestellt oder verworfen werden.

Sie können einen Netzwerkplaner wie Linux Traffic Control verwenden, um Ihren Durchsatz zu beschleunigen und zu vermeiden, dass Pakete aufgrund von Micro-Bursting in die Warteschlange gestellt oder verworfen werden.

Anzahl der Datenflüsse

Ein einzelner Datenfluss ist auf 5 Gbit/s begrenzt, es sei denn, er gehört zu einer Cluster-Platzierungsgruppe, die bis zu 10 Gbit/s unterstützt, oder er verwendet ENA Express, das bis zu 25 Gbit/s unterstützt.

In ähnlicher Weise kann eine Nitro-Karte mehr Pakete über mehrere Datenflüsse verarbeiten, anstatt einen einzigen Datenfluss zu verwenden. Um die maximale Paketverarbeitungsrate pro Instance zu erreichen, empfehlen wir mindestens 100 Flows auf Instances mit einer

Gesamtbandbreite von 100 Gbit/s oder mehr. Mit zunehmender Gesamtbandbreitenkapazität steigt auch die Anzahl der Datenflüsse, die zur Erreichung der Spitzenverarbeitungsraten erforderlich sind. Mithilfe von Benchmarking können Sie ermitteln, welche Konfiguration Sie benötigen, um Spitzenraten in Ihrem Netzwerk zu erreichen.

Anzahl der Elastic Network Adapter (ENA) -Warteschlangen

Standardmäßig wird einer Netzwerkschnittstelle die maximale Anzahl von ENA-Warteschlangen zugewiesen, die auf Ihrer Instance-Größe und Ihrem Instance-Typ basiert. Durch die Reduzierung der Anzahl der Warteschlangen kann die maximal erreichbare PPS-Rate reduziert werden. Wir empfehlen, die standardmäßige Warteschlangenzuweisung zu verwenden, um eine optimale Leistung zu erzielen.

Für Linux ist eine Netzwerkschnittstelle standardmäßig mit dem Maximum konfiguriert. Für Anwendungen, die auf dem Data Plane Development Kit (DPDK) basieren, empfehlen wir, die maximale Anzahl verfügbarer Warteschlangen zu konfigurieren.

Mehraufwand für den Funktionsprozess

Funktionen wie Traffic Mirroring und ENA Express können den Verarbeitungsaufwand erhöhen, wodurch die absolute Paketverarbeitungsleistung reduziert werden kann. Sie können die Nutzung von Funktionen einschränken oder Funktionen deaktivieren, um die Paketverarbeitungsraten zu erhöhen.

Verbindungsverfolgung zur Aufrechterhaltung des Zustands

Ihre Sicherheitsgruppen verwenden die Verbindungsverfolgung, um Informationen über den Verkehr zur und von der Instance zu speichern. Die Verbindungsverfolgung wendet Regeln auf jeden einzelnen Netzwerkdatenverkehr an, um festzustellen, ob der Datenverkehr zugelassen oder verweigert wird. Die Nitro-Karte verwendet Flow-Tracking, um den Status des Datenflusses aufrechtzuerhalten. Je mehr Sicherheitsgruppenregeln angewendet werden, desto mehr Arbeit ist erforderlich, um den Flow auszuwerten.

> **Note**
>
> Nicht alle Netzwerkverkehrsflüsse werden verfolgt. Wenn eine Sicherheitsgruppenregel mit konfiguriert istUnverfolgte Verbindungen, ist keine zusätzliche Arbeit erforderlich, mit Ausnahme von Verbindungen, die automatisch nachverfolgt werden, um symmetrisches Routing zu gewährleisten, wenn mehrere gültige Antwortpfade vorhanden sind.

Pakete, die keine Hardwarebeschleunigung verwenden

Nicht alle Pakete können die Hardwarebeschleunigung nutzen. Die Behandlung dieser Ausnahmen ist mit einem gewissen Verarbeitungsaufwand verbunden, der erforderlich ist, um die Integrität Ihrer Netzwerkflüsse sicherzustellen. Netzwerkflüsse müssen zuverlässig den Protokollstandards entsprechen, Änderungen im VPC-Design entsprechen und Pakete nur an zulässige Ziele weiterleiten. Der Overhead reduziert jedoch Ihre Leistung.

Fragmente von Paketen

Wie unter Überlegungen zu Anwendungen erwähnt, werden Paketfragmente, die aus Paketen resultieren, die die Netzwerk-MTU überschreiten, als Ausnahmen behandelt und können die Vorteile der Hardwarebeschleunigung nicht nutzen.

Verbindungen im Leerlauf

Wenn eine Verbindung eine Zeit lang nicht aktiv ist, kann das System ihre Priorität herabsetzen, auch wenn die Verbindung ihr Timeout-Limit noch nicht erreicht hat. Wenn dann Daten eingehen, nachdem die Verbindung nicht mehr priorisiert wurde, muss das System sie ausnahmsweise behandeln, um die Verbindung wieder herzustellen.

Um Ihre Verbindungen zu verwalten, können Sie Timeouts für die Verbindungsverfolgung verwenden, um inaktive Verbindungen zu schließen. Sie können auch TCP-Keepalives verwenden, um inaktive Verbindungen aufrechtzuerhalten. Weitere Informationen finden Sie unter Timeout für die Nachverfolgung von Leerlaufverbindungen.

VPC-Mutation

Aktualisierungen von Sicherheitsgruppen, Routentabellen und Zugriffskontrolllisten müssen alle im Verarbeitungspfad neu bewertet werden, um sicherzustellen, dass Routeneinträge und Sicherheitsgruppenregeln weiterhin wie erwartet gelten.

ICMP-Flows

Das Internet Control Message Protocol (ICMP) ist ein Netzwerkschichtprotokoll, das Netzwerkgeräte zur Diagnose von Netzwerkkommunikationsproblemen verwenden. Diese Pakete verwenden immer den vollen Datenfluss.

Maximieren Sie die Netzwerkleistung auf Ihrem Nitro-System

Bevor Sie Designentscheidungen treffen oder Netzwerkeinstellungen auf Ihrer Instance anpassen, empfehlen wir Ihnen, die folgenden Schritte durchzuführen, um sicherzustellen, dass Sie das beste Ergebnis erzielen:

1. Machen Sie sich mit den Vor- und Nachteilen der Maßnahmen vertraut, die Sie ergreifen können, um die Leistung zu verbessernÜberlegungen.

   Weitere Überlegungen und bewährte Methoden für Ihre Instanzkonfiguration finden Sie unter:

   Linux-Instances — Leitfaden für bewährte Verfahren und Leistungsoptimierung für ENA-Linux-Treiber auf der GitHub Website.

   Windows-Instanzen —Bewährte Methoden zum Konfigurieren von Netzwerkschnittstellen.
2. Vergleichen Sie Ihre Workloads anhand der maximalen Anzahl an aktiven Datenströmen, um einen Basiswert für Ihre Anwendungsleistung zu ermitteln. Anhand einer Leistungsbasislinie können Sie Variationen in Ihren Einstellungen oder Ihrem Anwendungsdesign testen, um herauszufinden, welche Überlegungen die größte Wirkung haben werden, insbesondere, wenn Sie eine Hochskalierung oder Skalierung planen.

Die folgende Liste enthält Maßnahmen, die Sie je nach Ihren Systemanforderungen ergreifen können, um die Leistung Ihres PPS zu optimieren.

- Reduzieren Sie die physische Entfernung zwischen zwei Instanzen. Wenn sich sendende und empfangende Instances in derselben Availability Zone befinden oder Cluster-Platzierungsgruppen verwenden, können Sie die Anzahl der Hops reduzieren, die ein Paket zurücklegen muss, um von einem Endpunkt zum anderen zu gelangen.
- Verwenden Sie Unverfolgte Verbindungen.
- Verwenden Sie das UDP-Protokoll für den Netzwerkverkehr.
- Verteilen Sie bei EC2-Instances mit einer Gesamtbandbreite von 100 Gbit/s oder mehr die Arbeitslast auf 100 oder mehr einzelne Datenflüsse, um die Arbeit gleichmäßig auf die Nitro-Karte zu verteilen.

Überwachen Sie die Leistung auf Linux-Instances

Sie können Ethtool-Metriken auf Linux-Instances verwenden, um Leistungsindikatoren für das Instance-Netzwerk wie Bandbreite, Paketrate und Verbindungsverfolgung zu überwachen. Weitere Informationen finden Sie unter Überwachen der Netzwerkleistung für Ihre EC2-Instance.

Optimieren Sie die Netzwerkleistung auf Windows-Instances

Um die maximale Netzwerkleistung auf Ihren Windows-Instanzen mit erweitertem Netzwerk zu erreichen, müssen Sie möglicherweise die Standardbetriebssystemkonfiguration ändern. Wir empfehlen die folgenden Konfigurationsänderungen für Anwendungen, die eine hohe Netzwerkleistung erfordern. Andere Optimierungen (z. B. das Aktivieren des Prüfsummen-Offloads und das Aktivieren von RSS) sind auf offiziellen Windows-AMIs bereits konfiguriert.

> **Note**
>
> TCP-Chimney-Verschiebung sollte in den meisten Anwendungsfällen deaktiviert werden und ist ab Windows Server 2016 veraltet.

Zusätzlich zu diesen Betriebssystemoptimierungen sollten Sie auch die Maximum Transmission Unit (MTU, maximale Übertragungseinheit) Ihres Netzwerkverkehrs berücksichtigen und an Ihren Workload und Ihre Netzwerkarchitektur anpassen. Weitere Informationen finden Sie unter Netzwerk-MTU (Maximum Transmission Unit) für Ihre EC2-Instance.

AWS misst regelmäßig durchschnittliche Round-Trip-Latenzen zwischen Instances, die in einer Cluster-Platzierungsgruppe von 50 us gestartet werden, und Tail-Latenzen von 200 us bei 99,9 Perzentil. Wenn Ihre Anwendungen konsistent niedrige Latenzen erfordern, empfehlen wir, die neueste Version der ENA-Treiber auf Instances mit fester Leistung, die auf dem Nitro-System basieren.

Konfigurieren von RSS-CPU-Affinität

Empfangsseitige Skalierung (RSS, Receive Side Scaling) wird verwendet, um die CPU-Auslastung von Netzwerkverkehr auf mehrere Prozessoren zu verteilen. Standardmäßig ist für die offiziellen Amazon Windows-AMIs RSS aktiviert. ENA-ENIs stellen bis zu acht RSS-Warteschlangen bereit. Durch das Definieren der CPU-Affinität für RSS-Warteschlangen und andere Systemprozesse lässt sich die CPU-Auslastung auf Multi-Core-Systeme verteilen, wodurch mehr Netzwerkverkehr verarbeitet werden kann. Bei Instance-Typen mit mehr als 16 vCPUs empfehlen wir die Verwendung des `Set-NetAdapterRSS` PowerShell Cmdlets, das den Startprozessor (logische Prozessoren

0 und 1, wenn Hyperthreading aktiviert ist) manuell aus der RSS-Konfiguration für alle ENIs ausschließt, um Konflikte mit verschiedenen Systemkomponenten zu vermeiden.

Windows unterstützt Hyper-Threading und stellt sicher, dass die RSS-Warteschlangen einer einzelnen NIC immer in verschiedenen physischen Cores platziert werden. Sofern Hyper-Threading nicht deaktiviert ist, sollten Sie die RSS-Konfiguration jeder NIC auf einen Bereich von 16 logischen Prozessoren verteilen, um Konflikte unter anderen NICs vollständig zu vermeiden. Mit dem `Set-NetAdapterRss` Cmdlet können Sie den Bereich gültiger logischer Prozessoren pro NIC definieren, indem Sie die Werte von,,, und (optional) definieren. BaseProcessorGroup BaseProcessorNumber MaxProcessingGroup MaxProcessorNumber NumaNode Wenn es nicht genügend physische Cores gibt, um Konflikte zwischen NICs vollkommen zu beseitigen, sollten Sie die überlappenden Bereiche minimieren oder die Anzahl der logischen Prozessoren in den ENI-Bereichen abhängig von den voraussichtlichen Workload der ENI reduzieren (das heißt, ggf. müssen einer Administrator-Netzwerk-ENI mit geringem Volumen nicht so viele RSS-Warteschlangen zugewiesen werden). Zudem müssen, wie zuvor erwähnt, verschiedene Komponenten in der CPU 0 ausgeführt werden. Daher wird empfohlen, sie aus allen RSS-Konfigurationen auszuschließen, wenn genügend vCPUs verfügbar sind.

Wenn es beispielsweise drei ENIs auf einer Instance mit 72 vCPU gibt, die 2 NUMA-Knoten mit aktiviertem Hyper-Threading aufweist, wird mit den folgenden Befehlen die Netzwerklast zwischen zwei CPUs ohne Überlappung verteilt, sodass die Verwendung des Cores 0 vollständig verhindert wird.

```
Set-NetAdapterRss -Name NIC1 -BaseProcessorGroup 0 -BaseProcessorNumber 2 -
MaxProcessorNumber 16
Set-NetAdapterRss -Name NIC2 -BaseProcessorGroup 1 -BaseProcessorNumber 0 -
MaxProcessorNumber 14
Set-NetAdapterRss -Name NIC3 -BaseProcessorGroup 1 -BaseProcessorNumber 16 -
MaxProcessorNumber 30
```

Beachten Sie, dass diese Einstellungen für jeden Netzwerkadapter bestehen bleiben. Wenn die Größe einer Instance geändert wird und die Instance danach eine andere Anzahl von vCPUs hat, sollten Sie die RSS-Konfiguration für jede aktivierte ENI erneut auswerten. Die vollständige Microsoft-Dokumentation für das `Set-NetAdapterRss`-Cmdlet finden Sie hier: https://docs.microsoft.com/en-us/powershell/module/netadapter/set-netadapterrss.

Besonderer Hinweis für SQL-Workloads: Wir empfehlen auch, die I/O-Threadaffinitätseinstellungen zusammen mit Ihrer ENI-RSS-Konfiguration zu prüfen, um I/O- und Netzwerkkonflikte für

dieselben CPUs zu minimieren. Weitere Informationen finden Sie unter Affinitätsmaske (Serverkonfigurationsoption).

Elastic Fabric Adapter

Ein Elastic Fabric Adapter (EFA) ist ein Netzwerkgerät, das Sie an Ihre Amazon EC2-Instance anfügen können, um High-Performance-Computing (HPC)- und Machine-Learning-Anwendungen zu beschleunigen. EFA ermöglicht es Ihnen, die Anwendungsleistung eines lokalen HPC-Clusters mit der Skalierbarkeit, Flexibilität und Elastizität der Cloud zu erreichen. AWS

EFAs bieten eine niedrigere und konsistentere Latenz und einen höheren Durchsatz als der TCP-Transport, der traditionell in cloudbasierten HPC-Systemen verwendet wird. Es verbessert die Leistung der Kommunikation zwischen Instances, die für das Skalieren von HPC- und Machine-Learning-Anwendungen wichtig ist. Es ist für die Verwendung in der vorhandenen AWS Netzwerkinfrastruktur optimiert und kann je nach Anwendungsanforderungen skaliert werden.

EFAs lassen sich in Libfabric 1.7.0 und höher integrieren und unterstützen Open MPI 5 und höher und Intel MPI 2019 Update 5 und höher für HPC-Anwendungen sowie Nvidia Collective Communications Library (NCCL) für Machine-Learning-Anwendungen.

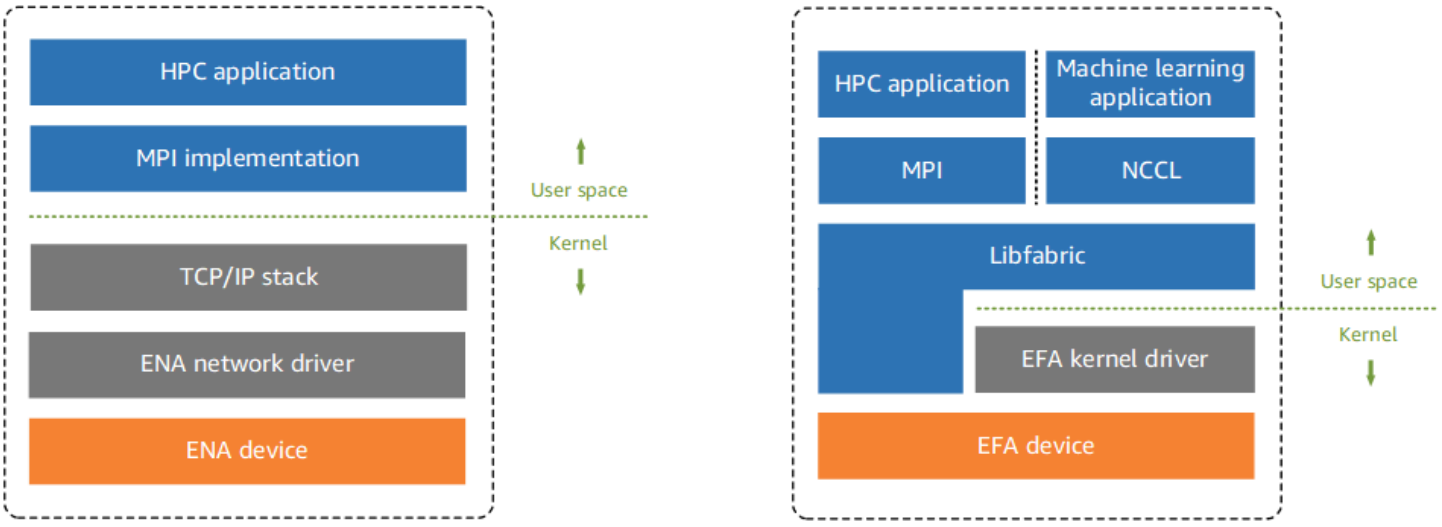
> **Note**
>
> Die Funktionen zur Betriebssystemumgehung von EFAs werden auf Windows-Instances nicht unterstützt. Wenn Sie ein EFA an eine Windows-Instances anfügen, fungiert diese als Elastic Network Adapter ohne die hinzugefügten EFA-Funktionen.

Inhalt

- Erste Schritte mit EFA und MPI
- Erste Schritte mit EFA und NCCL
- Arbeiten mit EFA
- Überwachen von EFA
- Überprüfen des EFA-Installationsprogramms mithilfe einer Prüfsumme

EFA-Grundlagen

Ein EFA ist ein Elastic Network Adapter (ENA) mit hinzugefügten Funktionen. Es bietet die gleichen Funktionen wie ein ENA, mit einer zusätzlichen Funktion zur Betriebssystemumgehung. Die Betriebssystemumgehung ist ein Zugriffsmodell, mit dem HPC- und Machine-Learning-Anwendungen direkt mit der Hardware der Netzwerkschnittstelle kommunizieren können, um eine zuverlässige Transportfunktionalität mit niedriger Latenz bereitzustellen.



Traditional HPC software stack in EC2

HPC software stack in EC2 with EFA

Üblicherweise verwenden HPC-Anwendungen die Message Passing Interface (MPI), um eine Schnittstelle zum Netzwerktransport des Systems herzustellen. In der AWS Cloud bedeutet dies, dass Anwendungen eine Schnittstelle zu MPI haben, das dann den TCP/IP-Stack des Betriebssystems und den ENA-Gerätetreiber verwendet, um die Netzwerkkommunikation zwischen Instanzen zu ermöglichen.

Mit einem EFA verwenden HPC-Anwendungen MPI oder NCCL als Schnittstelle zur Libfabric-API. Die Libfabric-API umgeht den Betriebssystem-Kernel und kommuniziert direkt mit dem EFA-Gerät, um Pakete auf dem Netzwerk zu platzieren. Dies reduziert den Aufwand und sorgt dafür, dass die HPC-Anwendung effektiver ausgeführt wird.

> **Note**
>
> Libfabric ist eine Kernkomponente des OpenFabrics Interfaces (OFI) -Frameworks, das die Userspace-API von OFI definiert und exportiert. Weitere Informationen finden Sie auf der Libfabric-Website. OpenFabrics

Unterschiede zwischen EFAs und ENAs

Elastic Network Adapters (ENAs) bietet herkömmliche IP-Netzwerkfeatures, die zur Unterstützung von VPC-Netzwerken erforderlich sind. EFAs bieten dieselben herkömmlichen IP-Netzwerkfeatures wie ENAs und unterstützen außerdem Features zur Betriebssystemumgehung. Die Betriebssystemumgehung ermöglicht es HPC- und Machine-Learning-Anwendungen, den Betriebssystem-Kernel zu umgehen und direkt mit dem EFA-Gerät zu kommunizieren.

Unterstützte Schnittstellen und Bibliotheken

EFAs unterstützen die folgenden Schnittstellen und Bibliotheken:

- Open MPI 5 und höher
- Open MPI 4.0 oder neuer wird für Graviton bevorzugt
- Intel MPI 2019 Update 5 und höher
- NVIDIA Collective Communications Library (NCCL) 2.4.2 und neuer

Unterstützte Instance-Typen

Die folgenden Instance-Typen unterstützen EFAs:

- Allgemeiner Zweck: `m5dn.24xlarge` `m5dn.metal` | `m5n.24xlarge` `m5n.metal` | `m5zn.12xlarge` | `m5zn.metal` | `m6a.48xlarge` | `m6a.metal` | `m6i.32xlarge` | `m6i.metal` | `m6id.32xlarge` | `m6id.metal` | `m6idn.32xlarge` | `m6idn.metal` | `m6in.32xlarge` `m6in.metal` | `m7a.48xlarge` | `m7a.metal-48xl` | `m7g.16xlarge` | `m7g.metal` | `m7gd.16xlarge` | `m7gd.metal` | `m7i.48xlarge` `m7i.metal-48xl`
- Für die Datenverarbeitung optimiert: `c5n.9xlarge` `c5n.18xlarge` `c5n.metal` || `c6a.48xlarge` | `c6a.metal` | `c6gn.16xlarge` | `c6i.32xlarge` | `c6i.metal` | `c6id.32xlarge` | `c6id.metal` | `c6in.32xlarge` | `c6in.metal` | `c7a.48xlarge` |

c7a.metal-48xl | c7g.16xlarge | | c7g.metal | c7gd.16xlarge | c7gd.metal | c7gn.16xlarge | c7gn.metal | c7i.48xlarge | c7i.metal-48xl

- Speicheroptimiert: r5dn.24xlarge | r5dn.metal | r5n.24xlarge | r5n.metal | r6a.48xlarge r6a.metal | r6i.32xlarge | r6i.metal | r6idn.32xlarge | r6idn.metal | r6in.32xlarge | r6in.metal | r6id.32xlarge | r6id.metal | r7a.48xlarge | r7a.metal-48xl | r7g.16xlarge | r7g.metal | r7gd.16xlarge | r7gd.metal | r7i.48xlarge | r7i.metal-48xl | r7iz.32xlarge r7iz.metal-32xl | u7i-12tb.224xlarge | u7in-16tb.224xlarge | u7in-24tb.224xlarge | u7in-32tb.224xlarge | x2idn.32xlarge | x2idn.metal | x2iedn.32xlarge | x2iedn.metal | x2iezn.12xlarge | x2iezn.metal
- Speicheroptimiert: i3en.12xlarge | i3en.24xlarge | i3en.metal | i4g.16xlarge | i4i.32xlarge | i4i.metal | im4gn.16xlarge
- Beschleunigtes Rechnen: dl1.24xlarge dl2q.24xlarge g4dn.8xlarge | g4dn.12xlarge | g4dn.16xlarge | g4dn.metal | g5.8xlarge | g5.12xlarge | g5.16xlarge | g5.24xlarge g5.48xlarge | g6.8xlarge | g6.12xlarge | g6.16xlarge | g6.24xlarge | g6.48xlarge | gr6.8xlarge | inf1.24xlarge | p3dn.24xlarge | p4d.24xlarge | p4de.24xlarge | p5.48xlarge | trn1.32xlarge | trn1n.32xlarge | vt1.24xlarge
- Hochleistungsrechnen: hpc6a.48xlarge | hpc6id.32xlarge | hpc7a.12xlarge | hpc7a.24xlarge | hpc7a.48xlarge | hpc7a.96xlarge | hpc7g.4xlarge | hpc7g.8xlarge | hpc7g.16xlarge

So zeigen Sie die verfügbaren Instance-Typen an, die EFAs in einer bestimmten Region unterstützen

Die verfügbaren Instance-Typen variieren je nach Region. Um die verfügbaren Instance-Typen anzuzeigen, die EFAs in einer Region unterstützen, verwenden Sie den Befehl describe-instance-types mit dem `--region`-Parameter. Schließen Sie den Parameter `--filters` ein, um die Ergebnisse auf die Instance-Typen zu beschränken, die EFA unterstützen, und den Parameter `--query`, um die Ausgabe auf den Wert von `InstanceType` zu beschränken.

```
aws ec2 describe-instance-types  --region us-east-1  --filters Name=network-info.efa-supported,Values=true  --query "InstanceTypes[*].[InstanceType]"  --output text | sort
```

Unterstützte Betriebssysteme

Die folgenden Betriebssysteme unterstützen EFAs mit Intel-/AMD x86-basierten Instance-Typen:

- Amazon Linux 2023

- Amazon Linux 2
- CentOS 7
- RHEL 7, 8 und 9
- Debian 10 und 11
- Rocky Linux 8 und 9
- Ubuntu 20.04 und 22.04
- SUSE Linux Enterprise 15 SP2 und höher
- OpenSUSE Leap 15.4 und höher

> **Note**
>
> Ubuntu 20.04 unterstützt bei Verwendung mit `dl1.24xlarge`-Instances die direkte Peer-Unterstützung.

Die folgenden Betriebssysteme unterstützen EFAs mit Arm-basierten (Graviton) Instance-Typen:

- Amazon Linux 2023
- Amazon Linux 2
- RHEL 8/9 und Rocky Linux 8/9
- Debian 10 und 11
- Ubuntu 20.04 und 22.04
- SUSE Linux Enterprise 15 SP2 und höher

EFA-Einschränkungen

EFAs haben die folgenden Einschränkungen:

- Alle P4d- und P5-Instance-Typen unterstützen NVIDIA GPUDirect Remote Direct Memory Access (RDMA).
- EFA-Datenverkehr zwischen P4D/P4DE/DL1-Instances und anderen Instance-Typen wird derzeit nicht unterstützt.

- Instance-Typen, die mehrere Netzwerkkarten unterstützen, können mit einer EFA pro Netzwerkkarte konfiguriert werden. Alle anderen unterstützten Instance-Typen unterstützen nur einen EFA pro Instance.
- Für `c7g.16xlarge`, `m7g.16xlarge` und `r7g.16xlarge` werden Dedicated Instances und Dedicated Hosts nicht unterstützt, wenn ein EFA angefügt ist.
- Der Datenverkehr der Betriebssystemumgehung von EFA ist auf ein einzelnes Sunbetz begrenzt. Mit anderen Worten kann EFA-Datenverkehr nicht von einem Subnetz an ein anderes gesendet werden. Normaler IP-Datenverkehr vom EFA kann von einem Subnetz an ein anderes gesendet werden.
- Der Datenverkehr der Betriebssystemumgehung von EFA kann nicht umgeleitet werden. Normaler IP-Datenverkehr vom EFA bleibt umleitbar.
- Das EFA muss zu einer Sicherheitsgruppe gehören, die allen eingehenden und ausgehenden Datenverkehr von und zu der Sicherheitsgruppe selbst zulässt.
- EFA wird auf Windows-Instances nicht unterstützt.
- EFA wird auf AWS Outposts nicht unterstützt.

EFA-Preisgestaltung

EFA ist als optionales Amazon-EC2-Netzwerkfeature verfügbar, das Sie ohne zusätzliche Kosten auf jeder unterstützten Instance aktivieren können.

Erste Schritte mit P5-Instances und EFA

P5-Instances bieten durch den Einsatz mehrerer EFA-Schnittstellen 3 200 Gbit/s Netzwerkbandbreite. P5-Instances unterstützen 32 Netzwerkkarten. Weitere Informationen zu den ersten Schritten mit P5-Instances für finden Sie unter Erste Schritte mit P5-Instances für Linux.

Es empfiehlt sich, pro Netzwerkkarte eine einzige EFA-Netzwerkschnittstelle zu definieren. Um diese Schnittstellen beim Start zu konfigurieren, empfehlen sich die folgenden Einstellungen:

- Für die Netzwerkschnittstelle `0` geben Sie den Geräteindex `0` an.
- Für die Netzwerkschnittstellen 1 bis 31 geben Sie den Geräteindex 1 an.

Bei Verwendung der Amazon-EC2-Konsole wählen Sie im Launch Instance Wizard die Option Bearbeiten im Abschnitt Netzwerkeinstellungen. Erweitern Sie Erweiterte Netzwerkkonfiguration und wählen Sie Netzwerkschnittstelle hinzufügen, um die erforderliche Anzahl von Netzwerkschnittstellen

hinzuzufügen. Für jede Netzwerkschnittstelle wählen Sie unter EFA die Option Aktivieren aus. Für alle Netzwerkschnittstellen, außer der primären Netzwerkschnittstelle, geben Sie unter Geräteindex den Wert 1 an. Konfigurieren Sie die verbleibenden Einstellungen nach Bedarf.

Wenn Sie den verwenden AWS CLI, verwenden Sie den Befehl run-instances für`--network-interfaces`, geben Sie die erforderliche Anzahl von Netzwerkschnittstellen an. Geben Sie für jede Netzwerkschnittstelle unter `InterfaceType` den Typ `efa` an. Geben Sie für die primäre Netzwerkschnittstelle unter `NetworkCardIndex` und `DeviceIndex` jeweils `0` an. Für die übrigen Netzwerkschnittstellen geben Sie unter `NetworkCardIndex` einen eindeutigen Wert von 1 bis 31 und unter `DeviceIndex` den Wert 1 an.

Der folgende Ausschnitt eines Beispielbefehls zeigt eine Anfrage mit 32 EFA-Netzwerkschnittstellen.

```
$ aws --region $REGION ec2 run-instances \
 --instance-type p5.48xlarge \
 --count 1 \
 --key-name key_pair_name \
 --image-id ami_id \
 --network-interfaces
 "NetworkCardIndex=0,DeviceIndex=0,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=1,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=2,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=3,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=4,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=5,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=6,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \

 "NetworkCardIndex=7,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
 \
```

```
"NetworkCardIndex=8,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\

"NetworkCardIndex=9,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=ef
\

"NetworkCardIndex=10,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=11,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=12,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=13,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=14,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=15,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=16,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=17,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=18,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=19,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=20,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\

"NetworkCardIndex=21,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
\
```

```
 "NetworkCardIndex=22,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=23,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=24,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=25,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=26,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=27,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=28,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=29,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=30,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
 \
 "NetworkCardIndex=31,DeviceIndex=1,Groups=security_group_id,SubnetId=subnet_id,InterfaceType=e
...
```

Geben Sie bei Verwendung einer Startvorlage die erforderliche Anzahl von Netzwerkschnittstellen in der Startvorlage an. Geben Sie für jede Netzwerkschnittstelle unter `InterfaceType` den Typ `efa` an. Geben Sie für die primäre Netzwerkschnittstelle unter `NetworkCardIndex` und `DeviceIndex` jeweils `0` an. Für die übrigen Netzwerkschnittstellen geben Sie unter `NetworkCardIndex` einen eindeutigen Wert von `1` bis `31` und unter `DeviceIndex` den Wert `1` an. Der folgende Ausschnitt zeigt ein Beispiel mit 3 Netzwerkschnittstellen (von möglichen 32 Netzwerkschnittstellen).

```
"NetworkInterfaces":[
{
  "NetworkCardIndex":0,
  "DeviceIndex":0,
```

```
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 1,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
},
{
  "NetworkCardIndex": 2,
  "DeviceIndex": 1,
  "InterfaceType": "efa",
  "AssociatePublicIpAddress":false,
  "Groups":[
    "security_group_id"
  ],
  "DeleteOnTermination":true
}
...
```

Wenn Sie eine P5-Instance mit mehr als einer Netzwerkschnittstelle starten, können Sie öffentliche IP-Adressen nicht automatisch zuweisen. Sie können jedoch nach dem Start eine Elastic IP-Adresse an die primäre Netzwerkschnittstelle (NetworkCardIndex=0, DeviceIndex =0) anhängen, um eine Internetverbindung herzustellen. Sowohl Ubuntu 20.04 und höher als auch Amazon Linux 2 und höher sind so konfiguriert, dass die primäre Netzwerkschnittstelle für den Internetverkehr verwendet wird, wenn die Instance wie oben empfohlen gestartet wird.

Erste Schritte mit EFA und MPI

Dieses Tutorial unterstützt Sie beim Starten eines EFA- und MPI-konformen Instance-Clusters für HPC-Workloads. In diesem Tutorial führen Sie die folgenden Schritte durch:

Inhalt

Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe

Ein EFA erfordert eine Sicherheitsgruppe, die allen ein- und ausgehenden Datenverkehr von und zur Sicherheitsgruppe zulässt. Mit dem folgenden Verfahren wird eine Sicherheitsgruppe erstellt, die den gesamten ein- und ausgehenden Datenverkehr der Gruppe sowie eingehenden SSH-Datenverkehr von jeder IPv4-Adresse zwecks SSH-Konnektivität zulässt.

> **Important**
>
> Diese Sicherheitsgruppe dient nur zu Testzwecken. Für Produktionsumgebungen sollten Sie eine Regel für eingehenden SSH-Datenverkehr erstellen, die Datenverkehr nur von der IP-Adresse zulässt, von der aus Sie eine Verbindung herstellen, z. B. die IP-Adresse Ihres Computers oder einen Bereich von IP-Adressen im lokalen Netzwerk.

Weitere Szenarien finden Sie unter Sicherheitsgruppenregeln für verschiedene Anwendungsfälle.

So erstellen Sie eine EFA-fähige Sicherheitsgruppe:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) und anschließend Create Security Group (Sicherheitsgruppe erstellen) aus.

3. Führen Sie im Fenster Create Security Group Folgendes aus:

   a. Geben Sie für Security group name (Name der Sicherheitsgruppe) einen beschreibenden Namen für die Sicherheitsgruppe ein, wie etwa `EFA-enabled security group`.

   b. (Optional:) Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Sicherheitsgruppe ein.

   c. Wählen Sie bei VPC die VPC aus, in der Sie Ihre EFA-fähigen Instances starten möchten.

   d. Wählen Sie Sicherheitsgruppe erstellen aus.

4. Wählen Sie die von Ihnen erstellte Sicherheitsgruppe aus und kopieren Sie dann auf der Registerkarte Details die Security group ID (Sicherheitsgruppen-ID).

5. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit inbound rules (Eingangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:

   a. Wählen Sie Regel hinzufügen aus.

   b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.

   c. Wählen Sie bei Source type (Quellentyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.

   d. Wählen Sie Regel hinzufügen aus.

   e. Wählen Sie unter Typ die Option SSH aus.

   f. Wählen Sie unter Source (Quelle) die Option Anywhere-IPv4 (Alle IPv4) aus.

   g. Wählen Sie Save rules (Regeln speichern) aus.

6. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit outbound rules (Ausgangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:

   a. Wählen Sie Regel hinzufügen aus.

   b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.

   c. Wählen Sie bei Destination type (Zieltyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.

   d. Wählen Sie Save rules (Regeln speichern) aus.

Schritt 2: Starten einer temporären Instance

Starten Sie eine temporäre Instance, die Sie verwenden können, um die EFA-Softwarekomponenten zu installieren und zu konfigurieren. Sie können mit dieser Instance ein EFA-aktiviertes AMI erstellen, von dem Sie Ihre EFA-aktivierten Instances starten können.

So starten Sie eine temporäre Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.
4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI für eines der unterstützten Betriebssysteme aus.
5. Wählen Sie im Bereich Instance type (Instance-Typ) einen supported instance type (unterstützten Instance-Typ) aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:

   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.

   b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.

   c. Erweitern Sie den Bereich Advanced network configuration (Erweiterte Netzwerkkonfiguration) und wählen Sie bei Elastic Fabric Adapter Enable (Aktivieren) aus.
8. Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.
9. Wählen Sie im Bereich Summary (Zusammenfassung) rechts Launch instance (Instance starten) aus.

Schritt 3: Installieren der EFA-Software

Installieren Sie den EFA-fähigen Kernel, die EFA-Treiber, Libfabric und den Open MPI-Stack, der zur Unterstützung von EFA auf Ihrer temporären Instance erforderlich ist.

Die Schritte unterscheiden sich abhängig davon, ob Sie EFA mit Open MPI, Intel MPI oder mit Open MPI und Intel MPI verwenden möchten.

So installieren Sie die EFA-Software

1. Stellen Sie eine Verbindung zu der Instance her, die Sie gestartet haben. Weitere Informationen finden Sie unter Herstellen einer Verbindung zur Linux-Instance.
2. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus. Dieser Vorgang kann einige Minuten dauern.

   - Amazon Linux 2023, Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9

     ```
     $ sudo yum update -y
     ```

   - Ubuntu 20.04/22.04 und Debian 10/11

     ```
     $ sudo apt-get update && sudo apt-get upgrade -y
     ```

   - SUSE Linux Enterprise

     ```
     $ sudo zypper update -y
     ```

3. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
4. Laden Sie die EFA-Software-Installationsdateien herunter. Die Software-Installationsdateien sind in einer komprimierten Tarball-Datei (`.tar.gz`) verpackt. Laden Sie die neueste stabile Version mit dem folgenden Befehl herunter.

   ```
   $ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz
   ```

   Sie erhalten die neueste Version auch, indem Sie anstelle der Versionsnummer im vorangegangenen Befehl `latest` eingeben.
5. (Optional) Überprüfen Sie die Authentizität und Integrität der EFA-Tarball-Datei (`.tar.gz`).

Diese Vorgehensweise wird empfohlen, um die Identität des Software-Publishers zu überprüfen und sicherzustellen, dass die Datei seit ihrer Veröffentlichung nicht verändert oder beschädigt wurde. Wenn Sie die Tarball-Datei nicht überprüfen möchten, überspringen Sie diesen Schritt.

> **Note**
>
> Wenn Sie die Tarball-Datei lieber mit einer MD5- oder SHA256-Prüfsumme überprüfen möchten, finden Sie Informationen unter Überprüfen des EFA-Installationsprogramms mithilfe einer Prüfsumme.

a. Laden Sie den öffentlichen GPG-Schlüssel herunter und importieren Sie ihn in Ihren Schlüsselbund.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
import aws-efa-installer.key
```

Der Befehl sollte einen Schlüsselwert zurückgeben. Notieren Sie sich den Schlüsselwert. Sie benötigen ihn im nächsten Schritt.

b. Überprüfen Sie den Fingerabdruck des GPG-Schlüssels. Führen Sie den folgenden Befehl aus und geben den Schlüsselwert aus dem vorherigen Schritt an.

```
$ gpg --fingerprint key_value
```

Der Befehl sollte einen Fingerabdruck zurückgeben, der mit `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC` identisch ist. Wenn der Fingerabdruck nicht übereinstimmt, führen Sie das EFA-Installationsskript nicht aus und wenden Sie sich an den AWS Support.

c. Laden Sie die Signaturdatei herunter und überprüfen Sie die Signatur der EFA-Tarball-Datei.

```
$ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz.sig
 && gpg --verify ./aws-efa-installer-1.32.0.tar.gz.sig
```

Das folgende Beispiel zeigt eine Ausgabe.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
```

```
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Wenn das Ergebnis `Good signature` enthält und der Fingerabdruck mit dem Fingerabdruck übereinstimmt, der im vorherigen Schritt zurückgegeben wurde, fahren Sie mit dem nächsten Schritt fort. Wenn nicht, führen Sie das EFA-Installationsskript nicht aus und wenden Sie sich an den AWS Support.

6. Extrahieren Sie die Daten aus der komprimierten `.tar.gz`-Datei und wechseln Sie in das extrahierte Verzeichnis.

```
$ C:\> tar -xf aws-efa-installer-1.32.0.tar.gz && cd aws-efa-installer
```

7. Installieren Sie die EFA-Software. Führen Sie je nach Anwendungsfall einen der folgenden Schritte durch.

> **Note**
>
> EFA unterstützt NVIDIA GPUDirect unter SUSE Linux nicht. Wenn Sie SUSE Linux verwenden, müssen Sie zusätzlich `--skip-kmod` festlegen, um die Installation von kmod zu verhindern. Standardmäßig erlaubt SUSE Linux keine Kernelmodule. out-of-tree

Open MPI and Intel MPI

Falls Sie EFA mit Open MPI und Intel MPI verwenden möchten, müssen Sie die EFA-Software mit Libfabric und Open MPI installieren und Schritt 5: Intel MPI installieren abschließen.

Führen Sie den folgenden Befehl aus, um die EFA-Software mit Libfabric und Open MPI zu installieren.

> **Note**
>
> Ab EFA 1.30.0 sind sowohl Open MPI 4 als auch Open MPI 5 standardmäßig installiert. Sie können optional die Version von Open MPI angeben, die Sie installieren möchten. Um nur Open MPI 4 zu installieren, schließen Sie `--`

`mpi=openmpi4` ein. Um nur Open MPI 5 zu installieren, schließen Sie `--mpi=openmpi5` ein. Um beide zu installieren, lassen Sie die `--mpi`-Option weg.

```
$ C:\> sudo ./efa_installer.sh -y
```

Libfabric ist auf `/opt/amazon/efa` installiert. Open MPI 4 ist auf `/opt/amazon/openmpi` installiert. Open MPI 5 ist auf `/opt/amazon/openmpi5` installiert.

Open MPI only

Falls Sie EFA nur mit Open MPI verwenden möchten, müssen Sie die EFA-Software mit Libfabric und Open MPI installieren und können Schritt 5: Intel MPI installieren überspringen. Führen Sie den folgenden Befehl aus, um die EFA-Software mit Libfabric und Open MPI zu installieren.

> **Note**
>
> Ab EFA 1.30.0 sind sowohl Open MPI 4 als auch Open MPI 5 standardmäßig installiert. Sie können optional die Version von Open MPI angeben, die Sie installieren möchten. Um nur Open MPI 4 zu installieren, schließen Sie `--mpi=openmpi4` ein. Um nur Open MPI 5 zu installieren, schließen Sie `--mpi=openmpi5` ein. Um beide zu installieren, lassen Sie die `--mpi`-Option weg.

```
$ C:\> sudo ./efa_installer.sh -y
```

Libfabric ist auf `/opt/amazon/efa` installiert. Open MPI 4 ist auf `/opt/amazon/openmpi` installiert. Open MPI 5 ist auf `/opt/amazon/openmpi5` installiert.

Intel MPI only

Wenn Sie EFA nur mit Intel MPI verwenden möchten, können Sie die EFA-Software ohne Libfabric und Open MPI installieren. In diesem Fall verwendet Intel MPI seine eingebettete Libfabric. Wenn Sie dies tun, müssen Sie Schritt :5 Intel MPI installieren abschließen.

Führen Sie den folgenden Befehl aus, um die EFA-Software ohne Libfabric und Open MPI zu installieren.

```
$ C:\> sudo ./efa_installer.sh -y --minimal
```

8. Wenn das EFA-Installationsprogramm Sie auffordert, die Instance neu zu starten, tun Sie dies und stellen Sie dann erneut eine Verbindung mit der Instance her. Melden Sie sich andernfalls von der Instance ab und wieder an, um die Installation abzuschließen.

Schritt 4: (Optional) Open MPI 5 aktivieren

> **Note**
>
> Führen Sie diesen Schritt nur aus, wenn Sie Open MPI 5 verwenden wollen.

Ab EFA 1.30.0 sind sowohl Open MPI 4 als auch Open MPI 5 standardmäßig installiert. Alternativ können Sie wählen, nur Open MPI 4 oder Open MPI 5 zu installieren.

Wenn Sie sich in Schritt 3: EFA-Software installieren für die Installation von Open MPI 5 entschieden haben und diese Software verwenden möchten, müssen Sie die folgenden Schritte ausführen, um sie zu aktivieren.

So aktivieren Sie Open MPI 5

1. Fügen Sie Open MPI 5 zur Umgebungsvariablen PATH hinzu.

   ```
   $ module load openmpi5
   ```

2. Stellen Sie sicher, dass Open MPI 5 für die Verwendung aktiviert ist.

   ```
   $ which mpicc
   ```

   Der Befehl sollte das Open-MPI-5-Installationsverzeichnis zurückgeben – `/opt/amazon/openmpi5`.

3. (Optional) Gehen Sie wie folgt vor, um sicherzustellen, dass Open MPI 5 bei jedem Start der Instance zur Umgebungsvariablen PATH hinzugefügt wird:

bash shell

Fügen Sie `module load openmpi5` zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

csh and tcsh shells

Fügen Sie `module load openmpi5` zu /home/*username*/.cshrc hinzu.

Wenn Sie Open MPI 5 aus der Umgebungsvariablen PATH entfernen müssen, führen Sie den folgenden Befehl aus und entfernen Sie den Befehl aus den Shell-Startup-Skripten.

```
$ module unload openmpi5
```

Schritt 5: (Optional) Installieren von Intel MPI

> **Important**
>
> Führen Sie diesen Schritt nur aus, wenn Sie vorhaben, Intel MPI zu verwenden. Wenn Sie vorhaben, nur Open MPI zu verwenden, überspringen Sie diesen Schritt.

Intel MPI erfordert eine zusätzliche Einrichtung und Konfiguration der Umgebungsvariablen.

Voraussetzung

Stellen Sie sicher, dass der Benutzer, der die folgenden Schritte ausführt, über sudo-Berechtigungen verfügt.

So installieren Sie Intel MPI

1. Gehen Sie wie folgt vor, um das Intel MPI-Installationsskript herunterzuladen
   a. Besuchen Sie die Intel-Website.
   b. Wählen Sie im Abschnitt Intel MPI Library (Intel-MPI-Bibliothek) auf der Website den Link für Intel MPI Library for Linux, Offline-Installationsprogramm aus.
2. Führen Sie das Skript für die Installation aus, das Sie im vorherigen Schritt heruntergeladen haben.

```
$ C:\> sudo bash installation_script_name.sh
```

3. Wählen Sie im Installationsprogramm Accept & install (Akzeptieren und installieren) aus.
4. Lesen Sie das Intel-Verbesserungsprogramm durch, wählen Sie die entsprechende Option und dann Begin Installation (Mit der Installation beginnen) aus.
5. Nach abgeschlossener Installation wählen Sie Schließen aus.
6. Standardmäßig verwendet Intel MPI seine eingebettete (interne) Libfabric. Sie können Intel MPI so konfigurieren, dass stattdessen die Libfabric verwendet wird, die im EFA-Installationsprogramm enthalten ist. Typischerweise wird das EFA-Installationsprogramm mit einer neueren Version von Libfabric als Intel MPI ausgeliefert. In einigen Fällen ist Libfabric, die mit dem EFA-Installationsprogramm geliefert wird, leistungsfähiger als Intel MPI. Führen Sie je nach Shell einen der folgenden Schritte aus, um Intel MPI für die Verwendung von Libfabric zu konfigurieren, die mit dem EFA-Installationsprogramm geliefert wird.

   bash shells

   Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

   ```
   export I_MPI_OFI_LIBRARY_INTERNAL=0
   ```

   csh and tcsh shells

   Fügen Sie die folgende Anweisung zu /home/*username*/.cshrc hinzu.

   ```
   setenv I_MPI_OFI_LIBRARY_INTERNAL 0
   ```

7. Fügen Sie Ihrem Shell-Skript den folgenden Quell-Befehl hinzu, um das `vars.sh`-Skript aus dem Installationsverzeichnis zum Einrichten der Compiler-Umgebung bei jedem Start der Instance zu beziehen. Führen Sie je nach Shell einen der folgenden Schritte durch.

   bash shells

   Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

   ```
   source /opt/intel/oneapi/mpi/latest/env/vars.sh
   ```

csh and tcsh shells

Fügen Sie die folgende Anweisung zu /home/*username*/.cshrc hinzu.

```
source /opt/intel/oneapi/mpi/latest/env/vars.csh
```

8. Wenn EFA aufgrund einer Fehlkonfiguration nicht verfügbar ist, verwendet Intel MPI standardmäßig den TCP/IP-Netzwerk-Stack, was zu einer langsameren Anwendungsleistung führen kann. Sie können dies verhindern, indem Sie `I_MPI_OFI_PROVIDER` auf `efa` setzen. Dies führt dazu, dass Intel MPI mit dem folgenden Fehler fehlschlägt, wenn EFA nicht verfügbar ist:

```
Abort (XXXXXX) on node 0 (rank 0 in comm 0): Fatal error in PMPI_Init: OtherMPI
 error,
MPIR_Init_thread (XXX).......:
MPID_Init (XXXX).............:
MPIDI_OFI_mpi_init_hook (XXXX):
open_fabric (XXXX)...........:
find_provider (XXXX).........:
OFI fi_getinfo() failed (ofi_init.c:2684:find_provider:
```

Führen Sie je nach Shell einen der folgenden Schritte durch.

bash shells

Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

```
export I_MPI_OFI_PROVIDER=efa
```

csh and tcsh shells

Fügen Sie die folgende Anweisung zu /home/*username*/.cshrc hinzu.

```
setenv I_MPI_OFI_PROVIDER efa
```

9. Standardmäßig gibt Intel MPI keine Debugging-Informationen aus. Sie können verschiedene Ausführlichkeitsstufen angeben, um die Debugging-Informationen zu steuern. Mögliche Werte (in der Reihenfolge der bereitgestellten Details) sind: `0` (Standard), `1`, `2`, `3`, `4`, `5`. Level `1` und höher druckt `libfabric version` und `libfabric provider`. Verwenden Sie `libfabric`

`version`, um zu überprüfen, ob Intel MPI die interne Libfabric verwendet oder die Libfabric, die mit dem EFA-Installationsprogramm geliefert wird. Wenn es die interne Libfabric verwendet, wird der Version ein `impi` angehängt. Verwenden Sie `libfabric provider`, um zu überprüfen, ob Intel MPI EFA oder das TCP/IP-Netzwerk verwendet. Wenn es EFA verwendet, ist der Wert `efa`. Wenn es TCP/IP verwendet, ist der Wert `tcp;ofi_rxm`.

Um Debugging-Informationen zu aktivieren, führen Sie je nach Shell einen der folgenden Schritte durch.

bash shells

Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

```
export I_MPI_DEBUG=value
```

csh and tcsh shells

Fügen Sie die folgende Anweisung zu /home/*username*/.cshrc hinzu.

```
setenv I_MPI_DEBUG value
```

10. Standardmäßig verwendet Intel MPI den gemeinsam genutzten Speicher des Betriebssystems (`shm`) für die Kommunikation innerhalb des Knotens und verwendet Libfabric (`ofi`) nur für die Kommunikation zwischen Knoten. Im Allgemeinen bietet diese Konfiguration die beste Leistung. In einigen Fällen kann die Intel-MPI-shm-Fabric jedoch dazu führen, dass bestimmte Anwendungen auf unbestimmte Zeit hängen bleiben.

    Um dieses Problem zu lösen, können Sie Intel MPI zwingen, Libfabric sowohl für die Kommunikation innerhalb von Knoten als auch zwischen Knoten zu verwenden. Führen Sie dazu je nach Shell einen der folgenden Schritte aus.

    bash shells

    Fügen Sie die folgende Anweisung zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

    ```
    export I_MPI_FABRICS=ofi
    ```

csh and tcsh shells

Fügen Sie die folgende Anweisung zu `/home/username/.cshrc` hinzu.

```
setenv I_MPI_FABRICS ofi
```

> **Note**
>
> Der EFA-Libfabric-Anbieter verwendet den gemeinsam genutzten Speicher des Betriebssystems für die Kommunikation innerhalb des Knotens. Das bedeutet, dass die Einstellung von `I_MPI_FABRICS` auf `ofi` zu einer ähnlichen Leistung führt wie die Standardkonfiguration `shm:ofi`.

11. Melden Sie sich von der Instance ab. Melden Sie sich anschließend wieder an.

Wenn Sie Intel MPI nicht mehr verwenden möchten, entfernen Sie die Umgebungsvariablen aus den Shell-Startupskripts.

Schritt 6: Ptrace-Schutz aktivieren

Um die Leistung Ihrer HPC-Anwendung zu verbessern, verwendet Libfabric den lokalen Speicher der Instance für die Kommunikation zwischen Prozessen, wenn die Prozesse auf derselben Instance ausgeführt werden.

Das Shared Memory Feature verwendet Cross Memory Attach (CMA), das mit Ptrace-Schutz nicht unterstützt wird. Wenn Sie eine Linux-Distribution verwenden, beider standardmäßig Ptrace-Schutz aktiviert hat, z. B. Ubuntu, müssen Sie ihn deaktivieren. Wenn für Ihre Linux-Distribution standardmäßig kein Ptrace-Schutz aktiviert ist, überspringen Sie diesen Schritt.

So deaktivieren Sie den Ptrace-Schutz

Führen Sie eine der folgenden Aufgaben aus:

- Führen Sie den folgenden Befehl aus, um den Ptrace-Schutz vorübergehend zu deaktivieren.

```
$ sudo sysctl -w kernel.yama.ptrace_scope=0
```

- Um den Ptrace-Schutz dauerhaft zu deaktivieren, fügen Sie `kernel.yama.ptrace_scope = 0` zu `/etc/sysctl.d/10-ptrace.conf` hinzu und starten Sie die Instance neu.

Schritt 7. Bestätigen der Installation

So bestätigen Sie die erfolgreiche Installation

1. Bestätigen Sie durch Ausführen des folgenden Befehls, dass MPI erfolgreich installiert wurde:

   ```
   $ which mpicc
   ```

   - Für Open MPI muss der zurückgegebene Pfad `/opt/amazon/` enthalten
   - Für Intel MPI muss der zurückgegebene Pfad `/opt/intel/` enthalten. Wenn Sie nicht die erwartete Ausgabe erhalten, stellen Sie sicher, dass Sie das `vars.sh`-Skript für Intel MPI bezogen haben.

2. Um zu überprüfen, ob die EFA-Softwarekomponenten und Libfabric erfolgreich installiert wurden, führen Sie den folgenden Befehl aus.

   ```
   $ C:\> fi_info -p efa -t FI_EP_RDM
   ```

   Der Befehl muss Informationen zu den Libfabric-EFA-Schnittstellen zurückgeben. Das folgende Beispiel zeigt die Befehlsausgabe.

   ```
   provider: efa
       fabric: EFA-fe80::94:3dff:fe89:1b70
       domain: efa_0-rdm
       version: 2.0
       type: FI_EP_RDM
       protocol: FI_PROTO_EFA
   ```

Schritt 8: Ihre HPC-Anwendung installieren

Installieren Sie die HPC-Anwendung auf der temporären Instance. Der Installationsvorgang unterscheidet sich je nach spezifischer HPC-Anwendung. Weitere Informationen finden Sie unter Software auf Ihrer AL2-Instance verwalten im Amazon Linux 2-Benutzerhandbuch.

> **Note**
>
> In der Dokumentation Ihrer HPC-Anwendung finden Sie Installationsanweisungen.

Schritt 9: Ein EFA-fähiges AMI erstellen

Nachdem Sie die erforderlichen Softwarekomponenten installiert haben, erstellen Sie ein AMI, das Sie erneut verwenden können, um Ihre EFA-fähigen Instances zu starten.

So erstellen Sie ein AMI aus Ihrer temporären Instance:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre Instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Image und Create Image (Image erstellen) aus.
4. Gehen Sie bei Create Image (Image erstellen) wie folgt vor:
   a. Geben Sie unter Image name (Image-Name) einen beschreibenden Namen für das AMI ein.
   b. (Optional:) Geben Sie bei Image description (Image-Beschreibung) eine kurze Beschreibung des Zwecks des AMI ein.
   c. Wählen Sie Create Image (Image erstellen) aus.
5. Wählen Sie im Navigationsbereich die Option AMIs.
6. Suchen Sie das AMI, das Sie erstellt haben, in der Liste. Warten Sie, bis der Status von `pending` zu `available` wechselt, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 10: EFA-fähige Instances in einer Cluster-Placement-Gruppe starten

Starten Sie die EFA-aktivierten Instances unter Verwendung des EFA-aktiviertenAMI, das Sie in Schritt 7 erstellt haben, in einer Cluster Placement-Gruppe. Starten Sie dann die EFA-aktivierte Sicherheitsgruppe, die Sie in Schritt 1 erstellt haben.

> **Note**
>
> - Es ist keine absolute Voraussetzung, Ihre EFA-aktivierten Instances in einer Cluster-Platzierungsgruppe zu starten. Wir empfehlen allerdings, Ihre EFA-Instances in einer

Cluster-Placement-Gruppe zu starten, da die Instances dadurch in einer Gruppe mit niedriger Latenz in einer einzelnen Availability Zone gestartet werden.

- Um die Verfügbarkeit von Kapazitäten sicherzustellen, wenn Sie die Instances Ihres Clusters skalieren, können Sie eine Kapazitätsreservierung für Ihre Cluster-Placement-Gruppe erstellen. Weitere Informationen finden Sie unter Kapazitätsreservierungen in Cluster-Placement-Gruppen.

So starten Sie eine temporäre Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.
4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) My AMIs (Meine AMIs) und dann das AMI aus, das Sie im vorherigen Schritt erstellt haben.
5. Wählen Sie im Bereich Instance type (Instance-Typ) einen supported instance type (unterstützten Instance-Typ) aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:

   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.

   b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.

   c. Erweitern Sie den Bereich Advanced network configuration (Erweiterte Netzwerkkonfiguration) und wählen Sie bei Elastic Fabric Adapter Enable (Aktivieren) aus.
8. (Optional) Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.
9. Wählen Sie im Bereich Advanced details (Erweiterte Details) bei Placement group name (Placement-Gruppen-Name) die Cluster-Placement-Gruppe aus, in der die Instances gestartet

werden sollen. Wenn Sie eine neue Cluster-Placement-Gruppe erstellen müssen, wählen Sie Create new placement group (Neue Placement-Gruppe erstellen).

10. Geben Sie im Bereich Summary (Zusammenfassung) rechts bei Number of instances (Anzahl der Instances) die Anzahl EFA-fähiger Instances ein, die Sie starten möchten, und wählen Sie dann Launch instance (Instance starten).

Schritt 11: Beenden der temporären Instance

An diesem Punkt benötigen Sie die temporäre Instance, die Sie gestartet haben, nicht mehr. Sie können die Instance beenden, damit keine weiteren Kosten dafür anfallen.

So beenden Sie die temporäre Instance:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Instance state (Instance-Zustand) und Terminate instance (Instance beenden) aus.
4. Wählen Sie Terminate (Kündigen) aus, wenn Sie zur Bestätigung aufgefordert werden.

Schritt 12: Passwortloses SSH aktivieren

Damit Ihre Anwendungen auf allen Instances in Ihrem Cluster ausgeführt werden können, müssen Sie passwortlosen SSH-Zugriff vom Führungsknoten auf die Mitgliedsknoten aktivieren. Der Führungsknoten ist die Instance, von der aus Sie die Anwendungen ausführen. Die verbleibenden Instances im Cluster sind die Mitgliedsknoten.

So aktivieren Sie passwortloses SSH zwischen den Instances im Cluster:

1. Wählen Sie eine Instance im Cluster als Führungsknoten aus und stellen Sie eine Verbindung zu ihr her.
2. Deaktivieren Sie `strictHostKeyChecking` und aktivieren Sie `ForwardAgent` für den Führungsknoten. Öffnen Sie `~/.ssh/config` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
Host *
    ForwardAgent yes
```

```
Host *
    StrictHostKeyChecking no
```

3. Generieren Sie ein RSA-Schlüsselpaar.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   Das Schlüsselpaar wird im `$HOME/.ssh/`-Verzeichnis erstellt.

4. Ändern Sie die Berechtigungen des privaten Schlüssels auf dem Führungsknoten.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Öffnen Sie `~/.ssh/id_rsa.pub` mit Ihrem bevorzugten Texteditor und kopieren Sie den Schlüssel.
6. Gehen Sie für jeden Mitgliedsknoten im Cluster wie folgt vor:
   a. Stellen Sie eine Verbindung mit der Instance her.
   b. Öffnen Sie `~/.ssh/authorized_keys` mit Ihrem bevorzugten Texteditor und fügen Sie den öffentlichen Schlüssel hinzu, den Sie zuvor kopiert haben.
7. Um zu testen, ob das passwortlose SSH wie erwartet funktioniert, stellen Sie eine Verbindung zum Leaderknoten her und führen Sie den folgenden Befehl aus.

```
$ ssh member_node_private_ip
```

   Sie sollten eine Verbindung zum Mitgliedsknoten herstellen können, ohne zur Eingabe eines Schlüssels oder Passworts aufgefordert zu werden.

Erste Schritte mit EFA und NCCL

Die NVIDIA Collective Communications Library (NCCL) ist eine Bibliothek kollektiver Standardkommunikationsroutinen für mehrere GPUs über einen oder mehrere Knoten. Die NCCL kann zusammen mit EFA, libfabric und MPI verwendet werden, um verschiedene Machine-Learning-Workloads zu unterstützen. Weitere Informationen finden Sie auf der NCCL-Website.

> **Note**
>
> - NCCL mit EFA wird nur mit `p3dn.24xlarge`, `p4d.24xlarge` und `p5.48xlarge` unterstützt.
> - Die NCCL wird erst ab Version 2.4.2 mit EFA unterstützt.

Die folgenden Tutorials unterstützen Sie beim Starten eines EFA- und NCCL-konformen Instance-Clusters für Machine-Learning-Workloads.

- Verwenden einer Basis AMI
- Verwenden Sie ein AWS Deep Learning-AMI

Verwenden einer Basis AMI

Die folgenden Schritte unterstützen Sie bei den ersten Schritten mit Elastic Fabric Adapter mithilfe eines AMIs für eines der unterstützten Basis-Betriebssysteme.

> **Note**
>
> - Nur die Instance-Typen `p3dn.24xlarge`, `p4d.24xlarge` und `p5.48xlarge` werden unterstützt.
> - Nur Basis-AMIs von Amazon Linux 2, RHEL 7/8/9, CentOS 7, Rocky Linux 8/9 und Ubuntu 20.04/22.04 werden unterstützt.

Inhalt

Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe

Ein EFA erfordert eine Sicherheitsgruppe, die allen ein- und ausgehenden Datenverkehr von und zur Sicherheitsgruppe zulässt. Mit dem folgenden Verfahren wird eine Sicherheitsgruppe erstellt, die den gesamten ein- und ausgehenden Datenverkehr der Gruppe sowie eingehenden SSH-Datenverkehr von jeder IPv4-Adresse zwecks SSH-Konnektivität zulässt.

> **Important**
>
> Diese Sicherheitsgruppe dient nur zu Testzwecken. Für Produktionsumgebungen sollten Sie eine Regel für eingehenden SSH-Datenverkehr erstellen, die Datenverkehr nur von der IP-Adresse zulässt, von der aus Sie eine Verbindung herstellen, z. B. die IP-Adresse Ihres Computers oder einen Bereich von IP-Adressen im lokalen Netzwerk.

Weitere Szenarien finden Sie unter Sicherheitsgruppenregeln für verschiedene Anwendungsfälle.

So erstellen Sie eine EFA-fähige Sicherheitsgruppe:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) und anschließend Create Security Group (Sicherheitsgruppe erstellen) aus.
3. Führen Sie im Fenster Create Security Group Folgendes aus:
   a. Geben Sie für Security group name (Name der Sicherheitsgruppe) einen beschreibenden Namen für die Sicherheitsgruppe ein, wie etwa `EFA-enabled security group`.
   b. (Optional:) Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Sicherheitsgruppe ein.

c. Wählen Sie bei VPC die VPC aus, in der Sie Ihre EFA-fähigen Instances starten möchten.

d. Wählen Sie Sicherheitsgruppe erstellen aus.

4. Wählen Sie die von Ihnen erstellte Sicherheitsgruppe aus und kopieren Sie dann auf der Registerkarte Details die Security group ID (Sicherheitsgruppen-ID).

5. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit inbound rules (Eingangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:

   a. Wählen Sie Regel hinzufügen aus.

   b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.

   c. Wählen Sie bei Source type (Quellentyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.

   d. Wählen Sie Regel hinzufügen aus.

   e. Wählen Sie unter Typ die Option SSH aus.

   f. Wählen Sie unter Source (Quelle) die Option Anywhere-IPv4 (Alle IPv4) aus.

   g. Wählen Sie Save rules (Regeln speichern) aus.

6. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit outbound rules (Ausgangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:

   a. Wählen Sie Regel hinzufügen aus.

   b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.

   c. Wählen Sie bei Destination type (Zieltyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.

   d. Wählen Sie Save rules (Regeln speichern) aus.

Schritt 2: Starten einer temporären Instance

Starten Sie eine temporäre Instance, die Sie verwenden können, um die EFA-Softwarekomponenten zu installieren und zu konfigurieren. Sie können mit dieser Instance ein EFA-aktiviertes AMI erstellen, von dem Sie Ihre EFA-aktivierten Instances starten können.

So starten Sie eine temporäre Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.

3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.
4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) ein AMI für eines der unterstützten Betriebssysteme aus.
5. Wählen Sie im Bereich Instance-Typ entweder `p3dn.24xlarge`, `p4d.24xlarge` oder `p5.48xlarge` aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:
   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.
   b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.
   c. Erweitern Sie den Bereich Advanced network configuration (Erweiterte Netzwerkkonfiguration) und wählen Sie bei Elastic Fabric Adapter Enable (Aktivieren) aus.
8. Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.

   > **Note**
   >
   > Sie müssen zusätzliche 10 bis 20 GiB Speicher für das Nvidia CUDA Toolkit bereitstellen. Wenn Sie nicht genügend Speicherplatz bereitstellen, erhalten Sie einen `insufficient disk space`-Fehler beim Versuch, die Nvidia-Treiber und das CUDA-Toolkit zu installieren.

9. Wählen Sie im Bereich Summary (Zusammenfassung) rechts Launch instance (Instance starten) aus.

Schritt 3: Installieren der Nvidia-GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN

Amazon Linux 2

Installieren der Nvidia GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN

1. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus.

   ```
   $ sudo yum upgrade -y && sudo reboot
   ```

   Stellen Sie nach dem Neustart der Instance erneut eine Verbindung dazu her.

2. Installieren Sie die Dienstprogramme, die zum Installieren der Nvidia GPU-Treiber und des Nvidia CUDA-Toolkits benötigt werden.

   ```
   $ sudo yum groupinstall 'Development Tools' -y
   ```

3. Deaktivieren Sie die `nouveau`-Open-Source-Treiber.

   a. Installieren Sie die erforderlichen Dienstprogramme und das Kernel-Header-Paket für Ihre derzeit ausgeführte Kernel-Version.

      ```
      $ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -
      r)
      ```

   b. Fügen Sie `nouveau` der Verweigerungsliste `/etc/modprobe.d/blacklist.conf` hinzu.

      ```
      $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
      blacklist vga16fb
      blacklist nouveau
      blacklist rivafb
      blacklist nvidiafb
      blacklist rivatv
      EOF
      ```

   c. Hängen Sie `GRUB_CMDLINE_LINUX="rdblacklist=nouveau"` an die `grub`-Datei an und erstellen Sie die Grub-Konfiguration neu.

      ```
      $ echo 'GRUB_CMDLINE_LINUX="rdblacklist=nouveau"' | sudo tee -a /etc/
      default/grub \
      ```

```
&& sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
5. Vorbereiten der erforderlichen Repositorys

   a. Installieren Sie das EPEL-Respository für DKMS und aktivieren Sie alle optionalen Repositorys für Ihre Linux-Distribution.

   ```
   $ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
   latest-7.noarch.rpm
   ```

   b. Installieren Sie den öffentlichen GPG-Schlüssel des CUDA-Repositorys.

   ```
   $ distribution='rhel7'
   ```

   c. Richten Sie das CUDA Netzwerk-Repository ein und aktualisieren Sie den Repository-Cache.

   ```
   $ ARCH=$( /bin/arch ) \
   && sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
   compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
   && sudo yum clean expire-cache
   ```

   d. (Nur Kernel-Version 5.10) Führen Sie diese Schritte nur aus, wenn Sie Amazon Linux 2 mit Kernel-Version 5.10 nutzen. Überspringen Sie dieses Schritte, wenn Sie Amazon Linux 2 mit Kernel-Version 4.12 verwenden. Um Ihre Kernel-Version zu überprüfen, führen Sie uname -r aus.

      i. Erstellen Sie die Nvidia-Treiberkonfigurationsdatei mit dem Namen `/etc/dkms/nvidia.conf`.

      ```
      $ sudo mkdir -p /etc/dkms \
      && echo "MAKE[0]=\"'make' -j2 module SYSSRC=\${kernel_source_dir}
       IGNORE_XEN_PRESENCE=1 IGNORE_PREEMPT_RT_PRESENCE=1 IGNORE_CC_MISMATCH=1
       CC=/usr/bin/gcc10-gcc\"" | sudo tee /etc/dkms/nvidia.conf
      ```

      ii. (Nur `p4d.24xlarge` und `p5.48xlarge`) Kopieren Sie die Konfigurationsdatei des Nvidia-Treibers.

      ```
      $ sudo cp /etc/dkms/nvidia.conf /etc/dkms/nvidia-open.conf
      ```

6. Installieren Sie die Nvidia-GPU-Treiber, das NVIDIA CUDA-Toolkit und cuDNN.

   - `p3dn.24xlarge`

     ```
     $ sudo yum clean all \
     && sudo yum -y install kmod-nvidia-latest-dkms nvidia-driver-latest-dkms \
     && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
     ```

   - `p4d.24xlarge` und `p5.48xlarge`

     ```
     $ sudo yum clean all \
     && sudo yum -y install kmod-nvidia-open-dkms nvidia-driver-latest-dkms \
     && sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
     ```

7. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
8. (Nur `p4d.24xlarge` und `p5.48xlarge`) Starten Sie den NVIDIA Fabric Manager Service und stellen Sie sicher, dass er beim Start der Instance automatisch gestartet wird. Nvidia Fabric Manager ist für das NV Switch Management erforderlich.

   ```
   $ sudo systemctl enable nvidia-fabricmanager && sudo systemctl start nvidia-
   fabricmanager
   ```

9. Stellen Sie sicher, dass die CUDA-Pfade bei jedem Start der Instance festgelegt werden.

   - Fügen Sie für Bash-Shells die folgenden Anweisungen zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Fügen Sie für tcsh-Shells die folgenden Anweisungen zu /home/*username*/.cshrc hinzu.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

10. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass die Nvidia GPU-Treiber funktionieren.

```
$ nvidia-smi -q | head
```

Der Befehl sollte Informationen zu Nvidia-GPUs, Nvidia GPU-Treibern und zum Nvidia CUDA-Toolkit zurückgeben.

CentOS 7

Installieren der Nvidia GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN

1. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus.

   ```
   $ sudo yum upgrade -y && sudo reboot
   ```

   Stellen Sie nach dem Neustart der Instance erneut eine Verbindung dazu her.

2. Installieren Sie die Dienstprogramme, die zum Installieren der Nvidia GPU-Treiber und des Nvidia CUDA-Toolkits benötigt werden.

   ```
   $ sudo yum groupinstall 'Development Tools' -y \
   && sudo yum install -y tar bzip2 make automake pciutils elfutils-libelf-devel
    libglvnd-devel iptables firewalld vim bind-utils
   ```

3. Um den Nvidia GPU-Treiber verwenden zu können, müssen Sie zunächst die `nouveau`-Open-Source-Treiber deaktivieren.

   a. Installieren Sie die erforderlichen Dienstprogramme und das Kernel-Header-Paket für Ihre derzeit ausgeführte Kernel-Version.

      ```
      $ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -
      r)
      ```

   b. Fügen Sie `nouveau` der Verweigerungsliste `/etc/modprobe.d/blacklist.conf` hinzu.

      ```
      $ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
      blacklist vga16fb
      blacklist nouveau
      blacklist rivafb
      ```

```
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Öffnen Sie `/etc/default/grub` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Erstellen Sie die neue Grub-Konfiguration.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
5. Installieren Sie die Nvidia-GPU-Treiber, das NVIDIA CUDA-Toolkit und cuDNN.

a. Installieren Sie das EPEL-Respository für DKMS und aktivieren Sie alle optionalen Repositorys für Ihre Linux-Distribution.

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-
latest-7.noarch.rpm
```

b. Installieren Sie den öffentlichen GPG-Schlüssel des CUDA-Repositorys.

```
$ distribution='rhel7'
```

c. Richten Sie das CUDA Netzwerk-Repository ein und aktualisieren Sie den Repository-Cache.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/
compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

d. Installieren Sie die NVIDIA- und CUDA-Treiber und cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

6. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.

7. (Nur `p4d.24xlarge` und `p5.48xlarge`) Starten Sie den NVIDIA Fabric Manager Service und stellen Sie sicher, dass er beim Start der Instance automatisch gestartet wird. Nvidia Fabric Manager ist für das NV Switch Management erforderlich.

```
$ sudo systemctl start nvidia-fabricmanager \
&& sudo systemctl enable nvidia-fabricmanager
```

8. Stellen Sie sicher, dass die CUDA-Pfade bei jedem Start der Instance festgelegt werden.

   - Fügen Sie für Bash-Shells die folgenden Anweisungen zu `/home/`*`username`*`/.bashrc` und `/home/`*`username`*`/.bash_profile` hinzu.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

   - Fügen Sie für tcsh-Shells die folgenden Anweisungen zu `/home/`*`username`*`/.cshrc` hinzu.

```
setenv PATH=/usr/local/cuda/bin:$PATH
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass die Nvidia GPU-Treiber funktionieren.

```
$ nvidia-smi -q | head
```

   Der Befehl sollte Informationen zu Nvidia-GPUs, Nvidia GPU-Treibern und zum Nvidia CUDA-Toolkit zurückgeben.

RHEL 7/8/9 and Rocky Linux 8/9

Installieren der Nvidia GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN

1. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus.

```
$ sudo yum upgrade -y && sudo reboot
```

Stellen Sie nach dem Neustart der Instance erneut eine Verbindung dazu her.

2. Installieren Sie die Dienstprogramme, die zum Installieren der Nvidia GPU-Treiber und des Nvidia CUDA-Toolkits benötigt werden.

```
$ sudo yum groupinstall 'Development Tools' -y
```

3. Um den Nvidia GPU-Treiber verwenden zu können, müssen Sie zunächst die `nouveau`-Open-Source-Treiber deaktivieren.

   a. Installieren Sie die erforderlichen Dienstprogramme und das Kernel-Header-Paket für Ihre derzeit ausgeführte Kernel-Version.

```
$ sudo yum install -y wget kernel-devel-$(uname -r) kernel-headers-$(uname -r)
```

   b. Fügen Sie `nouveau` der Verweigerungsliste `/etc/modprobe.d/blacklist.conf` hinzu.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

   c. Öffnen Sie `/etc/default/grub` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

   d. Erstellen Sie die neue Grub-Konfiguration.

```
$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

4. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
5. Installieren Sie die Nvidia-GPU-Treiber, das NVIDIA CUDA-Toolkit und cuDNN.

   a. Installieren Sie das EPEL-Respository für DKMS und aktivieren Sie alle optionalen Repositorys für Ihre Linux-Distribution.

- RHEL 7

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

- RHEL 8 und Rocky Linux 8/9

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

- RHEL 9

```
$ sudo yum install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

b. Installieren Sie den öffentlichen GPG-Schlüssel des CUDA-Repositorys.

```
$ distribution=$(. /etc/os-release;echo $ID`rpm -E "%{?rhel}%{?fedora}"`)
```

c. Richten Sie das CUDA Netzwerk-Repository ein und aktualisieren Sie den Repository-Cache.

```
$ ARCH=$( /bin/arch ) \
&& sudo yum-config-manager --add-repo http://developer.download.nvidia.com/compute/cuda/repos/$distribution/${ARCH}/cuda-$distribution.repo \
&& sudo yum clean expire-cache
```

d. Installieren Sie die NVIDIA- und CUDA-Treiber und cuDNN.

```
$ sudo yum clean all \
&& sudo yum -y install cuda-drivers-fabricmanager cuda libcudnn8-devel
```

6. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
7. (Nur `p4d.24xlarge` und `p5.48xlarge`) Starten Sie den NVIDIA Fabric Manager Service und stellen Sie sicher, dass er beim Start der Instance automatisch gestartet wird. Nvidia Fabric Manager ist für das NV Switch Management erforderlich.

```
$ sudo systemctl start nvidia-fabricmanager \
&& sudo systemctl enable nvidia-fabricmanager
```

8. Stellen Sie sicher, dass die CUDA-Pfade bei jedem Start der Instance festgelegt werden.

   - Fügen Sie für Bash-Shells die folgenden Anweisungen zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

     ```
     export PATH=/usr/local/cuda/bin:$PATH
     export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

   - Fügen Sie für tcsh-Shells die folgenden Anweisungen zu /home/*username*/.cshrc hinzu.

     ```
     setenv PATH=/usr/local/cuda/bin:$PATH
     setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
     lib64:$LD_LIBRARY_PATH
     ```

9. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass die Nvidia GPU-Treiber funktionieren.

   ```
   $ nvidia-smi -q | head
   ```

   Der Befehl sollte Informationen zu Nvidia-GPUs, Nvidia GPU-Treibern und zum Nvidia CUDA-Toolkit zurückgeben.

Ubuntu 20.04/22.04

Installieren der Nvidia GPU-Treiber, des Nvidia-CUDA-Toolkits und cuDNN

1. Um sicherzustellen, dass alle Ihre Softwarepakete aktuell sind, führen Sie ein schnelles Softwareupdate auf Ihrer Instance aus.

   ```
   $ sudo apt-get update && sudo apt-get upgrade -y
   ```

2. Installieren Sie die Dienstprogramme, die zum Installieren der Nvidia GPU-Treiber und des Nvidia CUDA-Toolkits benötigt werden.

   ```
   $ sudo apt-get update && sudo apt-get install build-essential -y
   ```

3. Um den Nvidia GPU-Treiber verwenden zu können, müssen Sie zunächst die nouveau-Open-Source-Treiber deaktivieren.

a. Installieren Sie die erforderlichen Dienstprogramme und das Kernel-Header-Paket für Ihre derzeit ausgeführte Kernel-Version.

```
$ sudo apt-get install -y gcc make linux-headers-$(uname -r)
```

b. Fügen Sie nouveau der Verweigerungsliste `/etc/modprobe.d/blacklist.conf` hinzu.

```
$ cat << EOF | sudo tee --append /etc/modprobe.d/blacklist.conf
blacklist vga16fb
blacklist nouveau
blacklist rivafb
blacklist nvidiafb
blacklist rivatv
EOF
```

c. Öffnen Sie `/etc/default/grub` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
GRUB_CMDLINE_LINUX="rdblacklist=nouveau"
```

d. Erstellen Sie die neue Grub-Konfiguration.

```
$ sudo update-grub
```

4. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
5. Fügen Sie das CUDA-Repository hinzu und installieren Sie die Nvidia-GPU-Treiber, das NVIDIA-CUDA-Toolkit und cuDNN.

   • `p3dn.24xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
```

```
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-dkms-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

- `p4d.24xlarge` und `p5.48xlarge`

```
$ sudo apt-key adv --fetch-keys http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/7fa2af80.pub \
&& wget -O /tmp/deeplearning.deb http://developer.download.nvidia.com/compute/
machine-learning/repos/ubuntu2004/x86_64/nvidia-machine-learning-repo-
ubuntu2004_1.0.0-1_amd64.deb \
&& sudo dpkg -i /tmp/deeplearning.deb \
&& wget -O /tmp/cuda.pin https://developer.download.nvidia.com/compute/cuda/
repos/ubuntu2004/x86_64/cuda-ubuntu2004.pin \
&& sudo mv /tmp/cuda.pin /etc/apt/preferences.d/cuda-repository-pin-600 \
&& sudo apt-key adv --fetch-keys https://developer.download.nvidia.com/
compute/cuda/repos/ubuntu2004/x86_64/3bf863cc.pub \
&& sudo add-apt-repository 'deb http://developer.download.nvidia.com/compute/
cuda/repos/ubuntu2004/x86_64/ /' \
&& sudo apt update \
&& sudo apt install nvidia-kernel-open-535 \
&& sudo apt install -o Dpkg::Options::='--force-overwrite' cuda-drivers-535
 cuda-toolkit-12-3 libcudnn8 libcudnn8-dev -y
```

6. Starten Sie die Instance neu und stellen Sie die Verbindung zur Instance wieder her.
7. (Nur `p4d.24xlarge` und `p5.48xlarge`) Installieren Sie den NVIDIA Fabric Manager.

   a. Sie müssen die Version von Nvidia Fabric Manager installieren, die mit der Version des Nvidia-Kernelmoduls übereinstimmt, die Sie im vorherigen Schritt installiert haben.

      Führen Sie den folgenden Befehl aus, um die Version des Nvidia Kernelmoduls zu bestimmen.

      ```
      $ cat /proc/driver/nvidia/version | grep "Kernel Module"
      ```

      Es folgt eine Beispielausgabe.

```
NVRM version: NVIDIA UNIX x86_64 Kernel Module  450.42.01  Tue Jun 15
 21:26:37 UTC 2021
```

Im obigen Beispiel wurde die Hauptversion `450` des Kernel-Moduls installiert. Dies bedeutet, dass Sie die Nvidia Fabric Manager-Version `450` installieren müssen.

b. Installieren Sie den Nvidia Fabric Manager. Führen Sie den folgenden Befehl aus, und geben Sie die im vorherigen Schritt angegebene Hauptversion an.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-major_version_number
```

Zum Beispiel, wenn die Hauptversion `450` des Kernelmoduls installiert wurde, verwenden Sie den folgenden Befehl, um die passende Version von Nvidia Fabric Manager zu installieren.

```
$ sudo apt install -o Dpkg::Options::='--force-overwrite' nvidia-
fabricmanager-450
```

c. Starten Sie den Dienst und stellen Sie sicher, dass er beim Start der Instance automatisch gestartet wird. Nvidia Fabric Manager ist für das NV Switch Management erforderlich.

```
$ sudo systemctl start nvidia-fabricmanager && sudo systemctl enable nvidia-
fabricmanager
```

8. Stellen Sie sicher, dass die CUDA-Pfade bei jedem Start der Instance festgelegt werden.

- Fügen Sie für Bash-Shells die folgenden Anweisungen zu /home/*username*/.bashrc und /home/*username*/.bash_profile hinzu.

```
export PATH=/usr/local/cuda/bin:$PATH
export LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

- Fügen Sie für tcsh-Shells die folgenden Anweisungen zu /home/*username*/.cshrc hinzu.

```
setenv PATH=/usr/local/cuda/bin:$PATH
```

```
setenv LD_LIBRARY_PATH=/usr/local/cuda/lib64:/usr/local/cuda/extras/CUPTI/
lib64:$LD_LIBRARY_PATH
```

9. Führen Sie den folgenden Befehl aus, um zu bestätigen, dass die Nvidia GPU-Treiber funktionieren.

```
$ nvidia-smi -q | head
```

Der Befehl sollte Informationen zu Nvidia-GPUs, Nvidia GPU-Treibern und zum Nvidia CUDA-Toolkit zurückgeben.

Schritt 4: Installieren der GDRCopy

Installieren Sie GDRCopy, um die Leistung von Libfabric zu verbessern. Weitere Informationen zu GDRCopy finden Sie im GDRCopy-Repository.

Amazon Linux 2, CentOS 7, RHEL 7/8/9, and Rocky Linux 8/9

So installieren Sie GDRCopy

1. Installieren Sie die erforderlichen Abhängigkeiten.

```
$ sudo yum -y install dkms rpm-build make check check-devel subunit subunit-
devel
```

2. Laden Sie das GDRCopy-Paket herunter und extrahieren Sie es.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz ; cd gdrcopy-2.4/packages
```

3. Erstellen Sie das GDRCopy-RPM-Paket.

```
$ CUDA=/usr/local/cuda ./build-rpm-packages.sh
```

4. Installieren Sie das GDRCopy-RPM-Paket.

```
$ sudo rpm -Uvh gdrcopy-kmod-2.4-1dkms.noarch*.rpm \
&& sudo rpm -Uvh gdrcopy-2.4-1.x86_64*.rpm \
&& sudo rpm -Uvh gdrcopy-devel-2.4-1.noarch*.rpm
```

Ubuntu 20.04/22.04

So installieren Sie GDRCopy

1. Installieren Sie die erforderlichen Abhängigkeiten.

```
$ sudo apt -y install build-essential devscripts debhelper check libsubunit-dev
 fakeroot pkg-config dkms
```

2. Laden Sie das GDRCopy-Paket herunter und extrahieren Sie es.

```
$ wget https://github.com/NVIDIA/gdrcopy/archive/refs/tags/v2.4.tar.gz \
&& tar xf v2.4.tar.gz \
&& cd gdrcopy-2.4/packages
```

3. Erstellen Sie das GDRCopy-RPM-Paket.

```
$ CUDA=/usr/local/cuda ./build-deb-packages.sh
```

4. Installieren Sie das GDRCopy-RPM-Paket.

```
$ sudo dpkg -i gdrdrv-dkms_2.4-1_amd64.*.deb \
&& sudo dpkg -i libgdrapi_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy-tests_2.4-1_amd64.*.deb \
&& sudo dpkg -i gdrcopy_2.4-1_amd64.*.deb
```

Schritt 5: Installieren der EFA-Software

Installieren Sie den EFA-fähigen Kernel, die EFA-Treiber, Libfabric und den Open MPI-Stack, der zur Unterstützung von EFA auf Ihrer temporären Instance erforderlich ist.

So installieren Sie die EFA-Software

1. Stellen Sie eine Verbindung zu der Instance her, die Sie gestartet haben. Weitere Informationen finden Sie unter Herstellen einer Verbindung zur Linux-Instance.
2. Laden Sie die EFA-Software-Installationsdateien herunter. Die Software-Installationsdateien sind in einer komprimierten Tarball-Datei (`.tar.gz`) verpackt. Laden Sie die neueste stabile Version mit dem folgenden Befehl herunter.

```
$ C:\> curl -O https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz
```

Sie erhalten die neueste Version auch, indem Sie anstelle der Versionsnummer im vorangegangenen Befehl `latest` eingeben.

3. (Optional) Überprüfen Sie die Authentizität und Integrität der EFA-Tarball-Datei (`.tar.gz`).

   Diese Vorgehensweise wird empfohlen, um die Identität des Software-Publishers zu überprüfen und sicherzustellen, dass die Datei seit ihrer Veröffentlichung nicht verändert oder beschädigt wurde. Wenn Sie die Tarball-Datei nicht überprüfen möchten, überspringen Sie diesen Schritt.

   > **Note**
   >
   > Wenn Sie die Tarball-Datei lieber mit einer MD5- oder SHA256-Prüfsumme überprüfen möchten, finden Sie Informationen unter Überprüfen des EFA-Installationsprogramms mithilfe einer Prüfsumme.

   a. Laden Sie den öffentlichen GPG-Schlüssel herunter und importieren Sie ihn in Ihren Schlüsselbund.

   ```
   $ wget https://efa-installer.amazonaws.com/aws-efa-installer.key && gpg --
   import aws-efa-installer.key
   ```

   Der Befehl sollte einen Schlüsselwert zurückgeben. Notieren Sie sich den Schlüsselwert. Sie benötigen ihn im nächsten Schritt.

   b. Überprüfen Sie den Fingerabdruck des GPG-Schlüssels. Führen Sie den folgenden Befehl aus und geben den Schlüsselwert aus dem vorherigen Schritt an.

   ```
   $ gpg --fingerprint key_value
   ```

   Der Befehl sollte einen Fingerabdruck zurückgeben, der mit `4E90 91BC BB97 A96B 26B1 5E59 A054 80B1 DD2D 3CCC` identisch ist. Wenn der Fingerabdruck nicht übereinstimmt, führen Sie das EFA-Installationsskript nicht aus und wenden Sie sich an den AWS Support.

   c. Laden Sie die Signaturdatei herunter und überprüfen Sie die Signatur der EFA-Tarball-Datei.

   ```
   $ wget https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz.sig
    && gpg --verify ./aws-efa-installer-1.32.0.tar.gz.sig
   ```

Das folgende Beispiel zeigt eine Ausgabe.

```
gpg: Signature made Wed 29 Jul 2020 12:50:13 AM UTC using RSA key ID DD2D3CCC
gpg: Good signature from "Amazon EC2 EFA <ec2-efa-maintainers@amazon.com>"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:          There is no indication that the signature belongs to the owner.
Primary key fingerprint: 4E90 91BC BB97 A96B 26B1  5E59 A054 80B1 DD2D 3CCC
```

Wenn das Ergebnis `Good signature` enthält und der Fingerabdruck mit dem Fingerabdruck übereinstimmt, der im vorherigen Schritt zurückgegeben wurde, fahren Sie mit dem nächsten Schritt fort. Wenn nicht, führen Sie das EFA-Installationsskript nicht aus und wenden Sie sich an den AWS Support.

4. Extrahieren Sie die Daten aus der komprimierten `.tar.gz`-Datei und wechseln Sie in das extrahierte Verzeichnis.

```
$ C:\> tar -xf aws-efa-installer-1.32.0.tar.gz && cd aws-efa-installer
```

5. Führen Sie das EFA-Software-Installationsskript aus.

> **Note**
>
> Ab EFA 1.30.0 sind sowohl Open MPI 4 als auch Open MPI 5 standardmäßig installiert. Sofern Sie Open MPI 5 nicht benötigen, empfehlen wir, nur Open MPI 4 zu installieren. Mit dem folgenden Befehl wird nur Open MPI 4 installiert. Wenn Sie Open MPI 4 und Open MPI 5 installieren möchten, entfernen Sie `--mpi=openmpi4`.

```
$ C:\> sudo ./efa_installer.sh -y --mpi=openmpi4
```

Libfabric ist im Verzeichnis `/opt/amazon/efa` installiert, während Open MPI im Verzeichnis `/opt/amazon/openmpi` installiert ist.

6. Wenn das EFA-Installationsprogramm Sie auffordert, die Instance neu zu starten, tun Sie dies und stellen Sie dann erneut eine Verbindung mit der Instance her. Melden Sie sich andernfalls von der Instance ab und wieder an, um die Installation abzuschließen.
7. Überprüfen Sie, ob die EFA-Softwarekomponenten erfolgreich installiert wurden.

```
$ C:\> fi_info -p efa -t FI_EP_RDM
```

Der Befehl muss Informationen zu den Libfabric-EFA-Schnittstellen zurückgeben. Das folgende Beispiel zeigt die Befehlsausgabe.

- `p3dn.24xlarge` mit einer einzigen Netzwerkschnittstelle

```
provider: efa
fabric: EFA-fe80::94:3dff:fe89:1b70
domain: efa_0-rdm
version: 2.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

- `p4d.24xlarge` und `p5.48xlarge` mit mehreren Netzwerkschnittstellen

```
provider: efa
fabric: EFA-fe80::c6e:8fff:fef6:e7ff
domain: efa_0-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c34:3eff:feb2:3c35
domain: efa_1-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::c0f:7bff:fe68:a775
domain: efa_2-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
provider: efa
fabric: EFA-fe80::ca7:b0ff:fea6:5e99
domain: efa_3-rdm
version: 111.0
type: FI_EP_RDM
protocol: FI_PROTO_EFA
```

Schritt 6: Installieren der NCCL

Installieren Sie die NCCL Weitere Informationen zur NCCL finden Sie im NCCL-Repository.

So installieren Sie die NCCL

1. Navigieren Sie zum Verzeichnis `/opt`.

```
$ cd /opt
```

2. Klonen Sie das offizielle NCCL-Repository in die Instance und navigieren Sie zum lokal geklonten Repository.

```
$ sudo git clone https://github.com/NVIDIA/nccl.git && cd nccl
```

3. Erstellen und installieren Sie die NCCL und geben Sie das CUDA-Installationsverzeichnis an.

```
$ sudo make -j src.build CUDA_HOME=/usr/local/cuda
```

Schritt 7: Installieren Sie das Plugin aws-ofi-nccl

Das aws-ofi-nccl Plugin ordnet die verbindungsorientierten Transport-APIs von NCCL der verbindungslosen, zuverlässigen Schnittstelle von Libfabric zu. Sie können dann libfabric als Netzwerkanbieter verwenden, während NCCL-basierte Anwendungen ausgeführt werden. Weitere Informationen über das Plugin finden Sie im Repository. aws-ofi-nccl aws-ofi-nccl

Um das aws-ofi-nccl Plugin zu installieren

1. Navigieren Sie zum Stammverzeichnis.

```
$ cd $HOME
```

2. (Nur Amazon Linux 2 und Ubuntu) Installieren Sie die erforderlichen Dienstprogramme.

   - Amazon Linux 2

```
$ sudo yum install hwloc-devel
```

   - Ubuntu 20.04

```
$ sudo apt-get install libhwloc-dev
```

3. Laden Sie die aws-ofi-nccl Plugin-Dateien herunter. Die Dateien sind in einer komprimierten Tarball-Datei (`.tar.gz`) gepackt.

```
$ wget https://github.com/aws/aws-ofi-nccl/releases/download/v1.9.1-aws/aws-ofi-nccl-1.9.1-aws.tar.gz
```

4. Extrahieren Sie die Daten aus der komprimierten Datei mit der Endung „.tar.gz“ und wechseln Sie in das extrahierte Verzeichnis.

```
$ tar -xf aws-ofi-nccl-1.9.1-aws.tar.gz && cd aws-ofi-nccl-1.9.1-aws
```

5. Führen Sie zum Generieren der make-Dateien das Skript `configure` aus und geben Sie die Installationsverzeichnisse für MPI, libfabric, NCCL und CUDA an.

```
$ ./configure --prefix=/opt/aws-ofi-nccl --with-mpi=/opt/amazon/openmpi \
--with-libfabric=/opt/amazon/efa \
--with-cuda=/usr/local/cuda \
--enable-platform-aws
```

6. Fügen Sie der PATH-Variablen das Open MPI-Verzeichnis hinzu.

```
$ export PATH=/opt/amazon/openmpi/bin/:$PATH
```

7. Installiere das aws-ofi-nccl Plugin.

```
$ make && sudo make install
```

Schritt 8: Installieren der NCCL-Tests

Installieren Sie die NCCL-Tests. Mit den NCCL-Tests können Sie bestätigen, dass die NCCL richtig installiert wurde und wie erwartet funktioniert. Weitere Informationen zu den NCCL-Tests finden Sie unter nccl-tests repository.

So installieren Sie die NCCL-Tests

1. Navigieren Sie zum Stammverzeichnis.

```
$ cd $HOME
```

2. Klonen Sie das offizielle nccl-tests-Repository in die Instance und navigieren Sie zum lokal geklonten Repository.

```
$ git clone https://github.com/NVIDIA/nccl-tests.git && cd nccl-tests
```

3. Fügen Sie das libfabric-Verzeichnis in die Variable `LD_LIBRARY_PATH` ein.

   - Amazon Linux, Amazon Linux 2, RHEL, Rocky Linux 8/9 und CentOS

   ```
   $ export LD_LIBRARY_PATH=/opt/amazon/efa/lib64:$LD_LIBRARY_PATH
   ```

   - Ubuntu

   ```
   $ export LD_LIBRARY_PATH=/opt/amazon/efa/lib:$LD_LIBRARY_PATH
   ```

4. Installieren Sie die NCCL-Tests und geben Sie die Installationsverzeichnisse für MPI, NCCL und CUDA an.

```
$ make MPI=1 MPI_HOME=/opt/amazon/openmpi NCCL_HOME=/opt/nccl/build CUDA_HOME=/usr/
local/cuda
```

Schritt 9: Testen der EFA- und NCCL-Konfiguration

Führen Sie einen Test durch, um sicherzustellen, dass Ihre temporäre Instance richtig für EFA und NCCL konfiguriert ist.

So testen Sie EFA- und NCCL-Konfiguration

1. Erstellen Sie eine Host-Datei, die die Hosts angibt, auf denen die Tests ausgeführt werden sollen. Der folgende Befehl erstellt eine Host-Datei namens `my-hosts`, die eine Referenz auf die Instance selbst enthält.

   IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
meta-data/local-ipv4 >> my-hosts
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
hosts
```

2. Führen Sie den Test aus und geben Sie die Host-Datei (`--hostfile`) und die Anzahl zu verwendender GPUs (`-n`) an. Der folgende Befehl führt den Test `all_reduce_perf` auf 8 GPUs in der Instance selbst aus und gibt die folgenden Umgebungsvariablen an.

   - `FI_EFA_USE_DEVICE_RDMA=1` – (nur `p4d.24xlarge`) verwendet die RDMA-Funktion des Geräts für einseitige und zweiseitige Übertragungen.
   - `NCCL_DEBUG=INFO`: ermöglicht eine detaillierte Debugging-Ausgabe. Sie können auch `VERSION` angeben, damit nur die NCCL-Version am Anfang des Tests ausgegeben wird oder `WARN`, damit nur Fehlermeldungen ausgegeben werden.

   Weitere Informationen zu den Argumenten für NCCL-Tests finden Sie unter NCCL Tests README im offiziellen nccl-tests-Repository.

   - `p3dn.24xlarge`

   ```
   $ /opt/amazon/openmpi/bin/mpirun \
       -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
   lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
       -x NCCL_DEBUG=INFO \
       --hostfile my-hosts -n 8 -N 8 \
       --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
   to none \
       $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
   ```

   - `p4d.24xlarge` und `p5.48xlarge`

   ```
   $ /opt/amazon/openmpi/bin/mpirun \
       -x FI_EFA_USE_DEVICE_RDMA=1 \
       -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
   lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
       -x NCCL_DEBUG=INFO \
       --hostfile my-hosts -n 8 -N 8 \
   ```

```
    --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
to none \
    $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Sie können bestätigen, dass EFA als zugrunde liegender Anbieter für NCCL aktiv ist, wenn das NCCL_DEBUG-Protokoll gedruckt wird.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Die folgenden zusätzlichen Informationen werden angezeigt, wenn Sie eine p4d.24xlarge-Instance verwenden.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Schritt 10: Installieren der Machine-Learning-Anwendungen

Installieren Sie die Machine-Learning-Anwendungen auf der temporären Instance. Der Installationsvorgang variiert je nach Machine-Learning-Anwendung. Weitere Informationen zur Installation von Software auf Ihrer Linux-Instance finden Sie unter Software auf Ihrer Amazon Linux 2-Instance verwalten.

> **Note**
>
> In der Dokumentation Ihrer Machine-Learning-Anwendung finden Sie Installationsanleitungen.

Schritt 11: Erstellen eines EFA- und NCCL-konformen AMI

Nachdem Sie die erforderlichen Softwarekomponenten installiert haben, erstellen Sie ein AMI, das Sie erneut verwenden können, um Ihre EFA-fähigen Instances zu starten.

So erstellen Sie ein AMI aus Ihrer temporären Instance:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie die temporäre Instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Image und Create Image (Image erstellen) aus.
4. Gehen Sie bei Create Image (Image erstellen) wie folgt vor:
   a. Geben Sie unter Image name (Image-Name) einen beschreibenden Namen für das AMI ein.
   b. (Optional:) Geben Sie bei Image description (Image-Beschreibung) eine kurze Beschreibung des Zwecks des AMI ein.
   c. Wählen Sie Create Image (Image erstellen) aus.
5. Wählen Sie im Navigationsbereich die Option AMIs.
6. Suchen Sie das AMI, das Sie erstellt haben, in der Liste. Warten Sie, bis der Status von `pending` zu `available` wechselt, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 12: Beenden der temporären Instance

An diesem Punkt benötigen Sie die temporäre Instance, die Sie gestartet haben, nicht mehr. Sie können die Instance beenden, damit keine weiteren Kosten dafür anfallen.

So beenden Sie die temporäre Instance:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Instance state (Instance-Zustand) und Terminate instance (Instance beenden) aus.
4. Wählen Sie Terminate (Kündigen) aus, wenn Sie zur Bestätigung aufgefordert werden.

Schritt 13: Starten von EFA- und NCCL-konformen Instances in einer Cluster-Placement-Gruppe

Starten Sie die EFA- und NCCL-fähigen Instances in einer Cluster-Placement-Gruppe, indem Sie das EFA-fähige AMI und die EFA-fähige Sicherheitsgruppe verwenden, die Sie zuvor erstellt haben.

> **Note**
>
> - Es ist keine absolute Voraussetzung, Ihre EFA-aktivierten Instances in einer Cluster-Placement-Gruppe zu starten. Wir empfehlen allerdings, Ihre EFA-Instances in einer

Cluster-Placement-Gruppe zu starten, da die Instances dadurch in einer Gruppe mit niedriger Latenz in einer einzelnen Availability Zone gestartet werden.

- Um die Verfügbarkeit von Kapazitäten sicherzustellen, wenn Sie die Instances Ihres Clusters skalieren, können Sie eine Kapazitätsreservierung für Ihre Cluster-Placement-Gruppe erstellen. Weitere Informationen finden Sie unter Kapazitätsreservierungen in Cluster-Placement-Gruppen.

New console

So starten Sie eine temporäre Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=EFA-instance`) zugewiesen.
4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) My AMIs (Meine AMIs) und dann das AMI aus, das Sie im vorherigen Schritt erstellt haben.
5. Wählen Sie im Bereich Instance type (Instance-Typ) entweder `p3dn.24xlarge` oder `p4d.24xlarge` aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:

   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.

   b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.

   c. Erweitern Sie den Bereich Advanced network configuration (Erweiterte Netzwerkkonfiguration) und wählen Sie bei Elastic Fabric Adapter Enable (Aktivieren) aus.

8. (Optional) Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.
9. Wählen Sie im Bereich Advanced details (Erweiterte Details) bei Placement group name (Placement-Gruppen-Name) die Cluster-Placement-Gruppe aus, in der die Instance gestartet werden soll. Wenn Sie eine neue Cluster-Placement-Gruppe erstellen müssen, wählen Sie Create new placement group (Neue Placement-Gruppe erstellen).
10. Geben Sie im Bereich Summary (Zusammenfassung) rechts bei Number of instances (Anzahl der Instances) die Anzahl EFA-fähiger Instances ein, die Sie starten möchten, und wählen Sie dann Launch instance (Instance starten).

Old console

So starten Sie EFA- und NCCL-fähige Instances in einer Cluster-Placement-Gruppe:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance aus.
3. Wählen Sie auf der Seite Choose an AMI (AMI auswählen) die Option My AMIs (Meine AMIs), suchen Sie das AMI, das Sie zuvor erstellt haben, und wählen Sie anschließend Select (Auswählen) aus.
4. Wählen Sie auf der Seite Choose an Instance Type (Instance-Typ auswählen) die Option p3dn.24xlarge und dann Next: Configure Instance Details (Weiter: Instance-Details konfigurieren) aus.
5. Führen Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) die folgenden Schritte aus:

    a. Geben Sie bei Number of instances (Anzahl der Instances) die Anzahl der EFA- und NCCL-fähigen Instances ein, die gestartet werden sollen.

    b. Wählen Sie für Network (Netzwerk) und Subnet (Subnetz) die VPC und das Subnetz an, in das Sie die Instances starten möchten.

    c. Wählen Sie für Placement group (Placement-Gruppe) die Option Add instance to placement group (Instance der Placement-Gruppe hinzufügen) aus.

    d. Wählen Sie bei Placement group name (Name der Placement-Gruppe) die Option Add to a new placement group (Zu neuer Placement-Gruppe hinzufügen) aus und geben Sie dann einen beschreibenden Namen für die Placement-Gruppe ein. Wählen Sie dann bei Placement group strategy (Strategie für Placement-Gruppe) cluster aus.

    e. Wählen Sie für EFA Enable (Aktivieren) aus.

f. Wählen Sie im Abschnitt Network Interfaces (Netzwerkschnittstellen für das Gerät eth0 die Option New network interface (Neue Netzwerkschnittstelle) aus. Sie können zudem optional eine primäre IPv4-Adresse und eine oder mehrere sekundäre IPv4-Adressen eingeben. Wenn Sie die Instance in einem Subnetz starten, dem ein IPv6-CIDR-Block zugeordnet ist, können Sie optional eine primäre IPv6-Adresse und eine oder mehrere sekundäre IPv6-Adressen angeben.

g. Wählen Sie Next: Add Storage aus.

6. Geben Sie auf der Seite Add Storage (Speicher hinzufügen) die Volumes an, die an die Instances angefügt werden sollen, ergänzend zu den Volumes, die vom AMI angegeben werden (z. B. der Root-Gerät-Volume). Wählen Sie dann Next: Add Tags (Weiter: Tags (Markierungen) hinzufügen) aus.
7. Geben Sie auf der Seite Add Tags (Tags (Markierungen) hinzufügen) Tags (Markierungen) für die Instances an, z. B. einen benutzerfreundlichen Namen, und wählen Sie anschließend Next: Configure Security Group (Weiter: Sicherheitsgruppe konfigurieren).
8. Wählen Sie auf der Seite Configure Security Group (Sicherheitsgruppe konfigurieren) bei Assign a security group (Sicherheitsgruppe zuweisen) die Option Select an existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie zuvor erstellt haben.
9. Klicken Sie auf Review and Launch.
10. Überprüfen Sie auf der Seite Review Instance Launch (Instance-Start überprüfen) Ihre Einstellungen und wählen Sie anschließend Launch (Starten) aus, um ein Schlüsselpaar auszuwählen und Ihre Instance zu starten.

Schritt 14: Aktivieren von passwortlosem SSH

Damit Ihre Anwendungen auf allen Instances in Ihrem Cluster ausgeführt werden können, müssen Sie passwortlosen SSH-Zugriff vom Führungsknoten auf die Mitgliedsknoten aktivieren. Der Führungsknoten ist die Instance, von der aus Sie die Anwendungen ausführen. Die verbleibenden Instances im Cluster sind die Mitgliedsknoten.

So aktivieren Sie passwortloses SSH zwischen den Instances im Cluster:

1. Wählen Sie eine Instance im Cluster als Führungsknoten aus und stellen Sie eine Verbindung zu ihr her.

2. Deaktivieren Sie `strictHostKeyChecking` und aktivieren Sie `ForwardAgent` für den Führungsknoten. Öffnen Sie `~/.ssh/config` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
Host *
    ForwardAgent yes
Host *
    StrictHostKeyChecking no
```

3. Generieren Sie ein RSA-Schlüsselpaar.

```
$ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
```

   Das Schlüsselpaar wird im `$HOME/.ssh/`-Verzeichnis erstellt.

4. Ändern Sie die Berechtigungen des privaten Schlüssels auf dem Führungsknoten.

```
$ chmod 600 ~/.ssh/id_rsa
chmod 600 ~/.ssh/config
```

5. Öffnen Sie `~/.ssh/id_rsa.pub` mit Ihrem bevorzugten Texteditor und kopieren Sie den Schlüssel.

6. Gehen Sie für jeden Mitgliedsknoten im Cluster wie folgt vor:

   a. Stellen Sie eine Verbindung mit der Instance her.

   b. Öffnen Sie `~/.ssh/authorized_keys` mit Ihrem bevorzugten Texteditor und fügen Sie den öffentlichen Schlüssel hinzu, den Sie zuvor kopiert haben.

7. Um zu testen, ob das passwortlose SSH wie erwartet funktioniert, stellen Sie eine Verbindung zum Leaderknoten her und führen Sie den folgenden Befehl aus.

```
$ ssh member_node_private_ip
```

   Sie sollten eine Verbindung zum Mitgliedsknoten herstellen können, ohne zur Eingabe eines Schlüssels oder Passworts aufgefordert zu werden.

Verwenden Sie ein AWS Deep Learning-AMI

Die folgenden Schritte helfen Ihnen beim Einstieg in eines der folgenden AWS Deep Learning-AMIs:

- Deep-Learning-AMI (Amazon Linux 2)
- Deep-Learning-AMI (Ubuntu 20.04)

Weitere Informationen finden Sie im AWS Deep Learning AMI -Benutzerhandbuch.

> **Note**
>
> Nur die `p3dn.24xlarge`- und `p4d.24xlarge`-Instance-Typen werden unterstützt.

Inhalt

Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe

Ein EFA erfordert eine Sicherheitsgruppe, die allen ein- und ausgehenden Datenverkehr von und zur Sicherheitsgruppe zulässt. Mit dem folgenden Verfahren wird eine Sicherheitsgruppe erstellt, die den gesamten ein- und ausgehenden Datenverkehr der Gruppe sowie eingehenden SSH-Datenverkehr von jeder IPv4-Adresse zwecks SSH-Konnektivität zulässt.

> **Important**
>
> Diese Sicherheitsgruppe dient nur zu Testzwecken. Für Produktionsumgebungen sollten Sie eine Regel für eingehenden SSH-Datenverkehr erstellen, die Datenverkehr nur von der IP-Adresse zulässt, von der aus Sie eine Verbindung herstellen, z. B. die IP-Adresse Ihres Computers oder einen Bereich von IP-Adressen im lokalen Netzwerk.

Weitere Szenarien finden Sie unter Sicherheitsgruppenregeln für verschiedene Anwendungsfälle.

So erstellen Sie eine EFA-fähige Sicherheitsgruppe:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) und anschließend Create Security Group (Sicherheitsgruppe erstellen) aus.
3. Führen Sie im Fenster Create Security Group Folgendes aus:
   a. Geben Sie für Security group name (Name der Sicherheitsgruppe) einen beschreibenden Namen für die Sicherheitsgruppe ein, wie etwa `EFA-enabled security group`.
   b. (Optional:) Geben Sie unter Description (Beschreibung) eine kurze Beschreibung der Sicherheitsgruppe ein.
   c. Wählen Sie bei VPC die VPC aus, in der Sie Ihre EFA-fähigen Instances starten möchten.
   d. Wählen Sie Sicherheitsgruppe erstellen aus.
4. Wählen Sie die von Ihnen erstellte Sicherheitsgruppe aus und kopieren Sie dann auf der Registerkarte Details die Security group ID (Sicherheitsgruppen-ID).
5. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit inbound rules (Eingangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:
   a. Wählen Sie Regel hinzufügen aus.
   b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.
   c. Wählen Sie bei Source type (Quellentyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.
   d. Wählen Sie Regel hinzufügen aus.
   e. Wählen Sie unter Typ die Option SSH aus.
   f. Wählen Sie unter Source (Quelle) die Option Anywhere-IPv4 (Alle IPv4) aus.
   g. Wählen Sie Save rules (Regeln speichern) aus.
6. Bei noch ausgewählter Sicherheitsgruppe wählen Sie Actions (Aktionen), Edit outbound rules (Ausgangsregeln bearbeiten) aus und gehen dann folgendermaßen vor:
   a. Wählen Sie Regel hinzufügen aus.
   b. Wählen Sie für Type (Typ) die Option All traffic (Gesamter Datenverkehr) aus.
   c. Wählen Sie bei Destination type (Zieltyp) Custom (Benutzerdefiniert) aus und fügen Sie die Sicherheitsgruppen-ID, die Sie kopiert hatten, ins Feld ein.
   d. Wählen Sie Save rules (Regeln speichern) aus.

Schritt 2: Starten einer temporären Instance

Starten Sie eine temporäre Instance, die Sie verwenden können, um die EFA-Softwarekomponenten zu installieren und zu konfigurieren. Sie können mit dieser Instance ein EFA-aktiviertes AMI erstellen, von dem Sie Ihre EFA-aktivierten Instances starten können.

So starten Sie eine temporäre Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.
4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) eine unterstützte AWS Deep Learning AMI Version 25.0 oder neuer aus.
5. Wählen Sie im Bereich Instance type (Instance-Typ) entweder `p3dn.24xlarge` oder `p4d.24xlarge` aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:
   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.
   b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.
   c. Erweitern Sie den Bereich Advanced network configuration (Erweiterte Netzwerkkonfiguration) und wählen Sie bei Elastic Fabric Adapter Enable (Aktivieren) aus.
8. Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.

> **Note**
>
> Sie müssen zusätzliche 10 bis 20 GiB Speicher für das Nvidia CUDA Toolkit bereitstellen. Wenn Sie nicht genügend Speicherplatz bereitstellen, erhalten Sie einen

`insufficient disk space`-Fehler beim Versuch, die Nvidia-Treiber und das CUDA-Toolkit zu installieren.

9. Wählen Sie im Bereich Summary (Zusammenfassung) rechts Launch instance (Instance starten) aus.

Schritt 3: Testen der EFA- und NCCL-Konfiguration

Führen Sie einen Test durch, um sicherzustellen, dass Ihre temporäre Instance richtig für EFA und NCCL konfiguriert ist.

So testen Sie EFA- und NCCL-Konfiguration

1. Erstellen Sie eine Host-Datei, die die Hosts angibt, auf denen die Tests ausgeführt werden sollen. Der folgende Befehl erstellt eine Host-Datei namens `my-hosts`, die eine Referenz auf die Instance selbst enthält.

   IMDSv2

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/
   meta-data/local-ipv4 >> my-hosts
   ```

   IMDSv1

   ```
   [ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/local-ipv4 >> my-
   hosts
   ```

2. Führen Sie den Test aus und geben Sie die Host-Datei (`--hostfile`) und die Anzahl zu verwendender GPUs (`-n`) an. Der folgende Befehl führt den Test `all_reduce_perf` auf 8 GPUs in der Instance selbst aus und gibt die folgenden Umgebungsvariablen an.

   - `FI_EFA_USE_DEVICE_RDMA=1` – (nur `p4d.24xlarge`) verwendet die RDMA-Funktion des Geräts für einseitige und zweiseitige Übertragungen.
   - `NCCL_DEBUG=INFO`: ermöglicht eine detaillierte Debugging-Ausgabe. Sie können auch `VERSION` angeben, damit nur die NCCL-Version am Anfang des Tests ausgegeben wird oder `WARN`, damit nur Fehlermeldungen ausgegeben werden.

Weitere Informationen zu den Argumenten für NCCL-Tests finden Sie unter NCCL Tests README im offiziellen nccl-tests-Repository.

- `p3dn.24xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
    -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
    -x NCCL_DEBUG=INFO \
    --hostfile my-hosts -n 8 -N 8 \
    --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
to none \
    $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

- `p4d.24xlarge`

```
$ /opt/amazon/openmpi/bin/mpirun \
    -x FI_EFA_USE_DEVICE_RDMA=1 \
    -x LD_LIBRARY_PATH=/opt/nccl/build/lib:/usr/local/cuda/lib64:/opt/amazon/efa/
lib:/opt/amazon/openmpi/lib:/opt/aws-ofi-nccl/lib:$LD_LIBRARY_PATH \
    -x NCCL_DEBUG=INFO \
    --hostfile my-hosts -n 8 -N 8 \
    --mca pml ^cm --mca btl tcp,self --mca btl_tcp_if_exclude lo,docker0 --bind-
to none \
    $HOME/nccl-tests/build/all_reduce_perf -b 8 -e 1G -f 2 -g 1 -c 1 -n 100
```

3. Sie können bestätigen, dass EFA als zugrunde liegender Anbieter für NCCL aktiv ist, wenn das `NCCL_DEBUG`-Protokoll gedruckt wird.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Selected Provider is efa*
```

Die folgenden zusätzlichen Informationen werden angezeigt, wenn Sie eine `p4d.24xlarge`-Instance verwenden.

```
ip-192-168-2-54:14:14 [0] NCCL INFO NET/OFI Running on P4d platform, Setting
 NCCL_TOPO_FILE environment variable to /home/ec2-user/install/plugin/share/aws-
ofi-nccl/xml/p4d-24xl-topo.xml
```

Schritt 4: Installieren der Machine-Learning-Anwendungen

Installieren Sie die Machine-Learning-Anwendungen auf der temporären Instance. Der Installationsvorgang variiert je nach Machine-Learning-Anwendung. Weitere Informationen zur Installation von Software auf Ihrer Linux-Instance finden Sie unter Software auf Ihrer Amazon Linux 2-Instance verwalten.

> **Note**
>
> In der Dokumentation Ihrer Machine-Learning-Anwendung finden Sie Installationsanleitungen.

Schritt 5: Erstellen eines EFA- und NCCL-konformen AMI

Nachdem Sie die erforderlichen Softwarekomponenten installiert haben, erstellen Sie ein AMI, das Sie erneut verwenden können, um Ihre EFA-fähigen Instances zu starten.

So erstellen Sie ein AMI aus Ihrer temporären Instance:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre Instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Image und Create Image (Image erstellen) aus.
4. Gehen Sie bei Create Image (Image erstellen) wie folgt vor:
   a. Geben Sie unter Image name (Image-Name) einen beschreibenden Namen für das AMI ein.
   b. (Optional:) Geben Sie bei Image description (Image-Beschreibung) eine kurze Beschreibung des Zwecks des AMI ein.
   c. Wählen Sie Create Image (Image erstellen) aus.
5. Wählen Sie im Navigationsbereich die Option AMIs.
6. Suchen Sie das AMI, das Sie erstellt haben, in der Liste. Warten Sie, bis der Status von `pending` zu `available` wechselt, bevor Sie mit dem nächsten Schritt fortfahren.

Schritt 6: Beenden der temporären Instance

An diesem Punkt benötigen Sie die temporäre Instance, die Sie gestartet haben, nicht mehr. Sie können die Instance beenden, damit keine weiteren Kosten dafür anfallen.

So beenden Sie die temporäre Instance:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die temporäre instance aus, die Sie erstellt haben, und wählen Sie anschließend Actions (Aktionen), Instance state (Instance-Zustand) und Terminate instance (Instance beenden) aus.
4. Wählen Sie Terminate (Kündigen) aus, wenn Sie zur Bestätigung aufgefordert werden.

Schritt 7: Starten von EFA- und NCCL-konformen Instances in einer Cluster Placement-Gruppe

Starten Sie die EFA- und NCCL-fähigen Instances in einer Cluster-Placement-Gruppe, indem Sie das EFA-fähige AMI und die EFA-fähige Sicherheitsgruppe verwenden, die Sie zuvor erstellt haben.

> **Note**
>
> - Es ist keine absolute Voraussetzung, Ihre EFA-aktivierten Instances in einer Cluster-Placement-Gruppe zu starten. Wir empfehlen allerdings, Ihre EFA-Instances in einer Cluster-Placement-Gruppe zu starten, da die Instances dadurch in einer Gruppe mit niedriger Latenz in einer einzelnen Availability Zone gestartet werden.
> - Um die Verfügbarkeit von Kapazitäten sicherzustellen, wenn Sie die Instances Ihres Clusters skalieren, können Sie eine Kapazitätsreservierung für Ihre Cluster-Placement-Gruppe erstellen. Weitere Informationen finden Sie unter Kapazitätsreservierungen in Cluster-Placement-Gruppen.

New console

So starten Sie eine temporäre Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instances starten aus, um den Launch Instance Wizard zu öffnen.
3. (Optional) Geben Sie im Bereich Name and tags (Name und Tags) einen Namen für die Instance an, z. B. `EFA-instance`. Der Name wird der Instance als Ressourcen-Tag (`Name=`*`EFA-instance`*) zugewiesen.

4. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) My AMIs (Meine AMIs) und dann das AMI aus, das Sie im vorherigen Schritt erstellt haben.
5. Wählen Sie im Bereich Instance type (Instance-Typ) entweder `p3dn.24xlarge` oder `p4d.24xlarge` aus.
6. Wählen Sie im Bereich Key pair (Schlüsselpaar) das Schlüsselpaar aus, das für die Instance verwendet werden soll.
7. Wählen Sie im Bereich Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) aus und führen Sie dann Folgendes aus:
   a. Wählen Sie unter Subnetz das Subnetz aus, in dem die Instance gestartet werden soll. Wenn Sie kein Subnetz auswählen, können Sie die Instance nicht für EFA aktivieren.
   b. Wählen Sie bei Firewall (security groups) Firewall (Sicherheitsgruppen) Select existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie im vorherigen Schritt erstellt haben.
   c. Erweitern Sie den Bereich Advanced network configuration (Erweiterte Netzwerkkonfiguration) und wählen Sie bei Elastic Fabric Adapter Enable (Aktivieren) aus.
8. (Optional) Konfigurieren Sie im Bereich Storage (Speicher) die Volumes nach Bedarf.
9. Wählen Sie im Bereich Advanced details (Erweiterte Details) bei Placement group name (Placement-Gruppen-Name) die Cluster-Placement-Gruppe aus, in der die Instance gestartet werden soll. Wenn Sie eine neue Cluster-Placement-Gruppe erstellen müssen, wählen Sie Create new placement group (Neue Placement-Gruppe erstellen).
10. Geben Sie im Bereich Summary (Zusammenfassung) rechts bei Number of instances (Anzahl der Instances) die Anzahl EFA-fähiger Instances ein, die Sie starten möchten, und wählen Sie dann Launch instance (Instance starten).

Old console

So starten Sie EFA- und NCCL-fähige Instances in einer Cluster-Placement-Gruppe:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance aus.

3. Wählen Sie auf der Seite Choose an AMI (AMI auswählen) die Option My AMIs (Meine AMIs), suchen Sie das AMI, das Sie zuvor erstellt haben, und wählen Sie anschließend Select (Auswählen) aus.
4. Wählen Sie auf der Seite Choose an Instance Type (Instance-Typ auswählen) die Option p3dn.24xlarge und dann Next: Configure Instance Details (Weiter: Instance-Details konfigurieren) aus.
5. Führen Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) die folgenden Schritte aus:

   a. Geben Sie bei Number of instances (Anzahl der Instances) die Anzahl der EFA- und NCCL-fähigen Instances ein, die gestartet werden sollen.

   b. Wählen Sie für Network (Netzwerk) und Subnet (Subnetz) die VPC und das Subnetz an, in das Sie die Instances starten möchten.

   c. Wählen Sie für Placement group (Placement-Gruppe) die Option Add instance to placement group (Instance der Placement-Gruppe hinzufügen) aus.

   d. Wählen Sie bei Placement group name (Name der Placement-Gruppe) die Option Add to a new placement group (Zu neuer Placement-Gruppe hinzufügen) aus und geben Sie dann einen beschreibenden Namen für die Placement-Gruppe ein. Wählen Sie dann bei Placement group strategy (Strategie für Placement-Gruppe) cluster aus.

   e. Wählen Sie für EFA Enable (Aktivieren) aus.

   f. Wählen Sie im Abschnitt Network Interfaces (Netzwerkschnittstellen für das Gerät eth0 die Option New network interface (Neue Netzwerkschnittstelle) aus. Sie können zudem optional eine primäre IPv4-Adresse und eine oder mehrere sekundäre IPv4-Adressen eingeben. Wenn Sie die Instance in einem Subnetz starten, dem ein IPv6-CIDR-Block zugeordnet ist, können Sie optional eine primäre IPv6-Adresse und eine oder mehrere sekundäre IPv6-Adressen angeben.

   g. Wählen Sie Next: Add Storage aus.
6. Geben Sie auf der Seite Add Storage (Speicher hinzufügen) die Volumes an, die an die Instances angefügt werden sollen, ergänzend zu den Volumes, die vom AMI angegeben werden (z. B. der Root-Gerät-Volume). Wählen Sie dann Next: Add Tags (Weiter: Tags (Markierungen) hinzufügen) aus.
7. Geben Sie auf der Seite Add Tags (Tags (Markierungen) hinzufügen) Tags (Markierungen) für die Instances an, z. B. einen benutzerfreundlichen Namen, und wählen Sie anschließend Next: Configure Security Group (Weiter: Sicherheitsgruppe konfigurieren).

8. Wählen Sie auf der Seite Configure Security Group (Sicherheitsgruppe konfigurieren) bei Assign a security group (Sicherheitsgruppe zuweisen) die Option Select an existing security group (Vorhandene Sicherheitsgruppe auswählen) und dann die Sicherheitsgruppe aus, die Sie zuvor erstellt haben.
9. Klicken Sie auf Review and Launch.
10. Überprüfen Sie auf der Seite Review Instance Launch (Instance-Start überprüfen) Ihre Einstellungen und wählen Sie anschließend Launch (Starten) aus, um ein Schlüsselpaar auszuwählen und Ihre Instance zu starten.

Schritt 8: Aktivieren von passwortlosem SSH

Damit Ihre Anwendungen auf allen Instances in Ihrem Cluster ausgeführt werden können, müssen Sie passwortlosen SSH-Zugriff vom Führungsknoten auf die Mitgliedsknoten aktivieren. Der Führungsknoten ist die Instance, von der aus Sie die Anwendungen ausführen. Die verbleibenden Instances im Cluster sind die Mitgliedsknoten.

So aktivieren Sie passwortloses SSH zwischen den Instances im Cluster:

1. Wählen Sie eine Instance im Cluster als Führungsknoten aus und stellen Sie eine Verbindung zu ihr her.
2. Deaktivieren Sie `strictHostKeyChecking` und aktivieren Sie `ForwardAgent` für den Führungsknoten. Öffnen Sie `~/.ssh/config` mit dem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

   ```
   Host *
       ForwardAgent yes
   Host *
       StrictHostKeyChecking no
   ```

3. Generieren Sie ein RSA-Schlüsselpaar.

   ```
   $ ssh-keygen -t rsa -N "" -f ~/.ssh/id_rsa
   ```

   Das Schlüsselpaar wird im `$HOME/.ssh/`-Verzeichnis erstellt.
4. Ändern Sie die Berechtigungen des privaten Schlüssels auf dem Führungsknoten.

   ```
   $ chmod 600 ~/.ssh/id_rsa
   ```

```
chmod 600 ~/.ssh/config
```

5. Öffnen Sie `~/.ssh/id_rsa.pub` mit Ihrem bevorzugten Texteditor und kopieren Sie den Schlüssel.
6. Gehen Sie für jeden Mitgliedsknoten im Cluster wie folgt vor:
   a. Stellen Sie eine Verbindung mit der Instance her.
   b. Öffnen Sie `~/.ssh/authorized_keys` mit Ihrem bevorzugten Texteditor und fügen Sie den öffentlichen Schlüssel hinzu, den Sie zuvor kopiert haben.
7. Um zu testen, ob das passwortlose SSH wie erwartet funktioniert, stellen Sie eine Verbindung zum Leaderknoten her und führen Sie den folgenden Befehl aus.

   ```
   $ ssh member_node_private_ip
   ```

   Sie sollten eine Verbindung zum Mitgliedsknoten herstellen können, ohne zur Eingabe eines Schlüssels oder Passworts aufgefordert zu werden.

Arbeiten mit EFA

Sie können ein EFA praktisch genau wie alle anderen Elastic Network-Schnittstellen in Amazon EC2 erstellen, verwenden und verwalten. Anders als Elastic Network-Schnittstellen können EFAs allerdings nicht im laufenden Zustand an eine Instance angefügt oder von dieser getrennt werden.

EFA-Voraussetzungen

Zur Verwendung eines EFA gehen Sie wie folgt vor:

- Wählen Sie einen der unterstützten Instance-Typen aus.
- Verwenden Sie ein AMI für eines der unterstützten Betriebssysteme.
- Installieren Sie die EFA-Softwarekomponenten. Weitere Informationen finden Sie unter Schritt 3: Installieren der EFA-Software und Schritt 5: (Optional) Installieren von Intel MPI.
- Verwenden Sie eine Sicherheitsgruppe, die allen eingehenden und ausgehenden Datenverkehr von und zu der Sicherheitsgruppe selbst zulässt. Weitere Informationen finden Sie unter Schritt 1: Vorbereiten einer EFA-aktivierten Sicherheitsgruppe.

Inhalt

Erstellen eines EFA

Sie können ein EFA in einem Subnetz in einer VPC erstellen. Sie können das EFA nach der Erstellung nicht in ein anderes Subnetz verschieben und Sie können es nur an Instances in der gleichen Availability Zone anfügen.

So erstellen Sie ein neues EFA mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces aus.
3. Klicken Sie auf Create Network Interface (Netzwerkschnittstellen erstellen).
4. Geben Sie unter Description (Beschreibung) einen aussagekräftigen Namen für das EFA ein.
5. Wählen Sie für Subnet (Subnetz) das Subnetz aus, in das Sie das EFA erstellen möchten.
6. Geben Sie für Private IP die primäre private IPv4-Adresse ein. Wenn Sie keine primäre private IPv4-Adresse angeben, wählen wir im ausgewählten Subnetz eine verfügbare private IPv4-Adresse aus.
7. (Nur IPv6) Wenn Sie ein Subnetz ausgewählt haben, das über einen zugeordneten IPv6-CIDR-Block verfügt, können Sie im Feld IPv6 IP optional eine IPv6-Adresse angeben.
8. Wählen Sie unter Security groups (Sicherheitsgruppen) eine oder mehrere Sicherheitsgruppen aus.
9. Wählen Sie für EFA Enabled (Aktiviert) aus.
10. Wählen Sie Yes, Create (Ja, erstellen) aus.

Um eine neue EFA mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-network-interface und geben Sie für `interface-type` `efa` an, wie im folgenden Beispiel veranschaulicht.

```
aws ec2 create-network-interface --subnet-id subnet-01234567890 --
description example_efa --interface-type efa
```

Anfügen eines EFA an eine gestoppte Instance

Sie können ein EFA an jede unterstützte Instance anfügen, die sich im Zustand `stopped` befindet. Sie können keine EFA an eine Instance anfügen, die sich im Zustand `running` befindet. Weitere Informationen zu den unterstützten Instance-Typen finden Sie unter Unterstützte Instance-Typen.

Sie fügen einen EFA auf gleiche Weise an eine Instance an, wie Sie eine Schnittstelle an eine Instance anfügen. Weitere Informationen finden Sie unter Zuordnen einer Netzwerkschnittstelle zu einer Instance.

Anfügen einer EFA beim Starten einer Instance

Beim Starten einer Instance vorhandenen EFA anfügen (AWS CLI)

Verwenden Sie den Befehl run-instances und geben Sie für NetworkInterfaceId die ID der EFA an, wie im folgenden Beispiel gezeigt.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,NetworkInterfaceId=efa_id,Groups=sg_id,SubnetId=subnet_id
```

Beim Starten einer Instance neuen EFA anfügen (AWS CLI)

Verwenden Sie den Befehl run-instances und geben Sie for an InterfaceType`efa`, wie im folgenden Beispiel gezeigt.

```
aws ec2 run-instances --image-id ami_id --count 1 --instance-
type c5n.18xlarge --key-name my_key_pair --network-interfaces
 DeviceIndex=0,InterfaceType=efa,Groups=sg_id,SubnetId=subnet_id
```

Hinzufügen eines EFA zu einer Startvorlage

Sie können eine Startvorlage erstellen, die die Konfigurationsdaten zum Starten einer EFA-aktivierten Instance enthält. Zum Erstellen einer EFA-aktivierten Startvorlage erstellen Sie eine neue Startvorlage und geben einen unterstützten Instance-Typen, Ihr EFA-aktiviertes AMI und eine EFA-aktivierte Sicherheitsgruppe an. Weitere Informationen finden Sie unter Erste Schritte mit EFA und MPI.

Sie können Startvorlagen nutzen, um EFA-fähige Instances mit anderen AWS -Services zu starten, z. B. AWS Batch oder AWS ParallelCluster.

Weitere Informationen zum Erstellen von Startvorlagen finden Sie unter Erstellen einer Startvorlage.

Verwalten von IP-Adressen für einen EFA

Sie können die IP-Adressen ändern, die einem EFA zugeordnet sind. Wenn Sie eine Elastic IP-Adresse besitzen, können Sie diese einem EFA zuweisen. Wenn Ihr EFA in einem Subnetz bereitgestellt ist, das einen zugewiesenen IPv6-CIDR-Block hat, können Sie eine oder mehrere IPv6-Adressen zum EFA zuweisen.

Sie weisen eine Elastic IP-Adresse (IPv4) und IPv6-Adresse einem EFA auf gleiche Weise hinzu, wie Sie eine IP-Adresse eine Elastic Network-Schnittstelle hinzufügen. Weitere Informationen finden Sie unter Verwalten von IP-Adressen.

Ändern der Sicherheitsgruppe für einen EFA

Sie können die Sicherheitsgruppe ändern, die einem EFA zugeordnet ist. Zum Aktivieren der Funktion der Betriebssystemumgehung muss das EFA zu einer Sicherheitsgruppe gehören, die allen eingehenden und ausgehenden Datenverkehr von und zu der Sicherheitsgruppe selbst zulässt.

Sie können die Sicherheitsgruppe, die einem EFA zugewiesen ist, auf gleiche Weise ändern, wie Sie die Sicherheitsgruppe ändern, die einer Elastic Network Interface zugewiesen ist. Weitere Informationen finden Sie unter Ändern der Sicherheitsgruppe.

Trennen eines EFA

Zum Trennen eines EFA von der Instance müssen Sie zuerst die Instance stoppen. Sie können kein EFA von einer Instance trennen, die sich in einem laufenden Zustand befindet.

Sie trennen ein EFA auf gleiche Weise von einer Instance, wie Sie eine Elastic Network-Schnittstelle von einer Instance trennen. Weitere Informationen finden Sie unter Trennen einer Netzwerkschnittstelle von einer Instance.

Anzeigen von EFAs

Sie können alle Ihre EFAs in Ihrem Konto anzeigen.

Sie zeigen die EFAs auf gleiche Weise an, wie Sie Elastic Network-Schnittstellen anzeigen. Weitere Informationen finden Sie unter Anzeigen von Details zu einer Netzwerkschnittstelle.

Löschen eines EFA

Zum Löschen eines EFA müssen Sie es zuerst von der Instance trennen. Sie können keinen EFA löschen, während er an eine Instance angefügt ist.

Sie löschen die EFAs auf gleiche Weise, wie Sie Elastic Network-Schnittstellen löschen. Weitere Informationen finden Sie unter Löschen einer Netzwerkschnittstelle.

Überwachen von EFA

Sie können die folgenden Features zum Überwachen der Leistung Ihrer Elastic Fabric Adapter verwenden.

Amazon VPC-Flussprotokolle

Sie können ein Amazon VPC-Flow-Protokoll erstellen, um Informationen über den Datenverkehr zu und von Ihrem EFA zu erfassen. Flow-Protokolldaten können in Amazon CloudWatch Logs und Amazon S3 veröffentlicht werden. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die darin enthaltenen Daten abrufen und an dem gewählten Ziel anzeigen. Weitere Informationen finden Sie unter VPC-Flow-Protokolle im Amazon VPC Benutzerhandbuch.

Sie erstellen ein Flow-Protokoll für einen EFA auf gleiche Weise, wie Sie ein Flow-Protokoll für eine Elastic Network Interface erstellen. Weitere Informationen finden Sie unter Erstellen eines Flow-Protokolls im Amazon-VPC-Benutzerhandbuch.

In den Flow-Protokolleinträgen wird EFA-Datenverkehr von `srcAddress` und `destAddress` identifiziert, die beide als MAC-Adressen formatiert sind, wie im folgenden Beispiel veranschaulicht.

```
version accountId  eniId       srcAddress       destAddress       sourcePort destPort
 protocol packets bytes start      end        action log-status
```

```
2       3794735123 eni-10000001 01:23:45:67:89:ab 05:23:45:67:89:ab -          -
 -        9       5689  1521232534 1524512343 ACCEPT OK
```

Amazon CloudWatch

Amazon CloudWatch bietet Kennzahlen, mit denen Sie Ihre EFAs in Echtzeit überwachen können. Sie können Metriken erfassen und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme festlegen, die Sie benachrichtigen oder Maßnahmen ergreifen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.

Überprüfen des EFA-Installationsprogramms mithilfe einer Prüfsumme

Optional können Sie die EFA-Tarball (.tar.gz-Datei) mit einer MD5- oder SHA256-Prüfsumme überprüfen. Diese Vorgehensweise wird empfohlen, um die Identität des Software-Publishers zu überprüfen und zu prüfen, ob die Anwendung seit der Veröffentlichung nicht verändert oder beschädigt wurde.

So überprüfen Sie die Tarball

Verwenden Sie das Dienstprogramm md5sum für die MD5-Prüfsumme oder das Dienstprogramm sha256sum für die SHA256-Prüfsumme, und geben Sie den Tarball-Dateinamen an. Sie müssen den Befehl aus dem Verzeichnis heraus ausführen, in dem Sie die Tarball-Datei gespeichert haben.

- MD5

```
$  md5sum tarball_filename.tar.gz
```

- SHA256

```
$  sha256sum tarball_filename.tar.gz
```

Die Befehle sollten einen Prüfsummenwert im folgenden Format zurückgeben.

```
checksum_value tarball_filename.tar.gz
```

Vergleichen Sie den vom Befehl zurückgegebenen Prüfsummenwert mit dem in der folgenden Tabelle angegebenen Prüfsummenwert. Wenn die Prüfsummen übereinstimmen, ist es sicher,

das Installationsskript auszuführen. Wenn die Prüfsummen nicht übereinstimmen, führen Sie das Installationsskript nicht aus, und wenden Sie sich an den AWS Support Support.

Mit dem folgenden Befehl wird beispielsweise der EFA-1.9.4-Tarball mithilfe der SHA256-Prüfsumme überprüft.

```
$  sha256sum aws-efa-installer-1.9.4.tar.gz
```

```
1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14 aws-efa-
installer-1.9.4.tar.gz
```

In der folgenden Tabelle sind die Prüfsummen für aktuelle Versionen von EFA aufgeführt.

Version	URL herunterladen	Prüfsummen
EFA 1.32.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.32.0.tar.gz	MD5: db8d65cc028d8d08b5a9f2d88881c1b1 SHA256: 5f7233760be57f6fee6de8c09acbfbf59238de848e06048dc54d156ef578fc66
EFA 1.31.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.31.0.tar.gz	MD5: 856352f12bef2ccbadcd75e35aa52aaf SHA256: 943325bd37902a4300ac9e5715163537d56ecb4e7b87b37827c3e547aa1897bf
EFA 1.30.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.30.0.tar.gz	MD5: 31f48e1a47fe93ede8ebd273fb747358 SHA256: 876ab9403e07a0c3c91a1a34685a52eced890ae052df94857f6081c5f6c78a0a

Version	URL herunterladen	Prüfsummen
EFA 1.29.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.29.1.tar.gz	MD5: `e1872ca815d752c1d7c2b5c175e52a16` SHA256: `178b263b8c25845b63dc93b25bcdff5870df5204ec509af26f43e8d283488744`
EFA 1.29.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.29.0.tar.gz	MD5: `39d06a002154d94cd982ed348133f385` SHA256: `836655f87015547e733e7d9f7c760e4e24697f8bbc261bb5f3560abd4206bc36`
EFA 1.28.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.28.0.tar.gz	MD5: `9dc13b7446665822605e66febe074035` SHA256: `2e625d2d6d3e073b5178e8e861891273d896b66d03cb1a32244fd56789f1c435`
EFA 1.27.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.27.0.tar.gz	MD5: `98bfb515ea3e8d93f554020f3837fa15` SHA256: `1d49a97b0bf8d964d91652a79ac851f2550e33a5bf9d0cf86ec9357ff6579aa3`

Version	URL herunterladen	Prüfsummen
EFA 1.26.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.26.1.tar.gz	MD5: 884e74671fdef4725501f7cd2d451d0c SHA256: c616994c924f54ebfabfab32b7fe8ac56947fae00a0ff453d975e298d174fc96
EFA 1.26.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.26.0.tar.gz	MD5: f8839f12ff2e3b9ba09ae8a82b30e663 SHA256: bc1abc1f76e97d204d3755d2a9ca307fc423e51c63141f798c2f15be3715aa11
EFA 1.25.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.25.1.tar.gz	MD5: 6d876b894547847a45bb8854d4431f18 SHA256: d2abc553d22b89a4ce92882052c1fa6de450d3a801fe005da718b7d4b9602b06
EFA 1.25.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.25.0.tar.gz	MD5: 1993836ca749596051da04694ea0d00c SHA256: 98b7b26ce031a2d6a93de2297cc71b03af647194866369ca53b60d82d45ad342

Version	URL herunterladen	Prüfsummen
EFA 1.24.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.24.1.tar.gz	MD5: `211b249f39d53086f3cb0c07665f4e6f` SHA256: `120cfeec233af0955623ac7133b674143329f9561a9a8193e473060f596aec62`
EFA 1.24.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.24.0.tar.gz	MD5: `7afe0187951e2dd2c9cc4b572e62f924` SHA256: `878623f819a0d9099d76ecd41cf4f569d4c3aac0c9bb7ba9536347c50b6bf88e`
EFA 1.23.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.23.1.tar.gz	MD5: `22491e114b6ee7160a8290145dca0c28` SHA256: `5ca848d8e0ff4d1571cd443c36f8d27c8cdf2a0c97e9068ebf000c303fc40797`
EFA 1.23.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.23.0.tar.gz	MD5: `38a6d7c1861f5038dba4e441ca7683ca` SHA256: `555d497a60f22e3857fdeb3dfc53aa86d05926023c68c916d15d2dc3df6525bd`

Version	URL herunterladen	Prüfsummen
EFA 1.22.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.22.1.tar.gz	MD5: `600c0ad7cdbc06e8e846cb763f92901b` SHA256: `f90f3d5f59c031b9a964466b5401e86fd0429272408f6c207c3f9048254e9665`
EFA 1.22.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.22.0.tar.gz	MD5: `8f100c93dc8ab519c2aeb5dab89e98f8` SHA256: `f329e7d54a86a03ea51da6ea9a5b68fb354fbae4a57a02f9592e21fce431dc3a`
EFA 1.21.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.21.0.tar.gz	MD5: `959ccc3a4347461909ec02ed3ba7c372` SHA256: `c64e6ca34ccfc3ebe8e82d08899ae8442b3ef552541cf5429c43d11a04333050`
EFA 1.20.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.20.0.tar.gz	MD5: `7ebfbb8e85f1b94709df4ab3db47913b` SHA256: `aeefd2681ffd5c4c631d1502867db5b831621d6eb85b61fe3ec80df983d1dcf0`

Version	URL herunterladen	Prüfsummen
EFA 1.19.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.19.0.tar.gz	MD5: `2fd45324953347ec5518da7e3fefa0ec` SHA256: `99b77821b9e72c8dea015cc92c96193e8db307deee05b91a58094cc331f16709`
EFA 1.18.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.18.0.tar.gz	MD5: `fc2571a72f5d3c7b7b576ce2de38d91e` SHA256: `acb18a0808aedb9a5e485f1469225b9ac97f21db9af78e4cd6939700debe1cb6`
EFA 1.17.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.3.tar.gz	MD5: `0517df4a190356ab559235147174cafd` SHA256: `5130998b0d2883bbae189b21ab215ecbc1b01ae0231659a9b4a17b0a33ebc6ca`
EFA 1.17.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.2.tar.gz	MD5: `a329dedab53c4832df218a24449f4c9a` SHA256: `bca1fdde8b32b00346e175e597ffab32a09a08ee9ab136875fb38283cc4cd099`

Version	URL herunterladen	Prüfsummen
EFA 1.17.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.1.tar.gz	MD5: `733ae2cfc9d14b5201 7eaf0a2ab6b0ff` SHA256: `f29322640a88ae9279 805993cb836276ea24 0623820848463ca686 c8ce02136f`
EFA 1.17.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.17.0.tar.gz	MD5: `d430fc841563c11c38 05c5f82a4746b1` SHA256: `75ab0cee4fb6bd3888 9dce313183f5d3a83b d233e0a6ef6205d835 2821ea901d`
EFA 1.16.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.16.0.tar.gz	MD5: `399548d3b0d2e812d7 4dd67937b696b4` SHA256: `cecec36495a1bc6fdc 82f97761a541e4fb6c 9a3cbf3cfcb145acf2 5ea5dbd45b`
EFA 1.15.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.2.tar.gz	MD5: `955fea580d5170b058 23d51acde7ca21` SHA256: `84df4fbc1b3741b6c0 73176287789a601a58 9313accc8e6653434e 8d4c20bd49`

Version	URL herunterladen	Prüfsummen
EFA 1.15.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.1.tar.gz	MD5: `c4610267039f72bbe4e35d7bf53519bc` SHA256: `be871781a1b9a15fca342a9d169219260069942a8bda7a8ad06d4baeb5e2efd7`
EFA 1.15.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.15.0.tar.gz	MD5: `9861694e1cc00d884fadac07d22898be` SHA256: `b329862dd5729d2d098d0507fb486bf859d7c70ce18b61c302982234a3a5c88f`
EFA 1.14.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.14.1.tar.gz	MD5: `50ba56397d359e57872fde1f74d4168a` SHA256: `c7b1b48e86fe4b3eaa4299d3600930919c4fe6d88cc6e2c7e4a408a3f16452c7`
EFA 1.14.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.14.0.tar.gz	MD5: `40805e7fd842c36ececb9fd7f921b1ae` SHA256: `662d62c12de85116df33780d40e0533ef7dad92709f4f613907475a7a1b60a97`

Version	URL herunterladen	Prüfsummen
EFA 1.13.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.13.0.tar.gz	MD5: `c91d16556f4fd53becadbb345828221e` SHA256: `ad6705eb23a3fce44af3afc0f7643091595653a723ad0374084f4f2b715192e1`
EFA 1.12.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.3.tar.gz	MD5: `818aee81f097918cfaebd724eddea678` SHA256: `2c225321824788b8ca3fbc118207b944cdb096b847e1e0d1d853ef2f0d727172`
EFA 1.12.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.2.tar.gz	MD5: `956bb1fc5ae0d6f0f87d2e481d49fccf` SHA256: `083a868a2c212a5a4fcf3e4d732b685ce39cceb3ca7e5d50d0b74e7788d06259`
EFA 1.12.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.1.tar.gz	MD5: `f5bfe52779df435188b0a2874d0633ea` SHA256: `5665795c2b4f09d5f3f767506d4d4c429695b36d4a17e5758b27f033aee58900`

Version	URL herunterladen	Prüfsummen
EFA 1.12.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.12.0.tar.gz	MD5: d6c6b49fafb39b770297e1cc44fe68a6 SHA256: 28256c57e9ecc0b0778b41c1f777a9982b4e8eae782343dfe1246079933dca59
EFA 1.11.2	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.2.tar.gz	MD5: 2376cf18d1353a4551e35c33d269c404 SHA256: a25786f98a3628f7f54f7f74ee2b39bc6734ea9374720507d37d3e8bf8ee1371
EFA 1.11.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.1.tar.gz	MD5: 026b0d9a0a48780cc7406bd51997b1c0 SHA256: 6cb04baf5ffc58ddf319e956b5461289199c8dd805fe216f8f9ab8d102f6d02a
EFA 1.11.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.11.0.tar.gz	MD5: 7d9058e010ad65bf2e14259214a36949 SHA256: 7891f6d45ae33e822189511c4ea1d14c9d54d000f6696f97be54e915ce2c9dfa

Version	URL herunterladen	Prüfsummen
EFA 1.10.1	https://efa-installer.amazonaws.com/aws-efa-installer-1.10.1.tar.gz	MD5: 78521d3d668be22976f46c6fecc7b730 SHA256: 61564582de7320b21de319f532c3a677d26cc46785378eb3b95c636506b9bcb4
EFA 1.10.0	https://efa-installer.amazonaws.com/aws-efa-installer-1.10.0.tar.gz	MD5: 46f73f5a7afe41b4bb918c81888fefa9 SHA256: 136612f96f2a085a7d98296da0afb6fa807b38142e2fc0c548fa986c41186282
EFA 1.9.5	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.5.tar.gz	MD5: 95edb8a209c18ba8d250409846eb6ef4 SHA256: a4343308d7ea4dc943ccc21bcebed913e8868e59bfb2ac93599c61a7c87d7d25
EFA 1.9.4	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.4.tar.gz	MD5: f26dd5c350422c1a985e35947fa5aa28 SHA256: 1009b5182693490d908ef0ed2c1dd4f813cc310a5d2062ce9619c4c12b5a7f14

Version	URL herunterladen	Prüfsummen
EFA 1.9.3	https://efa-installer.amazonaws.com/aws-efa-installer-1.9.3.tar.gz	MD5: `95755765a097802d3e6d5018d1a5d3d6` SHA256: `46ce732d6f3fcc9edf6a6e9f9df0ad136054328e24675567f7029edab90c68f1`
EFA 1.8.4	https://efa-installer.amazonaws.com/aws-efa-installer-1.8.4.tar.gz	MD5: `85d594c41e831afc6c9305263140457e` SHA256: `0d974655a09b213d7859e658965e56dc4f23a0eee2dc44bb41b6d039cc5bab45`

Amazon-EC2-Instance-Topologie

Die Beschreibung Ihrer Instance-Topologie bietet einen hierarchischen Überblick über die relative Nähe zwischen Instances. Sie können diese Informationen verwenden, um die Recheninfrastruktur für High Performance Computing (HPC) und Machine Learning (ML) in großem Umfang zu verwalten und gleichzeitig die Stellenvermittlung zu optimieren. HPC- und ML-Aufträge sind latenz- und durchsatzempfindlich. Sie können die Instanztopologie verwenden, um den Standort Ihrer Instances zu ermitteln, und diese Informationen dann verwenden, um HPC- und ML-Jobs zu optimieren, indem Sie sie auf Instances ausführen, die physisch näher beieinander liegen.

Sie können die Instance-Topologie verwenden, um den Standort Ihrer vorhandenen Instances zu ermitteln, aber Sie können sie nicht verwenden, um auszuwählen, ob eine neue Instance physisch in der Nähe einer vorhandenen Instance gestartet werden soll. Um die Platzierung von Instanzen zu beeinflussen, können Sie verwendenKapazitätsreservierungen in Cluster-Placement-Gruppen.

Preisgestaltung

Für die Beschreibung Ihrer Instance-Topologie fallen keine zusätzlichen Kosten an.

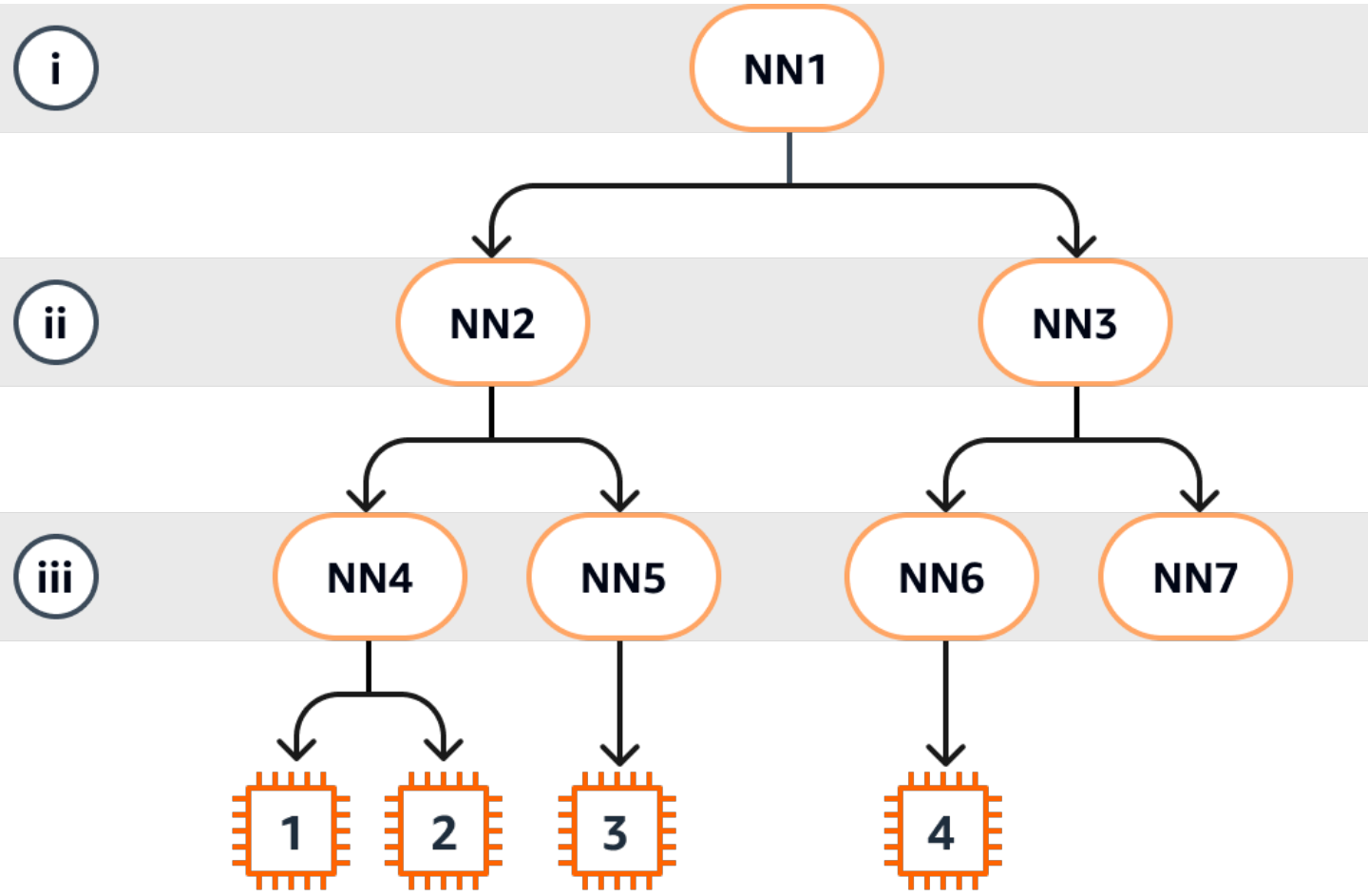
Inhalt

So funktioniert die Instanztopologie

Jede EC2-Instance stellt eine Verbindung mit einem Knotensatz her. Ein Knotensatz besteht aus drei Netzwerkknoten, wobei jeder Knoten eine andere Schicht im AWS Netzwerk darstellt. Die Netzwerkschichten sind in einer Hierarchie mit mindestens drei Schichten angeordnet. Der Knotensatz bietet eine hierarchische Ansicht. Die unterste Schicht ist einer Instance am nächsten und mit ihr verbunden.

Die Informationen über den Knotensatz werden als Instanztopologie bezeichnet.

Das folgende Diagramm bietet eine visuelle Darstellung, anhand derer Sie die Instanztopologie verstehen können. Die Netzwerkknoten werden als NN1 — NN7 identifiziert. Die Ziffern i, ii und iii kennzeichnen die Netzwerkschichten. Die Zahlen 1, 2, 3 und 4 identifizieren die EC2-Instances. Instances stellen eine Verbindung zu einem Knoten in der untersten Ebene her, der durch iii gekennzeichnet ist. Mehrere Instances können eine Verbindung mit dem gleichen Knoten herstellen.



In diesem Beispiel:

- Instanz 1 stellt eine Verbindung mit Netzwerkknoten 4 (NN4) in Schicht iii her. NN4 stellt eine Verbindung mit dem Netzwerkknoten 2 (NN2) in der Schicht ii her und NN2 stellt eine Verbindung mit dem Netzwerkknoten 1 (NN1) in der Schicht i her, die in diesem Beispiel die oberste Schicht der Netzwerkhierarchie darstellt. Der Netzwerkknotensatz umfasst NN1, NN2 und NN4, die hierarchisch von den oberen Schichten bis zur unteren Schicht ausgedrückt werden.
- Instance 2 stellt auch eine Verbindung mit dem Netzwerkknoten 4 (NN4) her. Die Instances 1 und 2 teilen sich den gleichen Netzwerkknotensatz: NN1, NN2 und NN4.
- Instance 3 stellt eine Verbindung mit dem Netzwerkknoten 5 (NN5) her. NN5 stellt eine Verbindung mit NN2 her und NN2 stellt eine Verbindung mit NN1 her. Der Netzwerkknotensatz für Instance 3 ist NN1, NN2 und NN5.
- Instance 4 stellt eine Verbindung mit dem Netzwerkknoten 6 (NN6) her. Der zugehörige Netzwerkknotensatz ist NN1, NN3 und NN6.

Bei der Betrachtung der Nähe der Instances 1, 2 und 3 wird deutlich, dass sich die Instances 1 und 2 näher beieinander befinden, weil sie mit dem gleichen Netzwerkknoten (NN4) verbunden sind. Instance 3 ist dagegen weiter entfernt, weil sie eine Verbindung mit einem anderen Netzwerkknoten (NN5) herstellt.

Bei der Betrachtung der Nähe aller Instances in diesem Diagramm wird deutlich, dass die Instances 1, 2 und 3 näher beieinander sind und die Entfernung zu Instance 4 jeweils größer ist, da sich die Instances 1, 2 und 3 den Netzwerkknoten 2 (NN2) in ihrer Netzwerkknotengruppe teilen.

Faustregel: Wenn zwei beliebige Instances mit dem gleichen Netzwerkknoten verbunden sind, befinden sie sich physisch nahe beieinander (wie bei den Instances 1 und 2). Außerdem gilt: Je weniger Hops zwischen Netzwerkknoten liegen, desto näher sind die Instances beieinander. So sind es beispielsweise bei den Instances 1 und 3 weniger Hops zu einem gemeinsamen Netzwerkknoten (NN2) als zu dem Netzwerkknoten (NN1), den sie mit Instance 4 gemeinsam haben. Daher ist die Entfernung zwischen ihnen geringer als zu Instance 4.

Da in diesem Beispiel keine Instances auf dem Netzwerkknoten 7 (NN7) ausgeführt werden, ist NN7 in der API-Ausgabe nicht enthalten.

So interpretieren Sie die Ausgabe

Sie erhalten die Informationen zur Instanztopologie mithilfe der DescribeInstanceTopologie-API. Die Ausgabe bietet eine hierarchische Ansicht der zugrunde liegenden Netzwerktopologie für eine Instance.

Die folgende Beispielausgabe entspricht den Netzwerktopologie-Informationen der vier Instances aus dem vorherigen Diagramm. Für dieses Beispiel wurden der Beispielausgabe Kommentare hinzugefügt.

Beachten Sie folgende wichtige Informationen in der Ausgabe:

- `NetworkNodes` beschreibt den Netzwerkknotensatz einer Instance.
- In jedem Netzwerkknotensatz sind die Netzwerkknoten absteigend in hierarchischer Reihenfolge aufgeführt.
- Der mit der Instance verbundene Netzwerkknoten ist der letzte Netzwerkknoten in der Liste (die unterste Schicht).
- Um zu ermitteln, welche Instances nahe beieinander liegen, suchen Sie zuerst nach gemeinsamen Netzwerkknoten in der untersten Schicht. Wenn es in der untersten Schicht keine gemeinsamen Netzwerkknoten gibt, suchen Sie nach gemeinsamen Netzwerkknoten in den oberen Schichten.

In der folgenden Beispielausgabe befinden sich `i-1111111111example` und `i-2222222222example` am nächsten beieinander (verglichen mit den anderen Instances des Beispiels), da sie den Netzwerkknoten `nn-4444444444example` in der untersten Schicht gemeinsam haben.

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",  //Corresponds to instance 1
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 in layer i
                "nn-2222222222example",           //Corresponds to NN2 in layer ii
                "nn-4444444444example"            //Corresponds to NN4 in layer iii -
 bottom layer, connected to the instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",  //Corresponds to instance 2
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-4444444444example"            //Corresponds to NN4 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",  //Corresponds to instance 3
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",           //Corresponds to NN1 - layer i
                "nn-2222222222example",           //Corresponds to NN2 - layer ii
                "nn-5555555555example"            //Corresponds to NN5 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
```

```
        },
        {
            "InstanceId": "i-444444444example",  //Corresponds to instance 4
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",          //Corresponds to NN1 - layer i
                "nn-3333333333example",          //Corresponds to NN3 - layer ii
                "nn-6666666666example"           //Corresponds to NN6 - layer iii -
 connected to instance
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Einschränkungen

Die folgenden Einschränkungen gelten:

- Die Instanzen müssen sich im Status befinden. `running`
- Jede Instance-Topologieansicht ist kontospezifisch.
- Das unterstützt AWS Management Console nicht die Anzeige der Instanztopologie.

Voraussetzungen für die Instanztopologie

Bevor Sie die Instance-Topologie für Ihre Instances beschreiben, stellen Sie sicher, dass Ihre Instances die folgenden Anforderungen erfüllen.

Anforderungen zur Beschreibung der Topologie Ihrer Instances

- AWS-Regionen
- Instance-Typen
- Instance-Status
- IAM-Berechtigung

AWS-Regionen

Unterstützt AWS-Regionen:

- USA Ost (Nord-Virginia), USA Ost (Ohio), USA West (Nordkalifornien), USA West (Oregon)
- Asien-Pazifik (Seoul), Asien-Pazifik (Tokio)
- Kanada (Zentral)
- Europa (Frankfurt), Europa (Irland), Europa (Stockholm)

Instance-Typen

Unterstützte Instance-Typen:

- `hpc6a.48xlarge` | `hpc6id.32xlarge` | `hpc7a.12xlarge` | `hpc7a.24xlarge` | `hpc7a.48xlarge` | `hpc7a.96xlarge` | `hpc7g.4xlarge` | `hpc7g.8xlarge` | `hpc7g.16xlarge`
- `p3dn.24xlarge` | `p4d.24xlarge` | `p4de.24xlarge` | `p5.48xlarge`
- `trn1.2xlarge` | `trn1.32xlarge` | `trn1n.32xlarge`

So zeigen Sie die verfügbaren Instance-Typen in einer bestimmten Region an

Die verfügbaren Instance-Typen variieren je nach Region. Um zu ermitteln, ob ein Instance-Typ in einer Region verfügbar ist, können Sie den Befehl describe-instance-types-offerings mit dem `--region`-Parameter verwenden. Schließen Sie den Parameter `--filters` ein, um die Ergebnisse auf die für Sie interessante Instance-Familie oder auf den für Sie interessanten Instance-Typ zu beschränken, und verwenden Sie den Parameter `--query`, um die Ausgabe auf den Wert von `InstanceType` zu beschränken.

```
aws ec2 describe-instance-type-offerings \
    --region us-east-2 \
    --filters 'Name=instance-type, Values=trn1*' \
    --query 'InstanceTypeOfferings[].InstanceType'
```

Erwartete Ausgabe

```
[
    "trn1.2xlarge",
    "trn1.32xlarge",
    "trn1n.32xlarge"
]
```

Instance-Status

Instances müssen sich im Zustand `running` befinden. Für Instances in einem anderen Zustand können keine Informationen zur Instance-Topologie abgerufen werden.

IAM-Berechtigung

Für Ihre IAM-Identität (Benutzer, Benutzergruppe oder Rolle) ist die folgende IAM-Berechtigung erforderlich:

- `ec2:DescribeInstanceTopology`

Beispiele Amazon EC2 EC2-Instance-Topologie

Sie können den describe-instance-topologyCLI-Befehl verwenden, um die Instance-Topologie für Ihre EC2-Instances zu beschreiben.

Wenn Sie den Befehl `describe-instance-topology` ohne Parameter oder Filter verwenden, umfasst die Antwort alle Ihre Instances, die den unterstützten Instance-Typen für diesen Befehl in der angegebenen Region entsprechen. Sie können die Region angeben, indem Sie den `--region`-Parameter einschließen oder eine Standardregion festlegen. Weitere Informationen zum Festlegen einer Standardregion finden Sie unter Angeben der Region für eine Ressource.

Sie können Parameter einschließen, um Instances zurückzugeben, die den angegebenen Instance-IDs oder Placement-Gruppennamen entsprechen. Sie können auch Filter einschließen, um Instances zurückzugeben, die einem angegebenen Instance-Typ oder einer angegebenen Instance-Familie entsprechen, oder Instances in einer angegebenen Availability Zone oder lokalen Zone. Sie können einen einzelnen Parameter oder Filter oder eine Kombination aus Parametern und Filtern einschließen.

Die Ausgabe ist paginiert und umfasst standardmäßig bis zu 20 Instances pro Seite. Mit dem Parameter `--max-results` können bis zu 100 Instances pro Seite angegeben werden.

Weitere Informationen finden Sie unter describe-instance-topology in der Referenz zum AWS CLI - Befehl.

Erforderliche Berechtigungen

Die folgende Berechtigung ist erforderlich, um die Instance-Topologie zu beschreiben:

- `ec2:DescribeInstanceTopology`

Beispiele

Beispiel 1 – Keine Parameter oder Filter

So beschreiben Sie die Instance-Topologie all Ihrer Instances

Verwenden Sie den CLI-Befehl describe-instance-topology ohne Angabe von Parametern oder Filtern.

```
aws ec2 describe-instance-topology --region us-west-2
```

In der Antwort werden nur die Instances zurückgegeben, die den unterstützten Instance-Typen für diese API entsprechen. Die Instances können sich in verschiedenen Availability Zones, lokalen Zonen (`ZoneId`) und Placement-Gruppen (`GroupName`) befinden. Wenn sich eine Instance nicht in einer Placement-Gruppe befindet, ist das Feld `GroupName` in der Ausgabe nicht enthalten. In der folgenden Beispielausgabe befindet sich nur eine einzelne Instance in einer Placement-Gruppe.

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
```

```
            "GroupName": "my-ml-cpg",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "p4d.24xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
```

```
}
```

Beispiel 2 – Instance-Typ-Filter

Sie können nach einem angegebenen Instance-Typ (exakte Übereinstimmung) oder nach einer Instance-Familie (mit einem Platzhalter) filtern. Sie können auch einen Filter für einen angegebenen Instance-Typ und einen Filter für eine Instance-Familie miteinander kombinieren.

Beispiel 2a – Filter mit exakter Übereinstimmung für einen angegebenen Instance-Typ

So beschreiben Sie die Instance-Topologie all Ihrer Instances, die einem angegebenen Instance-Typ entsprechen

Verwenden Sie den CLI-Befehl describe-instance-topology mit dem Filter `instance-type`. In diesem Beispiel wird die Ausgabe nach `trn1n.32xlarge`-Instances gefiltert. Die Antwort gibt nur Instances zurück, die dem angegebenen Instance-Typ entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1n.32xlarge
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Beispiel 2b – Platzhalterfilter für eine Instance-Familie

So beschreiben Sie die Instance-Topologie all Ihrer Instances, die einer Instance-Familie entsprechen

Verwenden Sie den CLI-Befehl describe-instance-topology mit dem Filter `instance-type`. In diesem Beispiel wird die Ausgabe nach `trn1*`-Instances gefiltert. Die Antwort gibt nur die Instances zurück, die der angegebenen Instance-Familie entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters Name=instance-type,Values=trn1*
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-3333333333example",
            "InstanceType": "trn1.32xlarge",
            "NetworkNodes": [
                "nn-1212121212example",
                "nn-1211122211example",
                "nn-1311133311example"
            ],
            "ZoneId": "usw2-az4",
            "AvailabilityZone": "us-west-2d"
        },
        {
            "InstanceId": "i-444444444example",
            "InstanceType": "trn1.2xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
```

```
                "nn-5434334334example",
                "nn-1235301234example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Beispiel 2c – Kombinierte Filter für Instance-Familie und exakte Übereinstimmung

So beschreiben Sie die Instance-Topologie all Ihrer Instances, die einer Instance-Familie oder einem angegebenen Instance-Typ entsprechen

Verwenden Sie den CLI-Befehl describe-instance-topology mit dem Filter `instance-type`. In diesem Beispiel wird die Ausgabe nach `pd4d*`- oder `trn1n.32xlarge`-Instances gefiltert. Die Antwort gibt Instances zurück, die einem beliebigen der angegebenen Filter entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge"
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
```

```
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-4343434343example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Beispiel 3 – Zonen-ID-Filter

Mit dem Filter `zone-id` können Sie nach einer Availability Zone oder nach einer lokalen Zone filtern. Sie können auch einen Availability-Zone-Filter und einen Filter für die lokale Zone miteinander kombinieren.

Beispiel 3a – Availability-Zone-Filter

So beschreiben Sie die Instance-Topologie all Ihrer Instances, die einer angegebenen Availability Zone entsprechen

Verwenden Sie den CLI-Befehl describe-instance-topology mit dem Filter `zone-id`. In diesem Beispiel wird die Ausgabe anhand der Availability Zone ID `use1-az1` gefiltert. Die Antwort gibt nur Instances zurück, die der angegebenen Availability Zone entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
```

```
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Beispiel 3b – Filter für lokale Zone

So beschreiben Sie die Instance-Topologie all Ihrer Instances, die einer angegebenen lokalen Zone entsprechen

Verwenden Sie den CLI-Befehl describe-instance-topology mit dem Filter `zone-id`. In diesem Beispiel wird die Ausgabe anhand der lokalen Zonen-ID gefiltert`use1-atl2-az1`. Die Antwort gibt nur Instances zurück, die der angegebenen lokalen Zone entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-atl2-az1
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Beispiel 3c – Kombination von Availability-Zone-Filter und Filter für die lokale Zone

So beschreiben Sie die Instance-Topologie all Ihrer Instances, die einer angegebenen Availability Zone oder einer angegebenen lokalen Zone entsprechen

Verwenden Sie den CLI-Befehl describe-instance-topology mit dem Filter `zone-id`. In diesem Beispiel wird die Ausgabe anhand der Availability Zone ID `use1-az1` und der Local Zone ID gefiltert`use1-atl2-az1`. Die Antwort gibt Instances zurück, die einem beliebigen der angegebenen Filter entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters Name=zone-id,Values=use1-az1,use1-atl2-az1
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
```

```
    "NextToken": "SomeEncryptedToken"
}
```

Beispiel 4 – Kombinierte Instance-Typ- und Zonen-ID-Filter

Sie können alle Filter in einem einzelnen Befehl miteinander kombinieren.

So beschreiben Sie die Instance-Topologie all Ihrer Instances, die einem angegebenen Instance-Typ, einer angegebenen Instance-Familie, einer angegebenen Availability Zone oder einer angegebenen lokalen Zone entsprechen

Verwenden Sie den CLI-Befehl describe-instance-topology mit den Filtern `instance-type` und `zone-id`. In diesem Beispiel wird die Ausgabe nach `p4d*` Instance-Familie, `trn1n.32xlarge` Instance-Typ, `use1-az1` Availability Zone ID und `use1-atl2-az1` Local Zone ID gefiltert. Die Antwort gibt Instances zurück, die `p4d*` entsprechen, oder Instances vom Typ `trn1n.32xlarge` in der Zone `us-east-1a` oder `us-east-1-atl-2a`.

```
aws ec2 describe-instance-topology \
    --region us-east-1 \
    --filters "Name=instance-type,Values=p4d*,trn1n.32xlarge" "Name=zone-
id,Values=use1-az1,use1-atl2-az1"
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "use1-atl2-az1",
            "AvailabilityZone": "us-east-1-atl-2a"
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
```

```
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "use1-az1",
            "AvailabilityZone": "us-east-1a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Beispiel 5 – Parameter für den Namen der Placement-Gruppe

So beschreiben Sie die Instance-Topologie all Ihrer Instances in einer angegebenen Placement-Gruppe

Verwenden Sie den CLI-Befehl describe-instance-topology mit dem Parameter `group-names`. Im folgenden Beispiel können sich die Instances in der Placement-Gruppe `ML-group` oder `HPC-group` befinden. In der Antwort werden Instances zurückgegeben, die sich in einer der Placement-Gruppe befinden.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --group-names ML-group HPC-group
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        },
```

```
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Beispiel 6 – Instance-IDs

So beschreiben Sie die Instance-Topologie angegebener Instances

Verwenden Sie den CLI-Befehl describe-instance-topology mit dem Parameter `--instance-ids`. Die Antwort gibt die Instances zurück, die den angegebenen Instance-IDs entsprechen.

```
aws ec2 describe-instance-topology \
    --region us-west-2 \
    --instance-ids i-1111111111example i-2222222222example
```

Beispielausgabe

```
{
    "Instances": [
        {
            "InstanceId": "i-1111111111example",
            "InstanceType": "p4d.24xlarge",
            "GroupName": "ML-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3333333333example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
```

```
        },
        {
            "InstanceId": "i-2222222222example",
            "InstanceType": "trn1n.32xlarge",
            "GroupName": "HPC-group",
            "NetworkNodes": [
                "nn-1111111111example",
                "nn-2222222222example",
                "nn-3214313214example"
            ],
            "ZoneId": "usw2-az2",
            "AvailabilityZone": "us-west-2a"
        }
    ],
    "NextToken": "SomeEncryptedToken"
}
```

Placement-Gruppen

Um den Anforderungen Ihres Workloads nachzukommen, können Sie eine Gruppe von untereinander abhängigen EC2-Instances in eine Placement-Gruppe starten, um ihre Platzierung zu beeinflussen.

Je nach Art des Workloads können Sie eine Placement-Gruppe mithilfe einer der folgenden Platzierungsstrategien erstellen:

- Cluster – Verpackt Instances nahe zusammen in einer Availability Zone. Diese Strategie ermöglicht es Workloads, die Netzwerkleistung mit niedriger Latenz zu erreichen, die für eng gekoppelte node-to-node Kommunikation erforderlich ist, wie sie für HPC-Anwendungen (High Performance Computing) typisch ist.
- Partition – Verteilt Instances auf logische Partitionen und gewährleistet dabei, dass Gruppen von Instances in einer Partition keine zugrunde liegende Hardware mit Instances in anderen Partitionen teilen. Diese Strategie wird in der Regel für große verteilte und replizierte Workloads wie Hadoop, Cassandra und Kafka verwendet.
- Spread – Verteilt eine kleine Gruppe von Instances strikt über verschiedene zugrundeliegende Hardware, um korrelierte Fehler zu reduzieren.

Placement-Gruppen sind optional. Wenn Sie eine neue EC2-Instance starten, versucht der EC2-Service die Instance auf eine Weise zu platzieren, dass alle Ihre Instances über die zugrundeliegende Hardware verbreitet werden, um korrelierte Fehler zu minimieren.

Für die Erstellung einer Placement-Gruppe fallen keine Gebühren an.

Platzierungsstrategien

Sie können eine Platzierungsgruppe mithilfe einer der folgenden Platzierungsstrategien erstellen.

Platzierungsstrategien:

- Cluster Placement-Gruppen
- Partitions-Placement-Gruppen
- Spread Placement-Gruppen

Cluster Placement-Gruppen

Eine Cluster Placement-Gruppe ist eine logische Gruppierung von Instances innerhalb einer einzelnen Availability Zone. Eine Cluster-Placement-Gruppe kann per Peering verbundene Virtual Private Networks (VPCs) in der gleichen Region umfassen. Instances in derselben Cluster Placement-Gruppe verfügen über ein höheres Durchsatzlimit pro Flow von bis zu 10 Gbit/s für TCP/IP-Datenverkehr und befinden sich in demselben Bandbreitensegment mit hoher Bisektion des Netzwerks.

Im folgenden Image werden Instances dargestellt, die in einer Cluster-Placement-Gruppe platziert sind.

Cluster-Placement-Gruppen sind für Anwendungen zu empfehlen, die von niedriger Netzwerklatenz, hohem Netzwerkdurchsatz oder von beidem profitieren. Sie werden auch empfohlen, wenn der Großteil des Netzwerkdatenverkehrs zwischen den Instances in der Gruppe liegt. Um die niedrigste Latenz und die höchste packet-per-second Netzwerkleistung für Ihre Platzierungsgruppe

bereitzustellen, wählen Sie einen Instance-Typ, der Enhanced Networking unterstützt. Weitere Informationen erhalten Sie unter Enhanced Networking.

Wir empfehlen Ihnen, Ihre Instances folgendermaßen zu starten:

- Verwenden Sie eine einzelne Startanforderung, um die Anzahl der benötigten Instances in der Placement-Gruppe zu starten.
- Verwenden Sie denselben Instance-Typ für alle Instances in der Placement-Gruppe.

Wenn Sie versuchen, der Placement-Gruppe später weitere Instances hinzuzufügen oder mehr als einen Instance-Typ in der Placement-Gruppe zu starten, steigt das Risiko, dass die Kapazität nicht ausreicht und ein entsprechender Fehler auftritt.

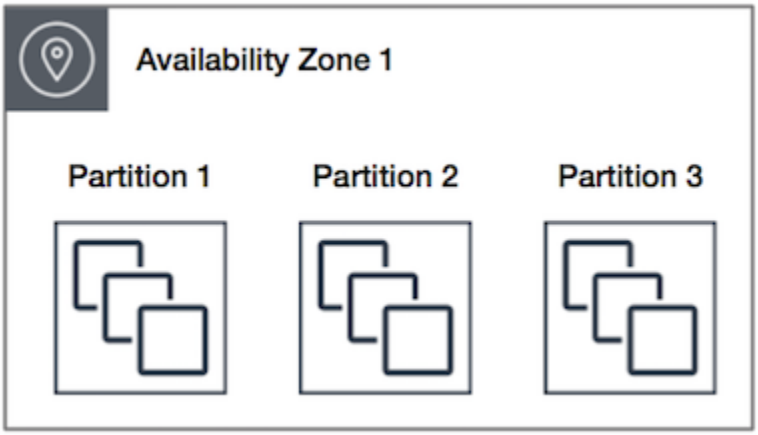
Wenn Sie eine Instance in einer Placement-Gruppe anhalten und dann wieder starten, wird sie in der Placement-Gruppe weiterhin ausgeführt. Der Startvorgang schlägt aber fehl, wenn für die Instance nicht genügend Kapazität vorhanden ist.

Wenn Sie beim Starten einer Instance in einer Placement-Gruppe, die bereits laufende Instances enthält, einen Kapazitätsfehler erhalten, sollten Sie alle Instances der Placement-Gruppe beenden und erneut starten und dann versuchen, den Vorgang zu wiederholen. Wenn Sie die Instances starten, werden diese unter Umständen zu Hardware migriert, die über Kapazität für alle angeforderten Instances verfügt.

Partitions-Placement-Gruppen

Partitions-Placement-Gruppen tragen zu einer verringerten Wahrscheinlichkeit korrelierter Hardwarefehler für Ihre Anwendung bei. Beim Verwenden von Partitions-Placement-Gruppen unterteilt Amazon EC2 jede Gruppe in logische Segmente, die als Partitionen bezeichnet werden. Amazon EC2 stellt sicher, dass jede Partition in einer Placement-Gruppe über einen eigenen Satz von Racks verfügt. Dabei verfügt jedes Rack über sein eigenes Netzwerk und seine eigene Stromquelle. Da keine der Partitionen innerhalb einer Placement-Gruppe dieselben Racks nutzen, können die Auswirkung von Hardwarefehlern auf Ihre Anwendungen reduziert werden.

Das folgende Image ist eine einfache visuelle Darstellung einer Partition-Placement-Gruppe in einer einzelnen Availability Zone. Es zeigt Instances in einer Partition-Placement-Gruppe mit drei Partitionen – Partition 1, Partition 2 und Partition 3. Jede Partition umfasst mehrere Instances. Die Instances in der jeweiligen Partition nutzen keine Racks mit den Instances in den anderen Partitionen gemeinsam. Die Auswirkungen eines einzelnen Hardwarefehlers werden somit auf nur die zugehörige Partition eingeschränkt.



Partitions-Placement-Gruppen können verwendet werden, um große verteilte und replizierte Workloads, wie beispielsweise HDFS, HBase und Cassandra, auf unterschiedlicher Hardware bereitzustellen. Wenn Sie Instances in einer Partition-Placement-Gruppe starten, versucht Amazon EC2, die Instances gleichmäßig auf die Anzahl der von Ihnen angegebenen Partitionen zu verteilen. Sie können Instances auch in einer bestimmten Partition starten, um eine bessere Kontrolle darüber zu haben, wo die Instances platziert werden.

Eine Partition-Placement-Gruppe kann Partitionen in mehreren Availability Zones in der gleichen Region umfassen. Eine Partition-Placement-Gruppe kann maximal sieben Partitionen pro Availability Zone aufweisen. Die Anzahl von Instances, die in einer Partition-Placement-Gruppe gestartet werden können, ist nur durch die Begrenzungen in Ihrem Konto limitiert.

Partitions-Placement-Gruppen bieten außerdem Einsicht in die Partitionen. Sie können sehen, welche Instances sich in welchen Partitionen befinden. Sie können diese Angaben an topologiegestützte Anwendungen wie HDFS, HBase und Cassandra übermitteln, die anhand dieser Informationen intelligente Datenreplikationsentscheidungen zur Steigerung der Verfügbarkeit und Lebensdauer von Daten treffen.

Wenn Sie eine Instance in einer Partitions-Placement-Gruppe starten und es nicht genügend eindeutige Hardware zur Erfüllung der Anforderung gibt, schlägt die Anforderung fehl. Amazon EC2 stellt mit der Zeit mehr eindeutig identifizierbare Hardware zur Verfügung, sodass Sie die Anforderung später erneut versuchen können.

Spread Placement-Gruppen

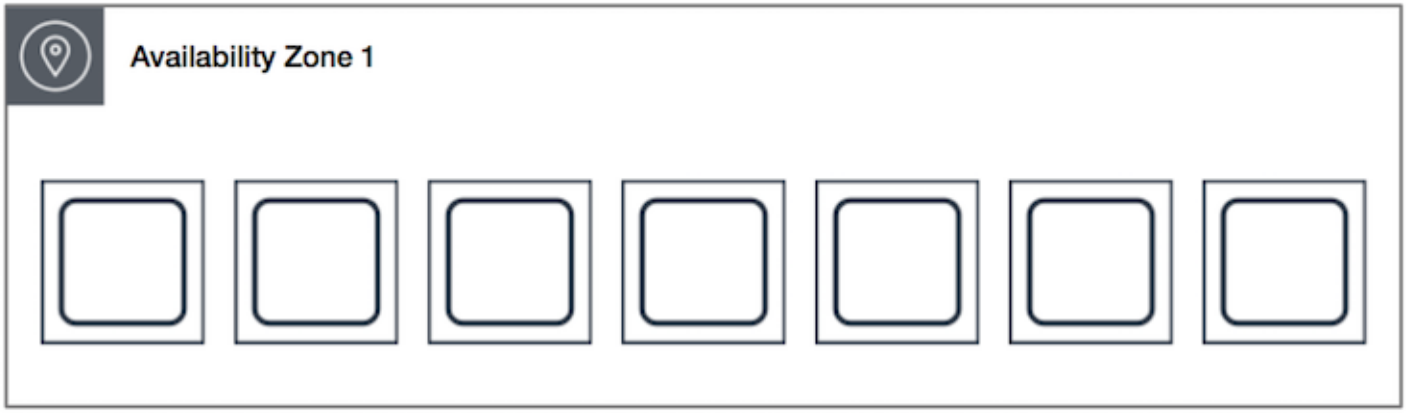
Eine Spread-Placement-Gruppe ist eine Gruppe von Instances, die jeweils auf einer bestimmten Hardware platziert werden.

Spread Placement-Gruppen werden für Anwendungen mit einer geringen Anzahl kritischer Instances empfohlen, die getrennt voneinander gehalten werden sollten. Das Launchen von Instances in einer Placement-Gruppe auf Spread-Ebene reduziert das Risiko gleichzeitiger Ausfälle, die auftreten können, wenn Instances dieselbe Ausstattung nutzen. Placement-Gruppen auf Spread-Ebene bieten Zugriff auf separate Hardware und eignen sich daher für die Vermischung von Instance-Typen oder das Launchen über eine Zeit hinweg.

Wenn Sie eine Instance in einer Spread-Placement-Gruppe starten und es nicht genügend eindeutige Hardware zur Erfüllung der Anforderung gibt, schlägt die Anforderung fehl. Amazon EC2 stellt mit der Zeit mehr eindeutig identifizierbare Hardware zur Verfügung, sodass Sie die Anforderung später erneut versuchen können. Placement-Gruppen können Instances auf Racks oder Hosts verteilen. Verteilte Platzierungsgruppen auf Rack-Level können in verschiedenen AWS Regionen und mehr verwendet werden AWS Outposts. Spread-Platzierungsgruppen auf Host-Ebene können AWS Outposts nur mit verwendet werden.

Spread-Platzierungsgruppen auf Rack-Ebene

Das folgende Image zeigt sieben Instances in einer einzelnen Availability Zone, die in einer Spread Placement-Gruppe platziert sind. Die sieben Instances sind in sieben verschiedenen Racks untergebracht, wobei jedes Rack über ein eigenes Netzwerk und eine eigene Stromquelle verfügt.



Eine verteilte Platzierungsgruppe auf Rackebene kann sich über mehrere Availability Zones in derselben Region erstrecken. In einer Region kann eine Spread-Platzierungsgruppe auf Rackebene maximal sieben laufende Instances pro Availability Zone pro Gruppe haben. Mit Outposts kann eine verteilte Platzierungsgruppe auf Rackebene so viele Instances aufnehmen, wie Sie Racks in Ihrer Outpost-Bereitstellung haben.

Spread-Placement-Gruppen auf Host-Ebene

Spread Placement-Gruppen auf Host-Ebene sind nur mit verfügbar. AWS Outposts Eine Platzierungsgruppe auf Host-Spread-Level kann so viele Instances aufnehmen, wie Sie Hosts in Ihrer Outpost-Bereitstellung haben. Weitere Informationen finden Sie unter the section called “Platzierungsgruppen auf AWS Outposts”.

Regeln und Einschränkungen von Placement-Gruppen

Themen

Allgemeine Regeln und Einschränkungen

Beachten Sie vor der Verwendung von Placement-Gruppen die folgenden Regeln:

- Sie können in jeder Region maximal 500 Placement-Gruppen pro Konto erstellen.
- Der Name, den Sie für eine Placement-Gruppe angeben, muss in Ihrem AWS -Konto für die Region eindeutig sein.
- Es ist nicht möglich, Placement-Gruppen zusammenzuführen.
- Eine Instance kann jeweils in einer Placement-Gruppe gestartet werden. Sie kann nicht mehrere Placement-Gruppen übergreifen.
- Kapazitätsreservierungen auf Abruf und zonale Reserved Instances ermöglichen es Ihnen, Kapazität für EC2-Instances in Availability Zones zu reservieren. Wenn Sie eine Instance starten und die Instance-Attribute denen entsprechen, die in einer On-Demand-Kapazitätsreservierung oder einer zonalen Reserved Instance angegeben wurden, wird die reservierte Kapazität automatisch von der Instance verwendet. Dies gilt auch, wenn Sie die Instance in einer Platzierungsgruppe starten.

  Wenn Sie planen, Instances in einer Cluster-Placement-Gruppe zu starten, empfehlen wir, dass Sie Kapazität explizit in der Cluster-Placement-Gruppe reservieren. Sie können dies tun, indem Sie eine On-Demand-Kapazitätsreservierung in einer bestimmten Cluster Placement-Gruppe erstellen. Beachten Sie, dass Sie mit On-Demand-Kapazitätsreservierungen zwar Kapazität auf diese Weise reservieren können, dies jedoch nicht mit zonalen Reserved Instances möglich ist, da diese Kapazitäten nicht explizit in einer Platzierungsgruppe reservieren können.

- Sie können Dedicated Hosts nicht in Placement-Gruppen starten.
- Sie können keine Spot-Instance starten, die so konfiguriert ist, dass sie bei einer Unterbrechung in einer Platzierungsgruppe angehalten oder in den Ruhezustand versetzt wird.

Regeln und Einschränkungen für Cluster Placement-Gruppen

Für Cluster Placement-Gruppen gelten die folgenden Regeln:

- Die folgenden Instance-Typen werden unterstützt:
  - Instances der aktuellen Generation, mit Ausnahme von Instances mit hoher Leistung (z. B. T2), Mac1-Instances und M7i-Flex-Instances.
  - Die folgenden Instances der vorherigen Generation: A1, C3, C4, I2, M4, R3 und R4.
- Eine Cluster Placement-Gruppe kann nicht übergreifend für mehrere Availability Zones gelten.
- Die maximale Netzwerk-Durchsatzgeschwindigkeit von Datenverkehr zwischen zwei Instances einer Cluster Placement-Gruppe richtet sich nach der langsameren der beiden Instances und ist entsprechend begrenzt. Wählen Sie für Anwendungen, die einen hohen Durchsatz erfordern, einen Instance-Typ mit einer Netzwerkkonnektivität, die Ihren Anforderungen entspricht.
- Für Instances, die Enhanced Networking unterstützen, gelten die folgenden Regeln:
  - Instances innerhalb einer Cluster Placement-Gruppe können bis zu 10 Gbit/s für Single-Flow-Verkehr verwenden. Instances außerhalb einer Cluster-Placement-Gruppe können bis zu 5 Gbit/s für Single-Flow-Verkehr verwenden.
  - Datenverkehr zu und von Amazon S3-Buckets innerhalb der gleichen Region über den öffentlichen IP-Adressraum oder durch einen VPC-Endpunkt kann die gesamte verfügbare aggregierte Bandbreite der Instance nutzen.
- In einer Cluster Placement-Gruppe können mehrere Instance-Typen gestartet werden. Dadurch verringert sich aber die Wahrscheinlichkeit, dass die erforderliche Kapazität vorhanden und der Startvorgang erfolgreich ist. Wir empfehlen Ihnen, für alle Instances einer Cluster Placement-Gruppe den gleichen Instance-Typ zu verwenden.
- Der Netzwerkverkehr zum Internet und über eine AWS Direct Connect Verbindung zu lokalen Ressourcen ist für Cluster-Platzierungsgruppen auf 5 Gbit/s begrenzt.

Regeln und Einschränkungen für Partition-Placement-Gruppe

Für Partitions-Placement-Gruppen gelten die folgenden Regeln:

- Eine Partition-Placement-Gruppe unterstützt maximal sieben Partitionen pro Availability Zone. Die Anzahl von Instances, die Sie in einer Partition-Placement-Gruppe starten können, ist nur durch die Begrenzungen in Ihrem Konto limitiert.
- Wenn Instances in einer Partitions-Placement-Gruppe gestartet werden, versucht Amazon EC2, die Instances gleichmäßig auf alle Partitionen zu verteilen. Amazon EC2 garantiert keine gleichmäßige Verteilung von Instances auf alle Partitionen.
- Eine Partition-Placement-Gruppe mit Dedicated Instances kann maximal zwei Partitionen umfassen.
- Kapazitätsreservierungen reservieren keine Kapazität in einer Partition-Placement-Gruppe.

Regeln und Einschränkungen für Spread Placement-Gruppen

Für Spread Placement-Gruppen gelten die folgenden Regeln:

- Eine Rack-Spread-Placement-Gruppen unterstützt maximal sieben laufende Instances pro Availability Zone. In einer Region mit drei Availability Zones können Sie beispielsweise insgesamt 21 Instances in der Gruppe ausführen, mit sieben Instances in jeder Availability Zone. Wenn Sie versuchen, eine achte Instance innerhalb derselben Availability Zone und in derselben Spread Placement-Gruppe zu starten, wird die Instance nicht gestartet. Wenn Sie mehr als sieben Instances in einer Availability Zone benötigen, empfehlen wir Ihnen, mehrere Spread-Placement-Gruppen zu verwenden. Die Verwendung mehrerer Spread-Placement-Gruppen garantiert nicht die Verteilung der Instances zwischen den Gruppen, stellt aber die Verteilung für jede Gruppe sicher, um den Einfluss von bestimmten Fehlerklassen zu begrenzen.
- Spread Placement-Gruppen werden für Dedicated Instances nicht unterstützt.
- Spread Placement-Gruppen auf Hostebene werden nur für Platzierungsgruppen unterstützt, die aktiviert sind. AWS Outposts Eine Spread Placement-Gruppe auf Host-Ebene kann so viele Instances enthalten, wie Sie Hosts in Ihrer Outpost-Bereitstellung haben.
- In einer Region kann eine Spread Placement-Gruppe auf Rack-Level maximal sieben laufende Instances pro Availability Zone pro Gruppe haben. Somit AWS Outposts kann eine verteilte Platzierungsgruppe auf Rackebene so viele Instances aufnehmen, wie Sie Racks in Ihrer Outpost-Bereitstellung haben.
- Kapazitätsreservierungen reservieren keine Kapazität in einer Spread-Placement-Gruppe.

Mit Platzierungsgruppe arbeiten

Inhalt

Erstellen einer Placement-Gruppe

Sie können eine Placement-Gruppe mit einer der folgenden Methoden erstellen.

Console

So erstellen Sie eine Placement-Gruppe mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Placement Groups (Placement-Gruppen).
3. Wählen Sie Platzierungsgruppe erstellen.
4. Geben Sie einen Namen für die Gruppe an.
5. Wählen Sie die Platzierungsstrategie für die Gruppe aus.
   - Wenn Sie Spread wählen, wählen Sie die Spread-Ebene.
     - Rack – keine Einschränkungen
     - Host – nur für Outposts
   - Wählen Sie bei Wahl von Partition die Anzahl der Partitionen innerhalb der Gruppe aus.
6. Um die Placement-Gruppe zu markieren, wählen Sie Add tag (Tag hinzufügen) und Geben Sie dann einen Schlüssel und einen Wert ein. Wählen Sie Add tag (Tag hinzufügen) für jedes Tag, das Sie hinzufügen möchten.
7. Wählen Sie Create group (Gruppe erstellen) aus.

AWS CLI

Um eine Platzierungsgruppe mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-placement-group. Im folgenden Beispiel wird eine Placement-Gruppe namens `my-cluster` erstellt, die die `cluster`-Platzierungsstrategie verwendet, und es wird ein Tag (Markierung) mit dem Schlüssel `purpose` und dem Wert `production` angewendet.

```
aws ec2 create-placement-group \
    --group-name my-cluster \
    --strategy cluster \
    --tag-specifications 'ResourceType=placement-
group,Tags={Key=purpose,Value=production}'
```

Um eine Partitionsplatzierungsgruppe zu erstellen, verwenden Sie AWS CLI

Verwenden Sie den Befehl create-placement-group. Geben Sie den `--strategy`-Parameter mit dem Wert `partition` an und geben Sie den `--partition-count`-Parameter mit der gewünschten Anzahl von Partitionen an. In diesem Beispiel erhält die Partition-Placement-Gruppe den Namen `HDFS-Group-A` und wird mit fünf Partitionen erstellt.

```
aws ec2 create-placement-group \
    --group-name HDFS-Group-A \
    --strategy partition \
    --partition-count 5
```

PowerShell

Um eine Platzierungsgruppe zu erstellen, verwenden Sie AWS Tools for Windows PowerShell

Verwenden Sie den New-EC2PlacementGroup-Befehl.

Informationen zur Platzierungsgruppe anzeigen

Sie können alle Ihre Platzierungsgruppen und die Informationen zu ihnen mit einer der folgenden Methoden anzeigen.

Console

Um Informationen zu einer oder mehreren Platzierungsgruppen anzuzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich unter Netzwerk und Sicherheit die Option Platzierungsgruppen aus.
3. In der Tabelle Platzierungsgruppen können Sie für jede Platzierungsgruppe die folgenden Informationen anzeigen:
   - Gruppenname — Der Name, den Sie der Platzierungsgruppe gegeben haben.
   - Gruppen-ID — Die ID der Platzierungsgruppe.
   - Strategie — Die Platzierungsstrategie für die Platzierungsgruppe.
   - Status — Der Status der Vermittlungsgruppe.
   - Partition — Die Anzahl der Partitionen. Nur gültig, wenn die Strategie Partition ist.
   - Gruppen-ARN — Der Amazon-Ressourcenname (ARN) der Platzierungsgruppe.

AWS CLI

Um all Ihre Platzierungsgruppen zu beschreiben

Verwenden Sie den Befehl describe-placement-groups AWS CLI .

```
aws ec2 describe-placement-groups
```

Beispielantwort

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster-pg",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789example",
            "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
        },
            ...
     ]
}
```

Um eine bestimmte Platzierungsgruppe zu beschreiben

Verwenden Sie den Befehl describe-placement-groups AWS CLI . Sie können entweder den oder den Parameter angeben. `--group-id` `--group-name`

Geben Sie die Platzierungsgruppen-ID an:

```
aws ec2 describe-placement-groups --group-id pg-0123456789example
```

Geben Sie den Namen der Platzierungsgruppe an:

```
aws ec2 describe-placement-groups --group-name my-cluster-pg
```

Beispielantwort

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster-pg",
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789example",
            "GroupArn": "arn:aws:ec2:eu-west-1:111111111111:placement-group/my-
cluster-pg"
        }
    ]
}
```

Markieren einer Placement-Gruppe

Zur leichteren Kategorisierung und Verwaltung vorhandener Placement-Gruppen können Sie diese mit benutzerdefinierten Metadaten markieren. Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

Wenn Sie eine Placement-Gruppe markieren, werden die Instances, die in der Placement-Gruppe gestartet werden, nicht automatisch markiert. Sie müssen die Instances, die in der Placement-Gruppe gestartet werden, explizit markieren. Weitere Informationen finden Sie unter Hinzufügen eines Tags (Markierung) beim Starten einer Instance.

Sie können Tags (Markierungen) mit einer der folgenden Methoden anzeigen, hinzufügen und löschen.

Console

So zeigen Sie ein Tag für eine vorhandene Placement-Gruppe an, fügen es hinzu oder löschen es

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Placement Groups (Placement-Gruppen).
3. Wählen Sie eine Placement-Gruppe aus, und wählen Sie dann Actions (Aktionen), Manage tags (Tags verwalten).
4. Im Bildschirm Tags verwalten werden alle Tags angezeigt, die der Platzierungsgruppe zugewiesen sind.
   - Um ein Tag (Markierunn) hinzuzufügen, wählen Sie Add tag (Tag (Markierung) hinzufügen) und geben Sie dann den Tag (Markierung)-Schlüssel und -Wert ein. Sie können bis zu 50 Tags pro Placement-Gruppe hinzufügen. Weitere Informationen finden Sie unter Tag (Markierung)-Einschränkungen.
   - Um ein Tag (Markierung) zu löschen, wählen Sie Remove (Entfernen) neben dem Tag (Markierung), das Sie löschen möchten.
5. Wählen Sie Speichern.

AWS CLI

So zeigen Sie Placement-Gruppen-Tags (Markierungen) an

Verwenden Sie den Befehl describe-tags, um die Tags (Markierungen) für die angegebene Ressource anzuzeigen. Im folgenden Beispiel beschreiben Sie die Tags (Markierungen) für alle Ihre Placement-Gruppen.

```
aws ec2 describe-tags \
    --filters Name=resource-type,Values=placement-group
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        },
        {
```

```
            "Key": "Environment",
            "ResourceId": "pg-9876543210EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

Sie können auch den Befehl describe-tags verwenden, um die Tags für eine Placement-Gruppe anzuzeigen, indem Sie deren ID angeben. Im folgenden Beispiel beschreiben Sie die Tags für pg-0123456789EXAMPLE.

```
aws ec2 describe-tags \

    --filters Name=resource-id,Values=pg-0123456789EXAMPLE
```

```
{
    "Tags": [
        {
            "Key": "Environment",
            "ResourceId": "pg-0123456789EXAMPLE",
            "ResourceType": "placement-group",
            "Value": "Production"
        }
    ]
}
```

Sie können die Tags einer Placement-Gruppe auch anzeigen, indem Sie die Placement-Gruppe beschreiben.

Verwenden Sie den Befehl describe-placement-groups, um die Konfiguration der angegebenen Placement-Gruppe anzuzeigen, die alle Tags enthält, die für die Placement-Gruppe angegeben wurden.

```
aws ec2 describe-placement-groups \
    --group-name my-cluster
```

```
{
    "PlacementGroups": [
        {
            "GroupName": "my-cluster",
```

```
            "State": "available",
            "Strategy": "cluster",
            "GroupId": "pg-0123456789EXAMPLE",
            "Tags": [
                {
                    "Key": "Environment",
                    "Value": "Production"
                }
            ]
        }
    ]
}
```

Um eine bestehende Platzierungsgruppe zu kennzeichnen, verwenden Sie AWS CLI

Sie können den Befehl create-tags verwenden, um vorhandene Ressourcen zu markieren. Im folgenden Beispiel wird die vorhandene Placement-Gruppe mit `Key=Cost-Center` und `Value=CC-123` gekennzeichnet.

```
aws ec2 create-tags \
    --resources pg-0123456789EXAMPLE \
    --tags Key=Cost-Center,Value=CC-123
```

Um ein Tag aus einer Platzierungsgruppe zu löschen, verwenden Sie AWS CLI

Mit dem Befehl delete-tags können Sie Tags (Markierungen) aus vorhandenen Ressourcen löschen. Beispiele finden Sie unter Examples (Beispiele) in der AWS CLI -Befehlsreferenz.

PowerShell

So zeigen Sie Placement-Gruppen-Tags (Markierungen) an

Verwenden Sie den Get-EC2Tag-Befehl.

So beschreiben Sie die Tags (Markierungen) für eine bestimmte Platzierungsgruppe

Verwenden Sie den Get-EC2PlacementGroup-Befehl.

So markieren Sie eine vorhandene Platzierungsgruppe

Verwenden Sie den New-EC2Tag-Befehl.

So löschen Sie ein Tag (Markierung) aus einer Platzierungsgruppe

Verwenden Sie den Remove-EC2Tag-Befehl.

Starten von Instances in einer Platzierungsgruppe

Sie können eine Instance in einer Placement-Gruppe starten, wenn die Placement-Gruppenregeln und -beschränkungen mit einer der folgenden Methoden erfüllt sind.

Console

So starten Sie Instances in einer Platzierungsgruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard der EC2-Konsole im Feld Instance starten die Option Instance starten. Füllen Sie das Formular wie angegeben aus und achten Sie darauf, dass Sie wie folgt vorgehen:
   - Wählen Sie unter Instance type (Instance-Typ) einen Instance-Typ aus, der in einer Platzierungsgruppe gelauncht werden kann.
   - Geben Sie im Feld Summary (Zusammenfassung) unter Number of instances (Anzahl von Instances) die Gesamtzahl der Instances an, die Sie in dieser Platzierungsgruppe benötigen, da Sie der Platzierungsgruppe später möglicherweise keine Instances mehr hinzufügen können.
   - Unter Advanced details (Erweiterte Details) können Sie bei Placement group name (Name der Platzierungsgruppe) wählen, ob Sie die Instances zu einer neuen oder bestehenden Platzierungsgruppe hinzufügen möchten. Wenn Sie eine Platzierungsgruppe mit einer Partitionsstrategie wählen, wählen Sie für Target partition (Ziel-Partition) die Partition, in der die Instances gelauncht werden sollen.

AWS CLI

So starten Sie Instances in einer Platzierungsgruppe

Verwenden Sie den Befehl run-instances und geben Sie den Placement-Gruppennamen über den `--placement "GroupName = my-cluster"`-Parameter an. In diesem Beispiel hat die Platzierungsgruppe den Namen `my-cluster`.

```
aws ec2 run-instances --placement "GroupName = my-cluster"
```

Um Instances in einer bestimmten Partition einer Partitionsplatzierungsgruppe zu starten, verwenden Sie den AWS CLI

Verwenden Sie den run-instances-Befehl und geben Sie den Placement-Gruppennnamen und die Partition über den `--placement "GroupName = HDFS-Group-A, PartitionNumber = 3"`-Parameter an. In diesem Beispiel hat die Platzierungsgruppe den Namen `HDFS-Group-A` und die Partitionsnummer lautet `3`.

```
aws ec2 run-instances --placement "GroupName = HDFS-Group-A, PartitionNumber = 3"
```

PowerShell

So starten Sie Instances in einer Platzierungsgruppe mithilfe von AWS Tools for Windows PowerShell

Verwenden Sie den New-EC2InstanceBefehl und geben Sie den Namen der Platzierungsgruppe mithilfe des `-Placement_GroupName` Parameters an.

Beschreiben von Instances in einer Platzierungsgruppe

Sie können die Platzierungsinformationen Ihrer Instances mit einer der folgenden Methoden anzeigen. Sie können Partitions-Placement-Gruppen auch nach der Partitionsnummer filtern, indem Sie die verwende AWS CLI.

Console

So zeigen Sie die Platzierungsgruppe und die Partitionsnummer einer Instance an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus.
4. Suchen Sie auf der Registerkarte Details unter Host- und Platzierungsgruppe nach der Platzierungsgruppe. Wenn die Instance keiner Platzierungsgruppe angehört, ist das Feld leer. Andernfalls enthält es den Namen der Platzierungsgruppe. Wenn die Placement-Gruppe eine Partition-Placement-Gruppe ist, enthält Partitionsnummer die Partitionsnummer für die Instance.

AWS CLI

So zeigen Sie die Partitionsnummer für eine Instance in einer Partition-Placement-Gruppe an

Verwenden Sie den describe-instances-Befehl und geben Sie den `--instance-id`-Parameter an.

```
aws ec2 describe-instances --instance-id i-0123a456700123456
```

Die Antwort enthält die Platzierungsinformationen, zu denen der Placement-Gruppennname und die Partitionsnummer der Instance zählen.

```
"Placement": {
     "AvailabilityZone": "us-east-1c",
     "GroupName": "HDFS-Group-A",
     "PartitionNumber": 3,
     "Tenancy": "default"
}
```

So filtern Sie Instances nach einer bestimmten Partition-Placement-Gruppe und Partitionsnummer

Verwenden Sie den describe-instances-Befehl und geben Sie den `--filters`-Parameter mit den `placement-group-name`- und `placement-partition-number`-Filtern an. In diesem Beispiel hat die Platzierungsgruppe den Namen `HDFS-Group-A` und die Partitionsnummer lautet `7`.

```
aws ec2 describe-instances --filters "Name = placement-group-name, Values = HDFS-
Group-A" "Name = placement-partition-number, Values = 7"
```

In der Antwort werden alle Instances aufgelistet, die sich in der angegebenen Partition innerhalb der angeführten Platzierungsgruppe befinden. Das folgende Ausgabebeispiel zeigt nur die Instance-ID, den Instance-Typ und die Platzierungsinformationen für die zurückgegebenen Instances an.

```
"Instances": [
                {
                    "InstanceId": "i-0a1bc23d4567e8f90",
                    "InstanceType": "r4.large",
                    },

                    "Placement": {
                        "AvailabilityZone": "us-east-1c",
                        "GroupName": "HDFS-Group-A",
                        "PartitionNumber": 7,
                        "Tenancy": "default"
```

```
                }

            {
                "InstanceId": "i-0a9b876cd5d4ef321",
                "InstanceType": "r4.large",
                },

                "Placement": {
                    "AvailabilityZone": "us-east-1c",
                    "GroupName": "HDFS-Group-A",
                    "PartitionNumber": 7,
                    "Tenancy": "default"
                }
        ],
```

Ändern der Platzierungsgruppe für eine Instance

Sie können die Platzierungsgruppe für eine Instance wie folgt ändern:

- Verschieben einer vorhandenen Instance in eine Platzierungsgruppe
- Verschieben einer Instance von einer Platzierungsgruppe in eine andere

Bevor Sie die Instance verschieben können, muss sich die Instance im Status `stopped` befinden.

Console

So verschieben Sie eine Instance in eine Platzierungsgruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und dann Instance-Status, Instance anhalten aus.
4. Wählen Sie bei ausgewählter Instance Aktionen, Instance-Einstellungen und Instance-Platzierung ändern.
5. Wählen Sie für Platzierungsgruppe die Platzierungsgruppe, in die die Instance verschoben werden soll.
6. Wählen Sie Speichern.

AWS CLI

So verschieben Sie eine Instance in eine Platzierungsgruppe

1. Beenden Sie die Instance mit dem Befehl stop-instances.
2. Verwenden Sie den Befehl modify-instance-placement und geben Sie den Namen der Platzierungsgruppe an, in die die Instance verschoben werden soll.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name MySpreadGroup
```

3. Starten Sie die Instance mit dem Befehl start-instances.

PowerShell

So verschieben Sie eine Instance in eine Platzierungsgruppe mithilfe der AWS Tools for Windows PowerShell

1. Stoppen Sie die Instanz mit dem Stop-EC2InstanceBefehl.
2. Verwenden Sie den Edit-EC2InstancePlacementBefehl und geben Sie den Namen der Platzierungsgruppe an, in die die Instanz verschoben werden soll.
3. Starten Sie die Instanz mit dem Start-EC2InstanceBefehl.

Entfernen einer Instance aus einer Platzierungsgruppe

Sie können eine Instance aus einer Platzierungsgruppe mit einer der folgenden Methoden entfernen.

Bevor Sie eine Instance aus einer Platzierungsgruppe entfernen können, muss sich die Instance im Status `stopped` befinden.

Console

So entfernen Sie eine Instance aus einer Platzierungsgruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und dann Instance-Status, Instance anhalten aus.

4. Wählen Sie bei ausgewählter Instance Aktionen, Instance-Einstellungen und Instance-Platzierung ändern.
5. Wählen Sie für Platzierungsgruppe die Option Keine aus.
6. Wählen Sie Speichern.

AWS CLI

So entfernen Sie eine Instance aus einer Platzierungsgruppe

1. Beenden Sie die Instance mit dem Befehl stop-instances.
2. Verwenden Sie den Befehl modify-instance-placement und geben Sie eine leere Zeichenfolge als Placement-Gruppennamen an.

```
aws ec2 modify-instance-placement \
    --instance-id i-0123a456700123456 \
    --group-name ""
```

3. Starten Sie die Instance mit dem Befehl start-instances.

PowerShell

So entfernen Sie eine Instance aus einer Platzierungsgruppe mithilfe der AWS Tools for Windows PowerShell

1. Stoppen Sie die Instanz mit dem Stop-EC2InstanceBefehl.
2. Verwenden Sie den Edit-EC2InstancePlacementBefehl und geben Sie eine leere Zeichenfolge für den Namen der Platzierungsgruppe an.
3. Starten Sie die Instanz mit dem Start-EC2InstanceBefehl.

Erstellen einer Platzierungsgruppe

Wenn Sie eine Platzierungsgruppe ersetzen müssen oder nicht mehr benötigen, können Sie sie löschen. Sie können eine Platzierungsgruppe mit einer der folgenden Methoden löschen.

Voraussetzung

Bevor Sie eine Platzierungsgruppe löschen können, darf sie keine Instances enthalten. Sie können alle Instances beenden, die Sie in der Platzierungsgruppe gestartet haben, Instances in eine andere Platzierungsgruppe verschieben oder Instances der Platzierungsgruppe entfernen.

Console

So löschen Sie eine Platzierungsgruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Placement Groups (Placement-Gruppen).
3. Wählen Sie die Platzierungsgruppe aus und wählen Sie Aktionen, Löschen.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`Delete`** ein und wählen Sie dann Löschen aus.

AWS CLI

So löschen Sie eine Platzierungsgruppe

Verwenden Sie den Befehl delete-placement-group und geben Sie den Placement-Gruppennamen an, um die Placement-Gruppe zu löschen. In diesem Beispiel lautet der Name der Platzierungsgruppe `my-cluster`.

```
aws ec2 delete-placement-group --group-name my-cluster
```

PowerShell

Um eine Platzierungsgruppe mit dem AWS Tools for Windows PowerShell

Verwenden Sie den Remove-EC2PlacementGroupBefehl, um die Platzierungsgruppe zu löschen.

Freigeben einer Placement-Gruppe

Durch die gemeinsame Nutzung von Platzierungsgruppen können Sie die Platzierung voneinander abhängiger Instances beeinflussen, die separaten AWS Konten gehören. Sie können eine Placement-Gruppe für mehrere AWS Konten oder innerhalb Ihrer Organisationen gemeinsam nutzen. Sie können Instances in einer freigegebenen Placement-Gruppe starten.

Ein Besitzer einer Placement-Gruppe kann eine Placement-Gruppe für folgendes freigeben:

- Bestimmte AWS Konten innerhalb oder außerhalb der Organisation
- eine Organisationseinheit innerhalb seiner -Organisation
- seine gesamte -Organisation

> **Note**
>
> Das AWS Konto, von dem aus Sie eine Placement-Gruppe teilen möchten, muss in der IAM-Richtlinie über die folgenden Berechtigungen verfügen.
>
> - `ec2:PutResourcePolicy`
> - `ec2:DeleteResourcePolicy`

Themen

Regeln und Einschränkungen

Die folgenden Regeln und Einschränkungen gelten, wenn Sie eine Placement-Gruppe freigeben oder wenn eine Placement-Gruppe mit Ihnen geteilt wird.

- Um eine Placement-Gruppe gemeinsam zu nutzen, müssen Sie sie in Ihrem AWS Konto besitzen. Sie können keine Placement-Gruppe freigeben, die für Sie freigegeben wurde.
- Wenn Sie eine Partition- oder eine Spread-Placement-Gruppe freigeben, ändern sich die Placement-Gruppenlimits nicht. Eine freigegebene Partition-Placement-Gruppe unterstützt maximal sieben Partitionen pro Availability Zone, und eine freigegebene verteilte Spread-Placement-Gruppe unterstützt maximal sieben laufende Instances pro Availability Zone.
- Um eine Platzierungsgruppe mit Ihrer Organisation oder einer Organisationseinheit in Ihrer Organisation gemeinsam zu nutzen, müssen Sie das Teilen mit aktivieren AWS Organizations. Weitere Informationen finden Sie unter Freigeben Ihrer AWS -Ressourcen.

- Sie sind dafür verantwortlich, die Ihnen gehörenden Instances in einer freigegebenen Placement-Gruppe zu verwalten.
- Sie können Instances und Kapazitätsreservierungen, die einer gemeinsam genutzten Placement-Gruppe zugeordnet sind, Ihnen aber nicht gehören, nicht anzeigen oder ändern.

Freigeben in mehreren Availability Zones

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes Konto zu. Dies könnte zu in mehreren Konten unterschiedlich benannten Availability Zones führen. Beispielsweise hat die Availability Zone `us-east-1a` für Ihr AWS Konto möglicherweise nicht denselben Standort wie `us-east-1a` für ein anderes AWS Konto.

Um den Ort Ihrer Dedicated Hosts relativ zu Ihren Konten zu bestimmen, verwenden Sie die Availability-Zone-ID (AZ-ID). Die Availability-Zone-ID ist eine eindeutige, konsistente Kennung für eine Availability Zone innerhalb aller AWS -Konten. Beispielsweise ist `use1-az1` eine Availability-Zone-ID für die `us-east-1`-Region und ist derselbe Speicherort in jedem AWS -Konto.

So lassen Sie sich die Availability-Zone-IDs für Availability Zones in Ihrem Konto anzeigen

1. Öffnen Sie die AWS RAM Konsole unter https://console.aws.amazon.com/ram.
2. Die Availability-Zone-IDs für die aktuelle Region werden unter Your AZ ID (Ihre AZ-ID) im rechten Feld angezeigt.

Freigeben einer Placement-Gruppe

Um eine Placement-Gruppe freigeben zu können, müssen Sie diese einer Ressourcenfreigabe hinzufügen. Eine Ressourcenfreigabe ist eine AWS RAM Ressource, mit der Sie Ihre Ressourcen für mehrere AWS Konten gemeinsam nutzen können. Eine Ressourcenfreigabe gibt die freizugebenden Ressourcen und die Konsumenten an, für die sie freigegeben werden.

Wenn Sie Teil einer Organisation sind und die AWS Organizations gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation Zugriff auf die gemeinsame Platzierungsgruppe.

Wenn die Placement-Gruppe mit einem AWS Account außerhalb Ihrer Organisation geteilt wird, erhält der AWS Kontoinhaber eine Einladung, der Resource Share beizutreten. Sie können auf die freigegebene Placement-Gruppe zugreifen, nachdem sie die Einladung angenommen haben.

Mithilfe von https://console.aws.amazon.com/ram oder können Sie eine Placement-Gruppe AWS für mehrere Konten gemeinsam nutzen AWS CLI.

AWS RAM console

Informationen über share a placement group (Eine Placement-Gruppe freigeben), die Ihnen gehört, mithilfe von https://console.aws.amazon.com/ram, finden Sie unter Erstellen einer Ressourcenfreigabe.

AWS CLI

Um eine Platzierungsgruppe, die Ihnen gehört, gemeinsam zu nutzen, verwenden Sie den Befehl create-resource-share.

Identifizieren einer freigegebene Placement-Gruppe

Der Amazon-Ressourcenname (ARN) einer Platzierungsgruppe enthält die 12-stellige Konto-ID des Kontos, dem die Platzierungsgruppe gehört. Sie können die Konto-ID verwenden, um den Besitzer einer Placement-Gruppe zu identifizieren, die mit Ihnen geteilt wurde.

Sie können den ARN der Platzierungsgruppe mit einer der folgenden Methoden ermitteln. Weitere Informationen finden Sie unter Informationen zur Platzierungsgruppe anzeigen.

Amazon EC2 console

Um eine gemeinsam genutzte Platzierungsgruppe zu identifizieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Netzwerk und Sicherheit die Option Placement Groups aus.
3. In der Tabelle Platzierungsgruppen sind alle Platzierungsgruppen aufgeführt, die Ihnen gehören und die mit Ihnen gemeinsam genutzt werden. In der Spalte Gruppen-ARN wird der ARN der Platzierungsgruppe angezeigt.

   Wenn die Spalte Gruppen-ARN nicht sichtbar ist, wählen Sie in der oberen rechten Ecke Einstellungen
   (),
   aktivieren Sie Gruppen-ARN und wählen Sie Bestätigen.

AWS CLI

Um eine gemeinsam genutzte Placement-Gruppe zu identifizieren

Verwenden Sie den `describe-placement-groups`Befehl, um alle Platzierungsgruppen aufzulisten, die Ihnen gehören und die mit Ihnen gemeinsam genutzt werden. In der Antwort zeigt der `GroupId` Parameter den ARN einer Platzierungsgruppe an.

Starten von Instances in einer freigegebenen Placement-Gruppe

> **Important**
>
> Wenn Sie die verwenden AWS CLI , um eine Instance in einer gemeinsam genutzten Placement-Gruppe zu starten, müssen Sie die Placement-Gruppen-ID mithilfe des `GroupId` Parameters angeben.

Sie können den Namen der Placement-Gruppe nur verwenden, wenn Sie der Besitzer der Placement-Gruppe sind, die gemeinsam genutzt wird. Wir empfehlen, die Platzierungsgruppen-ID zu verwenden, um mögliche Kollisionen zwischen Platzierungsgruppennamen zwischen AWS Konten zu vermeiden.

Sie finden die ID einer Placement-Gruppe in der Amazon EC2 EC2-Konsole auf dem Bildschirm Placement Groups oder mithilfe des `describe-placement-groups` AWS CLI Befehls. Weitere Informationen finden Sie unter Informationen zur Platzierungsgruppe anzeigen.

Console

Um Instances in einer gemeinsam genutzten Placement-Gruppe zu starten

1. Gehen Sie wie folgt vor, um eine Instance zu starten, starten Sie die Instance jedoch erst, wenn Sie die folgenden Schritte abgeschlossen haben, um die Einstellungen für die Placement-Gruppe anzugeben.
2. Wählen Sie unter Instance type (Instance-Typ) einen unterstützten Instance-Typ aus. Weitere Informationen finden Sie unter Regeln und Einschränkungen von Placement-Gruppen.
3. Erweitern Sie Erweiterte Details und konfigurieren Sie die Einstellungen für die Platzierungsgruppe wie folgt:

a. Wählen Sie unter Placement-Gruppe die Placement-Gruppe aus, die mit Ihnen geteilt wurde.

> **Note**
>
> Wenn Platzierungsgruppen mit demselben Namen vorhanden sind, überprüfen Sie die Platzierungsgruppen-ID, um sicherzustellen, dass Sie die richtige Platzierungsgruppe ausgewählt haben.

b. Wenn Sie eine Platzierungsgruppe mit einer Partitionsstrategie wählen, wählen Sie für Zielpartition die Partition aus, in der die Instance gestartet werden soll.

4. Gehen Sie im Übersichtsbereich wie folgt vor:

a. Geben Sie unter Number of instances (Anzahl der Instances) die Gesamtzahl der Instances ein, die Sie in dieser Platzierungsgruppe benötigen. Zu einen späteren Zeitpunkt können möglicherweise keine Instances mehr zur Platzierungsgruppe hinzugefügt werden.

b. Überprüfen Sie Ihre Instance-Konfiguration und wählen Sie dann Launch instance aus.

Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

AWS CLI

To launch instances in a shared placement group (So starten Sie Instances in einer freigegebenen Placement-Gruppe)

Verwenden Sie den `run-instances` Befehl und geben Sie die Platzierungsgruppen-ID der gemeinsam genutzten Platzierungsgruppe an.

```
aws ec2 run-instances –-placement "GroupId = pg-0123456789example"
```

To launch instances into a specific partition of a shared partition placement group(So starten Sie Instances in einer bestimmten Partition einer freigegebenen Partition-Placement-Gruppe)

Verwenden Sie den `run-instances` Befehl und geben Sie die Platzierungsgruppen-ID und die Partitionsnummer der gemeinsam genutzten Platzierungsgruppe an.

```
aws ec2 run-instances –-placement "GroupId = pg-0123456789example, PartitionNumber
 = 3"
```

> **Tip**
>
> Verwenden Sie VPC-Peering, um Instances zu verbinden, die separaten AWS Konten gehören, und nutzen Sie die vollen Latenzvorteile, die Shared Cluster Placement-Gruppen bieten. Weitere Informationen finden Sie unter Was ist VPC Peering?

Aufheben der Freigabe einer freigegebenen Placement-Gruppe

Der Placement-Gruppenbesitzer kann die Freigabe einer freigegebenen Placement-Gruppe jederzeit aufheben.

Wenn Sie die Freigabe einer freigegebenen Placement-Gruppen aufheben, werden die folgenden Änderungen wirksam.

- Die AWS Konten, mit denen eine Placement-Gruppe gemeinsam genutzt wurde, können keine Instances mehr starten oder Kapazitäten reservieren.
- Wenn Ihre Instances in einer gemeinsamen Placement-Gruppe ausgeführt wurden, werden sie von der Placement-Gruppe getrennt, laufen aber weiterhin normal in Ihrem AWS -Konto.
- Wenn Sie Kapazitätsreservierungen in einer gemeinsam genutzten Placement-Gruppe hatten, werden diese von der Placement-Gruppe getrennt, aber Sie haben weiterhin Zugriff darauf in Ihrem AWS Konto.

Sie können die Freigabe einer freigegebenen Placement-Gruppe mit einer der folgenden Methoden aufheben.

AWS RAM console

Weitere Informationen zum Aufheben der Freigabe einer Placement-Gruppe mithilfe von https://console.aws.amazon.com/ram finden Sie unter Löschen einer Ressourcenfreigabe.

AWS CLI

Verwenden Sie den Befehl disassociate-resource-share AWS Command Line Interface, um die gemeinsame Nutzung einer Placement-Gruppe aufzuheben.

Platzierungsgruppen auf AWS Outposts

AWS Outposts ist ein vollständig verwalteter Service, der AWS Infrastruktur, Dienste, APIs und Tools auf Kundenstandorte ausdehnt. Durch den lokalen Zugriff auf die AWS verwaltete Infrastruktur AWS Outposts können Kunden Anwendungen vor Ort mit denselben Programmierschnittstellen wie in AWS Regionen erstellen und ausführen und gleichzeitig lokale Rechen- und Speicherressourcen für geringere Latenz und lokale Datenverarbeitungsanforderungen nutzen.

Ein Outpost ist ein Pool von AWS Rechen- und Speicherkapazität, der am Standort eines Kunden bereitgestellt wird. AWS betreibt, überwacht und verwaltet diese Kapazität als Teil einer AWS Region.

Sie können Platzierungsgruppen auf Outposts erstellen, die Sie in Ihrem Konto angelegt haben. Auf diese Weise können Sie die Instances auf die zugrunde liegende Hardware auf einem Outpost an Ihrem Standort verteilen. Sie erstellen und verwenden Platzierungsgruppen auf Outposts auf die gleiche Weise wie Sie Platzierungsgruppen in regulären Availability Zones erstellen und verwenden. Wenn Sie eine Platzierungsgruppe mit einer Spread-Strategie auf einem Outpost erstellen, können Sie wählen, ob die Platzierungsgruppe Instances über Hosts oder Racks verteilt. Wenn Sie Instances auf Hosts verteilen, können Sie eine Spread-Strategie mit einem einzigen Rack-Outpost verwenden.

Überlegungen

- Eine verteilte Platzierungsgruppe auf Rackebene kann so viele Instances aufnehmen, wie Sie Racks in Ihrer Outpost-Bereitstellung haben.
- Eine Spread Placement-Gruppe auf Host-Ebene kann so viele Instances aufnehmen, wie Sie Hosts in Ihrer Outpost-Bereitstellung haben.

Voraussetzung

Sie müssen einen Outpost an Ihrem Standort installiert haben. Weitere Informationen finden Sie unter Outpost erstellen und die Kapazität dafür bestellen im AWS Outposts -Benutzerhandbuch.

So verwenden Sie eine Platzierungsgruppe für einen Outpost

1. Erstellen Sie ein Subnetz auf dem Outpost. Weitere Informationen finden Sie unter Erstellen eines Subnetzes im AWS Outposts -Benutzerhandbuch.
2. Erstellen Sie eine Platzierungsgruppe in der zugehörigen Region des Outposts. Wenn Sie eine Platzierungsgruppe mit einer Spread-Strategie erstellen, können Sie zwischen einer Verteilung auf Host- oder Rack-Ebene wählen, um zu bestimmen, wie die Gruppe die Instances auf die

zugrunde liegende Hardware in Ihrem Outpost verteilt. Weitere Informationen finden Sie unter the section called “Erstellen einer Placement-Gruppe”.

3. Launchen Sie eine Instance in die Platzierungsgruppe. Wählen Sie für Subnet (Subnetz) das Subnetz aus, das Sie in Schritt 1 erstellt haben, und für Placement group name (Name der Placement-Gruppe), wählen Sie die Platzierungsgruppe aus, die Sie in Schritt 2 erstellt haben. Weitere Informationen finden Sie unter Launch an Instance on your Outpost (Starten einer Instance auf Ihrem Outpost) im AWS Outposts -Benutzerhandbuch.

Netzwerk-MTU (Maximum Transmission Unit) für Ihre EC2-Instance

Die maximale Übertragungseinheit (MTU) einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Je größer die MTU einer Verbindung, desto mehr Daten können in einem einzelnen Paket übergeben werden. Ethernet-Rahmen bestehen aus dem Paket, also den eigentlichen Daten, die Sie senden, sowie aus den dazugehörigen Netzwerk-Overhead-Informationen.

Ethernet-Frames können in verschiedenen Formaten vorkommen, wobei das gängigste Format das standardmäßige Ethernet v2-Frameformat ist. Es unterstützt einen MTU-Wert von 1 500. Dies ist die größte unterstützte Ethernet-Paketgröße in den meisten Bereichen des Internets. Der maximal unterstützte MTU-Wert für eine Instance hängt von deren Instance-Typ ab.

Die folgenden Regeln gelten für Instances, die sich in Wavelength Zones befinden:

- Der Datenverkehr, der innerhalb einer VPC in derselben Wavelength-Zone von einer Instance zu einer anderen geht, hat eine MTU von 1300.
- Der Datenverkehr, der von einer Instance zur nächsten geht und die Carrier-IP innerhalb einer Wavelength-Zone verwendet, hat eine MTU von 1 500.
- Der Datenverkehr, der zwischen einer Wavelength-Zone und der Region, die eine öffentliche IP-Adresse verwendet, von einer Instance zur anderen führt, hat eine MTU von 1 500.
- Der Datenverkehr, der zwischen einer Wavelength-Zone und der Region, die eine private IP-Adresse verwendet, von einer Instance zur anderen führt, hat eine MTU von 1300.

Die folgenden Regeln gelten für Instances, die sich in Außenposten befinden:

- Der Datenverkehr, der von einer Instance in Outposts zu einer Instance in der Region geht, hat eine MTU von 1300.

Inhalt

Jumbo-Frames (9001 MTU)

Für Jumbo-Frames sind mehr als 1 500 Byte an Daten zulässig, indem die Nutzlastgröße pro Paket und somit der Prozentsatz des Pakets erhöht wird, bei dem es sich nicht um Paket-Overhead handelt. Es werden weniger Pakete benötigt, um die gleiche Menge an verwendbaren Daten zu übertragen. Der Verkehr ist jedoch in folgenden Fällen auf eine maximale MTU von 1 500 beschränkt:

- Datenverkehr über ein Internet-Gateway
- Datenverkehr über eine regionsübergreifende VPC-Peering-Verbindung
- Datenverkehr über VPN-Verbindungen
- Verkehr außerhalb einer bestimmten Region AWS

Sind die Pakete größer als 1 500 Byte, werden sie fragmentiert oder sie werden verworfen, wenn im IP-Header das Flag `Don't Fragment` gesetzt ist.

Jumbo-Frames sollten für Internet-Datenverkehr bzw. für Datenverkehr, der eine VPC verlässt, nur mit Vorsicht verwendet werden. Pakete werden durch zwischengeschaltete Systeme fragmentiert, sodass dieser Datenverkehr verlangsamt wird. Um Jumbo-Frames innerhalb einer VPC zu verwenden und dabei den Datenverkehr, der aus der VPC gesendet werden soll, nicht zu verlangsamen, können Sie die MTU-Größe nach Route konfigurieren oder mehrere Elastic Network-Schnittstellen mit unterschiedlichen MTU-Größen und Routen verwenden.

Bei Instances, die sich gemeinsam innerhalb einer Cluster Placement-Gruppe befinden, helfen Jumbo-Frames dabei, den maximal möglichen Netzwerkdurchsatz zu ermöglichen, und werden für diese Zwecke empfohlen. Weitere Informationen finden Sie unter Placement-Gruppen.

Sie können für Datenverkehr zwischen Ihren VPCs und Ihren On-Premises-Netzwerken über Jumbo-Frames verwende AWS Direct Connect. Weitere Informationen, einschließlich der Vorgehensweise

zur Überprüfung der Jumbo-Frame-Funktionen, finden Sie unter Festlegen des Netzwerk-MTU im Benutzerhandbuch zu AWS Direct Connect .

Alle Amazon EC2 EC2-Instance-Typen unterstützen 1500 MTU und alle Instance-Typen der aktuellen Generation unterstützen Jumbo Frames. Die folgenden Instance-Typen der vorherigen Generation unterstützen Jumbo-Frames: A1, C3, I2, M3 und R3.

Weitere Informationen zu den unterstützten MTU-Größen finden Sie hier:

- Für NAT-Gateways siehe NAT-Gateway Grundlagen im Amazon VPC Benutzerhandbuch.
- Für Transit-Gateways, siehe MTU im Amazon VPC Transit Gateways User Guide.
- Für lokale Zonen siehe Überlegungen im AWS Benutzerhandbuch für lokale Zonen.

Path MTU Discovery

Path MTU Discovery (PMTUD) wird verwendet, um den Pfad-MTU-Wert zwischen zwei Geräten zu ermitteln. Die Pfad-MTU ist die maximale Paketgröße, die auf dem Pfad zwischen dem sendenden Host und dem empfangenden Host unterstützt wird. Wenn es im Netzwerk zwischen zwei Hosts unterschiedliche MTU-Größen gibt, ermöglicht PMTUD dem empfangenden Host, mit einer ICMP-Nachricht für den ursprünglichen Host zu antworten. Diese ICMP-Nachricht weist den Ursprungshost an, die niedrigste MTU-Größe mit dem Netzwerkpfad zu verwenden und die Anforderung erneut zu senden. Ohne diese Verhandlung können Paketverluste auftreten, da die Anforderung für den empfangenden Host zu groß ist, um sie akzeptieren zu können.

Wenn ein Host ein Paket sendet, das größer als die MTU des empfangenden Hosts ist bzw. das größer als die MTU eines Geräts auf dem Pfad ist, löscht der empfangende Host bzw. das Gerät bei IPv4 das Paket und gibt dann die folgende ICMP-Meldung zurück: `Destination Unreachable: Fragmentation Needed and Don't Fragment was Set` (Typ 3, Code 4). Dies weist den übertragenden Host an, die Nutzlast in mehrere kleinere Pakete aufzuteilen und diese dann erneut zu übertragen.

Das IPv6-Protokoll unterstützt keine Fragmentierung im Netzwerk. Wenn ein Host ein Paket sendet, das größer als die MTU des empfangenden Hosts ist bzw. das größer als die MTU eines Geräts auf dem Pfad ist, löscht der empfangende Host bzw. das Gerät das Paket und gibt dann die folgende ICMP-Meldung zurück: `ICMPv6 Packet Too Big (PTB)` (Typ 2). Dies weist den übertragenden Host an, die Nutzlast in mehrere kleinere Pakete aufzuteilen und diese dann erneut zu übertragen.

Verbindungen, die über Komponenten wie NAT-Gateways und Load Balancer hergestellt werden, werden automatisch verfolgt. Das bedeutet, dass die Verfolgung von Sicherheitsgruppen für

ausgehende Verbindungsversuche automatisch aktiviert wird. Wenn Verbindungen automatisch verfolgt werden oder die Sicherheitsgruppenregeln eingehenden ICMP-Datenverkehr zulassen, können Sie PMTUD-Antworten erhalten.

Hinweis: Der ICMP-Datenverkehr kann auch dann blockiert werden, wenn der Datenverkehr auf Ebene der Sicherheitsgruppe zulässig ist, z. B. wenn ein Eintrag in der Liste der Netzwerkzugriffskontrolle den ICMP-Verkehr zum Subnetz verhindert.

> **Important**
>
> Path MTU Discovery garantiert nicht, dass Jumbo-Frames nicht von einigen Routern verworfen werden. Ein Internet-Gateway in Ihrer VPC leitet nur Pakete mit bis zu 1 500 Byte weiter. Für Internet-Datenverkehr empfehlen sich Pakete mit einem MTU-Wert von 1 500.

Überprüfen des Pfad-MTU-Werts zwischen zwei Hosts

Sie können die Pfad-MTU zwischen Ihrer EC2-Instance und einem anderen Host überprüfen. Sie können einen DNS-Namen oder eine IP-Adresse als Ziel angeben. Wenn das Ziel eine andere EC2-Instance ist, stellen Sie sicher, dass deren Sicherheitsgruppe eingehenden UDP-Verkehr zulässt.

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instance ab.

Linux-Instances

Führen Sie den tracepath Befehl auf Ihrer Instance aus, um den Pfad der MTU zwischen Ihrer EC2-Instance und dem angegebenen Ziel zu überprüfen. Dieser Befehl ist Teil des `iputils` Pakets, das standardmäßig in vielen Linux-Distributionen verfügbar ist.

In diesem Beispiel wird der Pfad MTU zwischen der EC2-Instance und überprüft. `amazon.com`

```
[ec2-user ~]$ tracepath amazon.com
```

In dieser Beispielausgabe ist die Pfad-MTU 1500.

```
1?: [LOCALHOST]      pmtu 9001
1:  ip-172-31-16-1.us-west-1.compute.internal (172.31.16.1)   0.187ms pmtu 1500
1:  no reply
2:  no reply
3:  no reply
```

```
 4:  100.64.16.241 (100.64.16.241)                      0.574ms
 5:  72.21.222.221 (72.21.222.221)                     84.447ms asymm 21
 6:  205.251.229.97 (205.251.229.97)                   79.970ms asymm 19
 7:  72.21.222.194 (72.21.222.194)                     96.546ms asymm 16
 8:  72.21.222.239 (72.21.222.239)                     79.244ms asymm 15
 9:  205.251.225.73 (205.251.225.73)                   91.867ms asymm 16
...
31:  no reply
     Too many hops: pmtu 1500
     Resume: pmtu 1500
```

Windows-Instances

Um die MTU des Pfads mit mturoute zu überprüfen

1. Laden Sie mturoute.exe es von http://www.elifulkerson.com/projects/mturoute.php auf Ihre EC2-Instance herunter.
2. Öffnen Sie ein Eingabeaufforderungsfenster und wechseln Sie zu dem Verzeichnis, in das Sie mturoute.exe heruntergeladen haben.
3. Verwenden Sie den folgenden Befehl, um den Pfad der MTU zwischen Ihrer EC2-Instance und dem angegebenen Ziel zu überprüfen. In diesem Beispiel wird die Pfad-MTU zwischen der EC2-Instance und überprüft. `www.elifulkerson.com`

   ```
   .\mturoute.exe www.elifulkerson.com
   ```

   In dieser Beispielausgabe ist die Pfad-MTU 1500.

   ```
   * ICMP Fragmentation is not permitted. *
   * Speed optimization is enabled. *
   * Maximum payload is 10000 bytes. *
   + ICMP payload of 1472 bytes succeeded.
   - ICMP payload of 1473 bytes is too big.
   Path MTU: 1500 bytes.
   ```

Überprüfen Sie die MTU für Ihre Instanz

Sie können den MTU-Wert für Ihre Instance überprüfen. Einige Instances sind so konfiguriert, dass sie Jumbo-Frames nutzen, während andere für die Nutzung von Standard-Framegrößen konfiguriert sind.

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instanz ab.

Linux-Instances

So überprüfen Sie die MTU-Einstellung auf einer Linux-Instance

Führen Sie den folgenden ip Befehl auf Ihrer EC2-Instance aus. Wenn die primäre Netzwerkschnittstelle nicht vorhanden ist`eth0`, `eth0` ersetzen Sie sie durch Ihre Netzwerkschnittstelle.

```
[ec2-user ~]$ ip link show eth0
```

In dieser Beispielausgabe gibt *`mtu 9001`* an, dass die Instanz Jumbo-Frames verwendet.

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc pfifo_fast state UP mode
 DEFAULT group default qlen 1000
    link/ether 02:90:c0:b7:9e:d1 brd ff:ff:ff:ff:ff:ff
```

Windows-Instances

Welches Verfahren Sie verwenden, hängt vom Treiber auf Ihrer Instanz ab.

ENA driver

Version 2.1.0 und höher

Verwenden Sie den folgenden Get-NetAdapterAdvancedProperty Befehl auf Ihrer EC2-Instance, um den MTU-Wert abzurufen. Verwenden Sie den Platzhalter (Sternchen), um alle Ethernet-Namen abzurufen. Suchen Sie in der Ausgabe nach dem Schnittstellennamen. `*JumboPacket` Der Wert 9015 bedeutet, dass Jumbo-Frames aktiviert sind. Jumbo-Frames sind standardmäßig deaktiviert.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet*"
```

Version 1.5 und früher

Verwenden Sie den folgenden Get-NetAdapterAdvancedProperty Befehl auf Ihrer EC2-Instance, um den MTU-Wert abzurufen. Suchen Sie in der Ausgabe nach dem Schnittstellennamen. `MTU` Ein Wert von 9001 zeigt an, dass Jumbo-Frames aktiviert sind. Jumbo-Frames sind standardmäßig deaktiviert.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

Intel SRIOV 82599 driver

Verwenden Sie den folgenden Get-NetAdapterAdvancedProperty Befehl auf Ihrer EC2-Instance, um den MTU-Wert abzurufen. Überprüfen Sie den Eintrag für die Schnittstelle mit dem Namen `*JumboPacket`. Ein Wert von 9014 zeigt an, dass Jumbo-Frames aktiviert sind. (Beachten Sie, dass in der MTU-Größe der Header und die Nutzlast enthalten sind.) Jumbo-Frames sind standardmäßig deaktiviert.

```
Get-NetAdapterAdvancedProperty -Name "Ethernet"
```

AWS PV driver

Verwenden Sie den folgenden Befehl auf Ihrer EC2-Instance, um den MTU-Wert abzurufen. Der Name der Schnittstelle kann hiervon abweichen. Suchen Sie in der Ausgabe nach einem Eintrag mit dem Namen „Ethernet“, „Ethernet 2“ oder „Local Area Connection“. Sie benötigen den Namen der Schnittstelle, um Jumbo-Frames zu aktivieren bzw. zu deaktivieren. Ein Wert von 9001 zeigt an, dass Jumbo-Frames aktiviert sind.

```
netsh interface ipv4 show subinterface
```

Stellen Sie die MTU für Ihre Instance ein

Möglicherweise möchten Sie Jumbo-Frames für den Netzwerkverkehr innerhalb Ihrer VPC und Standard-Frames für den Internetverkehr verwenden. Unabhängig von Ihrem Anwendungsfall empfehlen wir Ihnen, zu überprüfen, ob sich Ihre Instance wie erwartet verhält.

Welches Verfahren Sie verwenden, hängt vom Betriebssystem der Instanz ab.

Linux-Instances

So legen Sie den MTU-Wert auf einer Linux-Instance fest

1. Führen Sie den folgenden ip Befehl auf Ihrer Instance aus. Er setzt den gewünschten MTU-Wert auf 1500, aber Sie könnten stattdessen 9001 verwenden.

```
[ec2-user ~]$ sudo ip link set dev eth0 mtu 1500
```

2. (Optional) Um die MTU-Netzwerkeinstellung nach einem Neustart beizubehalten, müssen Sie die folgenden Konfigurationsdateien je nach verwendetem Betriebssystem ändern.

   - Fügen Sie für Amazon Linux 2 der Datei `/etc/sysconfig/network-scripts/ifcfg-eth0` die folgende Zeile hinzu:

     ```
     MTU=1500
     ```

     Fügen Sie der Datei `/etc/dhcp/dhclient.conf` die folgende Zeile hinzu:

     ```
     request subnet-mask, broadcast-address, time-offset, routers, domain-name,
      domain-search, domain-name-servers, host-name, nis-domain, nis-servers, ntp-
     servers;
     ```

   - Für Amazon Linux AMI fügen Sie Ihrer `/etc/dhcp/dhclient-eth0.conf` Datei die folgenden Zeilen hinzu.

     ```
     interface "eth0" {
     supersede interface-mtu 1500;
     }
     ```

   - Für andere Linux-Distributionen: Sehen Sie in der entsprechenden Dokumentation nach.

3. (Optional) Starten Sie Ihre Instance neu und vergewissern Sie sich, dass die MTU-Einstellung korrekt ist.

Windows-Instances

Welches Verfahren Sie verwenden, hängt vom Treiber auf Ihrer Instance ab.

ENA driver

Sie können die MTU mithilfe des Geräte-Managers oder des Set-NetAdapterAdvancedProperty Befehls auf Ihrer Instanz ändern.

Version 2.1.0 und höher

Verwenden Sie den folgenden Befehl, um Jumbo Frames zu aktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9015
```

Verwenden Sie den folgenden Befehl, um Jumbo-Frames zu deaktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

Version 1.5 und früher

Verwenden Sie den folgenden Befehl, um Jumbo Frames zu aktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 9001
```

Verwenden Sie den folgenden Befehl, um Jumbo-Frames zu deaktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "MTU" -
RegistryValue 1500
```

Intel SRIOV 82599 driver

Sie können die MTU mithilfe des Geräte-Managers oder des Set-NetAdapterAdvancedProperty Befehls auf Ihrer Instanz ändern.

Verwenden Sie den folgenden Befehl, um Jumbo Frames zu aktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 9014
```

Verwenden Sie den folgenden Befehl, um Jumbo-Frames zu deaktivieren.

```
Set-NetAdapterAdvancedProperty -Name "Ethernet" -RegistryKeyword "*JumboPacket" -
RegistryValue 1514
```

AWS PV driver

Sie können die MTU mithilfe des netsh Befehls auf Ihrer Instance ändern. Sie können die MTU nicht mit dem Geräte-Manager ändern.

Verwenden Sie den folgenden Befehl, um Jumbo Frames zu aktivieren.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=9001
```

Verwenden Sie den folgenden Befehl, um Jumbo-Frames zu deaktivieren.

```
netsh interface ipv4 set subinterface "Ethernet" mtu=1500
```

Fehlerbehebung

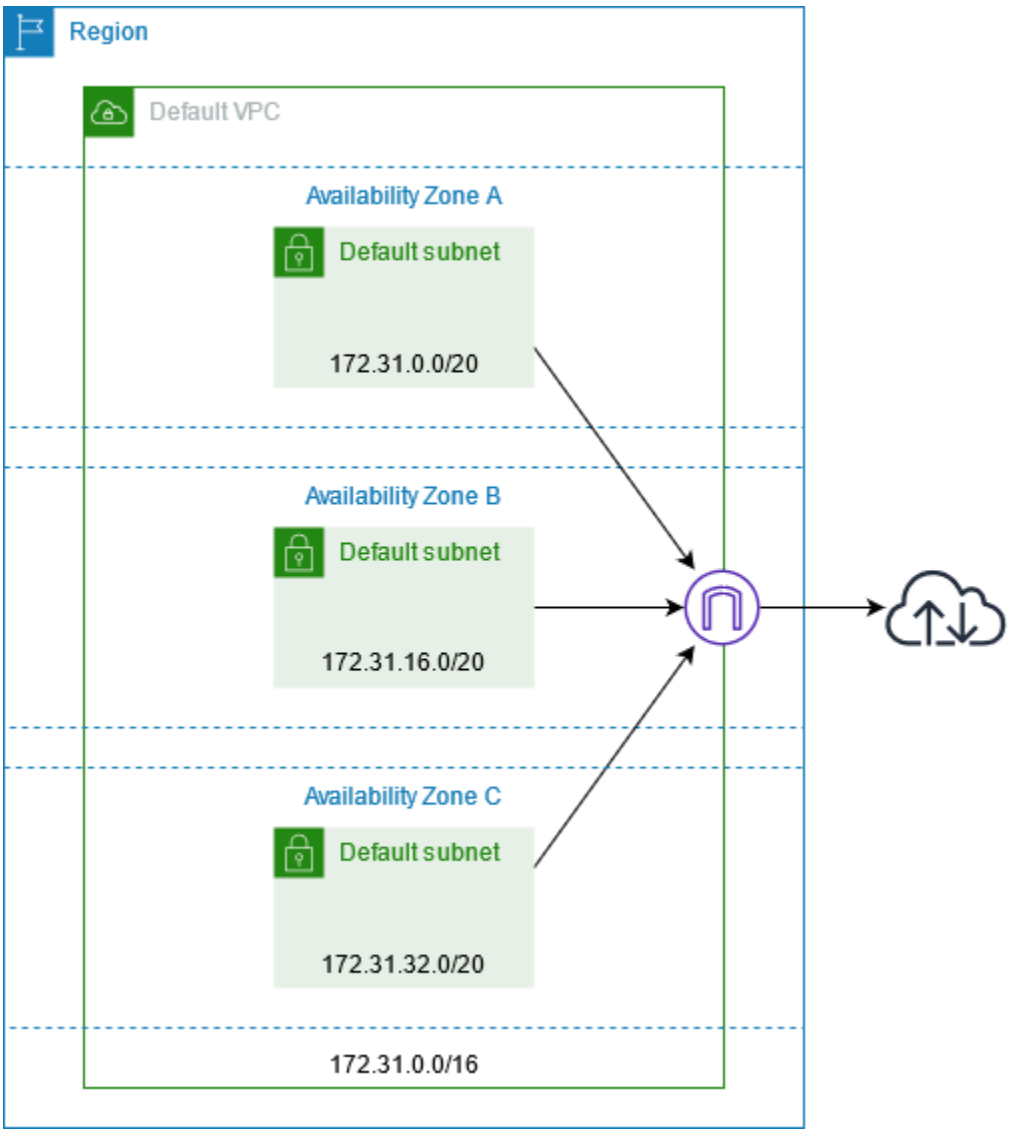
Wenn bei der Verwendung von Jumbo Frames Verbindungsprobleme zwischen Ihrer EC2-Instance und einem Amazon Redshift-Cluster auftreten, finden Sie weitere Informationen unter Abfragen, die hängen bleiben im Amazon Redshift Management Guide.

Virtuelle private Clouds für Ihre EC2-Instances

Amazon Virtual Private Cloud (Amazon VPC) ermöglicht es Ihnen, ein virtuelles Netzwerk in Ihrem eigenen logisch isolierten Bereich innerhalb der AWS Cloud zu definieren, das als virtuelle private Cloud oder VPC bezeichnet wird. Sie können AWS Ressourcen wie Amazon EC2 EC2-Instances in den Subnetzen Ihrer VPC erstellen. Ihre VPC ist einem herkömmlichen Netzwerk sehr ähnlich, das Sie möglicherweise in Ihrem eigenen Rechenzentrum betreiben, bietet jedoch die Vorteile, die mit der Nutzung der skalierbaren Infrastruktur von AWS einhergehen. Sie können Ihre VPC konfigurieren. Dazu ist es möglich, den IP-Adressbereich auszuwählen, Subnetze zu erstellen sowie Routing-Tabellen, Netzwerk-Gateways und Sicherheitseinstellungen zu konfigurieren. Sie können Instances in Ihrer VPC mit dem Internet oder Ihrem eigenen Rechenzentrum verbinden.

Ihre Standard-VPCs

Wenn Sie Ihr AWS Konto erstellen, erstellen wir in jeder Region eine Standard-VPC. Eine Standard-VPC ist eine VPC, die bereits vorkonfiguriert und betriebsbereit ist. In jeder Standard-VPC gibt es beispielsweise ein Standardsubnetz für jede Availability Zone, ein an die VPC angeschlossenes Internet-Gateway und eine Route in der Haupt-Routing-Tabelle, die den gesamten Datenverkehr (0.0.0.0/0) an das Internet-Gateway sendet. Alternativ können Sie Ihre eigene VPC erstellen und entsprechend Ihren Anforderungen konfigurieren.



Erstellen von zusätzlichen VPCs

Verwenden Sie das folgende Verfahren, um eine VPC mit den erforderlichen Subnetzen, Gateways und Routing-Konfigurationen zu erstellen.

So erstellen Sie eine VPC

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie VPC erstellen aus.
3. Wählen Sie unter Resources to create (Zu erstellende Ressourcen) die Option VPC and more (VPC und mehr) aus.

4. Geben Sie für die Name tag auto-generation (Automatische Generierung des Namens-Tags) einen Namen für die VPC ein.
5. Behalten Sie für den IPv4 CIDR block (IPv4-CIDR-Block) entweder den Standardvorschlag bei oder geben Sie den für Ihre Anwendung oder Ihr Netzwerk erforderlichen CIDR-Block ein.
6. Wählen Sie für Number of Availability Zones (Anzahl der Availability Zones) die Option 2, so dass Sie Instances in mehreren Availability Zones starten können, um eine hohe Verfügbarkeit sicherzustellen.
7. Wenn Ihre Instances über das Internet zugänglich sein müssen, führen Sie einen der folgenden Schritte aus:
   - Wenn sich Ihre Instances in einem öffentlichen Subnetz befinden können, wählen Sie einen Wert ungleich null für Number of public subnets (Anzahl der öffentlichen Subnetze) aus. Behalten Sie beide Optionen unter DNS options (DNS-Optionen) ausgewählt. Optional können Sie jetzt oder später private Subnetze hinzufügen.
   - Wenn sich Ihre Instances in einem privaten Subnetz befinden müssen, wählen Sie 0 für Number of public subnets (Anzahl der öffentlichen Subnetze) aus. Wählen Sie für Number of private subnets (Anzahl der privaten Subnetze) eine Zahl, die Ihren Anforderungen entspricht (die möglichen Werte entsprechen 1 oder 2 privaten Subnetzen pro Availability Zone). Wenn Ihre Instances in beiden Availability Zones ein erhebliches Volumen an Datenverkehr über die Availability Zones hinweg senden oder empfangen, wählen Sie für NAT gateways (NAT-Gateways) 1 per AZ (1 pro AZ) aus. Wählen Sie andernfalls In 1 AZ aus und starten Sie Instances, die zonenübergreifenden Datenverkehr in derselben Availability Zone wie das NAT-Gateway senden oder empfangen.
8. Erweitern Sie Customize subnet CIDR blocks (CIDR-Blöcke des Subnetzes anpassen). Behalten Sie entweder die Standardvorschläge bei oder geben Sie für jedes Subnetz einen CIDR-Block ein. Weitere Informationen finden Sie unter Subnetz-CIDR-Blöcke im Amazon-VPC-Benutzerhandbuch.
9. Überprüfen Sie den Bereich Preview (Vorschau), in dem die VPC-Ressourcen angezeigt werden, die basierend auf Ihrer Auswahl erstellt werden.
10. Wählen Sie VPC erstellen aus.

Zugriff auf das Internet über Ihre Instances

Instances, die in einem Standardsubnetz in einer Standard-VPC gestartet werden, haben Zugriff auf das Internet, da Standard-VPCs so konfiguriert sind, dass sie öffentliche IP-Adressen und

DNS-Hostnamen zuweisen, und die Haupt-Routing-Tabelle mit einer Route zu einem an die VPC angeschlossenen Internet-Gateway konfiguriert ist.

Für Instances, die Sie in nicht standardmäßigen Subnetzen und VPCs starten, können Sie eine der folgenden Optionen verwenden, um sicherzustellen, dass die Instances, die Sie in diesen Subnetzen starten, Zugriff auf das Internet haben:

- Konfigurieren Sie ein Internet-Gateway. Weitere Informationen finden Sie unter Verbinden mit dem Internet über ein Internet-Gateway im Amazon-VPC-Benutzerhandbuch.
- Konfigurieren Sie ein öffentliches NAT-Gateway. Weitere Informationen finden Sie unter Zugriff auf das Internet aus einem privaten Subnetz im Benutzerhandbuch für Amazon VPC.

Gemeinsam genutzte Subnetze

Beachten Sie beim Starten von EC2-Instances in gemeinsam genutzten VPC-Subnetzen Folgendes:

- Teilnehmer können Instances in einem gemeinsam genutzten Subnetz ausführen, indem sie die ID des gemeinsam genutzten Subnetzes angeben. Die Teilnehmer müssen Eigentümer aller von ihnen angegebenen Sicherheitsgruppen oder Netzwerkschnittstellen sein.
- Die Teilnehmer können Instances, die sie in einem gemeinsam genutzten Subnetz erstellt haben, starten, beenden und beschreiben. Teilnehmer können keine Instances starten, stoppen, beenden oder beschreiben, die der VPC-Besitzer im gemeinsam genutzten Subnetz erstellt hat.
- VPC-Besitzer können keine Instances starten, stoppen, beenden oder beschreiben, die von Teilnehmern in einem gemeinsam genutzten Subnetz erstellt wurden.
- Teilnehmer können mithilfe des EC2 Instance Connect Endpoint eine Verbindung zu einer Instance in einem gemeinsam genutzten Subnetz herstellen. Der Teilnehmer muss den EC2 Instance Connect-Endpunkt im gemeinsam genutzten Subnetz erstellen. Teilnehmer können keinen EC2 Instance Connect-Endpoint verwenden, den der VPC-Besitzer im gemeinsam genutzten Subnetz erstellt hat.

Weitere Informationen finden Sie unter Freigeben Ihrer VPC für andere Konten im Amazon-VPC-Benutzerhandbuch.

Nur IPv6-Subnetze

Eine EC2-Instance, die in einem reinen IPv6-Subnetz gestartet wird, erhält eine IPv6-Adresse, aber keine IPv4-Adresse. Bei allen Instances, die Sie in einem reinen IPv6-Subnetz starten, muss es sich um Instances handeln, die auf dem Nitro-System basieren. AWS

Sicherheit in Amazon EC2

Cloud-Sicherheit hat AWS höchste Priorität. Als AWS Kunde profitieren Sie von einem Rechenzentrum und einer Netzwerkarchitektur, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame Verantwortung von Ihnen AWS und Ihnen. Das Modell der übergreifenden Verantwortlichkeit beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der AWS Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Externe Prüfer testen und verifizieren regelmäßig die Wirksamkeit unserer Sicherheitsmaßnahmen im Rahmen der AWS . Weitere Informationen zu den Compliance-Programmen, die für Amazon EC2 gelten, finden Sie unter AWS Services in Scope by Compliance Program AWS .
- Sicherheit in der Cloud – Ihre Verantwortlichkeit umfasst die folgenden Bereiche.
  - Steuern des Netzwerkzugriffs auf Ihre Instances, z. B. durch die Konfiguration Ihrer VPC und Ihrer Sicherheitsgruppen. Weitere Informationen finden Sie unter Steuern des Netzwerkverkehrs.
  - Verwaltung der Anmeldedaten, die für die Verbindung mit Ihren Instances verwendet werden.
  - Verwaltung des Gastbetriebssystems und der Software, die für das Gastbetriebssystem bereitgestellt werden, einschließlich Updates und Sicherheitspatches. Weitere Informationen finden Sie unter Verwaltung von Updates für Amazon EC2 EC2-Windows-Instances.
  - Konfigurieren der IAM-Rollen, die an die Instance angehängt sind, und die mit diesen Rollen verknüpften Berechtigungen. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.

Diese Dokumentation zeigt Ihnen, wie Sie das Modell der übergreifenden Verantwortlichkeit bei der Verwendung von Amazon EC2 einsetzen können. Es zeigt Ihnen, wie Sie Amazon EC2 konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere AWS Dienste nutzen können, die Sie bei der Überwachung und Sicherung Ihrer Amazon EC2 EC2-Ressourcen unterstützen.

Inhalt

- Ausfallsicherheit in Amazon EC2
- Compliance-Validierung für Amazon EC2
- Identity and Access Management für Amazon EC2
- Zugreifen auf Amazon EC2 über einen Schnittstellen-VPC-Endpunkt
- Verwaltung von Updates für Amazon EC2 EC2-Windows-Instances
- Bewährte Sicherheitsmethoden für Windows-Instanzen
- Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances
- Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances
- NitroTPM
- Credential Guard für Windows-Instanzen

Datenschutz in Amazon EC2

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

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

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.

- Verwenden Sie erweiterte verwaltete Sicherheitsservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-2.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon EC2 oder anderen Geräten arbeiten und die Konsole AWS CLI, API oder AWS SDKs AWS-Services verwenden. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Inhalt

Datensicherheit bei Amazon EBS

Amazon-EBS-Volumes werden Ihnen als unformatierte Blockgeräte präsentiert. Diese logischen Geräte werden in der EBS-Infrastruktur erstellt und der Amazon-EBS-Service stellt sicher, dass die Geräte vor jeder (Wieder-)Verwendung durch einen Kunden logisch leer sind (d. h. die Rohblöcke werden auf Null gesetzt oder enthalten kryptografische pseudozufällige Daten).

Wenn Prozeduren erfordern, dass alle Daten mit einer bestimmten Methode gelöscht werden, entweder nach oder vor der Verwendung (oder beidem), wie z. B. in DoD 5220.22-M (National Industrial Security Program Operating Manual) oder NIST 800-88 (Guidelines for Media Sanitization), ist das in Amazon EBS entsprechend möglich. Diese Aktivität auf Blockebene wird auf die zugrunde liegenden Speichermedien im Amazon EBS-Service übertragen.

Verschlüsselung im Ruhezustand

EBS-Datenträger

Die Amazon EBS-Verschlüsselung ist eine Verschlüsselungslösung für Ihre EBS-Volumes und -Snapshots. Es benutzt AWS KMS keys. Weitere Informationen finden Sie unter Amazon EBS-Verschlüsselung im Amazon EBS-Benutzerhandbuch.

[Windows-Instanzen] Sie können auch Microsoft EFS- und NTFS-Berechtigungen für die Verschlüsselung auf Ordner- und Dateiebene verwenden.

Instance-Speicher-Volumes

Die Daten auf NVMe-Instance-Speichervolumes werden mit XTS-AES-256 verschlüsselt. Die Verschlüsselung ist auf einem Hardwaremodul der Instance implementiert. Die Schlüssel, die zum Verschlüsseln von Daten verwendet werden, welche auf lokal angefügte NVMe-Speichergeräte geschrieben werden, gelten pro Kunde und pro Volume. Die Schlüssel werden vom Hardwaremodul generiert, das für AWS -Personal unzugänglich ist, und befinden sich nur in diesem. Die Verschlüsselungsschlüssel werden vernichtet, wenn die Instance angehalten oder beendet wird, und können nicht wiederhergestellt werden. Sie können diese Verschlüsselung nicht deaktivieren und keine eigenen Verschlüsselungsschlüssel bereitstellen.

Die Daten auf HDD-Instance-Speichervolumes auf H1-, D3- und D3en-Instances werden mit XTS-AES-256 und Einmalschlüsseln verschlüsselt.

Wenn Sie eine Instance anhalten, in den Ruhezustand versetzen oder beenden, wird jeder Speicherblock im Instance-Speicher-Volume zurückgesetzt. Deshalb ist der Zugriff auf Ihre Daten nicht über den Instance-Speicher einer anderen Instance möglich.

Arbeitsspeicher

Die Speicherverschlüsselung ist auf den folgenden Instances aktiviert:

- Instanzen mit Graviton-Prozessoren AWS . AWS Graviton2, AWS Graviton3 und Graviton3E unterstützen die AWS Always-On-Speicherverschlüsselung. Die Verschlüsselungsschlüssel werden sicher im Hostsystem generiert, verlassen das Hostsystem nicht und werden zerstört, wenn der Host neu gestartet oder heruntergefahren wird. Weitere Informationen finden Sie unter AWS -Graviton-Processors.
- Instances mit skalierbaren Intel-Xeon-Prozessoren der 3. Generation (Ice Lake), z. B. M6i-Instances, und skalierbaren Intel-Xeon-Prozessoren der 4. Generation (Sapphire Rapids), z. B. M7i-Instances. Diese Prozessoren unterstützen eine immer aktive Speicherverschlüsselung mit Intel Total Memory Encryption (TME).
- Instances mit AMD-EPYC-Prozessoren der 3. Generation (Milan), z. B. M6a-Instances, und AMD-EPYC-Prozessoren der 4. Generation (Genoa), z. B. M7a-Instances. Diese Prozessoren

unterstützen eine immer aktive Speicherverschlüsselung mit AMD Secure Memory Encryption (SME). Instances mit AMD-EPYC-Prozessoren der 3. Generation (Milan) unterstützen auch AMD Secure Encrypted Virtualization-Secure Nested Paging (SEV-SNP).

Verschlüsselung während der Übertragung

Verschlüsselung auf physischer Ebene

Alle Daten, die über das AWS globale Netzwerk zwischen AWS Regionen fließen, werden auf der physischen Ebene automatisch verschlüsselt, bevor sie gesicherte Einrichtungen verlassen. AWS Der gesamte Datenverkehr zwischen AZs ist verschlüsselt. Zusätzliche Verschlüsselungsebenen, einschließlich der in diesem Abschnitt aufgeführten, bieten möglicherweise zusätzlichen Schutz.

Verschlüsselung durch Amazon VPC-Peering und regionsübergreifendes Transit Gateway Gateway-Peering

Der gesamte regionsübergreifende Datenverkehr, der Amazon VPC-Peering und Transit Gateway Gateway-Peering verwendet, wird automatisch massenverschlüsselt, wenn er eine Region verlässt. Auf der physischen Ebene wird automatisch eine zusätzliche Verschlüsselungsebene für den gesamten Datenverkehr bereitgestellt, bevor er AWS sichere Einrichtungen verlässt, wie bereits in diesem Abschnitt beschrieben.

Verschlüsselung zwischen den Instances

AWS bietet sichere und private Konnektivität zwischen EC2-Instances aller Typen. Darüber hinaus verwenden einige Instance-Typen die Offload-Funktionen der zugrunde liegenden Nitro-System-Hardware, um den Datenverkehr während der Übertragung zwischen Instances automatisch zu verschlüsseln. Diese Verschlüsselung verwendet AEAD-Algorithmen (Authenticated Encryption with Associated Data) mit 256-Bit-Verschlüsselung. Es gibt keine Auswirkungen auf die Netzwerkleistung. Um diese zusätzliche Verschlüsselung des Datenverkehrs während der Übertragung zwischen Instances zu unterstützen, müssen die folgenden Anforderungen erfüllt sein:

- Die Instances verwenden die folgenden Instance-Typen:
  - Allgemeiner Zweck: M5dn, M5n, M5Zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7g, M7GD, M7i, M7i-Flex
  - Computeroptimiert: C5a, C5ad, C5n, C6a, C6gn, C6i, C6id, C6in, C7a, C7g, C7GD, C7Gn, C7i, C7i-Flex

  - Speicheroptimiert: R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7g, R7gd, R7i, R7iz, U-3tb1, U-6tb1, U-9 tb1, U-12 tb1, U-18 tb1, U-24 tb1, U7i-12 TB, U7in-16 TB, U7in-16 TB 24 TB, U7-in-32 TB, X2IDN, X2iEDN, X2iEZN
  - Speicheroptimiert: D3, D3en, i3EN, i4G, i4I, i4GN, IS4Gen
  - Beschleunigte Datenverarbeitung: DL1, DL2q, G4ad, G4dn, G5, G6, Gr6, Inf1, Inf2, P3dn, P4d, P4de, P5, Trn1, Trn1n, VT1
  - Datenverarbeitung in Hochleistung: Hpc6a, Hpc6id, Hpc7a, Hpc7g
- Die Instances befinden sich in derselben Region.
- Die Instances befinden sich in derselben VPC oder in per Peering verbundenen VPCs und der Datenverkehr wird nicht durch ein virtuelles Netzwerkgerät, z. B. einen Load Balancer oder ein Transit Gateway, geleitet.

Auf der physischen Ebene wird automatisch eine zusätzliche Verschlüsselungsebene für den gesamten Datenverkehr bereitgestellt, bevor er sichere Einrichtungen verlässt, wie bereits in diesem Abschnitt erwähnt. AWS

So zeigen Sie die Instance-Typen an, die den Datenverkehr während des Transitverkehrs zwischen Instances mithilfe von AWS CLI verschlüsseln

Verwenden Sie den folgenden describe-instance-types-Befehl.

```
aws ec2 describe-instance-types \
    --filters Name=network-info.encryption-in-transit-supported,Values=true \
    --query "InstanceTypes[*].[InstanceType]" \
    --output text | sort
```

Verschlüsselung von und zu AWS Outposts

Ein Outpost stellt spezielle Netzwerkverbindungen her, die als Dienstlinks zu seiner AWS Heimatregion bezeichnet werden, und optional private Konnektivität zu einem von Ihnen angegebenen VPC-Subnetz. Der gesamte Datenverkehr über diese Verbindung ist vollständig verschlüsselt. Weitere Informationen finden Sie unter Konnektivität über Service-Links und Verschlüsselung während der Übertragung im AWS Outposts Benutzerhandbuch.

Verschlüsselung des Fernzugriffs

Die SSH- und RDP-Protokolle bieten sichere Kommunikationskanäle für den Fernzugriff auf Ihre Instances, sei es direkt oder über EC2 Instance Connect. Der Fernzugriff auf Ihre Instances mithilfe

von AWS Systems Manager Session Manager oder Run Command wird mit TLS 1.2 verschlüsselt, und Anfragen zum Herstellen einer Verbindung werden mit Sigv4 signiert und von authentifiziert und autorisiert. AWS Identity and Access Management

Es liegt in Ihrer Verantwortung, ein Verschlüsselungsprotokoll wie Transport Layer Security (TLS) zu verwenden, um sensible Daten bei der Übertragung zwischen Clients und Ihren Amazon-EC2-Instances zu verschlüsseln.

(Windows-Instanzen) Stellen Sie sicher, dass Sie nur verschlüsselte Verbindungen zwischen EC2-Instances und den AWS API-Endpunkten oder anderen sensiblen Remote-Netzwerkdiensten zulassen. Sie können dies über eine ausgehende Sicherheitsgruppe oder Windows-Firewall-Regeln erzwingen.

Infrastruktursicherheit in Amazon EC2

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

Sie verwenden AWS veröffentlichte API-Aufrufe, um über das Netzwerk auf Amazon EC2 zuzugreifen. Kunden müssen Folgendes unterstützen:

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

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

Weitere Informationen finden Sie unter Infrastructure Protection in the Security Pillar — AWS Well-Architected Framework.

Netzwerkisolierung

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk in Ihrem eigenen logisch isolierten Bereich in der AWS Cloud. Verwenden Sie separate VPCs, um die Infrastruktur nach Workload oder Organisationseinheit zu isolieren.

Ein Subnetz ist ein Bereich von IP-Adressen in einer VPC. Wenn Sie eine Instance starten, starten Sie sie in einem Subnetz in Ihrer VPC. Verwenden Sie Subnetze, um Ihre Anwendungsschichten (z. B. Web, Anwendung und Datenbank) innerhalb einer einzelnen VPC zu isolieren. Verwenden Sie für Ihre Instances private Subnetze, wenn Sie nicht direkt aus dem Internet erreichbar sein sollen.

Um die Amazon-EC2-API von Ihrer VPC aus mit privaten IP-Adressen aufzurufen, verwenden Sie AWS PrivateLink. Weitere Informationen finden Sie unter Zugreifen auf Amazon EC2 über einen Schnittstellen-VPC-Endpunkt.

Isolierung auf physischen Hosts

Verschiedene EC2-Instances auf demselben physischen Host werden so voneinander isoliert, als ob sie sich auf separaten physischen Hosts befinden. Der Hypervisor isoliert CPU und Speicher, und den Instances werden virtualisierte Festplatten anstelle des Zugriffs auf die Datenträger bereitgestellt.

Wenn Sie eine Instance stoppen oder beenden, wird der ihr zugewiesene Speicher vom Hypervisor gesäubert (mit Null überschrieben), bevor er einer neuen Instance zugewiesen wird. Jeder Speicherblock wird zurückgesetzt. Dadurch wird sichergestellt, dass Ihre Daten nicht unbeabsichtigt einer anderen Instance zugänglich gemacht werden.

Netzwerk-MAC-Adressen werden Instanzen von der AWS Netzwerkinfrastruktur dynamisch zugewiesen. IP-Adressen werden entweder dynamisch von der AWS -Netzwerkinfrastruktur oder von einem EC2-Administrator über authentifizierte API-Anfragen den Instances zugewiesen. Das AWS Netzwerk ermöglicht es Instanzen, Datenverkehr nur von den ihnen zugewiesenen MAC- und IP-Adressen zu senden. Andernfalls wird der Datenverkehr unterbrochen.

Standardmäßig kann eine Instance keinen Datenverkehr empfangen, der nicht speziell an sie gerichtet ist. Wenn Sie in Ihrer Instance Network Address Translation (NAT)-, Routing- oder Firewall-Services ausführen müssen, können Sie die Überprüfung der Quelle/des Ziel für die Netzwerkschnittstelle deaktivieren.

Steuern des Netzwerkverkehrs

Beachten Sie die folgenden Optionen zur Steuerung des Netzwerkverkehrs mit Ihren EC2-Instances:

- Beschränken Sie den Zugriff auf Ihre Instances über Sicherheitsgruppen. Konfigurieren Sie Regeln, die den minimal erforderlichen Netzwerkverkehr zulassen. Sie können beispielsweise nur Datenverkehr aus den Adressbereichen Ihres Unternehmensnetzwerks oder nur für bestimmte Protokolle wie HTTPS zulassen. Lassen Sie für Windows-Instances Windows-Verwaltungsdatenverkehr und minimale ausgehende Verbindungen zu.
- Nutzen Sie Sicherheitsgruppen als primären Mechanismus zur Steuerung des Netzwerkzugriffs auf Amazon EC2-Instances. Verwenden Sie bei Bedarf Netzwerk-ACLs sparsam, um zustandslose, grobkörnige Netzwerksteuerung zu ermöglichen. Sicherheitsgruppen sind vielseitiger als Netzwerk-ACLs aufgrund ihrer Fähigkeit, zustandsbehaftete Paketfilterungen durchzuführen und Regeln zu erstellen, die auf andere Sicherheitsgruppen verweisen. Netzwerk-ACLs können jedoch als sekundäres Steuerelement für die Verweigerung einer bestimmten Teilmenge des Datenverkehrs oder die Bereitstellung allgemeiner Subnetz-Schutzmechanismen wirksam sein. Da Netzwerk-ACLs für ein ganzes Subnetz gelten, können sie außerdem so verwendet werden, als ob defense-in-depth eine Instance versehentlich ohne die richtige Sicherheitsgruppe gestartet wird.
- [Windows-Instanzen] Verwalten Sie die Windows-Firewalleinstellungen zentral mit Gruppenrichtlinienobjekten (GPO), um die Netzwerksteuerung weiter zu verbessern. Kunden verwenden die Windows-Firewall häufig, um den Netzwerkverkehr besser zu erkennen und Sicherheitsgruppenfilter zu ergänzen, indem sie erweiterte Regeln erstellen, um den Zugriff auf bestimmte Anwendungen auf das Netzwerk zu blockieren oder den Datenverkehr von einer Teilmenge der IP-Adressen zu filtern. Beispielsweise kann die Windows-Firewall den Zugriff auf die IP-Adresse des EC2-Metadatenservices auf bestimmte Benutzer oder Anwendungen beschränken. Alternativ kann ein öffentlicher Service Sicherheitsgruppen verwenden, um den Datenverkehr auf bestimmte Ports zu beschränken, und die Windows-Firewall, um eine Liste explizit blockierter IP-Adressen zu führen.
- Verwenden Sie für Ihre Instances private Subnetze, wenn Sie nicht direkt aus dem Internet erreichbar sein sollen. Verwenden Sie einen Bastions-Host oder ein NAT-Gateway für den Internetzugriff von einer Instance in einem privaten Subnetz.
- [Windows-Instanzen] Verwenden Sie sichere Verwaltungsprotokolle wie RDP-Kapselung über SSL/TLS. Der Schnellstart zum Remote Desktop Gateway bietet bewährte Methoden für die Bereitstellung des Remote Desktop Gateway, einschließlich der Konfiguration von RDP für die Verwendung von SSL/TLS.
- [Windows-Instanzen] Verwenden Sie Active Directory oder, AWS Directory Service um den interaktiven Benutzer- und Gruppenzugriff auf Windows-Instanzen streng und zentral zu steuern und zu überwachen und lokale Benutzerberechtigungen zu vermeiden. Vermeiden Sie auch die Verwendung von Domain-Administratoren und erstellen Sie stattdessen detailliertere,

anwendungsspezifische rollenbasierte Konten. Just Enough Administration (JEA) ermöglicht die Verwaltung von Änderungen an Windows-Instances ohne interaktiven oder Administratorzugriff. Darüber hinaus ermöglicht JEA Unternehmen, den administrativen Zugriff auf die Teilmenge der PowerShell Windows-Befehle zu sperren, die für die Instanzverwaltung erforderlich sind. Weitere Informationen finden Sie im Whitepaper zu AWS Security Best Practices im Abschnitt „Verwalten des Zugriffs auf Betriebssystemebene auf Amazon EC2“.

- [Windows-Instanzen] Systemadministratoren sollten Windows-Konten mit eingeschränktem Zugriff für tägliche Aktivitäten verwenden und den Zugriff nur dann erhöhen, wenn dies für bestimmte Konfigurationsänderungen erforderlich ist. Greifen Sie darüber hinaus nur auf Windows-Instances direkt zu, wenn dies unbedingt erforderlich ist. Nutzen Sie stattdessen zentrale Konfigurationsmanagementsysteme wie EC2 Run Command, Systems Center Configuration Manager (SCCM), Windows PowerShell DSC oder Amazon EC2 Systems Manager (SSM), um Änderungen an Windows-Server zu übertragen.
- Konfigurieren Sie Amazon VPC-Subnetz-Routingtabellen mit den minimal erforderlichen Netzwerkrouten. Platzieren Sie beispielsweise nur Amazon EC2 EC2-Instances, die direkten Internetzugang benötigen, in Subnetzen mit Routen zu einem Internet-Gateway und platzieren Sie nur Amazon EC2 EC2-Instances, die direkten Zugriff auf interne Netzwerke benötigen, in Subnetzen mit Routen zu einem virtuellen privaten Gateway.
- Erwägen Sie, zusätzliche Sicherheitsgruppen oder Netwerk-Schnittstellen, um den Datenverkehr der Amazon Ec2-Instance-Verwaltung getrennt vom regulären Anwendungsdatenverkehr zu steuern und zu prüfen. Dieser Ansatz ermöglicht es Kunden, spezielle IAM-Richtlinien für die Änderungssteuerung zu implementieren, wodurch Änderungen an Sicherheitsgruppenregeln oder automatisierten Regelverifizierungsskripts leichter geprüft werden können. Die Verwendung mehrerer Netzwerkschnittstellen bietet auch zusätzliche Optionen zur Steuerung des Netzwerkverkehrs, einschließlich der Möglichkeit, hostbasierte Routing-Richtlinien zu erstellen oder unterschiedliche VPC-Subnetz-Routing-Regeln basierend auf dem zugewiesenen Subnetz der Netzwerkschnittstelle zu nutzen.
- Verwenden Sie AWS Virtual Private Network oder AWS Direct Connect , um private Verbindungen von Ihren Remote-Netzwerken zu Ihren VPCs herzustellen. Weitere Informationen finden Sie unter Verbindungsoptionen zwischen Netzwerk und Amazon VPC.
- Verwenden Sie VPC Flow-Protokolle, um den Datenverkehr zu überwachen, der Ihre Instances erreicht.
- Verwenden Sie den GuardDuty Malware-Schutz, um verdächtiges Verhalten auf Ihren Instances zu identifizieren, das auf bösartige Software hindeutet, die Ihre Arbeitslast gefährden, Ressourcen

für böswillige Zwecke wiederverwenden und sich unbefugten Zugriff auf Ihre Daten verschaffen könnte.

- Verwenden Sie GuardDuty Runtime Monitoring, um potenzielle Bedrohungen für Ihre Instanzen zu identifizieren und darauf zu reagieren. Weitere Informationen finden Sie unter So funktioniert Runtime Monitoring mit Amazon EC2 EC2-Instances.
- Verwenden Sie AWS Security HubReachability Analyzer oder Network Access Analyzer, um zu überprüfen, ob Ihre Instances unbeabsichtigt auf das Netzwerk zugreifen können.
- Verwenden Sie EC2 Instance Connect, um sich per Secure Shell (SSH) mit Ihren Instances zu verbinden, ohne dass Sie SSH-Schlüssel freigeben und verwalten müssen.
- Verwenden Sie AWS Systems Manager Session Manager, um remote auf Ihre Instanzen zuzugreifen, anstatt eingehende SSH- oder RDP-Ports zu öffnen und Schlüsselpaare zu verwalten.
- Verwenden Sie AWS Systems Manager Run Command, um allgemeine Verwaltungsaufgaben zu automatisieren, anstatt eine Verbindung zu Ihren Instanzen herzustellen.
- [Windows-Instanzen] Viele der Windows-Betriebssystemrollen und Microsoft-Geschäftsanwendungen bieten auch erweiterte Funktionen wie IP-Adressbereichsbeschränkungen innerhalb von IIS, TCP/IP-Filterrichtlinien in Microsoft SQL Server und Verbindungsfilterrichtlinien in Microsoft Exchange. Netzwerkeinschränkungsfunktionalität innerhalb der Anwendungsebene kann zusätzliche Verteidigungsebenen für kritische Geschäftsanwendungsserver bereitstellen.

Amazon VPC unterstützt zusätzliche Netzwerksicherheitskontrollen wie Gateways, Proxyserver und Netzwerküberwachungsoptionen. Weitere Informationen finden Sie unter Steuern des Netzwerkverkehrs im Amazon VPC-Benutzerhandbuch.

Ausfallsicherheit in Amazon EC2

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

Falls Sie Ihre Daten oder Anwendungen über größere geografische Distanzen hinweg replizieren müssen, verwenden Sie AWS -Local Zones. Eine AWS lokale Zone ist eine Erweiterung einer AWS

Region in geografischer Nähe zu Ihren Benutzern. Local Zones haben ihre eigenen Verbindungen mit dem Internet und unterstützen AWS Direct Connect. Wie alle AWS Regionen sind AWS Local Zones vollständig von anderen AWS Zonen isoliert.

Wenn Sie Ihre Daten oder Anwendungen in einer AWS lokalen Zone replizieren müssen, AWS empfiehlt es sich, eine der folgenden Zonen als Failover-Zone zu verwenden:

- Eine andere Local Zone
- Eine Availability Zone in der Region, bei der es sich nicht um die übergeordnete Zone handelt. Sie können den Befehl describe-availability-zones verwenden, um die übergeordnete Zone anzuzeigen.

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

Zusätzlich zur AWS globalen Infrastruktur bietet Amazon EC2 die folgenden Funktionen zur Unterstützung Ihrer Datenstabilität:

- Kopieren von AMIs über Regionen hinweg
- Kopieren von EBS-Snapshots über Regionen hinweg
- Automatisierung von EBS-gestützten AMIs mit Amazon Data Lifecycle Manager
- Automatisierung von EBS-Snapshots mit Amazon Data Lifecycle Manager
- Aufrechterhaltung der Funktionsfähigkeit und Verfügbarkeit Ihrer Flotte mit Amazon EC2 Auto Scaling
- Verteilung des eingehenden Datenverkehrs auf mehrere Instances in einer einzigen Availability Zone oder mehreren Availability Zones mit Elastic Load Balancing

Compliance-Validierung für Amazon EC2

Informationen darüber, ob AWS-Service ein AWS-Services in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter Umfang nach Compliance-Programm AWS-Services unter . Wählen Sie dort das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

Sie können Prüfberichte von Drittanbietern unter herunterladen AWS Artifact. Weitere Informationen finden Sie unter Berichte herunterladen unter .

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

- Schnellstartanleitungen zu Sicherheit und Compliance — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- Architecting for HIPAA Security and Compliance on Amazon Web Services — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

  > **Note**
  >
  > AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS Compliance-Ressourcen — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- AWS Leitfäden zur Einhaltung von Vorschriften für Kunden — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- Evaluierung von Ressourcen anhand von Regeln im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- AWS Security Hub— Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der Security-Hub-Steuerungsreferenz.
- Amazon GuardDuty — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen

wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.

- AWS Audit Manager— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Identity and Access Management für Amazon EC2

Ihre Sicherheitsnachweise identifizieren Sie gegenüber Diensten in AWS und gewähren Ihnen die uneingeschränkte Nutzung Ihrer AWS Ressourcen, wie z. B. Ihrer Amazon EC2 EC2-Ressourcen. Sie können anderen Benutzern, Services und Anwendungen mithilfe von Features in Amazon EC2 und AWS Identity and Access Management (IAM) die Nutzung Ihrer Amazon-EC2-Ressourcen erlauben, ohne Ihre Sicherheitsanmeldeinformationen freizugeben. Sie können IAM verwenden, um zu kontrollieren, wie andere Benutzer Ressourcen in Ihrem AWS Konto verwenden, und Sie können Sicherheitsgruppen verwenden, um den Zugriff auf Ihre Amazon EC2 EC2-Instances zu kontrollieren. Sie können die Verwendung der Amazon EC2-Ressourcen einschränken oder vollständig zulassen.

Bewährte Methoden für den Schutz Ihrer AWS Ressourcen mithilfe von IAM finden Sie unter Bewährte Sicherheitsmethoden in IAM.

Inhalt

Netzwerkzugriff auf die Instance

Eine Sicherheitsgruppe agiert als Firewall, die den zulässigen Verkehr steuert, der in eine oder mehrere -Instances eingeht. Wenn Sie eine Instance starten, können Sie diese einer oder mehreren Sicherheitsgruppen zuweisen. Sie fügen jeder Sicherheitsgruppe Regeln hinzu, um den Datenverkehr für die Instance zu kontrollieren. Diese Regeln können Sie jederzeit ändern, wobei die neuen Regeln

automatisch auf alle Instances angewendet werden, denen die entsprechende Sicherheitsgruppe zugeordnet ist.

Weitere Informationen finden Sie unter Sicherheitsgruppenregeln.

Amazon EC2-Berechtigungsattribute

Ihre Organisation hat möglicherweise mehrere AWS Konten. Mit Amazon EC2 können Sie zusätzliche AWS Konten angeben, die Ihre Amazon Machine Images (AMIs) und Amazon EBS-Snapshots verwenden können. Diese Berechtigungen gelten nur auf AWS Kontoebene. Sie können die Berechtigungen für bestimmte Benutzer innerhalb des angegebenen Kontos nicht einschränken. AWS Alle Benutzer des AWS -Kontos haben Zugriff auf das AMI bzw. den Snapshot.

Jedes AMI besitzt ein `LaunchPermission`-Attribut, das steuert, welche AWS -Konten Zugriff auf das AMI haben. Weitere Informationen finden Sie unter Veröffentlichen eines AMI.

Jeder Amazon EBS-Snapshot hat ein `createVolumePermission` Attribut, das steuert, welche AWS Konten den Snapshot verwenden können. Weitere Informationen finden Sie unter Einen Amazon EBS-Snapshot teilen im Amazon EBS-Benutzerhandbuch.

IAM und Amazon EC2

Mit IAM haben Sie folgende Möglichkeiten:

- Erstellen Sie Benutzer und Gruppen unter AWS-Konto
- Weisen Sie jedem Benutzer unter Ihrem eigenen Namen eindeutige Sicherheitsanmeldedaten zu AWS-Konto
- Kontrollieren Sie die Berechtigungen der einzelnen Benutzer zur Ausführung von Aufgaben unter Verwendung von AWS Ressourcen
- Erlauben Sie den Benutzern in einem anderen AWS-Konto , Ihre AWS Ressourcen gemeinsam zu nutzen
- Erstellen Sie Rollen für Sie AWS-Konto und definieren Sie die Benutzer oder Dienste, die diese übernehmen können
- Verwenden Sie bestehende Identitäten für Ihr Unternehmen, um Berechtigungen zur Ausführung von Aufgaben unter Verwendung von AWS Ressourcen zu erteilen

Wenn Sie IAM zusammen mit Amazon EC2 verwenden, können Sie steuern, ob Benutzer im Unternehmen eine Aufgabe mit bestimmten Amazon-EC2-API-Aktionen ausführen und bestimmte AWS -Ressourcen verwenden können.

In diesem Thema erhalten Sie Antworten zu den folgenden Fragen:

- Wie erstelle ich Gruppen und Benutzer in IAM?
- Wie erstelle ich eine Richtlinie?
- Welche IAM-Richtlinien benötige ich, um Aufgaben in Amazon EC2 durchzuführen?
- Wie erteile ich Berechtigungen, um Aktionen in Amazon EC2 auszuführen?
- Wie kann ich Berechtigungen gewähren, um Aktionen für bestimmte Ressourcen in Amazon EC2 auszuführen?

Erstellen von Benutzern, Gruppen und Rollen

Sie können Benutzer und Gruppen für Sie erstellen AWS-Konto und ihnen dann die erforderlichen Berechtigungen zuweisen. Als bewährte Methode sollten Benutzer die Berechtigungen erwerben, indem sie IAM-Rollen übernehmen.

Eine IAM-Rolle ist eine IAM-Identität, die Sie in Ihrem Konto mit bestimmten Berechtigungen erstellen können. Eine IAM-Rolle ähnelt einem IAM-Benutzer insofern, als es sich um eine AWS Identität mit Berechtigungsrichtlinien handelt, die festlegen, wofür die Identität zuständig ist und welche nicht. AWS Eine Rolle ist jedoch nicht einer einzigen Person zugeordnet, sondern kann von allen Personen angenommen werden, die diese Rolle benötigen. Einer Rolle sind außerdem keine standardmäßigen, langfristigen Anmeldeinformationen (Passwörter oder Zugriffsschlüssel) zugeordnet. Wenn Sie eine Rolle übernehmen, erhalten Sie stattdessen temporäre Anmeldeinformationen für Ihre Rollensitzung. Weitere Informationen zum Erstellen von IAM-Rollen und zum Erteilen von Berechtigungen finden Sie unter. the section called “IAM roles”

Verwandte Themen

Weitere Informationen zu IAM finden Sie unter:

- IAM-Richtlinien für Amazon EC2
- IAM-Rollen für Amazon EC2
- AWS Identity and Access Management (IAM)
- IAM Benutzerhandbuch

IAM-Richtlinien für Amazon EC2

Standardmäßig verfügen Benutzer nicht über die Berechtigung zum Erstellen oder Ändern von Amazon EC2-Ressourcen oder zum Ausführen von Aufgaben mithilfe der Amazon EC2-API, der Amazon EC2-Konsole oder der CLI. Damit Benutzer Ressourcen erstellen oder ändern und Aufgaben ausführen können, müssen Sie IAM-Richtlinien erstellen, die Benutzern die Berechtigung zur Verwendung der spezifischen Ressourcen und API-Aktionen gewähren, die sie benötigen. Anschließend fügen Sie diese Richtlinien den Benutzern, Gruppen oder IAM-Rollen an, die diese Berechtigungen benötigen.

Wenn Sie eine Richtlinie einem Benutzer, einer Benutzergruppe oder einer Rolle zuweisen, kann diese dem Benutzer die Berechtigung zur Durchführung der angegebenen Aufgaben auf den angegebenen Ressourcen gewähren oder verweigern. Weitere allgemeine Informationen zu IAM-Richtlinien finden Sie unter Berechtigungen und Richtlinien in IAM im IAM-Benutzerhandbuch. Weitere Informationen zum Verwalten und Erstellen von benutzerdefinierten IAM-Richtlinien finden Sie unter Verwalten von IAM-Richtlinien.

Erste Schritte

Eine IAM-Richtlinie erteilt bzw. verweigert die Berechtigungen, eine oder mehrere Amazon EC2-Aktionen auszuführen. Zudem muss die Richtlinie die Ressourcen benennen, die für diese Aktion verwendet werden dürfen. Dabei kann es sich um alle Ressourcen oder ggf. auch um bestimmte Ressourcen handeln. Eine Richtlinie kann auch Bedingungen enthalten, die für eine Ressource gelten.

Teilweise unterstützt Amazon EC2 auch Berechtigungen auf Ressourcenebene. Das heißt, dass Sie bei einigen EC2-API-Aktionen nicht angeben können, welche Ressource ein Benutzer für die Aktion verwenden darf. Stattdessen müssen Sie den Benutzern die Verwendung aller Ressourcen für diese Aktion gestatten.

Aufgabe	Topic
Grundlegende Struktur einer Richtlinie	Richtliniensyntax
Definieren von Aktionen in einer Richtlinie	Aktionen für Amazon EC2
Definieren von bestimmten Ressourcen in einer Richtlinie	Amazon-Ressourcennamen (ARNs) für Amazon EC2

Aufgabe	Topic
Anwenden von Bedingungen für die Verwendung der Ressourcen	Bedingungsschlüssel für Amazon EC2
Verwenden der verfügbaren Berechtigungen auf Ressourcenebene für Amazon EC2	Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2
Testen der Richtlinie	Prüfen, ob Benutzer über die erforderlichen Berechtigungen verfügen
Generieren einer IAM-Richtlinie	Generieren von Richtlinien basierend auf Zugriffsaktivitäten
Beispielrichtlinien für eine CLI oder ein SDK	Beispielrichtlinien für die Arbeit mit dem oder einem SDK AWS CLIAWS
Beispielrichtlinien für die Amazon EC2-Konsole	Beispielrichtlinien für die Arbeit in der Amazon EC2-Konsole

Gewähren von Berechtigungen für Benutzer, Gruppen und Rollen

Im Folgenden finden Sie Beispiele für einige AWS verwaltete Richtlinien, die Sie verwenden können, wenn sie Ihren Anforderungen entsprechen:

- `PowerUserAccess`
- `ReadOnlyAccess`
- `AmazonEC2FullAccess`
- `AmazonEC2ReadOnlyAccess`

Weitere Informationen finden Sie unter the section called “AWS verwaltete Richtlinien”.

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Richtlinienstruktur

In den folgenden Themen wird die Struktur einer IAM-Richtlinie erläutert.

Inhalt

Richtliniensyntax

Eine IAM-Richtlinie ist ein JSON-Dokument, das eine oder mehrere Anweisungen enthält. Jede Anweisung ist folgendermaßen strukturiert.

```
{
  "Statement":[{
    "Effect":"effect",
    "Action":"action",
    "Resource":"arn",
    "Condition":{
      "condition":{
        "key":"value"
        }
```

```
      }
    }
  ]
}
```

Eine Anweisung kann aus verschiedenen Elementen bestehen:

- Effect: Der effect-Wert kann `Allow` oder `Deny` lauten. -Benutzer verfügen standardmäßig nicht über die Berechtigung zur Verwendung von Ressourcen und API-Aktionen. Daher werden alle Anfragen abgelehnt. Dieser Standardwert kann durch eine explizite Zugriffserlaubnis überschrieben werden. Eine explizite Zugriffsverweigerung überschreibt jedwede Zugriffserlaubnis.
- Action: Mit action wird die API-Aktion spezifiziert, für die Sie Berechtigungen erteilen oder verweigern. Weitere Informationen zur Spezifizierung von action finden Sie unter Aktionen für Amazon EC2.
- Resource: Die von einer Aktion betroffene Ressource. Bei einigen Amazon EC2-API-Aktionen lassen sich bestimmte Ressourcen, die mit der Aktion erstellt oder geändert werden können, in die Richtlinie einbinden. Sie legen eine Ressource unter Verwendung eines Amazon-Ressourcennamens (ARN) oder eines Platzhalters (*) fest, um anzugeben, dass die Anweisung für alle Ressourcen gilt. Weitere Informationen finden Sie unter Unterstützte Berechtigungen auf Ressourcenebene für Amazon EC2-API-Aktionen.
- Condition: Bedingungen sind optional. Mit ihrer Hilfe können Sie bestimmen, wann Ihre Richtlinie wirksam ist. Weitere Informationen zur Angabe von Bedingungen für Amazon EC2 finden Sie unter Bedingungsschlüssel für Amazon EC2.

Weitere Informationen zu Richtlinienanforderungen finden Sie in der IAM-JSON-Richtlinienreferenz im IAM-Benutzerhandbuch. Beispiele mit IAM-Richtlinienanweisungen für Amazon EC2 finden Sie unter Beispielrichtlinien für die Arbeit mit dem oder einem SDK AWS CLIAWS.

Aktionen für Amazon EC2

In einer IAM-Richtlinienanweisung können Sie jede API-Aktion von jedem Service, der IAM unterstützt, angeben. Bei Amazon EC2 setzen Sie folgendes Präfix vor den Namen der API-Aktion: `ec2:`. Zum Beispiel `ec2:RunInstances` und `ec2:CreateImage`.

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

```
"Action": ["ec2:action1", "ec2:action2"]
```

Sie können auch mehrere Aktionen mittels Platzhaltern angeben. Beispielsweise können Sie alle Aktionen festlegen, deren Name mit dem Wort "Describe" beginnt:

```
"Action": "ec2:Describe*"
```

> **Note**
>
> Derzeit unterstützen die Amazon-EC2-Describe*-API-Aktionen Berechtigungen auf Ressourcenebene nicht. Weitere Informationen zu Berechtigungen auf Ressourcenebene für Amazon EC2 finden Sie unter IAM-Richtlinien für Amazon EC2.

Um alle Amazon EC2-API-Aktionen anzugeben, verwenden Sie den Platzhalter * folgendermaßen:

```
"Action": "ec2:*"
```

Eine Liste von Amazon-EC2-Aktionen finden Sie unter von Amazon EC2 definierte Aktionen in der Service-Autorisierungs-Referenz.

Unterstützte Berechtigungen auf Ressourcenebene für Amazon EC2-API-Aktionen

Berechtigungen auf Ressourcenebene bedeutet, dass Sie angeben können, für welche Ressourcen die Benutzer Aktionen ausführen dürfen. Amazon EC2 unterstützt teilweise Berechtigungen auf Ressourcenebene. Das heißt, Sie können bei bestimmten Amazon EC2-Aktionen kontrollieren, wann die Benutzer diese Aktionen verwenden dürfen. Dies basiert auf Bedingungen, die erfüllt sein müssen oder auf bestimmten Ressourcen, die von den Benutzern verwendet werden dürfen. Zum Beispiel können Sie Benutzern die Berechtigungen erteilen, Instances zu starten, aber nur für einen bestimmten Typ und nur mithilfe eines bestimmten AMI.

Um eine Ressource in einer IAM-Richtlinienanweisung anzugeben, verwenden Sie deren Amazon-Ressourcennamen (ARN). Mehr Informationen zur Angabe des ARN-Werts erhalten Sie unter Amazon-Ressourcennamen (ARNs) für Amazon EC2. Wenn eine API-Aktion einzelne ARNs nicht unterstützt, müssen Sie einen Platzhalter (*) verwenden, um anzugeben, dass alle Ressourcen von der Aktion betroffen sein können.

Tabellen, die identifizieren, welche Amazon EC2-API-Aktionen Berechtigungen auf Ressourcenebene unterstützen, und die ARNs und Bedingungsschlüssel, die Sie in einer Richtlinie verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Beachten Sie, dass Sie Tag (Markierungen)-basierte Berechtigungen auf Ressourcenebene in den IAM-Richtlinien anwenden können, die Sie für Amazon EC2-API-Aktionen verwenden. Dies ermöglicht Ihnen eine bessere Kontrolle darüber, welche Ressourcen ein Benutzer erstellen, ändern oder verwenden kann. Weitere Informationen finden Sie unter Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.

Amazon-Ressourcennamen (ARNs) für Amazon EC2

Jede IAM-Richtlinienanweisung gilt für die Ressourcen, die Sie mithilfe ihrer ARNs angegeben haben.

Ein ARN weist die folgende generelle Syntax auf:

```
arn:aws:[service]:[region]:[account-id]:resourceType/resourcePath
```

Service nicht zulässig

Der Service (z. B. `ec2`)

Region

Die Region für die Ressource (z. B. `us-east-1`)

account-id

Die AWS Konto-ID ohne Bindestriche (z. B.`123456789012`).

RessourcenTyp

Der Typ der Ressource (z. B. `instance`)

resourcePath

Ein Pfad zur Identifizierung der Ressource. Sie können in den Pfaden das Platzhalterzeichen Sternchen (*) verwenden.

Verwenden Sie beispielsweise den ARN wie folgt, um eine bestimmte Instance (`i-1234567890abcdef0`) in der Anweisung anzugeben.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

Sie können auch alle Instances angeben, die zu einem bestimmten Konto gehören, indem Sie das Platzhalterzeichen (*) folgendermaßen hinzufügen.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*"
```

Sie können auch alle Amazon EC2-Ressourcen angeben, die zu einem bestimmten Konto gehören, indem Sie das Platzhalterzeichen (*) folgendermaßen hinzufügen.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:*"
```

Wenn Sie alle Ressourcen angeben möchten oder wenn eine bestimmte API-Aktion keine ARNs unterstützt, verwenden Sie das Platzhalterzeichen Sternchen (*) wie folgt im `Resource`-Element.

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

Viele Amazon EC2-API-Aktionen umfassen mehrere Ressourcen. Beispielsweise fügt `AttachVolume` ein Amazon-EBS-Volume an eine Instance an, sodass ein Benutzer über Berechtigungen zum Verwenden des Volumes und der Instance verfügen muss. Um mehrere Ressourcen in nur einer Anweisung anzugeben, trennen Sie die ARNs wie folgt mit Kommas.

```
"Resource": ["arn1", "arn2"]
```

Eine Liste der ARNs für Amazon EC2-Ressourcen finden Sie unter Von Amazon EC2 definierte Ressourcentypen.

Bedingungsschlüssel für Amazon EC2

In einer Richtlinienanweisung können Sie optional Bedingungen angeben, mit denen gesteuert wird, wann die Richtlinie in Kraft tritt. Jede Bedingung enthält ein oder mehrere Schlüssel-Wert-Paare. Bei Bedingungsschlüsseln muss die Groß- und Kleinschreibung nicht beachtet werden. Wir haben AWS globale Bedingungsschlüssel sowie zusätzliche dienstspezifische Bedingungsschlüssel definiert.

Eine Liste der dienstspezifischen Bedingungsschlüssel für Amazon EC2 finden Sie unter Bedingungsschlüssel für Amazon EC2. Amazon EC2 implementiert auch die AWS globalen Bedingungsschlüssel. Für weitere Informationen vgl. In allen Anforderungen verfügbare Informationen im IAM-Benutzerhandbuch.

Verwenden Sie die `Condition`-Anweisung, um einen Bedingungsschlüssel in Ihrer IAM-Richtlinie zu verwenden. Die folgende Richtlinie gewährt Benutzern beispielsweise die Berechtigung, eingehende und ausgehende Regeln für jede Sicherheitsgruppe hinzuzufügen und zu entfernen.

Der `ec2:Vpc`-Bedingungsschlüssel wird verwendet, um anzugeben, dass diese Aktionen nur für Sicherheitsgruppen in einer bestimmten VPC ausgeführt werden können.

```
{
"Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupEgress"],
     "Resource": "arn:aws:ec2:region:account:security-group/*",
      "Condition": {
        "StringEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account:vpc/vpc-11223344556677889"
        }
      }
    }
  ]
}
```

Wenn Sie mehrere Bedingungen oder mehrere Schlüssel in einer einzelnen Bedingung angeben, werden diese mit einer logischen UND-Operation ausgewertet. Wenn Sie eine einzelne Bedingung mit mehreren Werten für einen Schlüssel angeben, wird die Bedingung mit einer logischen ODER-Operation ausgewertet. Damit die Berechtigungen erteilt werden, müssen alle Bedingungen erfüllt sein.

Bei der Angabe von Bedingungen können Sie auch Platzhalter verwenden. Weitere Informationen finden Sie unter IAM-Richtlinienelemente: Variablen und Tags (Markierungen) im IAM-Benutzerhandbuch.

Important

Einige API-Aktionen verwenden mehrere Ressourcen. Viele Bedingungsschlüssel sind jedoch ressourcenspezifisch. Wenn Sie eine Richtlinie mit einem Bedingungsschlüssel schreiben, legen Sie über das `Resource`-Element der Anweisung fest, für welche Ressource der Bedingungsschlüssel gültig ist. Andernfalls verhindert die Richtlinie möglicherweise, dass Benutzer die Aktion überhaupt ausführen, da die Bedingungsprüfung für die Ressourcen fehlschlägt, auf die der Bedingungsschlüssel nicht zutrifft. Wenn Sie keine Ressource angeben möchten oder über das `Action`-Element Ihrer Richtlinie mehrere API-Aktionen

hinzugefügt haben, müssen Sie mit dem `...IfExists`-Bedingungstyp sicherstellen, dass der Bedingungsschlüssel für die Ressourcen, die ihn nicht verwenden, ignoriert wird. Weitere Informationen finden Sie unter... IfExists Bedingungen im IAM-Benutzerhandbuch.

Alle Amazon EC2-Aktionen unterstützen die Bedingungsschlüssel `aws:RequestedRegion` und `ec2:Region`. Weitere Informationen finden Sie unter Beispiel: Beschränken des Zugriffs auf eine bestimmte Region.

`ec2:SourceInstanceARN`-Bedingungsschlüssel

Der `ec2:SourceInstanceARN`-Bedingungsschlüssel kann für Bedingungen verwendet werden, die den ARN der Instance angeben, von der aus eine Anfrage getätigt wird. Dies ist ein AWS globaler Bedingungsschlüssel und nicht dienstspezifisch. Für Beispiele für Richtlinien vgl. Amazon EC2: Volumes an EC2-Instances anfügen oder trennen und Beispiel: Erlauben Sie einer bestimmten Instanz, Ressourcen in anderen AWS Diensten anzuzeigen. Der `ec2:SourceInstanceARN`-Schlüssel kann nicht als Variable zur Angabe des ARN für das `Resource`-Element in einer Anweisung verwendet werden.

Beispiele mit Richtlinienanweisungen für Amazon EC2 finden Sie unter Beispielrichtlinien für die Arbeit mit dem oder einem SDK AWS CLIAWS.

`ec2:Attribute`-Bedingungsschlüssel

Der `ec2:Attribute`-Bedingungsschlüssel kann für Bedingungen verwendet werden, die den Zugriff nach einem Attribut einer Ressource filtern. Der Bedingungsschlüssel unterstützt nur Eigenschaften eines primitiven Datentyps (z. B. eine Zeichenfolge oder Ganzzahl) oder komplexe AttributeValueObjekte, die nur über eine Value-Eigenschaft verfügen (z. B. die Beschreibung oder ImdsSupportObjekte der ModifyImageAttribut-API-Aktion).

Important

Der Bedingungsschlüssel kann nicht für komplexe Objekte verwendet werden, die mehrere Eigenschaften haben, wie z. B. das LaunchPermissionObjekt der ModifyImageAttribut-API-Aktion.

Die folgende Richtlinie verwendet beispielsweise den `ec2:Attribute/Description` Bedingungsschlüssel, um den Zugriff nach dem komplexen Description-Objekt der

ModifyImageAttribut-API-Aktion zu filtern. Der Bedingungsschlüssel lässt nur Anforderungen zu, die die Beschreibung eines Images entweder in `Production` oder `Development` ändern.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute/Description": [
            "Production",
            "Development"
          ]
        }
      }
    }
  ]
}
```

Die folgende Beispielrichtlinie verwendet den `ec2:Attribute` Bedingungsschlüssel, um den Zugriff nach der primitiven Attributeigenschaft der ModifyImageAttribut-API-Aktion zu filtern. Der Bedingungsschlüssel lehnt alle Anforderungen ab, die versuchen, die Beschreibung eines Images zu ändern.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:ModifyImageAttribute",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:Attribute": "Description"
        }
      }
    }
  ]
}
```

ec2:ResourceID-Bedingungsschlüssel

Wenn Sie die folgenden ec2:*Resource*ID-Bedingungsschlüssel mit den angegebenen API-Aktionen verwenden, wird der Bedingungsschlüsselwert verwendet, um die resultierende Ressource anzugeben, die von der API-Aktion erstellt wird. ec2:*Resource*ID-Bedingungsschlüssel können nicht zum Angeben einer Quellressource verwendet werden, die in der API-Anfrage angegeben ist. Wenn Sie einen der folgenden ec2:*Resource*ID-Bedingungsschlüssel mit einer angegebenen API verwenden, müssen Sie immer den Platzhalter (*) angeben. Wenn Sie einen anderen Wert angeben, wird die Bedingung zur Laufzeit immer in * aufgelöst. Um beispielsweise den ec2:ImageId Bedingungsschlüssel mit der CopyImageAPI zu verwenden, müssen Sie den Bedingungsschlüssel wie folgt angeben:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          ec2:ImageID": "*"
        }
      }
    }
  ]
}
```

Bedingungsschlüssel	API-Aktion			
ec2:DhcpOptionsID	• CreateDhcpOptionen			
ec2:ImageID	• CopyImage • CreateImage			

Bedingungsschlüssel	API-Aktion			
	• ImportImage • RegisterImage			
ec2:InstanceID	• RunInstances • ImportInstance			
ec2:InternetGatewayID	• CreateInternetTor			
ec2:NetworkAclID	• CreateNetworkAcl			
ec2:NetworkInterfaceID	• CreateNetworkSchnittstelle			
ec2:PlacementGroupName	• CreatePlacementGruppe			
ec2:RouteTableID	• CreateRouteTabelle			

Bedingungsschlüssel	API-Aktion			
`ec2:SecurityGroupID`	• CreateSecurityGruppe			
`ec2:SnapshotID`	• CopySnapshot • CreateSnapshot • CreateSnapshots • ImportSnapshots			
`ec2:SubnetID`	• CreateSubnet			
`ec2:VolumeID`	• CreateVolume • ImportVolume			
`ec2:VpcID`	• CreateVpc			

Bedingungsschlüssel	API-Aktion			
`ec2:VpcPeeringConnectionID`	• CreateVpcPeeringConnection			

Es wird empfohlen, die Verwendung von `ec2:`*`Resource`*`ID`-Bedingungsschlüsseln bei diesen API-Aktionen zu vermeiden. Wenn Sie den Zugriff stattdessen basierend auf bestimmten Ressourcen-IDs filtern müssen, wird empfohlen, dies mithilfe des `Resource`-Richtlinienelements wie folgt zu tun:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CopyImage",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-01234567890abcdef"
    }
  ]
}
```

Prüfen, ob Benutzer über die erforderlichen Berechtigungen verfügen

Nach der Erstellung einer IAM-Richtlinie sollten Sie zunächst überprüfen, ob damit den Benutzern die benötigten Berechtigungen zur Verwendung bestimmter API-Aktionen und Ressourcen erteilt werden. Anschließend können Sie die Richtlinie anwenden.

Erstellen Sie zunächst einen Benutzer zu Testzwecken und fügen Sie dann die von Ihnen erstellte IAM-Richtlinie dem Testbenutzer an. Anschließend initiieren Sie mit dem Testbenutzer eine Anforderung.

Wenn durch die getestete Amazon-EC2-Aktion eine Ressource erstellt oder geändert wird, sollten Sie die Anforderung mit dem Parameter `DryRun` (oder über den AWS CLI -Befehl mit der Option `--dry-run`) ausführen. In diesem Fall schließt der Aufruf zwar die Autorisierungsprüfung, aber nicht die Operation ab. Beispielsweise können Sie prüfen, ob ein Benutzer eine bestimmte Instance beenden kann, ohne sie tatsächlich abzuschließen. Sofern der Testbenutzer über die erforderlichen

Berechtigungen verfügt, gibt die Anforderung `DryRunOperation` zurück. Andernfalls wird `UnauthorizedOperation` zurückgegeben.

Falls die Richtlinie dem Benutzer nicht die erwarteten Berechtigungen erteilt oder zu viele Berechtigungen gewährt, können Sie die Richtlinie entsprechend anpassen und erneut testen, bis Sie die gewünschten Ergebnisse erhalten.

> **Important**
>
> Es kann einige Minuten dauern, bis Richtlinienänderungen wirksam werden. Daher wird empfohlen, fünf Minuten verstreichen zu lassen, bevor Sie die aktualisierte Richtlinie testen.

Bei einer fehlgeschlagenen Autorisierungsprüfung gibt die Anforderung eine codierte Nachricht mit Diagnoseinformationen zurück. Sie können die Nachricht mit der Aktion `DecodeAuthorizationMessage` decodieren. Weitere Informationen finden Sie unter DecodeAuthorizationMessage in der AWS Security Token Service API-Referenz und unter decode-authorization-message in der Befehlsreferenz.AWS CLI

Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung

Mit einigen Amazon EC2-API-Aktionen zur Ressourcenerstellung können Sie Tags (Markierungen) beim Erstellen der Ressource angeben. Sie können Resource-Tags (Markierungen) verwenden, um eine attributbasierte Steuerung (ABAC) zu implementieren. Weitere Informationen finden Sie unter Markieren Ihrer -Ressourcen mit Tags (Markierungen) und Steuerung des Zugriffs auf EC2-Ressourcen mithilfe von Ressourcen-Tags (Markierungen).

Damit Benutzer diese Möglichkeit erhalten, benötigen sie die Berechtigungen zum Verwenden der Aktion, die die Ressource wie `ec2:RunInstances` oder `ec2:CreateVolume` erstellt. Wenn Tags in der Aktion angegeben werden, mit der die Ressource erstellt wird, führt Amazon eine zusätzliche Autorisierung für die `ec2:CreateTags`-Aktion aus, um die Berechtigungen der Benutzer zum Erstellen von Tags zu überprüfen. Daher benötigen die Benutzer außerdem die expliziten Berechtigungen zum Verwenden der `ec2:CreateTags`-Aktion.

Verwenden Sie in der IAM-Richtliniendefinition für die `ec2:CreateTags`-Aktion das `Condition`-Element mit dem `ec2:CreateAction`-Bedingungsschlüssel, um der Aktion, die die Ressource erstellt, Markierungsberechtigungen zu erteilen.

Die folgende Beispiel zeigt eine Richtlinie, die es Benutzern erlaubt, Instances zu starten und Instances und Volumes während des Starts beliebige Tags (Markierungen) hinzuzufügen. Die

Markierung von bestehenden Ressourcen durch die Benutzer ist nicht zulässig. (Sie können die `ec2:CreateTags`-Aktion nicht direkt aufrufen.)

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

In ähnlicher Weise erlaubt die folgende Richtline Benutzern, Volumes zu erstellen und ihnen dabei beliebige Tags (Markierungen) hinzuzufügen. Die Markierung von bestehenden Ressourcen durch die Benutzer ist nicht zulässig. (Sie können die `ec2:CreateTags`-Aktion nicht direkt aufrufen.)

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateVolume"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "CreateVolume"
          }
       }
    }
  ]
}
```

Die `ec2:CreateTags`-Aktion wird nur ausgewertet, wenn die Tags während der Aktion zur Ressourcenerstellung angewendet werden. Folglich benötigt ein Benutzer, der über die Berechtigungen zum Erstellen einer Ressource verfügt (vorausgesetzt, es bestehen keine Markierungsbedingungen), keine Berechtigungen zur Verwendung der `ec2:CreateTags`-Aktion, wenn keine Tags in der Anforderung angegeben werden. Wenn der Benutzer allerdings versucht, eine Ressource mit Tags zu erstellen, schlägt die Anforderung fehl, wenn der Benutzer nicht über die Berechtigungen für die `ec2:CreateTags`-Aktion verfügt.

Die `ec2:CreateTags`-Aktion wird auch ausgewertet, wenn Tags in einer Startvorlage bereitgestellt werden. Eine Beispielrichtlinie finden Sie unter Tags (Markierungen) in einer Startvorlage.

Kontrollieren des Zugriffs auf bestimmte Tags (Markierungen)

Sie können zusätzliche Bedingungen im `Condition`-Element Ihrer IAM-Richtlinien verwenden, um die Tag-Schlüssel und -Werte zu steuern, die auf Ressourcen angewendet werden können.

Die folgenden Bedingungsschlüssel können mit den Beispielen im vorangegangenen Abschnitt verwendet werden:

- `aws:RequestTag`: Gibt an, dass eine Anforderung einen bestimmten Tag-Schlüssel oder Tag-Schlüssel und -Wert enthalten muss. In der Anforderung können auch andere Tags (Markierungen) angegeben werden.
  - Zusammen mit dem `StringEquals`-Bedingungsoperator können Sie eine bestimmte Tag-Schlüssel- und -Wert-Kombination erzwingen, z. B. den Tag `cost-center=cc123`:

    ```
    "StringEquals": { "aws:RequestTag/cost-center": "cc123" }
    ```

  - In Kombination mit dem `StringLike`-Bedingungsoperator erzwingen Sie einen bestimmten Tag-Schlüssel in der Anforderung, beispielsweise den Tag-Schlüssel `purpose`:

    ```
    "StringLike": { "aws:RequestTag/purpose": "*" }
    ```

- `aws:TagKeys`: Erzwingt die Tag-Schlüssel, die in der Anforderung verwendet werden.
  - Verwenden Sie diesen Bedingungsschlüssel mit dem `ForAllValues`-Modifikator, um bestimmte Tag-Schlüssel zu erzwingen, die in der Anforderung bereitgestellt werden (wenn in der Anforderung Tags angegeben werden, sind nur bestimmte Tags erlaubt und keine anderen Tags gestattet). Im folgenden Beispiel sind die Tag-Schlüssel `environment` oder `cost-center` erlaubt:

    ```
    "ForAllValues:StringEquals": { "aws:TagKeys": ["environment","cost-center"] }
    ```

  - Zusammen mit dem `ForAnyValue`-Modifikator wird erzwungen, dass die Anforderung mindestens einen der angegebenen Tag-Schlüssel umfassen muss. Zum Beispiel muss mindestens einer der Tag-Schlüssel `environment` und `webserver` in der Anforderung enthalten sein:

    ```
    "ForAnyValue:StringEquals": { "aws:TagKeys": ["environment","webserver"] }
    ```

Diese Bedingungsschlüssel können auf Aktionen zur Ressourcenerstellung, die Markierungen unterstützen, sowie `ec2:CreateTags`- und `ec2:DeleteTags`-Aktionen angewendet werden. Informationen darüber, ob eine Amazon-EC2-API-Aktion das Markieren unterstützt, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Wenn Sie erzwingen möchten, dass die Benutzer beim Erstellen einer Ressource Tags angeben, müssen Sie den `aws:RequestTag`-Bedingungsschlüssel oder den `aws:TagKeys`-Bedingungsschlüssel mit dem `ForAnyValue`-Modifikator für die Aktion zur Erstellung von Ressourcen verwenden. Wenn ein Benutzer für diese Aktion zur Ressourcenerstellung keine Tags angibt, wird die `ec2:CreateTags`-Aktion nicht ausgewertet.

Bei Bedingungen gilt, dass die Groß- und Kleinschreibung für den Bedingungsschlüssel nicht berücksichtigt und für den Bedingungswert beachtet wird. Verwenden Sie aus diesem Grund den `aws:TagKeys`-Bedingungsschlüssel und geben Sie den Tag (Markierung)-Schlüssel als Wert dieser Bedingung an, wenn Sie die Berücksichtigung der Groß- und Kleinschreibung für einen Tag (Markierung)-Schlüssel erzwingen möchten.

Beispiele für IAM-Richtlinien finden Sie unter Beispielrichtlinien für die Arbeit mit dem oder einem SDK AWS CLIAWS. Weitere Informationen zu Bedingungen mit mehreren Werten erhalten Sie unter Erstellen einer Bedingung zum Testen von mehreren Schlüsselwerten im IAM-Benutzerhandbuch.

Steuerung des Zugriffs auf EC2-Ressourcen mithilfe von Ressourcen-Tags (Markierungen)

Wenn Sie eine IAM-Richtlinie erstellen, die Benutzern die Berechtigung zur Verwendung von EC2-Ressourcen gewährt, können Sie Tag-Informationen in das `Condition`-Element der Richtlinie einfügen, um den Zugriff basierend auf Tags zu steuern. Dies wird als attributbasierte Zugriffskontrolle (ABAC) bezeichnet. ABAC bietet eine besser Kontrolle darüber, welche Ressourcen ein Benutzer ändern, verwenden oder löschen kann. Weitere Informationen finden Sie unter Was ist ABAC für AWS?

Beispielsweise können Sie eine Richtlinie erstellen, die es Benutzern ermöglicht, eine Instance zu beenden, aber die Aktion verweigert, wenn die Instance über den `environment=production`-Tag (Markierungen) verfügt. Dazu verwenden Sie den `aws:ResourceTag`-Bedingungsschlüssel, um den Zugriff auf die Ressource basierend auf den der Ressource zugewiesenen Tags (Markierung) zu erlauben oder zu verweigern.

```
"StringEquals": { "aws:ResourceTag/environment": "production" }
```

Informationen darüber, ob eine Amazon EC2-API-Aktion das Steuern des Zugriffs mithilfe des `aws:ResourceTag`-Bedingungsschlüssels unterstützt finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2. Beachten Sie, dass die `Describe`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen, sodass sie in einer separaten Anweisung ohne Bedingungen angegeben werden müssen.

Beispiele für IAM-Richtlinien finden Sie unter Beispielrichtlinien für die Arbeit mit dem oder einem SDK AWS CLIAWS.

Wenn Sie Benutzern den Zugriff zu Ressourcen auf der Grundlage von Tags (Markierungen) gewähren oder verweigern, müssen Sie daran denken, Benutzern explizit das Hinzufügen und Entfernen dieser Tags (Markierungen) von den jeweiligen Ressourcen unmöglich zu machen. Andernfalls können Benutzer möglicherweise Ihre Einschränkungen umgehen und sich Zugriff auf eine Ressource verschaffen, indem sie ihre Tags (Markierungen) modifizieren.

Beispielrichtlinien für die Arbeit mit dem oder einem SDK AWS CLIAWS

Sie müssen Benutzern mithilfe von IAM-Richtlinien die Berechtigungen gewähren, die sie für Amazon EC2 benötigen. Die folgenden Beispiele veranschaulichen Richtlinienanweisungen, mit denen Sie die Berechtigungen, die Benutzer für Amazon EC2 haben, kontrollieren können. Diese Richtlinien sind für Anfragen konzipiert, die mit dem AWS CLI oder einem AWS SDK gestellt werden. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch. Wenn Sie die Amazon EC2-Konsole verwenden möchten, finden Sie Beispielrichtlinien unter Beispielrichtlinien für die Arbeit in der Amazon EC2-Konsole. Beispiele für Amazon VPC-spezifische IAM-Richtlinien finden Sie unter Identity and Access Management für Amazon VPC.

Ersetzen Sie in den folgenden Beispielen alle *Platzhalter für Benutzereingabe* durch Ihre eigenen Informationen.

Beispiele

- Beispiel: schreibgeschützter Zugriff
- Beispiel: Beschränken des Zugriffs auf eine bestimmte Region
- Arbeiten mit Instances
- Instanzen starten (RunInstances)
- Arbeiten mit Spot-Instances
- Beispiel: Arbeiten mit Reserved Instances
- Beispiel: Markieren von Ressourcen
- Beispiel: Arbeiten mit IAM-Rollen
- Beispiel: Arbeiten mit Routing-Tabellen
- Beispiel: Erlauben Sie einer bestimmten Instanz, Ressourcen in anderen AWS Diensten anzuzeigen
- Beispiel: Arbeiten mit Startvorlagen
- Arbeiten mit Instance-Metadaten
- Arbeiten Sie mit Amazon EBS-Volumes und -Snapshots

Beispiel: schreibgeschützter Zugriff

Mit der folgenden Richtlinie wird Benutzern Berechtigungen zur Verwendung aller Amazon EC2-API-Aktionen erteilt, deren Name mit `Describe` beginnt. Das `Resource`-Element verwendet einen Platzhalter, wodurch Benutzer alle Ressourcen mit diesen API-Aktionen angeben können. Das

Sternchen (*) als Platzhalter ist auch dann erforderlich, wenn die API-Aktion keine Berechtigungen auf Ressourcenebene unterstützt. Weitere Informationen dazu, welche ARNs Sie mit welchen Amazon EC2-API-Aktionen verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Die Benutzer haben keine Berechtigung zum Ausführen von Aktionen auf den Ressourcen (es sei denn, eine andere Anweisung erteilt ihnen diese Erlaubnis), da ihnen die Berechtigung für die Verwendung von API-Aktionen standardmäßig verweigert wird.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:Describe*",
      "Resource": "*"
    }
   ]
}
```

Beispiel: Beschränken des Zugriffs auf eine bestimmte Region

Die folgende Richtlinie verweigert Benutzern die Berechtigung, Amazon EC2-API-Aktionen in anderen Regionen als Europa (Frankfurt) zu verwenden. Sie verwendet den globalen Bedingungsschlüssel `aws:RequestedRegion`, der von allen Amazon EC2-API-Aktionen unterstützt wird.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-central-1"
        }
      }
    }
  ]
```

```
}
```

Alternativ können Sie den Bedingungsschlüssel `ec2:Region` verwenden, der speziell für Amazon EC2 verwendet wird und von allem Amazon EC2-API-Aktionen unterstützt wird.

```
{
  "Version":"2012-10-17",
  "Statement": [
       {
      "Effect": "Deny",
      "Action": "ec2:*",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:Region": "eu-central-1"
        }
      }
    }
  ]
}
```

Arbeiten mit Instances

Beispiele

- Beispiel: Beschreiben, Initiieren, Stoppen, Starten und Beenden aller Instances
- Beispiel: Beschreiben aller Instances sowie Stoppen, Starten und Beenden nur bestimmter Instances

Beispiel: Beschreiben, Initiieren, Stoppen, Starten und Beenden aller Instances

Mit der folgenden Richtlinie wird Benutzern Berechtigungen erteilt, die im Element `Action` angegebenen API-Aktionen zu verwenden. Das `Resource`-Element verwendet den Platzhalter "*", wodurch Benutzer alle Ressourcen mit diesen API-Aktionen angeben können. Das Sternchen (*) als Platzhalter ist auch dann erforderlich, wenn die API-Aktion keine Berechtigungen auf Ressourcenebene unterstützt. Weitere Informationen dazu, welche ARNs Sie mit welchen Amazon EC2-API-Aktionen verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Die Benutzer haben keine Berechtigung zur Verwendung von anderen API-Aktionen (es sei denn, eine andere Anweisung erteilt ihnen die entsprechende Erlaubnis), da den Benutzern die Berechtigung für die Verwendung von API-Aktionen standardmäßig verweigert wird.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeAvailabilityZones",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": "*"
    }
   ]
}
```

Beispiel: Beschreiben aller Instances sowie Stoppen, Starten und Beenden nur bestimmter Instances

Die folgende Richtlinie erlaubt den Benutzern, alle Instances zu beschreiben, nur die Instances i-1234567890abcdef0 und i-0598c7d356eba48d7 zu starten und anzuhalten sowie ausschließlich Instances in der Region USA Ost (N.-Virginia) (`us-east-1`) mit dem Ressourcen-Tag (Markierung) `purpose=test` zu beenden.

In der ersten Anweisung legt ein *-Platzhalter im `Resource`-Element fest, dass die Benutzer alle Ressourcen für die Aktion angeben können. In diesem Beispiel können sie alle Instances auflisten. Das Sternchen (*) als Platzhalter ist auch dann erforderlich, wenn die API-Aktion keine Berechtigungen auf Ressourcenebene unterstützt (in diesem Fall `ec2:DescribeInstances`). Weitere Informationen dazu, welche ARNs Sie mit welchen Amazon EC2-API-Aktionen verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Die zweite Anweisung erteilt Berechtigungen auf Ressourcenebene für die Aktionen `StopInstances` und `StartInstances`. Die genauen Instances werden durch ihre ARNs im `Resource`-Element angegeben.

Die dritte Anweisung ermöglicht es Benutzern, alle Instances in der Region USA Ost (Nord-Virginia) (`us-east-1`) zu beenden, die zu dem angegebenen AWS Konto gehören, aber nur dort, wo die Instance das Tag hat`"purpose=test"`. Das `Condition`-Element bestimmt, wann die Richtlinienanweisung wirksam ist.

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
   "Effect": "Allow",
      "Action": "ec2:DescribeInstances",
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
        "ec2:StopInstances",
        "ec2:StartInstances"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:account-id:instance/i-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:account-id:instance/i-0598c7d356eba48d7"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "ec2:TerminateInstances",
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/purpose": "test"
         }
      }
   }

   ]
}
```

Instanzen starten (RunInstances)

Die RunInstancesAPI-Aktion startet eine oder mehrere On-Demand-Instances oder eine oder mehrere Spot-Instances. `RunInstances`benötigt ein AMI und erstellt eine Instanz. Benutzer können in der Anforderung ein Schlüsselpaar und eine Sicherheitsgruppe angeben. Der Start in einer VPC erfordert ein Subnetz und generiert eine Netzwerkschnittstelle. Beim Starten von einem Amazon EBS-Backed AMI wird ein Volume erstellt. Der Benutzer muss daher über Berechtigungen zur Verwendung dieser Amazon EC2-Ressourcen verfügen. Sie können eine Richtlinienanweisung erstellen, damit die Benutzer einen optionalen Parameter für `RunInstances` angeben müssen oder die Werte einschränken, die den Benutzern für einen Parameter gestattet sind.

Weitere Informationen zu Berechtigungen auf Ressourcenebene, die zum Starten einer Instance erforderlich sind, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Standardmäßig verfügen Benutzer nicht über Berechtigungen, die resultierenden Instances zu beschreiben, zu starten, anzuhalten oder zu beenden. Eine Möglichkeit, den Benutzern die Berechtigung zum Verwalten der resultierenden Instances zu erteilen, besteht darin, ein spezielles Tags (Markierung) für jede Instance und eine Anweisung zu erstellen, welche dazu dient, die Instances mit diesem Tag (Markierung) zu verwalten. Weitere Informationen finden Sie unter Arbeiten mit Instances.

Ressourcen

- AMIs
- Instance-Typen
- Subnetze
- EBS-Datenträger
- Tags
- Tags (Markierungen) in einer Startvorlage
- Elastic GPUs
- Startvorlagen

AMIs

Die folgende Richtlinie erlaubt den Benutzern, Instances ausschließlich mit den AMIs `ami-9e1670f7` und `ami-45cf5c3c` zu starten. Die Benutzer können keine Instance mit anderen AMIs starten (es sei denn, eine andere Anweisung gewährt den Benutzern die entsprechende Berechtigung).

```
{
   "Version": "2012-10-17",
   "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-9e1670f7",
        "arn:aws:ec2:region::image/ami-45cf5c3c",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*",
        "arn:aws:ec2:region:account-id:subnet/*",
        "arn:aws:ec2:region:account-id:network-interface/*"
      ]
    }
   ]
}
```

Alternativ ermöglicht es die unten stehende Richtlinie den Benutzern, Instances von allen AMIs zu starten, die im Besitz von Amazon oder bestimmten vertrauenswürdigen und verifizierten Partnern sind. Das `Condition`-Element in der ersten Anweisung überprüft, ob `ec2:Owner` `amazon` ist. Die Benutzer können keine Instance mit anderen AMIs starten (es sei denn, eine andere Anweisung gewährt den Benutzern die entsprechende Berechtigung).

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:Owner": "amazon"
         }
      }
   },
   {
```

```
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Instance-Typen

Die folgende Richtlinie gestattet es Benutzern, Instances nur mit dem `t2.micro`- oder `t2.small`-Instance-Typ zu starten, wodurch die Kosten kontrolliert werden können. Die Benutzer können keine größeren Instances starten, da das `Condition`-Element der ersten Anweisung überprüft, ob `ec2:InstanceType` entweder `t2.micro` oder `t2.small` ist.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
```

```
            "arn:aws:ec2:region:account-id:volume/*",
            "arn:aws:ec2:region:account-id:key-pair/*",
            "arn:aws:ec2:region:account-id:security-group/*"
            ]
        }
    ]
}
```

Sie können alternativ eine Richtlinie erstellen, die Benutzern Berechtigungen zum Starten aller Instances, mit Ausnahme der Instance-Typen `t2.micro` und `t2.small`, verweigert.

```
{
   "Version": "2012-10-17",
   "Statement": [
        {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:instance/*"
      ],
      "Condition": {
         "StringNotEquals": {
            "ec2:InstanceType": ["t2.micro", "t2.small"]
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

Subnetze

Die folgende Richtlinie erlaubt den Benutzern, Instances ausschließlich im angegebenen Subnetz, `subnet-`*`12345678`*, zu starten. Die Gruppe kann keine Instances in einem anderen Subnetz starten (es sei denn, eine andere Anweisung gewährt den Benutzern die entsprechende Berechtigung).

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region:account-id:subnet/subnet-12345678",
        "arn:aws:ec2:region:account-id:network-interface/*",
        "arn:aws:ec2:region:account-id:instance/*",
        "arn:aws:ec2:region:account-id:volume/*",
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account-id:key-pair/*",
        "arn:aws:ec2:region:account-id:security-group/*"
      ]
    }
   ]
}
```

Alternativ können Sie eine Richtlinie erstellen, die Benutzern Berechtigungen zum Starten einer Instance in jedem anderen Subnetz verweigert. Zu diesem Zweck verweigert die Anweisung die Berechtigung zum Erstellen einer Netzwerkschnittstelle, außer wenn das `subnet-`*`12345678`*-Subnetz festgelegt wird. Diese Verweigerung setzt alle anderen Richtlinien außer Kraft, die erstellt werden, um zu gestatten, Instances in anderen Subnetzen zu starten.

```
{
   "Version": "2012-10-17",
   "Statement": [
         {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account-id:network-interface/*"
      ],
      "Condition": {
         "ArnNotEquals": {
```

```
            "ec2:Subnet": "arn:aws:ec2:region:account-id:subnet/subnet-12345678"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region::image/ami-*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:instance/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:volume/*",
         "arn:aws:ec2:region:account-id:key-pair/*",
         "arn:aws:ec2:region:account-id:security-group/*"
         ]
      }
   ]
}
```

EBS-Datenträger

Die Richtlinie unten ermöglicht es den Benutzern, Instances nur zu starten, wenn die EBS-Volumes für die Instance verschlüsselt sind. Der Benutzer muss eine Instance von einem AMI starten, das mit verschlüsselten Snapshots erstellt wurde, um sicherzustellen, dass das Stamm-Volume verschlüsselt wird. Jedes weitere Volume, das der Instance während des Starts vom Benutzer angefügt wird, muss auch verschlüsselt sein.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Condition": {
                "Bool": {
                    "ec2:Encrypted": "true"
                }
            }
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:key-pair/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        }
    ]
}
```

Tags

Markieren von Instances bei der Erstellung

Die folgende Richtlinie gestattet es den Benutzern, Instances zu starten und sie während ihrer Erstellung zu markieren. Bei Aktionen zur Ressourcenerstellung, die Tags anwenden, müssen Benutzer über Berechtigungen für die Aktion `CreateTags` verfügen. Die zweite Anweisung enthält den `ec2:CreateAction`-Bedingungsschlüssel, sodass die Benutzer Tags nur im Kontext von `RunInstances` und nur für Instances erstellen können. Die Benutzer können keine vorhandenen Ressourcen mit Tags versehen und Volumes nicht mit der `RunInstances`-Anforderung markieren.

Weitere Informationen finden Sie unter Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
```

```
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Markieren von Instances und Volumes bei der Erstellung mit bestimmten Tags

Die folgende Richtlinie umfasst den `aws:RequestTag`-Bedingungsschlüssel. Die Benutzer müssen daher alle Instances und Volumes, die durch `RunInstances` erstellt werden, mit den Tags `environment=production` und `purpose=webserver` versehen. Werden nicht genau diese Tags (Markierungen) übergeben oder überhaupt keine Tags (Markierungen) angegeben, schlägt die Anforderung fehl.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
         "arn:aws:ec2:region:account-id:security-group/*",
         "arn:aws:ec2:region:account-id:key-pair/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
          "arn:aws:ec2:region:account-id:volume/*",
          "arn:aws:ec2:region:account-id:instance/*"
```

```
      ],
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/environment": "production" ,
             "aws:RequestTag/purpose": "webserver"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Markieren von instances und Volumes bei der Erstellung mit mindestens einem bestimmten Tag

Die Richtlinie unten verwendet den `ForAnyValue`-Modifikator für die `aws:TagKeys`-Bedingung, um festzulegen, dass mindestens ein Tag (Markierung) in der Anforderung angegeben werden muss und der `environment`- oder `webserver`-Schlüssel enthalten sein muss. Das Tag (Markierung) muss sowohl auf Instances als auch auf Volumes angewendet werden. In der Anforderung können beliebige Tags (Markierungen)-Werte angegeben werden.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": [
         "arn:aws:ec2:region::image/*",
         "arn:aws:ec2:region:account-id:subnet/*",
         "arn:aws:ec2:region:account-id:network-interface/*",
```

```
            "arn:aws:ec2:region:account-id:security-group/*",
            "arn:aws:ec2:region:account-id:key-pair/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances"
        ],
        "Resource": [
            "arn:aws:ec2:region:account-id:volume/*",
            "arn:aws:ec2:region:account-id:instance/*"
        ],
        "Condition": {
            "ForAnyValue:StringEquals": {
                "aws:TagKeys": ["environment","webserver"]
            }
         }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": "arn:aws:ec2:region:account-id:*/*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction" : "RunInstances"
            }
         }
    }
  ]
}
```

Wenn Instances bei der Erstellung markiert werden, müssen sie mit einem bestimmten Tag markiert sein

In der folgenden Richtlinie ist es nicht notwendig, dass die Benutzer in der Anforderung Tags (Markierungen) angeben, aber wenn sie dies tun, muss es das Tag (Markierungen) `purpose=test` sein. Andere Tags (Markierungen) sind nicht zulässig. Die Benutzer können in der `RunInstances`-Anforderung die Tags auf jede Ressource anwenden, die mit Tags versehen werden kann.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
         "StringEquals": {
             "aws:RequestTag/purpose": "test",
             "ec2:CreateAction" : "RunInstances"
          },
          "ForAllValues:StringEquals": {
              "aws:TagKeys": "purpose"
          }
       }
    }
  ]
}
```

Um jeden Benutzer, der Tag bei create for aufgerufen hat, zu verbieten RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
```

```
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Erlaube nur bestimmte Tags für spot-instances-request. Hier kommt die überraschende Inkonsistenz Nr. 2 ins Spiel. Unter normalen Umständen führt das Angeben von keinen Tags (Markierungen) zu „Unauthenticated (Nicht authentifiziert)“. Im Fall von wird diese Richtlinie nicht ausgewertet spot-instances-request, wenn keine spot-instances-request Tags vorhanden sind, sodass eine Spot-on-Run-Anfrage ohne Tags erfolgreich ist.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
            ]
        },
        {
```

```
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

Tags (Markierungen) in einer Startvorlage

Im folgenden Beispiel können Benutzer Instances starten, jedoch nur über eine bestimmte Startvorlage (`lt-09477bcd97b0d310e`). Durch den Bedingungsschlüssel `ec2:IsLaunchTemplateResource` werden Benutzer daran gehindert, in der Startvorlage angegebene Ressourcen außer Kraft zu setzen. Der zweite Teil der Anweisung erlaubt Benutzern das Markieren von Instances bei der Erstellung – dieser Teil der Anweisung wird benötigt, wenn in der Startvorlage Tags (Markierungen) für die Instance angegeben werden.

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
            "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:CreateTags"
```

```
      ],
      "Resource": "arn:aws:ec2:region:account-id:instance/*",
      "Condition": {
         "StringEquals": {
             "ec2:CreateAction" : "RunInstances"
          }
       }
    }
  ]
}
```

Elastic GPUs

In der folgenden Richtlinie können Benutzer eine Instance starten und eine elastische GPU zum Anfügen an die Instance angeben. Benutzer können Instances in jeder Region starten, das Anfügen einer elastischen GPU ist beim Start jedoch nur in der Region `us-east-2` möglich.

Der `ec2:ElasticGpuType`-Bedingungsschlüssel stellt sicher, dass Instances entweder den Elastic `eg1.medium`- oder `eg1.large`-GPU-Typ verwenden.

```
{
    "Version": "2012-10-17",
    "Statement": [
             {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:account-id:elastic-gpu/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Region": "us-east-2",
                    "ec2:ElasticGpuType": [
                        "eg1.medium",
                        "eg1.large"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": "ec2:RunInstances",
            "Resource": [
                "arn:aws:ec2:*::image/ami-*",
                "arn:aws:ec2:*:account-id:network-interface/*",
                "arn:aws:ec2:*:account-id:instance/*",
                "arn:aws:ec2:*:account-id:subnet/*",
                "arn:aws:ec2:*:account-id:volume/*",
                "arn:aws:ec2:*:account-id:key-pair/*",
                "arn:aws:ec2:*:account-id:security-group/*"
            ]
        }
    ]
}
```

Startvorlagen

Im folgenden Beispiel können Benutzer Instances starten, jedoch nur über eine bestimmte Startvorlage (`lt-09477bcd97b0d310e`). Benutzer können die Parameter in der Startvorlage außer Kraft setzen, indem sie die Parameter in der Aktion `RunInstances` angeben.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/
lt-09477bcd97b0d310e"
          }
       }
    }
  ]
}
```

In diesem Beispiel können Benutzer Instances nur starten, wenn sie eine Startvorlage verwenden. Die Richtlinie verhindert mit dem Bedingungsschlüssel `ec2:IsLaunchTemplateResource`, dass Benutzer eventuell vorhandene ARNs in der Startvorlage übergehen.

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

Die folgende Beispielsrichtlinie erlaubt einem Benutzer, Instances zu starten, jedoch nur über eine Startvorlage. Benutzer können in der Anforderung keine Subnetz- und Netzwerkschnittstellen-Parameter außer Kraft setzen. Diese Parameter können nur in der Startvorlage angegeben werden. Im ersten Teil der Anweisung wird das NotResourceElement verwendet, um alle anderen Ressourcen außer Subnetzen und Netzwerkschnittstellen zuzulassen. Der zweite Teil der Anweisung erlaubt die Subnetz- und Netzwerkschnittstellen-Ressourcen, jedoch nur, wenn sie ihren Ursprung in der Startvorlage haben.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": ["arn:aws:ec2:region:account-id:subnet/*",
                      "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          }
       }
    },
    {
      "Effect": "Allow",
```

```
      "Action": "ec2:RunInstances",
      "Resource": ["arn:aws:ec2:region:account-id:subnet/*",
                   "arn:aws:ec2:region:account-id:network-interface/*" ],
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
          "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    }
  ]
}
```

Das folgende Beispiel erlaubt Benutzern, Instances zu starten, jedoch nur über eine Startvorlage und wenn die Startvorlage den Tag (Markierungen) `Purpose=Webservers` aufweist. Benutzer können mit der Aktion `RunInstances` keine Parameter der Startvorlage außer Kraft setzen.

```
{
  "Version": "2012-10-17",
  "Statement": [
        {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "NotResource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
         "ArnLike": {
             "ec2:LaunchTemplate": "arn:aws:ec2:region:account-id:launch-template/*"
          },
         "Bool": {
             "ec2:IsLaunchTemplateResource": "true"
          }
       }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
       "StringEquals": {
           "aws:ResourceTag/Purpose": "Webservers"
        }
```

```
        }
      }
  ]
}
```

Arbeiten mit Spot-Instances

Sie können die RunInstances Aktion verwenden, um Spot-Instance-Anfragen zu erstellen und die Spot-Instance-Anfragen bei der Erstellung mit einem Tag zu versehen. Die Ressource, für die Sie angeben müssen, RunInstances ist`spot-instances-request`.

Die `spot-instances-request`-Ressource wird in der IAM-Richtlinie wie folgt ausgewertet:

- Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung nicht taggen, bewertet Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung nicht.
- Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung taggen, bewertet Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung.

Daher gelten für die `spot-instances-request`-Ressource die folgenden Regeln für die IAM-Richtlinie:

- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und nicht beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource nicht explizit zulassen. Der Aufruf ist erfolgreich.
- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource in die RunInstances Allow-Anweisung aufnehmen, andernfalls schlägt der Aufruf fehl.
- Wenn Sie RunInstances eine Spot-Instance-Anfrage erstellen und beabsichtigen, die Spot-Instance-Anfrage bei der Erstellung zu taggen, müssen Sie die `spot-instances-request` Ressource oder den * Platzhalter in der Allow-Anweisung CreateTags angeben, andernfalls schlägt der Aufruf fehl.

Sie können Spot-Instances mit RunInstances oder RequestSpotInstances anfordern. Die folgenden Beispiel-IAM-Richtlinien gelten nur, wenn Sie Spot-Instances über RunInstances anfordern.

Beispiel: Spot-Instances anfordern mit RunInstances

Die folgende Richtlinie ermöglicht es Benutzern, Spot-Instances mithilfe der RunInstances Aktion anzufordern. Die `spot-instances-request` Ressource, die von erstellt wurde RunInstances, fordert Spot-Instances an.

> **Note**
>
> Um Spot-Instance-Anfragen RunInstances zu erstellen, können Sie sie `spot-instances-request` aus der `Resource` Liste streichen, wenn Sie nicht beabsichtigen, die Spot-Instance-Anfragen bei der Erstellung zu taggen. Das liegt daran, dass Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung nicht bewertet, wenn die Spot-Instance-Anfrage bei create nicht markiert ist.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        }
    ]
}
```

> **Warning**
>
> NICHT UNTERSTÜTZT — Beispiel: Benutzern die Erlaubnis verweigern, Spot-Instances anzufordern mit RunInstances

Die folgende Richtlinie wird für die `spot-instances-request`-Ressource nicht unterstützt. Die folgende Richtlinie soll Benutzern die Berechtigung zum Starten von On-Demand-Instances erteilen, ihnen jedoch die Berechtigung zum Anfordern von Spot-Instances verweigern. Die `spot-instances-request` Ressource, die von erstellt wurde RunInstances, ist die Ressource, die Spot-Instances anfordert. Die zweite Anweisung soll die RunInstances Aktion für die `spot-instances-request` Ressource verweigern. Diese Bedingung wird jedoch nicht unterstützt, da Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung nicht auswertet, wenn die Spot-Instance-Anfrage bei create nicht markiert ist.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests - NOT SUPPORTED - DO NOT USE!",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
        }
    ]
}
```

Beispiel: Markieren von Spot-Instance-Anforderungen beim Erstellen

Die folgende Richtlinie ermöglicht es Benutzern, alle Ressourcen zu markieren, die während des Instance-Starts erstellt werden. Die erste Anweisung ermöglicht es RunInstances , die aufgelisteten Ressourcen zu erstellen. Die `spot-instances-request` Ressource, die von erstellt wurde RunInstances, ist die Ressource, die Spot-Instances anfordert. Die zweite Anweisung stellt einen *-Platzhalter bereit, mit dem alle Ressourcen markiert werden können, wenn sie beim Start der Instance erstellt werden.

> **Note**
>
> Wenn Sie eine Spot-Instance-Anfrage bei der Erstellung taggen, bewertet Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung. Daher müssen Sie die `spot-instances-request` Ressource für die RunInstances Aktion explizit zulassen, andernfalls schlägt der Aufruf fehl.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
```

```
    ]
}
```

Beispiel: Markieren beim Erstellen von Spot-Instance-Anforderungen verweigern

Die folgende Richtlinie verweigert Benutzern die Berechtigung zum Markieren der Ressourcen, die während des Instance-Starts erstellt werden.

Die erste Anweisung ermöglicht RunInstances das Erstellen der aufgelisteten Ressourcen. Die `spot-instances-request` Ressource, die von erstellt wurde RunInstances, ist die Ressource, die Spot-Instances anfordert. Die zweite Anweisung stellt einen *-Platzhalter bereit, um alle Ressourcen zu verweigern, die markiert werden, wenn sie beim Start der Instance erstellt werden. Wenn `spot-instances-request` oder eine andere Ressource bei create markiert ist, schlägt der RunInstances Aufruf fehl.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenyTagResources",
            "Effect": "Deny",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
```

```
}
```

⚠ Warning

NICHT UNTERSTÜTZT – Beispiel: Erstellen einer Spot-Instance-Anforderung nur zulassen, wenn ihr ein bestimmtes Tag (Markierung) zugewiesen wird
Die folgende Richtlinie wird für die `spot-instances-request`-Ressource nicht unterstützt. Die folgende Richtlinie soll nur dann RunInstances die Erlaubnis zum Erstellen einer Spot-Instance-Anfrage gewähren, wenn die Anfrage mit einem bestimmten Tag gekennzeichnet ist. Die erste Anweisung ermöglicht es RunInstances , die aufgelisteten Ressourcen zu erstellen. Die zweite Anweisung soll Benutzern nur dann die Berechtigung erteilen, eine Spot-Instance-Anforderung zu erstellen, wenn die Anforderung den Tag (Markierung) `environment=production` enthält. Wenn diese Bedingung auf andere Ressourcen angewendet wird, die von erstellt wurden RunInstances, führt die Angabe keiner Tags zu einem `Unauthenticated` Fehler. Wenn jedoch keine Tags für die Spot-Instance-Anfrage angegeben sind, bewertet Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung nicht, was dazu führt, dass Spot-Instance-Anfragen ohne Tags von erstellt werden. RunInstances
Beachten Sie, dass die Angabe eines anderen Tags als zu einem `Unauthenticated` Fehler `environment=production` führt, denn wenn ein Benutzer eine Spot-Instance-Anfrage taggt, wertet Amazon EC2 die `spot-instances-request` Ressource in der RunInstances Anweisung aus.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
```

```
                "arn:aws:ec2:us-east-1:*:instance/*"
            ]
        },
        {
            "Sid": "RequestSpotInstancesOnlyIfTagIs_environment=production - NOT
 SUPPORTED - DO NOT USE!",
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }

    ]
}
```

Beispiel: Erstellen einer Spot-Instance-Anforderung verweigern, wenn ihr ein bestimmtes Tag (Markierung) zugewiesen ist

Die folgende Richtlinie verweigert RunInstances die Erlaubnis, eine Spot-Instance-Anfrage zu erstellen, wenn die Anfrage mit gekennzeichnet ist. `environment=production`

Die erste Anweisung ermöglicht RunInstances das Erstellen der aufgelisteten Ressourcen.

Die zweite Anweisung verweigert Benutzern die Berechtigung, eine Spot-Instance-Anforderung zu erstellen, wenn die Anforderung den Tag (Markierung) `environment=production` enthält. Die Angabe von `environment=production` als Tag führt zu einem `Unauthenticated`-Fehler. Wenn Sie andere oder keine Tags (Markierungen) angeben, wird eine Spot-Instance-Anforderung erstellt.

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

```
        {
            "Sid": "AllowRun",
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],
            "Resource": [
                "arn:aws:ec2:us-east-1::image/*",
                "arn:aws:ec2:us-east-1:*:subnet/*",
                "arn:aws:ec2:us-east-1:*:network-interface/*",
                "arn:aws:ec2:us-east-1:*:security-group/*",
                "arn:aws:ec2:us-east-1:*:key-pair/*",
                "arn:aws:ec2:us-east-1:*:volume/*",
                "arn:aws:ec2:us-east-1:*:instance/*",
                "arn:aws:ec2:us-east-1:*:spot-instances-request/*"
            ]
        },
        {
            "Sid": "DenySpotInstancesRequests",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:us-east-1:*:spot-instances-request/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        },
        {
            "Sid": "TagResources",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "*"
        }
    ]
}
```

Beispiel: Arbeiten mit Reserved Instances

Mit der folgenden Richtlinie wird Benutzern die Berechtigung zum Ansehen, Ändern und Kaufen von Reserved Instances in Ihrem Konto gewährt.

Für einzelne Reserved Instances können keine Berechtigungen auf Ressourcenebene erteilt werden. Diese Richtlinie bedeutet, dass die Benutzer Zugriff auf alle Reserved Instances im Konto haben.

Der Platzhalter * im Element `Resource` legt fest, dass Benutzer alle Ressourcen für die Aktion angeben können. In diesem Beispiel können sie alle Reserved Instances im Konto auflisten und bearbeiten. Sie haben auch die Möglichkeit, die Kontoanmeldeinformationen zu verwenden, um Reserved Instances zu kaufen. Das Sternchen (*) als Platzhalter ist auch dann erforderlich, wenn die API-Aktion keine Berechtigungen auf Ressourcenebene unterstützt.

```
{
   "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:PurchaseReservedInstancesOffering",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
    }
   ]
}
```

Benutzern wird die Berechtigung zum Ansehen und Ändern der Reserved Instances in Ihrem Konto erteilt, aber nicht zum Kauf von neuen Reserved Instances.

```
{
  "Version": "2012-10-17",
   "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeReservedInstances",
        "ec2:ModifyReservedInstances",
        "ec2:DescribeAvailabilityZones"
      ],
      "Resource": "*"
    }
  ]
```

```
}
```

Beispiel: Markieren von Ressourcen

Die folgende Richtlinie erlaubt Benutzern nur die Verwendung der `CreateTags`-Aktion, um einer Instance Tags hinzuzufügen, wenn das Tag den `environment`-Schlüssel und den `production`-Wert enthält. Es sind keine anderen Tags erlaubt und der Benutzer kann keine anderen Ressourcentypen markieren.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/environment": "production"
                }
            }
        }
    ]
}
```

Die Richtlinie unten ermöglicht es den Benutzern, jede markierbare Ressource, die bereits ein Tag mit dem `owner`-Schlüssel und einen Benutzernamen als Wert aufweist, mit Tags zu versehen. Zudem müssen die Benutzer ein Tag (Markierung) mit dem `anycompany:environment-type`-Schlüssel und dem Wert `test` oder `prod` in der Anforderung festlegen. Die Benutzer können zusätzliche Tags (Markierungen) in der Anforderung angeben.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
```

```
            "Resource": "arn:aws:ec2:region:account-id:*/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/anycompany:environment-type": ["test","prod"],
                    "aws:ResourceTag/owner": "${aws:username}"
                }
            }
        }
    ]
}
```

Sie können eine IAM-Richtlinie erstellen, die den Benutzern erlaubt, bestimmte Tags (Markierungen) für eine Ressource zu löschen. Die folgende Richtlinie gestattet es den Benutzern zum Beispiel, Tags für ein Volume zu löschen, sofern die Anforderung die Tag-Schlüssel `environment` oder `cost-center` enthält. Für den Tag (Markierung) kann ein beliebiger Wert angegeben werden, aber der Tag (Markierung)-Schlüssel muss einem der genannten Schlüssel entsprechen.

> **Note**
>
> Wenn Sie eine Ressource löschen, werden alle der Ressource zugeordneten Tags (Markierungen) ebenfalls gelöscht. Die Benutzer benötigen keine Berechtigungen für die Verwendung der Aktion `ec2:DeleteTags`, um eine Ressource zu löschen, die Tags aufweist. Sie müssen nur über Berechtigungen zum Ausführen der Löschaktion verfügen.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Effect": "Allow",
      "Action": "ec2:DeleteTags",
      "Resource": "arn:aws:ec2:us-east-1:account-id:volume/*",
      "Condition": {
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment","cost-center"]
        }
      }
    }
  ]
}
```

Diese Richtlinie erlaubt den Benutzern, auf beliebigen Ressourcen nur den `environment=prod`-Tag zu löschen. Dies gilt zudem nur, wenn die Ressource bereits den `owner`-Schlüssel-Tag und einen Benutzernamen als Wert aufweist. Benutzer können keine anderen Tags für eine Ressource löschen.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteTags"
      ],
      "Resource": "arn:aws:ec2:region:account-id:*/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/environment": "prod",
          "aws:ResourceTag/owner": "${aws:username}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": ["environment"]
        }
      }
    }
  ]
}
```

Beispiel: Arbeiten mit IAM-Rollen

Die folgende Richtlinie erlaubt Benutzern das Anfügen, Ersetzen und Trennen einer IAM-Rolle für Instances, die über den `department=test`-Tag (Markierung) verfügt. Das Ersetzen oder Trennen einer IAM-Rolle erfordert eine Zuordnungs-ID. Die Richtlinie erteilt den Benutzern daher außerdem die Berechtigung, die `ec2:DescribeIamInstanceProfileAssociations`-Aktion zu verwenden.

Die Benutzer müssen über die Berechtigung für die `iam:PassRole`-Aktion verfügen, um die Rollen an die Instance zu übergeben.

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

```
        "ec2:AssociateIamInstanceProfile",
        "ec2:ReplaceIamInstanceProfileAssociation",
        "ec2:DisassociateIamInstanceProfile"
      ],
      "Resource": "arn:aws:ec2:us-east-1:account-id:instance/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/department":"test"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeIamInstanceProfileAssociations",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::account-id:role/DevTeam*"
    }
  ]
}
```

Die folgende Richtlinie erlaubt Benutzern das Anfügen oder Ersetzen einer IAM-Rolle für eine beliebige Instance. Es können nur IAM-Rollen angefügt oder ersetzt werden, deren Namen mit `TestRole-` beginnen. Stellen Sie bei der `iam:PassRole`-Aktion sicher, dass Sie den Namen der IAM-Rolle und nicht den des Instance-Profils angeben, falls sich diese Namen unterscheiden. Weitere Informationen finden Sie unter Instance-Profile.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateIamInstanceProfile",
                "ec2:ReplaceIamInstanceProfileAssociation"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
```

```
            "Action": "ec2:DescribeIamInstanceProfileAssociations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:aws:iam::account-id:role/TestRole-*"
        }
    ]
}
```

Beispiel: Arbeiten mit Routing-Tabellen

Die folgende Richtlinie ermöglicht Benutzern das Hinzufügen, Entfernen und Ersetzen von Routings für Routing-Tabellen, die nur mit VPC `vpc-ec43eb89` verbunden sind. Zur Angabe einer VPC für den Bedingungsschlüssel `ec2:Vpc` müssen Sie den vollständigen ARN der VPC angeben.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRoute",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute"
            ],
            "Resource": [
                "arn:aws:ec2:region:account-id:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-ec43eb89"
                }
            }
        }
    ]
}
```

Beispiel: Erlauben Sie einer bestimmten Instanz, Ressourcen in anderen AWS Diensten anzuzeigen

Nachfolgend finden Sie ein Beispiel für eine Richtlinie, die Sie einer IAM-Rolle anhängen können. Die Richtlinie ermöglicht es einer Instanz, Ressourcen in verschiedenen AWS Diensten anzuzeigen. Sie

gibt mit dem Bedingungsschlüssel `ec2:SourceInstanceARN` an, dass es sich bei der Instance, von der die Anforderung ausging, um die Instance `i-093452212644b0dd6` handeln muss. Wenn die gleiche IAM-Rolle mit einer anderen Instance verbunden ist, kann die andere Instance keine dieser Aktionen ausführen.

Der `ec2:SourceInstanceARN` Schlüssel ist ein AWS globaler Bedingungsschlüssel und kann daher für andere Serviceaktionen verwendet werden, nicht nur für Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
              {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVolumes",
                "s3:ListAllMyBuckets",
                "dynamodb:ListTables",
                "rds:DescribeDBInstances"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "ArnEquals": {
                    "ec2:SourceInstanceARN": "arn:aws:ec2:region:account-id:instance/
i-093452212644b0dd6"
                }
            }
        }
    ]
}
```

Beispiel: Arbeiten mit Startvorlagen

Die folgende Richtlinie erlaubt Benutzern, eine Startvorlagenversion zu erstellen und eine Startvorlage zu bearbeiten, jedoch nur für eine bestimmte Startvorlage (`lt-09477bcd97b0d3abc`). Benutzer können nicht mit anderen Startvorlagen arbeiten.

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

```
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/lt-09477bcd97b0d3abc"
    }
  ]
}
```

Die folgende Richtlinie erlaubt Benutzern, eine Startvorlage und Startvorlagenversion zu löschen, vorausgesetzt, dass die Startvorlage den Tag (Markierungen) `Purpose=Testing` aufweist.

```
{
  "Version": "2012-10-17",
  "Statement": [
       {
      "Action": [
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteLaunchTemplateVersions"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:ec2:region:account-id:launch-template/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Purpose": "Testing"
        }
      }
    }
  ]
}
```

Arbeiten mit Instance-Metadaten

Die folgenden Richtlinien stellen sicher, dass Benutzer Instance-Metadaten nur mit Instance-Metadatenservice Version 2 (IMDSv2) abrufen können. Sie können die folgenden vier Richtlinien zu einer Richtlinie mit vier Anweisungen zusammenfassen. Wenn diese zu einer Richtlinie zusammengefasst werden, können Sie die Richtlinie als Service-Kontrollrichtlinie (SCP) verwenden. Sie kann gleichermaßen gut als Verweigerungsrichtlinie funktionieren, die Sie auf eine bestehende IAM-Richtlinie anwenden (zum Aufheben und Einschränken bestehender Berechtigungen) oder auch als SCP, die global auf ein Konto, eine OE oder eine gesamte Organisation angewendet wird.

> **Note**
>
> Die folgenden Richtlinien für RunInstances Metadatenoptionen müssen in Verbindung mit einer Richtlinie verwendet werden, die dem Prinzipal Berechtigungen zum Starten einer RunInstances Instance erteilt. Wenn der Prinzipal nicht auch über RunInstances Berechtigungen verfügt, kann er keine Instance starten. Weitere Informationen finden Sie in den Richtlinien unter Arbeiten mit Instances und Instanzen starten (RunInstances).

> **Important**
>
> Wenn Sie Auto Scaling-Gruppen verwenden und für alle neuen Instances die Verwendung von IMDSv2 vorschreiben, müssen Ihre Auto Scaling-Gruppen Startvorlagen verwenden. Wenn eine Auto Scaling-Gruppe eine Startvorlage verwendet, werden die `ec2:RunInstances`-Berechtigungen des IAM-Prinzipals beim Erstellen einer neuen Auto Scaling-Gruppe überprüft. Sie werden auch überprüft, wenn eine vorhandene Auto Scaling-Gruppe so aktualisiert wird, dass eine neue Startvorlage oder eine neue Version einer Startvorlage verwendet wird.
> Einschränkungen für die Verwendung von IMDSv1 auf IAM-Prinzipalen für `RunInstances` werden nur überprüft, wenn eine Auto-Scaling-Gruppe erstellt oder aktualisiert wird, die eine Startvorlage verwendet. Für eine Auto Scaling-Gruppe, die für die Verwendung der Startvorlage `Latest` oder `Default` konfiguriert ist, werden die Berechtigungen nicht überprüft, wenn eine neue Version der Startvorlage erstellt wird. Damit Berechtigungen überprüft werden können, müssen Sie die Auto Scaling-Gruppe so konfigurieren, dass eine bestimmte Version der Startvorlage verwendet wird.
>
> Um die Verwendung von IMDSv2 auf Instances zu erzwingen, die von Auto Scaling-Gruppen gestartet werden, sind die folgenden zusätzlichen Schritte erforderlich:
>
> 1. Deaktivieren Sie die Verwendung von Startkonfigurationen für alle Konten in Ihrer Organisation, indem Sie entweder Service-Kontrollrichtlinien (SCPs) oder IAM-Berechtigungsgrenzen für neue erstellte Prinzipale verwenden. Aktualisieren Sie für vorhandene IAM-Prinzipale mit Auto Scaling-Gruppenberechtigungen die zugehörigen Richtlinien mit diesem Bedingungsschlüssel. Um die Verwendung von Startkonfigurationen zu deaktivieren, erstellen oder ändern Sie den entsprechenden SCP, die Berechtigungsgrenze oder die IAM-Richtlinie mit dem Bedingungsschlüssel `"autoscaling:LaunchConfigurationName"` mit dem als `null` angegebenen Wert.

2. Konfigurieren Sie für neue Startvorlagen die Instance-Metadatenoptionen in der Startvorlage. Erstellen Sie für vorhandene Startvorlagen eine neue Version der Startvorlage und konfigurieren Sie die Instance-Metadatenoptionen in der neuen Version.
3. In der Richtlinie, die einen jeden Prinzipal zur Verwendung einer Startvorlage berechtigt, beschränken Sie die Zuordnung von `$latest` und `$default` durch Angabe von `"autoscaling:LaunchTemplateVersionSpecified": "true"`. Indem Sie die Verwendung auf eine bestimmte Version einer Startvorlage beschränken, können Sie sicherstellen, dass neue Instances mit der Version gestartet werden, in der die Instance-Metadatenoptionen konfiguriert sind. Weitere Informationen finden Sie unter LaunchTemplateSpezifikation in der Amazon EC2 Auto Scaling API-Referenz, insbesondere unter dem `Version` Parameter.
4. Ersetzen Sie bei einer Auto Scaling-Gruppe, die eine Startkonfiguration verwendet, die Startkonfiguration durch eine Startvorlage. Weitere Informationen finden Sie unter Ersetzen einer Startkonfiguration durch eine Startvorlage im Amazon EC2 Auto Scaling-Benutzerhandbuch.
5. Stellen Sie bei einer Auto Scaling-Gruppe, die eine Startvorlage verwendet, sicher, dass sie eine neue Startvorlage mit den konfigurierten Instance-Metadatenoptionen oder eine neue Version der aktuellen Startvorlage mit den konfigurierten Instance-Metadatenoptionen verwendet. Weitere Informationen finden Sie update-auto-scaling-group in der AWS CLI Befehlsreferenz.

Beispiele

- Erzwingen der Verwendung von IMDSv2
- Abmeldung von IMDSv2 verweigern
- Angeben des maximalen Hop-Limits
- Beschränken, wer die Instance-Metadatenoptionen ändern kann
- Erzwingen, dass Rollen-Anmeldeinformationen aus IMDSv2 abgerufen werden

Erzwingen der Verwendung von IMDSv2

Die folgende Richtlinie legt fest, dass Sie die RunInstances API nur aufrufen können, wenn für die Instanz auch die Verwendung von IMDSv2 aktiviert wurde (angegeben durch`"ec2:MetadataHttpTokens": "required"`). Wenn Sie nicht angeben, dass die

Instanz IMDSv2 benötigt, erhalten Sie beim Aufrufen der `UnauthorizedOperation` API eine Fehlermeldung. RunInstances

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "RequireImdsV2",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:MetadataHttpTokens": "required"
                }
            }
        }
    ]
}
```

Abmeldung von IMDSv2 verweigern

Die folgende Richtlinie legt fest, dass Sie die `ModifyInstanceMetadataOptions`-API nicht aufrufen und die Option IMDSv1 oder IMDSv2 nicht zulassen können. Wenn Sie die `ModifyInstanceMetadataOptions`-API aufrufen, muss das `HttpTokens`-Attribut auf `required` gesetzt sein.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "DenyIMDSv1HttpTokensModification",
        "Effect": "Deny",
        "Action": "ec2:ModifyInstanceMetadataOptions",
        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "StringNotEquals": {
                "ec2:Attribute/HttpTokens": "required"
            },
            "Null": {
                "ec2:Attribute/HttpTokens": false
            }
        }
```

```
    }]
}
```

Angeben des maximalen Hop-Limits

Die folgende Richtlinie legt fest, dass Sie die RunInstances API nur aufrufen können, wenn Sie auch ein Hop-Limit angeben, und das Hop-Limit darf nicht mehr als 3 betragen. Wenn Sie das nicht tun, erhalten Sie beim Aufrufen der RunInstances API eine `Unauthorized0peration` Fehlermeldung.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "MaxImdsHopLimit",
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "NumericGreaterThan": {
                    "ec2:MetadataHttpPutResponseHopLimit": "3"
                }
            }
        }
    ]
}
```

Beschränken, wer die Instance-Metadatenoptionen ändern kann

Die folgende Richtlinie erlaubt es nur Benutzern mit der `ec2-imds-admins`-Rolle, Änderungen an den Optionen für die Instance-Metadaten vorzunehmen. Wenn ein anderer Principal als die `ec2-imds-admins` Rolle versucht, die ModifyInstanceMetadataOptions API aufzurufen, wird eine `Unauthorized0peration` Fehlermeldung angezeigt. Diese Anweisung könnte verwendet werden, um die Verwendung der ModifyInstanceMetadataOptions API zu kontrollieren. Derzeit gibt es keine detaillierten Zugriffskontrollen (Bedingungen) für die ModifyInstanceMetadataOptions API.

```
{
    "Version": "2012-10-17",
    "Statement": [
                {
            "Sid": "AllowOnlyImdsAdminsToModifySettings",
            "Effect": "Deny",
```

```
            "Action": "ec2:ModifyInstanceMetadataOptions",
            "Resource": "*",
            "Condition": {
                "StringNotLike": {
                    "aws:PrincipalARN": "arn:aws:iam::*:role/ec2-imds-admins"
                }
            }
        }
    ]
}
```

Erzwingen, dass Rollen-Anmeldeinformationen aus IMDSv2 abgerufen werden

Die folgende Richtlinie legt fest, dass wenn diese Richtlinie auf eine Rolle angewendet wird und die Rolle vom EC2-Service übernommen wird und die daraus resultierenden Anmeldeinformationen zum Signieren einer Anforderung verwendet werden, die Anforderung mit Anmeldeinformationen für EC2-Rollen signiert werden muss, die von IMDSv2 abgerufen werden. Andernfalls erhalten alle API-Aufrufe einen `UnauthorizedOperation`-Fehler. Diese Anweisung/Richtlinie kann generell angewendet werden, da sie keine Wirkung hat, wenn die Anforderung nicht mit Anmeldeinformationen für EC2-Rollen signiert wird.

```
{
    "Version": "2012-10-17",
    "Statement": [
               {
            "Sid": "RequireAllEc2RolesToUseV2",
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NumericLessThan": {
                    "ec2:RoleDelivery": "2.0"
                }
            }
        }
    ]
}
```

Arbeiten Sie mit Amazon EBS-Volumes und -Snapshots

Beispielrichtlinien für die Arbeit mit Amazon EBS-Volumes und -Snapshots finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon EBS.

Beispielrichtlinien für die Arbeit in der Amazon EC2-Konsole

Sie müssen Benutzern mithilfe von IAM-Richtlinien die Berechtigungen gewähren, die sie für Amazon EC2 benötigen. Mit IAM-Richtlinien können Sie Benutzern Berechtigungen erteilen, um bestimmte Ressourcen in der Amazon EC2-Konsole anzusehen und mit diesen zu arbeiten. Sie können die Beispielrichtlinien aus dem vorherigen Abschnitt verwenden. Sie sind jedoch für Anfragen konzipiert, die mit dem oder einem SDK gestellt werden. AWS CLI AWS Weitere Informationen finden Sie unter Beispielrichtlinien für die Arbeit mit dem oder einem SDK AWS CLIAWS und Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Für die Konsole werden zusätzliche API-Aktionen für bestimmte Features verwendet, was bei diesen Richtlinien zu unerwarteten Ergebnissen führen kann. Wenn ein Benutzer zum Beispiel über die Berechtigung verfügt, nur die `DescribeVolumes`-API-Aktion zu verwenden, schlägt sein Versuch fehl, Volumes in der Konsole anzusehen. In diesem Abschnitt werden Richtlinien vorgestellt, mit denen Benutzer mit bestimmten Teilen der Konsole arbeiten können. Weitere Informationen zum Erstellen von Richtlinien für die Amazon EC2 EC2-Konsole finden Sie im folgenden AWS Sicherheits-Blogbeitrag: Benutzern die Erlaubnis erteilen, in der Amazon EC2 EC2-Konsole zu arbeiten.

> **Tip**
>
> Verwenden Sie einen Service wie , um einfacher herauszufinden, welche API-Aktionen zum Ausführen von Aufgaben in der Konsole erforderlich sind AWS CloudTrail. Weitere Informationen finden Sie im AWS CloudTrail -Benutzerhandbuch. Wenn Ihre Richtlinie keine Berechtigung zum Erstellen oder Ändern einer bestimmten Ressource erteilt, zeigt die Konsole eine codierte Meldung mit Diagnoseinformationen an. Sie können die Nachricht mit der Nachrichten-API-Aktion für oder mit dem DecodeAuthorizationBefehl AWS STSdecode-authorization-message in der dekodieren. AWS CLI

Beispiele

- Beispiel: schreibgeschützter Zugriff
- Beispiel: Verwenden des EC2 Launch Instance Wizard
- Beispiel: Arbeiten mit Sicherheitsgruppen
- Beispiel: Arbeiten mit Elastic-IP-Adressen
- Beispiel: Arbeiten mit Reserved Instances

Beispiel: schreibgeschützter Zugriff

Damit Benutzer die Berechtigung haben, alle Ressourcen in der Amazon EC2-Konsole anzusehen, können Sie die gleiche Richtlinie wie im folgenden Beispiel verwenden: Beispiel: schreibgeschützter Zugriff. Die Benutzer können keine Aktionen für diese Ressourcen ausführen und keine neuen Ressourcen erstellen, sofern ihnen keine andere Anweisung die Berechtigung dazu gewährt.

Ansehen von Instances, AMIs und Snapshots

Alternativ haben Sie die Möglichkeit, schreibgeschützten Zugriff auf eine Untermenge von Ressourcen bereitzustellen. Ersetzen Sie hierfür den *-Platzhalter in der `ec2:Describe`-API-Aktion mit konkreten `ec2:Describe`-Aktionen für jede Ressource. Die folgende Richtlinie erlaubt Benutzern, alle Instances, AMIs und Snapshots in der Amazon EC2-Konsole anzusehen. Die `ec2:DescribeTags`-Aktion ermöglicht es den Benutzern, öffentliche AMIs angezeigt zu bekommen. Die Konsole benötigt die Markierungsinformationen, um öffentliche AMIs anzuzeigen. Sie können diese Aktion jedoch entfernen, damit die Benutzer nur private AMIs ansehen dürfen.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeTags",
         "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
   }
   ]
}
```

> **Note**
>
> Die Amazon EC2-`ec2:Describe*`-API-Aktionen unterstützen keine Berechtigungen auf Ressourcenebene. Es ist daher nicht möglich, zu steuern, welche einzelnen Ressourcen die Benutzer in der Konsole ansehen können. Aus diesem Grund ist in der obigen Anweisung der *-Platzhalter im `Resource`-Element erforderlich. Weitere Informationen dazu, welche ARNs Sie mit welchen Amazon EC2-API-Aktionen verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2.

Instanzen CloudWatch und Metriken anzeigen

Die folgende Richtlinie ermöglicht es Benutzern, Instances in der Amazon EC2 EC2-Konsole sowie CloudWatch Alarme und Metriken auf der Registerkarte Überwachung der Seite Instances anzuzeigen. Die Amazon EC2 EC2-Konsole verwendet die CloudWatch API, um die Alarme und Metriken anzuzeigen. Daher müssen Sie Benutzern die Erlaubnis erteilen`cloudwatch:DescribeAlarms`, die,, `cloudwatch:DescribeAlarmsForMetric` `cloudwatch:ListMetrics``cloudwatch:GetMetricStatistics`, und `cloudwatch:GetMetricData` Aktionen zu verwenden.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "cloudwatch:DescribeAlarms",
         "cloudwatch:DescribeAlarmsForMetric",
         "cloudwatch:ListMetrics",
         "cloudwatch:GetMetricStatistics",
         "cloudwatch:GetMetricData"
      ],
      "Resource": "*"
   }
   ]
}
```

Beispiel: Verwenden des EC2 Launch Instance Wizard

Der Launch Instance Wizard von Amazon EC2 ist eine Ansicht mit Optionen zum Konfigurieren und Starten einer Instance. Ihre Richtlinie muss die Berechtigung für die API-Aktionen enthalten, die den Benutzern ermöglichen, mit den Optionen des Assistenten zu arbeiten. Fehlt eine solche Berechtigung in der Richtlinie, werden einige Elemente im Assistenten nicht ordnungsgemäß geladen und die Benutzer können den Start nicht abschließen.

Grundlegender Zugriff auf den Launch Instance Wizard

Für einen erfolgreich abgeschlossenen Start müssen Sie den Benutzern die Berechtigung erteilen, die `ec2:RunInstances`-API-Aktion und mindestens die folgenden API-Aktionen zu verwenden:

- `ec2:DescribeImages`: Zum Ansehen und Auswählen eines AMI.

- `ec2:DescribeInstanceTypes`: Zum Anzeigen und Auswählen eines Instance-Typs.
- `ec2:DescribeVpcs`: Zum Anzeigen der verfügbaren Versionen von Ruby.
- `ec2:DescribeSubnets`: Zum Ansehen aller verfügbaren Subnetze für die ausgewählte VPC.
- `ec2:DescribeSecurityGroups` oder `ec2:CreateSecurityGroup`: Zum Anzeigen und Auswählen einer vorhandenen Sicherheitsgruppe oder zum Erstellen einer neuen Sicherheitsgruppe.
- `ec2:DescribeKeyPairs` oder `ec2:CreateKeyPair`: Um ein vorhandenes Schlüsselpaar auszuwählen oder ein neues Schlüsselpaar zu erstellen.
- `ec2:AuthorizeSecurityGroupIngress`: Zum Hinzufügen von Regeln für eingehenden Datenverkehr.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateKeyPair"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:RunInstances",
            "Resource": "*"
        }
    ]
}
```

Sie können den Benutzern mehr Optionen zur Verfügung stellen, indem Sie der Richtlinie weitere API-Aktionen hinzufügen, zum Beispiel:

- `ec2:DescribeAvailabilityZones`: Zum Anzeigen und Auswählen einer spezifischen Availability Zone.
- `ec2:DescribeNetworkInterfaces`:Zum Ansehen und Auswählen von vorhandenen Netzwerkschnittstellen für das ausgewählte Subnetz.
- Zum Hinzufügen von Regeln für ausgehenden Datenverkehr zu VPC-Sicherheitsgruppen müssen die Benutzer für die `ec2:AuthorizeSecurityGroupEgress`-API-Aktion berechtigt sein. Zum Ändern oder Löschen von vorhandenen Regeln muss den Benutzern die Berechtigung erteilt werden, die relevante `ec2:RevokeSecurityGroup*`-API-Aktion zu verwenden.
- `ec2:CreateTags`: Zum Markieren der Ressourcen, die von `RunInstances` erstellt werden. Weitere Informationen finden Sie unter Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung. Wenn die Benutzer keine Berechtigung zur Verwendung dieser Aktion haben und auf der Markierungsseite des Launch Instance Wizard versuchen, Tags anzuwenden, schlägt der Start fehl.

  > **Important**
  >
  > Das Angeben eines Namens beim Starten einer Instance erstellt ein Tag und erfordert die Aktion `ec2:CreateTags`. Seien Sie vorsichtig, wenn Sie Benutzern die Erlaubnis zur Verwendung der Aktion `ec2:CreateTags` erteilen, da dies Ihre Möglichkeit einschränkt, den `aws:ResourceTag`-Bedingungsschlüssel zu nutzen, um die Verwendung anderer Ressourcen einzuschränken. Wenn Sie Benutzern die Berechtigung zur Verwendung der Aktion `ec2:CreateTags` erteilen, können sie den Tag (Markierung) einer Ressource ändern, um diese Einschränkungen zu umgehen. Weitere Informationen finden Sie unter Steuerung des Zugriffs auf EC2-Ressourcen mithilfe von Ressourcen-Tags (Markierungen).

- Um Systems-Manager-Parameter bei der Auswahl eines AMIs zu verwenden, müssen Sie `ssm:DescribeParameters` und `ssm:GetParameters` zu Ihrer Richtlinie hinzufügen. `ssm:DescribeParameters` gewährt Ihren Benutzern die Berechtigung, Systems-Manager-Parameter anzuzeigen und auszuwählen. `ssm:GetParameters` gewährt Ihren Benutzern die Berechtigung, die Werte der Systems-Manager-Parameter abzurufen. Sie können auch den Zugriff auf bestimmte Systems Manager-Parameter beschränken. Weitere Informationen finden Sie unter Zugriff auf bestimmte Systems Manager-Parameter weiter unten in diesem Abschnitt.

Die `Describe*`-API-Aktionen von Amazon EC2 unterstützen derzeit keine Berechtigungen auf Ressourcenebene. Es ist daher nicht möglich, einzuschränken, welche einzelnen Ressourcen die Benutzer im Launch Instance Wizard ansehen können. Sie können allerdings Berechtigungen auf Ressourcenebene auf die `ec2:RunInstances`-API-Aktion anwenden, um die Ressourcen zu begrenzen, die die Benutzer beim Starten einer Instance nutzen dürfen. Der Start schlägt fehl, wenn die Benutzer Optionen auswählen, für deren Verwendung sie nicht autorisiert sind.

Zugriff auf einen bestimmten Instance-Typ, ein Subnetz und eine Region einschränken

Die folgende Richtlinie erlaubt den Benutzern, nur in einem angegebenen Subnetz (`t2.micro`) `subnet-1a2b3c4d`-Instances mit AMIs, deren Eigentümer Amazon ist, zu starten. Benutzer können Starts nur in der Region `sa-east-1` durchführen. Wenn Benutzer im Launch Instance Wizard eine andere Region, einen anderen Instance-Typ, ein anderes AMI oder ein anderes Subnetz auswählen, schlägt der Start fehl.

In der ersten Anweisung wird den Benutzern die Berechtigung erteilt, die Optionen im Launch Instance Wizard anzuzeigen oder neue zu erstellen, wie im Beispiel oben gezeigt. Dank der zweiten Anweisung haben die Benutzer die Berechtigung, die zum Starten einer Instance in einer VPC erforderlichen Ressourcen – Netzwerkschnittstelle, Volume, Schlüsselpaar, Sicherheitsgruppe und Subnetz – für die `ec2:RunInstances`-Aktion zu verwenden. Weitere Informationen zur Verwendung der `ec2:RunInstances`-Aktion finden Sie unter Instanzen starten (RunInstances). Mit der dritten und vierten Anweisung wird den Benutzern die Berechtigung gewährt, die Instance- bzw. AMI-Ressourcen zu nutzen. Dabei muss allerdings die Instance eine `t2.micro`-Instance und Amazon oder bestimmte vertrauenswürdige und verifizierte Partner der Eigentümer des AMI sein.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeInstances",
         "ec2:DescribeImages",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeKeyPairs",
         "ec2:CreateKeyPair",
         "ec2:DescribeVpcs",
         "ec2:DescribeSubnets",
         "ec2:DescribeSecurityGroups",
         "ec2:CreateSecurityGroup",
         "ec2:AuthorizeSecurityGroupIngress"
```

```
    ],
    "Resource": "*"
    },
    {
       "Effect": "Allow",
       "Action":"ec2:RunInstances",
       "Resource": [
          "arn:aws:ec2:sa-east-1:111122223333:network-interface/*",
          "arn:aws:ec2:sa-east-1:111122223333:volume/*",
          "arn:aws:ec2:sa-east-1:111122223333:key-pair/*",
          "arn:aws:ec2:sa-east-1:111122223333:security-group/*",
          "arn:aws:ec2:sa-east-1:111122223333:subnet/subnet-1a2b3c4d"
       ]
    },
    {
       "Effect": "Allow",
       "Action": "ec2:RunInstances",
       "Resource": [
          "arn:aws:ec2:sa-east-1:111122223333:instance/*"
       ],
       "Condition": {
          "StringEquals": {
             "ec2:InstanceType": "t2.micro"
          }
       }
    },
    {
       "Effect": "Allow",
       "Action": "ec2:RunInstances",
       "Resource": [
            "arn:aws:ec2:sa-east-1::image/ami-*"
       ],
       "Condition": {
          "StringEquals": {
             "ec2:Owner": "amazon"
          }
       }
    }
    ]
}
```

Zugriff auf bestimmte Systems Manager-Parameter einschränken

Die folgende Richtlinie gewährt Zugriff auf die Verwendung von Systems Manager-Parametern mit einem bestimmten Namen.

Die erste Anweisung gewährt Benutzern die Erlaubnis, Systems Manager-Parameter anzuzeigen, wenn sie im Launch Instance Wizard ein AMI auswählen. Die zweite Anweisung gibt Benutzern die Berechtigung, nur Parameter zu verwenden, die mit `prod-*` bezeichnet sind.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ssm:DescribeParameters"
      ],
      "Resource": "*"
   },
   {
      "Effect": "Allow",
      "Action": [
         "ssm:GetParameters"
      ],
     "Resource": "arn:aws:ssm:us-east-2:123456123:parameter/prod-*"
   }
   ]
}
```

Beispiel: Arbeiten mit Sicherheitsgruppen

Anzeigen von Sicherheitsgruppen sowie Hinzufügen und Entfernen von Regeln

Die folgende Richtlinie erteilt Benutzern die Berechtigung, Sicherheitsgruppen in der Amazon EC2-Konsole anzuzeigen, Regeln für ein- und ausgehenden Datenverkehr hinzuzufügen und zu entfernen und Regelbeschreibungen für vorhandene Sicherheitsgruppen, die über das `Department=Test`-Tag verfügen, aufzuführen und zu ändern.

In der ersten Anweisung erlaubt die `ec2:DescribeTags`-Aktion den Benutzern, Tags in der Konsole anzusehen. Damit wird es für die Benutzer einfacher, die Sicherheitsgruppen zu bestimmen, die sie bearbeiten dürfen.

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

```
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeSecurityGroups",
         "ec2:DescribeSecurityGroupRules",
         "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "ec2:AuthorizeSecurityGroupIngress",
         "ec2:RevokeSecurityGroupIngress",
         "ec2:AuthorizeSecurityGroupEgress",
         "ec2:RevokeSecurityGroupEgress",
         "ec2:ModifySecurityGroupRules",
         "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
         "ec2:UpdateSecurityGroupRuleDescriptionsEgress"
      ],
      "Resource": [
         "arn:aws:ec2:region:111122223333:security-group/*"
      ],
      "Condition": {
         "StringEquals": {
            "aws:ResourceTag/Department": "Test"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": [
         "ec2:ModifySecurityGroupRules"
      ],
      "Resource": [
         "arn:aws:ec2:region:111122223333:security-group-rule/*"
      ]
   }
]}
```

Arbeiten mit dem Dialogfeld Create Security Group (Sicherheitsgruppe erstellen)

Sie können eine Richtlinie erstellen, die es den Benutzern ermöglicht, mit dem Dialogfeld Create Security Group in der Amazon EC2-Konsole zu arbeiten. Damit die Benutzer dieses Dialogfeld

verwenden können, müssen sie mindestens über Berechtigungen für die folgenden API-Aktionen verfügen:

- `ec2:CreateSecurityGroup`: Zum Erstellen einer neuen Sicherheitsgruppe.
- `ec2:DescribeVpcs`: Zum Ansehen einer Liste von vorhandenen VPCs in der Liste VPC.

Mit diesen Berechtigungen können die Benutzer eine neue Sicherheitsgruppe erstellen, dieser aber keine Regeln hinzufügen. Für die Arbeit mit Regeln im Dialogfeld Create Security Group fügen Sie der Richtlinie die folgenden API-Aktionen hinzu:

- `ec2:AuthorizeSecurityGroupIngress`: Zum Hinzufügen von Regeln für eingehenden Datenverkehr.
- `ec2:AuthorizeSecurityGroupEgress`: Zum Hinzufügen von Regeln für ausgehenden Datenverkehr zu VPC-Sicherheitsgruppen.
- `ec2:RevokeSecurityGroupIngress`: Zum Ändern oder Löschen vorhandener eingehender Regeln. Diese Aktion ist hilfreich, damit die Benutzer in der Konsole das Feature Copy to new verwenden können. Mit diesem Feature wird das Dialogfeld Create Security Group geöffnet und mit den gleichen Regeln vorausgefüllt, die in der ausgewählten vorhandenen Sicherheitsgruppe enthalten sind.
- `ec2:RevokeSecurityGroupEgress`: Zum Ändern oder Löschen von Regeln für ausgehenden Datenverkehr für VPC-Sicherheitsgruppen. Dies ist nützlich, um Benutzern zu ermöglichen, die ausgehende Standardregel zu ändern oder zu löschen, die jeden ausgehenden Datenverkehr erlaubt.
- `ec2:DeleteSecurityGroup`: Für den Fall, dass ungültige Regeln nicht gespeichert werden können. Die Konsole erstellt zuerst die Sicherheitsgruppe und fügt dann die angegebenen Regeln hinzu. Wenn die Regeln ungültig sind, schlägt die Aktion fehl und die Konsole versucht, die Sicherheitsgruppe zu löschen. Das Dialogfeld Create Security Group bleibt geöffnet, sodass die Benutzer die unwirksame Regel korrigieren und erneut versuchen können, die Sicherheitsgruppe zu erstellen. Die API-Aktion ist nicht erforderlich. Wenn aber ein Benutzer nicht über die Berechtigung zu ihrer Verwendung verfügt und versucht, eine Sicherheitsgruppe mit ungültigen Regeln zu erstellen, wird die Sicherheitsgruppe ohne jede Regel erstellt. Der Benutzer muss die Regeln danach hinzufügen.
- `ec2:UpdateSecurityGroupRuleDescriptionsIngress`: Zum Hinzufügen oder Aktualisieren von Beschreibungen von Sicherheitsgruppenregeln für eingehenden Datenverkehr.

- `ec2:UpdateSecurityGroupRuleDescriptionsEgress`: Zum Hinzufügen oder Aktualisieren von Beschreibungen von Sicherheitsgruppenregeln für ausgehenden Datenverkehr.
- `ec2:ModifySecurityGroupRules`: Zum Modifizieren von Sicherheitsgruppenregeln.
- `ec2:DescribeSecurityGroupRules`: Zum Auflisten von Sicherheitsgruppenregeln.

Die folgende Richtlinie erteilt Benutzern die Berechtigung, das Dialogfeld Create Security Group zu verwenden und für Sicherheitsgruppen, die mit einer bestimmten VPC (`vpc-1a2b3c4d`) verknüpft sind, Regeln für ein- und ausgehenden Datenverkehr zu erstellen. Benutzer können Sicherheitsgruppen für eine VPC erstellen, ihnen jedoch keine Regeln hinzufügen. Ebenso können die Benutzer vorhandenen Sicherheitsgruppen, die nicht mit der VPC verknüpft sind, keine Regeln hinzufüge `vpc-1a2b3c4d`. Den Benutzern wird außerdem die Berechtigung erteilt, alle Sicherheitsgruppen in der Konsole anzusehen. Damit wird es für die Benutzer einfacher, die Sicherheitsgruppen zu bestimmen, denen sie Regeln für eingehenden Datenverkehr hinzufügen können. Die Richtlinie gewährt den Benutzern zudem die Berechtigung zum Löschen von Sicherheitsgruppen, die mit der VPC `vpc-1a2b3c4d` verknüpft sind.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeVpcs"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress"
      ],
      "Resource": "arn:aws:ec2:region:111122223333:security-group/*",
      "Condition":{
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:111122223333:vpc/vpc-1a2b3c4d"
         }
      }
```

```
    }
   ]
}
```

Beispiel: Arbeiten mit Elastic-IP-Adressen

Damit Benutzer Elastic IP-Adressen in der Amazon EC2-Konsole ansehen können, müssen Sie ihnen die Berechtigung zum Verwenden der `ec2:DescribeAddresses`-Aktion gewähren.

Sie können Benutzern die Arbeit mit Elastic IP-Adressen ermöglichen, indem Sie der Richtlinie folgende Aktionen hinzufügen.

- `ec2:AllocateAddress`: Zum Zuweisen einer Elastic IP-Adresse.
- `ec2:ReleaseAddress`: Zum Freigeben einer Elastic IP-Adresse.
- `ec2:AssociateAddress`: Zum Zuordnen einer Elastic IP-Adresse zu einer Instance oder Netzwerkschnittstelle.
- `ec2:DescribeNetworkInterfaces` und `ec2:DescribeInstances`: Zum Arbeiten mit der Seite Associate address. Auf der Seite werden die verfügbaren Instances oder Netzwerkschnittstellen angezeigt, denen Sie eine Elastic IP-Adresse zuordnen können.
- `ec2:DisassociateAddress`: Zum Aufheben der Zuordnung einer Elastic IP-Adresse zu einer Instance oder Netzwerkschnittstelle.

Die Richtlinie unten erlaubt den Benutzern, Elastic IP-Adressen anzusehen, zuzuordnen und mit Instances zu verknüpfen. Die Benutzer können die Elastic IP-Adressen nicht freigeben, nicht mit Netzwerkschnittstellen verknüpfen und keine Verknüpfungen aufheben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAddresses",
                "ec2:AllocateAddress",
                "ec2:DescribeInstances",
                "ec2:AssociateAddress"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Beispiel: Arbeiten mit Reserved Instances

Mit der folgenden Richtlinie können Benutzer Reserved Instances in Ihrem Konto anzeigen und ändern sowie neue Reserved Instances in der AWS Management Console erwerben.

Diese Richtlinie ermöglicht es Benutzern, alle Reserved Instances sowie On-Demand-Instances im Konto anzuzeigen. Für einzelne Reserved Instances können keine Berechtigungen auf Ressourcenebene erteilt werden.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
         "ec2:DescribeReservedInstances",
         "ec2:ModifyReservedInstances",
         "ec2:PurchaseReservedInstancesOffering",
         "ec2:DescribeInstances",
         "ec2:DescribeInstanceTypes",
         "ec2:DescribeAvailabilityZones",
         "ec2:DescribeReservedInstancesOfferings"
      ],
      "Resource": "*"
   }
   ]
}
```

Die `ec2:DescribeAvailabilityZones`-Aktion ist erforderlich, um sicherzustellen, dass die Amazon EC2-Konsole Informationen zu den Availability Zones anzeigen kann, in denen Sie Reserved Instances kaufen können. Die `ec2:DescribeInstances`-Aktion ist nicht erforderlich, sorgt aber dafür, dass der Benutzer die Instance im Konto sehen kann und Reservierungen kauft, die den richtigen Anforderungen entsprechen.

Wenn Sie den Benutzerzugriff begrenzen möchten, passen Sie die API-Aktionen an.
Zum Beispiel hat der Benutzer nach dem Entfernen von `ec2:DescribeInstances` und `ec2:DescribeAvailabilityZones` schreibgeschützten Zugriff.

AWS verwaltete Richtlinien für Amazon EC2

Um Benutzern, Gruppen und Rollen Berechtigungen hinzuzufügen, ist es einfacher, AWS verwaltete Richtlinien zu verwenden, als Richtlinien selbst zu schreiben. Es erfordert Zeit und Fachwissen, um von Kunden verwaltete IAM-Richtlinien zu erstellen, die Ihrem Team nur die benötigten Berechtigungen bieten. Um schnell loszulegen, können Sie unsere AWS verwalteten Richtlinien verwenden. Diese Richtlinien decken allgemeine Anwendungsfälle ab und sind in Ihrem AWS Konto verfügbar. Weitere Informationen zu AWS verwalteten Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

AWS Dienste verwalten und aktualisieren AWS verwaltete Richtlinien. Sie können die Berechtigungen in AWS verwalteten Richtlinien nicht ändern. Services fügen einer von AWS verwalteten Richtlinien gelegentlich zusätzliche Berechtigungen hinzu, um neue Features zu unterstützen. Diese Art von Update betrifft alle Identitäten (Benutzer, Gruppen und Rollen), an welche die Richtlinie angehängt ist. Services aktualisieren eine von AWS verwaltete Richtlinie am ehesten, ein neues Feature gestartet wird oder neue Vorgänge verfügbar werden. Dienste entfernen keine Berechtigungen aus einer AWS verwalteten Richtlinie, sodass durch Richtlinienaktualisierungen Ihre bestehenden Berechtigungen nicht beeinträchtigt werden.

AWS Unterstützt außerdem verwaltete Richtlinien für Jobfunktionen, die sich über mehrere Dienste erstrecken. Die AWS verwaltete ReadOnlyAccess-Richtlinie bietet beispielsweise schreibgeschützten Zugriff auf alle AWS Dienste und Ressourcen. Wenn ein Dienst ein neues Feature startet, werden nur Leseberechtigungen für neue Operationen und Ressourcen AWS hinzugefügt. Eine Liste und Beschreibungen der Richtlinien für Auftragsfunktionen finden Sie in Verwaltete AWS -Richtlinien für Auftragsfunktionen im IAM-Leitfaden.

AWS verwaltete Richtlinie: AmazonEC2FullAccess

Sie können die `AmazonEC2FullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die vollen Zugriff auf Amazon EC2 ermöglichen.

Die Berechtigungen für diese Richtlinie finden Sie AmazonEC2FullAccessin der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AmazonEC2ReadOnlyAccess

Sie können die `AmazonEC2ReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die einen schreibgeschützten Zugriff auf Amazon EC2 erlauben.

Die Berechtigungen für diese Richtlinie finden Sie AmazonEC2ReadOnlyAccessin der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2CapacityReservationFleetRolePolicy

Diese Richtlinie ist an die mit einem Service verknüpfte Rolle namens AWSServiceRoleForEC2CapacityReservationFleet angefügt, damit Kapazitätsreservierungen in Ihrem Namen erstellt, geändert und storniert werden können. Weitere Informationen finden Sie unter serviceverknüpften Rolle der Kapazitätsreservierungs-Flotte.

Die Berechtigungen für diese Richtlinie finden Sie AWSEC2CapacityReservationFleetRolePolicyin der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2FleetServiceRolePolicy

Diese Richtlinie ist an die servicegebundene Rolle namens AWSServiceRoleForEC2Fleet angefügt, damit die EC2-Flotte in Ihrem Namen Instances anfordern, starten, beenden und markieren kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für EC2-Flotte.

Die Berechtigungen für diese Richtlinie finden Sie AWSEC2FleetServiceRolePolicyin der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2SpotFleetServiceRolePolicy

Diese Richtlinie ist an die servicegebundene Rolle namens AWSServiceRoleForEC2SpotFleet angefügt, damit die Spot-Flotte in Ihrem Namen Instances starten und verwalten kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für Spot-Flotte.

Die Berechtigungen für diese Richtlinie finden Sie AWSEC2SpotFleetServiceRolePolicyin der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2SpotServiceRolePolicy

Diese Richtlinie ist an die servicegebundene Rolle namens AWSServiceRoleForEC2Spot angefügt, damit Amazon EC2 in Ihrem Namen Spot-Instances starten und verwalten kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für Spot-Instance-Anforderungen.

Die Berechtigungen für diese Richtlinie finden Sie AWSEC2SpotServiceRolePolicyin der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSEC2VssSnapshotPolicy

Sie können diese verwaltete Richtlinie an die IAM-Instance-Profilrolle anhängen, die Sie für Ihre Amazon EC2 EC2-Windows-Instances verwenden. Die Richtlinie gewährt Amazon EC2 die Erlaubnis, VSS-Snapshots in Ihrem Namen zu erstellen und zu verwalten.

Die Berechtigungen für diese Richtlinie finden Sie AWSEC2VssSnapshotPolicyin der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: EC2FastLaunchFullAccess

Sie können die `EC2FastLaunchFullAccess` Richtlinie an Ihr Instance-Profil oder eine andere IAM-Rolle anhängen. Diese Richtlinie gewährt vollen Zugriff auf EC2 Fast Launch-Aktionen sowie gezielte Berechtigungen wie folgt.

Details zu Berechtigungen

- EC2 Fast Launch — Administratorzugriff wird gewährt, sodass die Rolle EC2 Fast Launch aktivieren oder deaktivieren und EC2 Fast Launch-Images beschreiben kann.
- Amazon EC2 — Der Zugriff wird für Amazon EC2 gewährt. Beschreiben Sie die Aktionen RunInstances, CreateTags die zur Überprüfung von Ressourcenberechtigungen erforderlich sind.
- IAM — Zugriff wird gewährt, um Instance-Profile abzurufen und zu verwenden, deren Name enthält, um die `ec2fastlaunch` EC2FastLaunchServiceRolePolicy serviceverknüpfte Rolle zu erstellen.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie EC2FastLaunchFullAccessin der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: EC2FastLaunchServiceRolePolicy

Diese Richtlinie ist der serviceverknüpften Rolle mit dem Namen AWSServiceRoleForEC2FastLaunchzugeordnet, sodass Amazon EC2 eine Reihe von vorab bereitgestellten Snapshots erstellen und verwalten kann, die die Zeit reduzieren, die zum Starten von Instances über Ihr EC2 Fast Launch-fähiges AMI benötigt wird. Weitere Informationen finden Sie unter the section called “Servicegebundene Rolle”.

Die Berechtigungen für diese Richtlinie finden Sie in der Referenz zu verwalteten Richtlinien. EC2FastLaunchServiceRolePolicyAWS

AWS verwaltete Richtlinie: Ec2InstanceConnectEndpoint

Diese Richtlinie ist einer serviceverknüpften Rolle zugeordnet, die so benannt ist AWSServiceRoleForEC2InstanceConnect, dass EC2 Instance Connect Endpoint Aktionen in Ihrem Namen ausführen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rolle für EC2-Instance-Connect-Endpunkt.

Die Berechtigungen für diese Richtlinie finden Sie Ec2InstanceConnectEndpointin der Referenz zu AWS verwalteten Richtlinien.

Amazon EC2 EC2-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon EC2 an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen.

Änderung	Beschreibung	Datum
EC2FastLaunchFullAccess – Neue Richtlinie.	Amazon EC2 hat diese Richtlinie hinzugefügt, um API-Aktionen im Zusammenhang mit der EC2-Schnellstartfunktion von einer Instance aus durchzuführen. Die Richtlinie kann an das Instance-Profil für eine Instance angehängt werden, die über ein EC2 Fast Launch-fähiges AMI gestartet wurde.	14. Mai 2024
AWSEC2VssSnapshotPolicy – Neue Richtlinie.	Amazon EC2 hat die `AWSEC2VssSnapshotPolicy` Richtlinie hinzugefügt, die Berechtigungen zum Erstellen und Hinzufügen von Tags zu Amazon Machine Images (AMI) und EBS-Snapshots enthält.	28. März 2024

Änderung	Beschreibung	Datum
EC2FastLaunchServiceRolePolicy – Neue Richtlinie.	Amazon EC2 hat die EC2-Schnellstartfunktion hinzugefügt, damit Windows-AMIs Instances schneller starten können, indem sie eine Reihe von vorab bereitgestellten Snapshots erstellen.	26. November 2021
Amazon EC2 hat mit der Verfolgung von Änderungen begonnen	Amazon EC2 hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen	1. März 2021

IAM-Rollen für Amazon EC2

Anwendungen müssen ihre API-Anfragen mit AWS Anmeldeinformationen signieren. Als Anwendungs-Developer benötigen Sie daher eine Strategie zur Verwaltung der Anmeldeinformationen für die Anwendungen, die auf EC2-Instances ausgeführt werden. Sie können zum Beispiel die AWS -Anmeldeinformationen sicher an die Instances verteilen, damit die Anwendungen auf diesen Instances sie zum Signieren von Anforderungen verwenden können, während Ihre Anmeldeinformationen vor anderen Benutzern geschützt bleiben. Es ist jedoch schwierig, Anmeldeinformationen sicher an jede Instance zu verteilen, insbesondere an diejenigen, die in Ihrem Namen AWS erstellt werden, wie Spot-Instances oder Instances in Auto Scaling Scaling-Gruppen. Sie müssen auch in der Lage sein, die Anmeldeinformationen für jede Instance zu aktualisieren, wenn Sie Ihre AWS Anmeldeinformationen wechseln.

> **Note**
>
> Für Ihre Amazon-EC2-Workloads empfehlen wir, dass Sie die Anmeldeinformationen für die Sitzung mit der unten beschriebenen Methode abrufen. Diese Anmeldeinformationen sollten es Ihrem Workload ermöglichen, AWS -API-Anfragen zu stellen, ohne `sts:AssumeRole` verwenden zu müssen, um dieselbe Rolle zu übernehmen, die bereits mit dieser Instance verknüpft ist. Nur wenn Sie Sitzungs-Tags für die attributbasierte Zugriffskontrolle (ABAC) übergeben oder eine Sitzungsrichtlinie übergeben müssen, um die Berechtigungen der Rolle

weiter einzuschränken, sind solche Rollenannahmeaufrufe erforderlich, da sie einen neuen Satz derselben temporären Anmeldeinformationen für die Rollensitzung erstellen.
Wenn Ihr Workload eine Rolle verwendet, um sich selbst anzunehmen, müssen Sie eine Vertrauensrichtlinie erstellen, die ausdrücklich zulässt, dass diese Rolle sich selbst annimmt. Wenn Sie die Vertrauensrichtlinie nicht erstellen, erhalten Sie den Fehler `AccessDenied`. Weitere Informationen finden Sie unter Ändern einer Vertrauensrichtlinie für Rollen im IAM-Benutzerhandbuch.

Wir haben IAM-Rollen entworfen, damit Ihre Anwendungen die API-Anforderungen sicher von Ihren Instances senden können, ohne dass Sie die von den Anwendungen verwendeten Sicherheitsanmeldeinformationen verwalten müssen. Anstatt Ihre AWS Anmeldeinformationen zu erstellen und zu verteilen, können Sie die Berechtigung zum Stellen von API-Anfragen mithilfe von IAM-Rollen wie folgt delegieren:

1. Erstellen Sie eine IAM-Rolle.
2. Definieren Sie, welche Konten oder AWS Dienste die Rolle übernehmen können.
3. Definieren Sie, welche API-Aktionen und -Ressourcen die Anwendung nach Annahme der Rolle verwenden kann.
4. Geben Sie die Rolle beim Starten der Instance an oder verknüpfen Sie die Rolle mit einer vorhandenen Instance.
5. Lassen Sie die Anwendung einen Satz vorübergehende Anmeldeinformationen abrufen und verwenden.

Verwenden Sie IAM-Rollen zum Beispiel zum Erteilen von Berechtigungen für Anwendungen, die auf Instances ausgeführt werden, die einen Bucket in Amazon S3 verwenden müssen. Sie können Berechtigungen für IAM-Rollen angeben, indem Sie eine Richtlinie im JSON-Format erstellen. Diese Richtlinien sind denen ähnlich, die Sie für -Benutzer erstellen. Wenn Sie an einer Rolle etwas ändern, wird diese Änderung an alle Instances weitergegeben.

> **Note**
>
> Die Anmeldeinformationen für Amazon EC2 IAM-Rollen unterliegen nicht der in der Rolle konfigurierten maximalen Sitzungsdauer. Weitere Informationen finden Sie unter IAM-Rollen verwenden im IAM-Benutzerhandbuch.

Beim Erstellen von IAM-Rollen ordnen Sie IAM-Richtlinien mit geringsten Berechtigungen zu, die den Zugriff auf die spezifischen API-Aufrufe einschränken, die die Anwendung benötigt. Verwenden Sie für die Windows-Kommunikation gut definierte und gut dokumentierte Windows-Gruppen und -Rollen, um den Zugriff auf Anwendungsebene zwischen Windows-Instances zu gewähren. Gruppen und Rollen ermöglichen es Kunden, Berechtigungen auf Anwendungs- und NTFS-Ordnerebene zu definieren, um den Zugriff auf anwendungsspezifische Anforderungen zu beschränken.

Sie können nur eine IAM-Rolle an eine Instance anhängen, aber Sie können die gleiche Rolle an viele Instances anhängen. Weitere Informationen zum Erstellen und Verwenden von IAM-Rollen finden Sie unter Rollen im IAM-Benutzerhandbuch.

Sie können Berechtigungen auf Ressourcenebene auf Ihre IAM-Richtlinien anwenden, um zu steuern, ob Benutzer einer Instance IAM-Rollen anfügen, diese ersetzen oder trennen können. Weitere Informationen finden Sie unter Unterstützte Berechtigungen auf Ressourcenebene für Amazon EC2-API-Aktionen und in diesem Beispiel: Beispiel: Arbeiten mit IAM-Rollen.

Inhalt

Instance-Profile

Amazon EC2 verwendet ein Instance-Profil als Container für eine IAM-Rolle. Wenn Sie eine IAM-Rolle mithilfe der IAM-Konsole erstellen, erzeugt die Konsole automatisch ein Instance-Profil und gibt ihm denselben Namen wie der entsprechenden Rolle. Wenn Sie die Amazon EC2-Konsole verwenden, um eine Instance mit einer IAM-Rolle zu starten oder einer Instance eine IAM-Rolle anzufügen, wählen Sie die Rolle aus einer Liste von Instance-Profilnamen aus.

Wenn Sie die AWS CLI API oder ein AWS SDK verwenden, um eine Rolle zu erstellen, erstellen Sie die Rolle und das Instance-Profil als separate Aktionen mit möglicherweise unterschiedlichen Namen. Wenn Sie dann die AWS CLI API oder ein AWS SDK verwenden, um eine Instance mit einer IAM-Rolle zu starten oder einer Instance eine IAM-Rolle zuzuweisen, geben Sie den Namen des Instanzprofils an.

Ein Instance-Profil kann nur eine IAM-Rolle enthalten. Dieses Limit kann nicht erhöht werden.

Weitere Informationen finden Sie unter Instance-Profile im IAM-Benutzerhandbuch.

Abrufen von Sicherheitsanmeldeinformationen aus Instance-Metadaten

Eine Anwendung auf der Instance ruft die von der Rolle bereitgestellten Sicherheitsanmeldeinformationen aus dem Instance-Metadatenelement `iam/security-credentials/`Rollenname ab. Über die mit der Rolle verknüpften Sicherheitsanmeldeinformationen werden der Anwendung die Berechtigungen für die Aktionen und Ressourcen gewährt, die Sie für die Rolle definiert haben. Diese Sicherheitsanmeldeinformationen sind temporär und werden automatisch gewechselt. Neue Anmeldeinformationen stehen spätestens fünf Minuten vor dem Ablauf der alten zur Verfügung.

> **Warning**
>
> Wenn Sie Services verwenden, die Instance-Metadaten mit IAM-Rollen nutzen, müssen Sie sicherstellen, dass Sie Ihre Anmeldeinformationen nicht zur Verfügung stellen, wenn die Services HTTP-Aufrufe in Ihrem Auftrag senden. Zu den Service-Typen, die Anmeldeinformationen verfügbar machen könnten, gehören HTTP-Proxys, HTML-/CSS-Validierungs-Services und XML-Prozessoren, die die XML-Aufnahme unterstützen.

Mit dem folgenden Befehl werden die Sicherheitsanmeldeinformationen für eine IAM-Rolle namens `s3access` abgerufen.

Linux

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

Windows

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-credentials/s3access
```

Es folgt eine Beispielausgabe.

```
{
  "Code" : "Success",
  "LastUpdated" : "2012-04-26T16:39:16Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAIOSFODNN7EXAMPLE",
  "SecretAccessKey" : "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY",
  "Token" : "token",
  "Expiration" : "2017-05-17T15:09:54Z"
}
```

Für Anwendungen und Tools for PowerShell Windows-Befehle AWS CLI, die auf der Instance ausgeführt werden, müssen Sie die temporären Sicherheitsanmeldedaten nicht explizit abrufen — die AWS SDKs AWS CLI, und Tools für Windows rufen die Anmeldeinformationen PowerShell automatisch vom EC2-Instance-Metadatendienst ab und verwenden sie. Für einen Aufruf außerhalb der Instance mithilfe der temporären Sicherheitsanmeldeinformationen (beispielsweise um IAM-Richtlinien zu testen) müssen Sie den Zugriffsschlüssel, den geheimen Schlüssel und das Sitzungs-Token zur Verfügung stellen. Weitere Informationen finden Sie unter Verwenden temporärer Sicherheitsanmeldedaten, um Zugriff auf AWS Ressourcen anzufordern im IAM-Benutzerhandbuch.

Weitere Informationen zu Instance-Metadaten erhalten Sie unter Arbeiten mit Instance-Metadaten. Hinweise zur IP-Adresse der Instance-Metadaten finden Sie unter Abrufen von Instance-Metadaten.

Gewähren von Berechtigungen für Benutzer zur Weitergabe einer IAM-Rolle an eine Instance

Damit ein Benutzer eine Instance mit einer IAM-Rolle aktivieren oder eine IAM-Rolle für eine vorhandene Instance anfügen oder ersetzen kann, müssen Sie dem Benutzer die Berechtigung zur Verwendung der folgenden API-Aktionen gewähren:

- `iam:PassRole`
- `ec2:AssociateIamInstanceProfile`
- `ec2:ReplaceIamInstanceProfileAssociation`

Die folgende IAM-Richtlinie erteilt Benutzern beispielsweise die Berechtigung zum Starten von Instances mit einer IAM-Rolle oder zum Anhängen oder Ersetzen einer IAM-Rolle für eine vorhandene Instance mithilfe von AWS CLI.

> **Note**
>
> Wenn Sie möchten, dass die Richtlinie Benutzern Zugriff auf alle Ihre Rollen gewährt, geben Sie die Ressource als `*` in der Richtlinie an. Als bewährte Methode sollten Sie dabei jedoch das Prinzip der minimalen Rechtevergabe beachten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "ec2:RunInstances",
         "ec2:AssociateIamInstanceProfile",
         "ec2:ReplaceIamInstanceProfileAssociation"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/DevTeam*"
    }
```

```
  ]
}
```

Um Benutzern die Berechtigung zum Starten von Instances mit einer IAM-Rolle oder zum Anhängen oder Ersetzen einer IAM-Rolle für eine vorhandene Instance mithilfe der Amazon-EC2-Konsole zu erteilen, müssen Sie ihnen die Berechtigung erteilen, `iam:ListInstanceProfiles`, `iam:PassRole`, `ec2:AssociateIamInstanceProfile` und `ec2:ReplaceIamInstanceProfileAssociation` zusätzlich zu anderen zu verwenden Berechtigungen, die sie möglicherweise benötigen. Beispiele für Richtlinien finden Sie unter Beispielrichtlinien für die Arbeit in der Amazon EC2-Konsole.

Arbeiten mit IAM-Rollen

Sie können eine IAM-Rolle erstellen und sie während des Starts oder danach einer Instance anfügen. Sie können eine IAM-Rolle für eine Instance auch ersetzen oder trennen.

Inhalt

Erstellen Sie eine IAM-Rolle

Sie müssen eine IAM-Rolle erstellen, bevor Sie eine Instance mit dieser Rolle starten oder die Rolle einer Instance anfügen können.

Console

So erstellen Sie eine IAM-Rolle mit der IAM-Konsole

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Rollen und dann Rolle erstellen aus.
3. Wählen Sie auf der Seite Vertrauenswürdige Entität auswählen die Option AWS-Service und dann den EC2-Anwendungsfall aus. Wählen Sie Weiter aus.

4. Wählen Sie auf der Seite Berechtigungen hinzufügen die Richtlinien aus, die Ihren Instances Zugriff auf die benötigten Ressourcen gewähren. Wählen Sie Weiter aus.
5. Geben Sie auf der Seite Name, Überprüfung und Erstellung einen Namen und eine Beschreibung für die Rolle ein. Fügen Sie der Rolle optional Tags hinzu. Wählen Sie Rolle erstellen aus.

Command line

Im folgenden Beispiel wird eine IAM-Rolle mit einer Richtlinie erstellt, die es der Rolle ermöglicht, einen Amazon S3-Bucket zu verwenden.

IAM-Rolle und Instance-Profil erstellen (AWS CLI)

1. Definieren Sie die folgende Richtlinie und speichern Sie sie in einer Textdatei namens `ec2-role-trust-policy.json`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": { "Service": "ec2.amazonaws.com"},
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. Erstellen Sie die `s3access`-Rolle und geben Sie die Vertrauensrichtlinie an, die Sie mit dem Befehl create-role erstellt haben.

```
aws iam create-role \
    --role-name s3access \
    --assume-role-policy-document file://ec2-role-trust-policy.json
```

Beispielantwort

```
{
    "Role": {
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
```

```
            "Statement": [
                {
                    "Action": "sts:AssumeRole",
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "ec2.amazonaws.com"
                    }
                }
            ]
        },
        "RoleId": "AROAIIZKPBKS2LEXAMPLE",
        "CreateDate": "2013-12-12T23:46:37.247Z",
        "RoleName": "s3access",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:role/s3access"
    }
}
```

3. Schreiben Sie eine Zugriffsrichtlinie und speichern Sie sie in einer Textdatei mit Namen `ec2-role-access-policy.json`. Zum Beispiel gewährt diese Richtlinie Anwendungen, die auf der Instance ausgeführt werden, administrative Berechtigungen für Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:*"],
      "Resource": ["*"]
    }
  ]
}
```

4. Weisen Sie die Zugriffsrichtlinie mit dem Befehl put-role-policy der Rolle zu.

```
aws iam put-role-policy \
    --role-name s3access \
    --policy-name S3-Permissions \
    --policy-document file://ec2-role-access-policy.json
```

5. Erstellen Sie ein Instance-Profil namens „`s3access-profile`“, indem Sie den Befehl create-instance-profile verwenden.

```
aws iam create-instance-profile --instance-profile-name s3access-profile
```

Beispielantwort

```
{
    "InstanceProfile": {
        "InstanceProfileId": "AIPAJTLBPJLEGREXAMPLE",
        "Roles": [],
        "CreateDate": "2013-12-12T23:53:34.093Z",
        "InstanceProfileName": "s3access-profile",
        "Path": "/",
        "Arn": "arn:aws:iam::123456789012:instance-profile/s3access-profile"
    }
}
```

6. Fügen Sie dem Instance-Profil `s3access` die IAM-Rolle `s3access-profile` hinzu.

```
aws iam add-role-to-instance-profile \
    --instance-profile-name s3access-profile \
    --role-name s3access
```

Alternativ können Sie die folgenden AWS Tools for Windows PowerShell Befehle verwenden:

- New-IAMRole
- Registrieren-IAM RolePolicy
- Neu - ich bin InstanceProfile

Starten einer Instance mit einer IAM-Rolle

Nachdem Sie eine IAM-Rolle erstellt haben, können Sie eine Instance starten und dabei die Rolle mit der Instance verknüpfen.

> **Important**
>
> Nach der Erstellung einer IAM-Rolle kann es mehrere Sekunden dauern, bis die Weiterleitung der Berechtigungen abgeschlossen ist. Wenn Sie beim ersten Versuch, eine Instance mit einer Rolle zu starten, einen Fehler erhalten, warten Sie einige Sekunden, bevor Sie es

erneut versuchen. Weitere Informationen finden Sie unter Fehlerbehebung bei IAM-Rollen im IAM-Benutzerhandbuch.

New console

So starten Sie eine Instance mit einer IAM-Rolle (Konsole)

1. Befolgen Sie das Verfahren zum Starten einer Instance.
2. Erweitern Sie Advanced details (Erweiterte Details) und wählen Sie für das IAM instance profile (IAM-Instance-Profil) die von Ihnen erstellte IAM-Rolle aus.

   > **Note**
   >
   > In der Liste der IAM instance profile (IAM-Instance-Profile) wird der Name des Instance-Profils angezeigt, das Sie beim Erstellen Ihrer IAM-Rolle erstellt haben. Wenn Sie die IAM-Rolle mit der Konsole erstellt haben, wurde das Instance-Profil für Sie angelegt und hat denselben Namen wie die Rolle erhalten. Wenn Sie Ihre IAM-Rolle mithilfe der AWS CLI API oder eines AWS SDK erstellt haben, haben Sie Ihr Instanzprofil möglicherweise anders benannt.

3. Konfigurieren Sie alle anderen Details, die Sie für Ihre Instance benötigen oder akzeptieren Sie die Standardeinstellungen und wählen Sie ein Schlüsselpaar aus. Weitere Informationen zu den Feldern im Launch Instance Wizard finden Sie unter Starten einer Instance mit definierten Parametern.
4. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus.
5. Wenn Sie die Amazon EC2 EC2-API-Aktionen in Ihrer Anwendung verwenden, rufen Sie die auf der Instance verfügbaren AWS Sicherheitsanmeldedaten ab und verwenden Sie sie, um die Anfragen zu signieren. Das AWS SDK erledigt das für Sie.

   IMDSv2

   Für Linux-Instances sehen Sie sich das folgende Beispiel an:

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
 "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
meta-data/iam/security-credentials/role_name
```

Für Windows-Instanzen sehen Sie sich das folgende Beispiel an:

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
 -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

IMDSv1

Für Linux-Instances sehen Sie sich das folgende Beispiel an:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-
credentials/role_name
```

Für Windows-Instanzen sehen Sie sich das folgende Beispiel an:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/
security-credentials/role_name
```

Old console

So starten Sie eine Instance mit einer IAM-Rolle (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard Launch Instance (Instance starten) aus.
3. Wählen Sie ein AMI und einen Instance-Typ aus und klicken Sie auf Next: Configure Instance Details.
4. Wählen Sie auf der Seite Configure Instance Details für IAM role die IAM-Rolle aus, die Sie erstellt haben.

> **Note**
>
> In der Liste IAM role wird der Name des Instance-Profils angezeigt, das Sie bei der Erstellung der IAM-Rolle definiert haben. Wenn Sie die IAM-Rolle mit der Konsole erstellt haben, wurde das Instance-Profil für Sie angelegt und hat denselben Namen wie die Rolle erhalten. Wenn Sie Ihre IAM-Rolle mithilfe der AWS CLI API oder eines AWS SDK erstellt haben, haben Sie Ihr Instanzprofil möglicherweise anders benannt.

5. Konfigurieren Sie ggf. andere Details. Folgen Sie den weiteren Anleitungen des Assistenten oder klicken Sie auf Review and Launch, um die Standardeinstellungen zu akzeptieren und direkt die Seite Review Instance Launch aufzurufen.
6. Überprüfen Sie Ihre Einstellungen und klicken Sie auf Launch, um ein Schlüsselpaar auszuwählen und die Instance zu starten.
7. Wenn Sie die Amazon EC2 EC2-API-Aktionen in Ihrer Anwendung verwenden, rufen Sie die auf der Instance verfügbaren AWS Sicherheitsanmeldedaten ab und verwenden Sie sie, um die Anfragen zu signieren. Das AWS SDK erledigt das für Sie.

   IMDSv2

   Für Linux-Instances sehen Sie sich das folgende Beispiel an:

   ```
   [ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H
    "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
   && curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/
   meta-data/iam/security-credentials/role_name
   ```

   Für Windows-Instanzen sehen Sie sich das folgende Beispiel an:

   ```
   PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-
   ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
   ```

   ```
   PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token}
    -Method GET -Uri http://169.254.169.254/latest/meta-data/iam/security-
   credentials/role_name
   ```

   IMDSv1

Für Linux-Instances sehen Sie sich das folgende Beispiel an:

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Für Windows-Instanzen sehen Sie sich das folgende Beispiel an:

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
```

Command line

Sie können den verwenden AWS CLI , um einer Instanz beim Start eine Rolle zuzuordnen. Sie müssen das Instance-Profil im Befehl angeben.

Instance mit IAM-Rolle starten (AWS CLI)

1. Verwenden Sie den run-instances-Befehl, um eine Instance mithilfe des Instance-Profils zu starten. Im folgenden Beispiel wird gezeigt, wie eine Instance mit dem Instance-Profil gestartet wird.

   ```
   aws ec2 run-instances \
       --image-id ami-11aa22bb \
       --iam-instance-profile Name="s3access-profile" \
       --key-name my-key-pair \
       --security-groups my-security-group \
       --subnet-id subnet-1a2b3c4d
   ```

   Verwenden Sie alternativ den PowerShell Befehl New-EC2InstanceTools für Windows.

2. Wenn Sie die Amazon EC2 EC2-API-Aktionen in Ihrer Anwendung verwenden, rufen Sie die auf der Instance verfügbaren AWS Sicherheitsanmeldedaten ab und verwenden Sie sie, um die Anfragen zu signieren. Das AWS SDK erledigt das für Sie.

   ```
   curl http://169.254.169.254/latest/meta-data/iam/security-credentials/role_name
   ```

Anfügen einer IAM-Rolle an eine Instance

Um eine IAM-Rolle an eine Instance ohne Rolle anzufügen, kann sich die Instance im Zustand `stopped` oder `running` befinden.

Console

So fügen Sie einer Instance eine IAM-Rolle an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, klicken Sie auf Actions (Aktionen), Security (Sicherheit), Modify IAM role (IAM-Rolle ändern).
4. Wählen Sie die IAM-Rolle zum Anfügen an die Instance aus und klicken Sie auf Speichern.

Command line

IAM-Rolle einer Instance anfügen (AWS CLI)

1. Falls erforderlich, beschreiben Sie die Instances, um die ID der Instance zu erhalten, der Sie die Rolle anfügen möchten.

```
aws ec2 describe-instances
```

2. Verwenden Sie den associate-iam-instance-profile-Befehl, um der Instance die IAM-Rolle anzufügen, indem Sie das Instance-Profil angeben. Sie können den Amazon-Ressourcennamen (ARN) des Instance-Profils oder dessen Namen angeben.

```
aws ec2 associate-iam-instance-profile \
    --instance-id i-1234567890abcdef0 \
    --iam-instance-profile Name="TestRole-1"
```

Beispielantwort

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-1234567890abcdef0",
        "State": "associating",
        "AssociationId": "iip-assoc-0dbd8529a48294120",
        "IamInstanceProfile": {
```

```
            "Id": "AIPAJLNLDX3AMYZNWYYAY",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-1"
        }
    }
}
```

Verwenden Sie alternativ die folgenden Tools for PowerShell Windows-Befehle:

- Get-EC2Instance
- Register-EC2IamInstanceProfile

Ersetzen einer IAM-Rolle

Um die IAM-Rolle in einer Instance zu ersetzen, an die bereits eine IAM-Rolle angefügt ist, muss sich die Instance im Zustand `running` befinden. Sie können dies tun, wenn Sie die IAM-Rolle für eine Instance ändern möchten, ohne zuvor die vorhandene Instance zu trennen. Sie können dies beispielsweise tun, um sicherzustellen, dass die von Anwendungen auf der Instance ausgeführten API-Aktionen nicht unterbrochen werden.

Console

So ersetzen Sie eine IAM-Rolle für eine Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, klicken Sie auf Actions (Aktionen), Security (Sicherheit), Modify IAM role (IAM-Rolle ändern).
4. Wählen Sie die IAM-Rolle zum Anfügen an die Instance aus und klicken Sie auf Speichern.

Command line

IAM-Rolle für eine Instance ersetzen (AWS CLI)

1. Falls erforderlich, beschreiben Sie Ihre IAM-Instance-Profilverknüpfungen, um die Verknüpfungs-ID für das IAM-Instance-Profil zu erhalten, das Sie ersetzen möchten.

```
aws ec2 describe-iam-instance-profile-associations
```

2. Verwenden Sie den replace-iam-instance-profile-association-Befehl, um das IAM-Instance-Profil zu ersetzen. Geben Sie die Verknüpfungs-ID für das vorhandene Instance-Profil und den ARN oder Namen des Instance-Profils an, welches das vorhandene ersetzen soll.

```
aws ec2 replace-iam-instance-profile-association \
    --association-id iip-assoc-0044d817db6c0a4ba \
    --iam-instance-profile Name="TestRole-2"
```

Beispielantwort

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
        "State": "associating",
        "AssociationId": "iip-assoc-09654be48e33b91e0",
        "IamInstanceProfile": {
            "Id": "AIPAJCJEDKX7QYHWYK7GS",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

Verwenden Sie alternativ die folgenden Tools für PowerShell Windows-Befehle:

- Get-EC2IamInstanceProfileAssociation
- Set-EC2IamInstanceProfileAssociation

Trennen einer IAM-Rolle

Sie können eine IAM-Rolle von einer laufenden oder angehaltenen Instance trennen.

Console

So trennen Sie eine IAM-Rolle von einer Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, klicken Sie auf Actions (Aktionen), Security (Sicherheit), Modify IAM role (IAM-Rolle ändern).

4. Klicken Sie unter IAM-Rolle auf die Option Keine IAM-Rolle. Wählen Sie Save aus.
5. Geben Sie im Bestätigungsdialogfeld Trennen, ein, und wählen Sie dann Trennen.

Command line

IAM-Rolle von einer Instance trennen (AWS CLI)

1. Falls erforderlich, beschreiben Sie Ihre IAM-Instance-Profilverknüpfungen mit dem describe-iam-instance-profile-associations-Befehl, um die Verknüpfungs-ID für das gewünschte IAM-Instance-Profil zu erhalten.

```
aws ec2 describe-iam-instance-profile-associations
```

Beispielantwort

```
{
    "IamInstanceProfileAssociations": [
        {
            "InstanceId": "i-088ce778fbfeb4361",
            "State": "associated",
            "AssociationId": "iip-assoc-0044d817db6c0a4ba",
            "IamInstanceProfile": {
                "Id": "AIPAJEDNCAA64SSD265D6",
                "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
            }
        }
    ]
}
```

2. Verwenden Sie den disassociate-iam-instance-profile-Befehl mit der Verknüpfungs-ID des IAM-Instance-Profils, um dieses zu trennen.

```
aws ec2 disassociate-iam-instance-profile --association-id iip-
assoc-0044d817db6c0a4ba
```

Beispielantwort

```
{
    "IamInstanceProfileAssociation": {
        "InstanceId": "i-087711ddaf98f9489",
```

```
        "State": "disassociating",
        "AssociationId": "iip-assoc-0044d817db6c0a4ba",
        "IamInstanceProfile": {
            "Id": "AIPAJEDNCAA64SSD265D6",
            "Arn": "arn:aws:iam::123456789012:instance-profile/TestRole-2"
        }
    }
}
```

Verwenden Sie alternativ die folgenden Tools für PowerShell Windows-Befehle:

- Get-EC2IamInstanceProfileAssociation
- Unregister-EC2IamInstanceProfile

Generieren einer Richtlinie für Ihre IAM-Rolle basierend auf Zugriffsaktivitäten

Wenn Sie zum ersten Mal eine IAM-Rolle für Ihre Anwendungen erstellen, können Sie manchmal Berechtigungen erteilen, die über das erforderliche hinausgehen. Bevor Sie Ihre Anwendung in Ihrer Produktionsumgebung starten, können Sie eine IAM-Richtlinie generieren, die auf der Zugriffsaktivität für eine IAM-Rolle basiert. IAM Access Analyzer überprüft Ihre AWS CloudTrail Protokolle und generiert eine Richtlinienvorlage, die die Berechtigungen enthält, die von der Rolle in Ihrem angegebenen Zeitraum verwendet wurden. Sie können die Vorlage verwenden, um eine verwaltete Richtlinie mit definierten Berechtigungen zu erstellen und sie dann an die IAM-Rolle anzuhängen. Auf diese Weise gewähren Sie nur die Berechtigungen, die die Rolle für die Interaktion mit AWS Ressourcen für Ihren speziellen Anwendungsfall benötigt. Dies hilft Ihnen, die Best Practice einzuhalten, die geringsten Privilegien zu gewähren. Weitere Informationen finden Sie unter Generieren von Richtlinien basierend auf Zugriffsaktivitäten im IAM-Benutzerhandbuch.

Zugreifen auf Amazon EC2 über einen Schnittstellen-VPC-Endpunkt

Sie können die Sicherheit Ihrer VPC erhöhen, indem Sie eine private Verbindung zwischen Ihrer VPC und Amazon EC2 herstellen. Sie können auf Amazon EC2 zugreifen, als wäre es in Ihrer VPC, ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder AWS Direct Connect eine Verbindung verwenden zu müssen. Die Instances in Ihrer VPC benötigen den Zugriff auf Amazon EC2 keine öffentlichen IP-Adressen.

Weitere Informationen finden Sie AWS PrivateLink im Leitfaden unter Zugriff AWS-Services durch.AWS PrivateLink

Inhalt

Erstellen eines Schnittstellen-VPC-Endpunkts

Erstellen Sie einen Schnittstellen-Endpunkt für Amazon EC2 mit dem folgenden Service-Namen:

- com.amazonaws.***region***.ec2: Erstellt einen Endpunkt für die API-Aktionen für Amazon EC2.

Weitere Informationen finden Sie im AWS PrivateLink Handbuch unter Zugreifen und AWS-Service Verwenden eines Schnittstellen-VPC-Endpunkts.

Erstellen einer Endpunktrichtlinie

Eine Endpunktrichtlinie ist eine IAM-Ressource, die Sie Ihrem Schnittstellen-Endpunkt anfügen können. Die Standard-Endpunktrichtlinie ermöglicht den vollständigen Zugriff auf die Amazon-EC2-API über den Schnittstellen-Endpunkt. Um den Zugriff auf die Amazon-EC2-API von Ihrer VPC aus zu steuern, fügen Sie eine benutzerdefinierte Endpunktrichtlinie an den Endpunkt der Schnittstelle an.

Eine Endpunktrichtlinie gibt die folgenden Informationen an:

- Die Prinzipale, die Aktionen ausführen können.
- Die Aktionen, die ausgeführt werden können.
- Die Ressource, auf der die Aktionen ausgeführt werden können.

> **Important**
>
> Wenn eine nicht standardmäßige Richtlinie auf einen VPC-Schnittstellen-Endpunkt für Amazon EC2 angewendet wird, werden bestimmte fehlgeschlagene API-Anfragen, z. B. solche, die von fehlschlagen`RequestLimitExceeded`, möglicherweise nicht bei Amazon protokolliert. AWS CloudTrail CloudWatch

Weitere Informationen finden Sie unter Steuern des Zugriffs auf Services mit Endpunktrichtlinien im AWS PrivateLink -Leitfaden.

Das folgende Beispiel zeigt eine VPC-Endpunktrichtlinie, die die Berechtigung zum Erstellen unverschlüsselter Volumes oder zum Starten von Instances mit unverschlüsselten Volumes ablehnt. Die Beispielrichtlinie gewährt auch die Berechtigung, alle anderen Amazon EC2-Aktionen auszuführen.

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Action": "ec2:*",
        "Effect": "Allow",
        "Resource": "*",
        "Principal": "*"
    },
    {
        "Action": [
            "ec2:CreateVolume"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    },
    {
        "Action": [
            "ec2:RunInstances"
        ],
        "Effect": "Deny",
        "Resource": "*",
        "Principal": "*",
        "Condition": {
            "Bool": {
                "ec2:Encrypted": "false"
            }
        }
    }]
```

```
}
```

Verwaltung von Updates für Amazon EC2 EC2-Windows-Instances

Wir empfehlen Ihnen, das Betriebssystem und die Anwendungen auf Ihren EC2-Instances regelmäßig zu patchen, zu aktualisieren und zu sichern. Mit dem AWS Systems Manager Patch Manager können Sie den Prozess der Installation sicherheitsrelevanter Updates sowohl für das Betriebssystem als auch für Anwendungen automatisieren.

Für EC2-Instances in einer Auto-Scaling-Gruppe können Sie das AWS-PatchAsgInstance-Runbook verwenden, um zu verhindern, dass Instances, die gerade gepatcht werden, ersetzt werden. Alternativ können Sie alle Services zur automatischen Aktualisierung oder empfohlenen Prozesse für die Installation von Aktualisierungen verwenden, die vom Anwendungsanbieter bereitgestellt werden.

Ressourcen

- AL2023 — Aktualisierung von AL2023 im Amazon Linux 2023-Benutzerhandbuch.
- AL2 — Software auf Ihrer Amazon Linux 2-Instance verwalten Sie im Amazon Linux 2-Benutzerhandbuch.
- Windows-Instanzen —the section called “Update-Management”.

Bewährte Sicherheitsmethoden für Windows-Instanzen

Wir empfehlen Ihnen, diese bewährten Sicherheitsmethoden für Ihre Windows-Instances zu befolgen.

Inhalt

Bewährte Sicherheitsmethoden auf hohem Niveau

Sie sollten die folgenden bewährten Sicherheitsmethoden auf hoher Ebene für Ihre Windows-Instances einhalten:

- Geringster Zugriff — Gewähren Sie nur Systemen und Standorten Zugriff, die vertrauenswürdig sind und von denen erwartet wird. Dies gilt für alle Microsoft-Produkte wie Active Directory, Microsoft-Geschäftsproduktivitätsserver und Infrastruktur-Services wie Remote Desktop-Dienste, Reverse-Proxy-Server, IIS-Webserver usw. Verwenden Sie AWS Funktionen wie Amazon EC2 EC2-Instance-Sicherheitsgruppen, Network Access Control Lists (ACLs) und öffentliche/private Amazon VPC-Subnetze, um die Sicherheit über mehrere Standorte in einer Architektur zu verteilen. Innerhalb einer Windows-Instance können Kunden die Windows-Firewall verwenden, um eine weitere Strategie innerhalb ihrer Implementierung zu entwickeln. defense-in-depth Installieren Sie nur die Betriebssystemkomponenten und -anwendungen, die für die gewünschte Funktion des Systems erforderlich sind. Konfigurieren Sie Infrastruktur-Services wie IIS für die Ausführung unter Servicekonten oder für die Verwendung von Funktionen wie Anwendungspool-Identitäten, um lokal und remote auf Ressourcen in Ihrer gesamten Infrastruktur zuzugreifen.
- Geringste Rechte — Ermitteln Sie die Mindestanzahl an Rechten, die Instanzen und Konten benötigen, um ihre Funktionen auszuführen. Schränken Sie diese Server und Benutzer so ein, dass nur diese definierten Berechtigungen gewährt werden. Verwenden Sie Techniken wie rollenbasierte Zugriffskontrollen, um die Angriffsfläche von Administratorkonten zu reduzieren, und erstellen Sie maximal eingeschränkte Rollen für die Ausführung einer Aufgabe. Verwenden Sie Betriebssystemfunktionen wie Encrypting File System (EFS) in NTFS, um sensible Daten im Ruhezustand zu verschlüsseln und den Anwendungs- und Benutzerzugriff darauf zu kontrollieren.
- Konfigurationsmanagement — Erstellen Sie eine grundlegende Serverkonfiguration, die up-to-date Sicherheitspatches und hostbasierte Schutzpakete umfasst, zu denen Virenschutz, Anti-Malware, Eindringlingserkennung/-prävention und Überwachung der Dateiintegrität gehören. Bewerten Sie jeden Server anhand der aktuell aufgezeichneten Basislinie, um Abweichungen zu identifizieren und zu kennzeichnen. Stellen Sie sicher, dass jeder Server so konfiguriert ist, dass entsprechende Protokoll- und Prüfungsdaten generiert und sicher gespeichert werden.
- Change Management — Erstellen Sie Prozesse zur Kontrolle von Änderungen an den Baselines der Serverkonfiguration und arbeiten Sie auf vollautomatische Änderungsprozesse hin. Nutzen Sie außerdem Just Enough Administration (JEA) mit Windows PowerShell DSC, um den Administratorzugriff auf die minimal erforderlichen Funktionen zu beschränken.
- Patch-Management — Implementieren Sie Prozesse, die das Betriebssystem und die Anwendungen auf Ihren EC2-Instances regelmäßig patchen, aktualisieren und sichern.
- Audit-Logs — Überwachen Sie den Zugriff und alle Änderungen an Amazon EC2 EC2-Instances, um die Serverintegrität zu überprüfen und sicherzustellen, dass nur autorisierte Änderungen vorgenommen werden. Nutzen Sie Funktionen wie Enhanced Logging for IIS, um die standardmäßigen Protokollierungsfunktionen zu verbessern. AWS Funktionen wie VPC Flow

Logs AWS CloudTrail sind auch verfügbar, um den Netzwerkzugriff zu überprüfen, einschließlich erlaubter/verweigerter Anfragen und API-Aufrufe.

Update-Management

Um die besten Ergebnisse zu erzielen, wenn Sie Windows Server auf Amazon EC2 ausführen, empfehlen wir Ihnen, die folgenden bewährten Methoden zu implementieren:

- Configure Windows Update
- Update drivers
- Use the latest Windows AMIs
- Test performance before migration
- Update launch agents
- Starten Sie Ihre Windows-Instance neu, nachdem Sie Updates installiert haben. Weitere Informationen finden Sie unter Durchführen eines Neustarts Ihrer Instance.

Weitere Informationen über den Upgrade oder die Migration einer Windows-Instance auf eine neuere Version von Windows Server finden Sie unter Aktualisieren einer Amazon EC2-Instance unter Windows Server auf eine neuere Version von Windows.

Konfigurieren Sie Windows Update

Standardmäßig erhalten Instances, die über AWS Windows Server-AMIs gestartet werden, keine Updates über Windows Update.

Aktualisieren von Windows-Treibern

Verwenden Sie auf allen Windows-EC2-Instances die neuesten Treiber, damit auf allen Systemen die neuesten Fehlerbehebungen und Leistungsverbesserungen angewendet werden. Abhängig von Ihrem Instance-Typ sollten Sie die AWS PV-, Amazon ENA- und AWS NVMe-Treiber aktualisieren.

- Verwenden Sie SNS-Themen, um Informationen über neue Treiber-Releases zu erhalten.
- Verwenden Sie das AWS Systems Manager Automation-Runbook AWSSupport UpgradeWindowsAWSDrivers, um die Updates einfach auf Ihre Instances anzuwenden.

Starten Sie Instances mit den neuesten Windows-AMIs

AWS veröffentlicht jeden Monat neue Windows-AMIs, die die neuesten Betriebssystem-Patches, Treiber und Start-Agents enthalten. Nutzen Sie das neueste AMI, wenn Sie neue Instances starten oder eigene, benutzerdefinierte Images erstellen.

- Updates für die einzelnen Versionen der AWS Windows-AMIs finden Sie im AWS Windows AMI-Versionsverlauf.
- Weitere Informationen zur Verwendung der neuesten verfügbaren AMIs finden Sie unter Query for the Latest Windows AMI Using Systems Manager Parameter Store.
- Weitere Informationen zu speziellen Windows-AMIs, mit denen Sie Instances für Ihre Datenbank starten können, und zu Anwendungsfällen zur Compliance-Härtung finden Sie unter Spezialisierte Windows-AMIs in der AWS Windows AMI-Referenz.

Testen der System-/Anwendungsleistung vor der Migration

Die Migration von Unternehmensanwendungen zu AWS kann viele Variablen und Konfigurationen beinhalten. Führen Sie immer Tests für die Leistung der EC2-Lösung durch, um Folgendes zu gewährleisten:

- Die Instance-Typen müssen ordnungsgemäß konfiguriert sein, inklusive Instance-Größe, Enhanced Networking und Tenancy (geteilte oder Dedicated).
- Die Instance-Topologie muss für die Workload geeignet sein und bei Bedarf Hochleistungsfunktionen wie Dedicated Tenancy, Platzierungsgruppen, Instance-Speicher-Volumes und Bare-Metal-Instances nutzen.

Aktualisieren von Launch-Agenten

Aktualisieren Sie auf die neueste Launch-Agent-Version von EC2Launch V2, um sicherzustellen, dass aktuelle Verbesserungen auf die gesamte Flotte angewendet werden. Weitere Informationen finden Sie unter the section called “Migrieren”.

Wenn Sie über eine gemischte Flotte verfügen oder wenn Sie die Agenten EC2Launch (Windows Server 2016 und 2019) oder EC2 Config (nur ältere Betriebssysteme) weiterhin verwenden möchten, aktualisieren Sie auf die neuesten Versionen der entsprechenden Agenten.

Automatische Aktualisierungen werden auf den folgenden Kombinationen von Windows-Server-Version und Launch-Agenten unterstützt. Sie können sich in der SSM-Quick Setup des Host-Managements-Konsole unter Amazon-EC2-Launch-Agenten für automatische Updates anmelden.

Windows-Version	EC2Launch v1	EC2Launch v2
2016	✓	✓
2019	✓	✓
2022		✓

- Weitere Informationen zur Aktualisierung auf EC2Launch v2 finden Sie unter. the section called “Installieren”
- Informationen zur manuellen Aktualisierung von EC2Config finden Sie unter. the section called “Installieren von EC2Config”
- Informationen zur manuellen Aktualisierung von EC2Launch finden Sie unter. the section called “Installieren von EC2Launch”

Konfigurationsmanagement

Amazon Machine Images (AMIs) bieten eine Erstkonfiguration für eine Amazon EC2-Instance, die das Windows-Betriebssystem und optionale kundenspezifische Anpassungen wie Anwendungen und Sicherheitskontrollen beinhaltet. Erstellen Sie einen AMI-Katalog mit benutzerdefinierten Sicherheitskonfigurations-Baselines, um sicherzustellen, dass alle Windows-Instances mit Standardsicherheitskontrollen gestartet werden. Sicherheitsbasislinien können in ein AMI integriert, beim Start einer EC2-Instance dynamisch gebootet oder als Produkt für eine einheitliche Verteilung über Service Catalog-Portfolios verpackt werden. AWS Weitere Informationen zum Sichern eines AMIs finden Sie unter Bewährte Methoden für die Erstellung eines AMIs.

Jede Amazon EC2-Instance sollte die organisatorischen Sicherheitsstandards einhalten. Installieren Sie keine Windows-Rollen und -Features, die nicht erforderlich sind, und installieren Sie Software zum Schutz vor bösartigem Code (Antivirus-, Antischadsoftware, Exploit-Begrenzung), überwachen Sie die Host-Integrität und führen Sie Angriffserkennungsmaßnahmen durch. Konfigurieren Sie Sicherheitssoftware, um Betriebssystem-Sicherheitseinstellungen zu überwachen und zu verwalten, die Integrität kritischer Betriebssystemdateien zu schützen und Warnungen zu Abweichungen von

der Sicherheitsbasis zu erhalten. Erwägen Sie, empfohlene Sicherheitskonfigurations-Benchmarks zu implementieren, die von Microsoft, dem Center for Internet Security (CIS) oder dem National Institute of Standards and Technology (NIST) veröffentlicht wurden. Erwägen Sie, andere Microsoft-Tools für bestimmte Anwendungsserver zu verwenden, z. B. Best Practice Analyzer for SQL Server.

AWS Kunden können auch Amazon Inspector-Assessments durchführen, um die Sicherheit und Konformität der auf Amazon EC2 EC2-Instances bereitgestellten Anwendungen zu verbessern. Amazon Inspector prüft Anwendungen automatisch auf Schwachstellen oder Abweichungen von bewährten Methoden und enthält eine Wissensdatenbank aus Hunderten von Regeln, die den gängigen Standards der Sicherheits-Compliance (z. B. PCI DSS) und Schwachstellendefinitionen zugeordnet sind. Beispiele für integrierte Regeln sind die Überprüfung, ob die Remote-Root-Anmeldung aktiviert ist oder, ob anfällige Softwareversionen installiert sind. Diese Regeln werden regelmäßig von AWS Sicherheitsforschern aktualisiert.

Beim Sichern von Windows-Instances wird empfohlen, Active-Directory-Domain-Services zu implementieren, um eine skalierbare, sichere und verwaltbare Infrastruktur für verteilte Standorte zu ermöglichen. Darüber hinaus empfiehlt es sich, nach dem Starten von Instances über die Amazon EC2 EC2-Konsole oder mithilfe eines Amazon EC2-Bereitstellungstools AWS CloudFormation, z. B. native Betriebssystemfunktionen wie Microsoft Windows PowerShell DSC zu verwenden, um den Konfigurationsstatus aufrechtzuerhalten, falls es zu einer Konfigurationsabweichung kommt.

Änderungsmanagement

Nachdem beim Start anfängliche Sicherheits-Baselines auf Amazon EC2-Instances angewendet wurden, kontrollieren Sie fortlaufende Amazon EC2-Änderungen, um die Sicherheit Ihrer virtuellen Maschinen zu wahren. Richten Sie einen Change-Management-Prozess ein, um Änderungen an AWS Ressourcen (wie Sicherheitsgruppen, Routing-Tabellen und Netzwerk-ACLs) sowie an Betriebssystem- und Anwendungskonfigurationen (wie Windows- oder Anwendungspatching, Software-Upgrades oder Updates von Konfigurationsdateien) zu autorisieren und zu integrieren.

AWS stellt mehrere Tools zur Verfügung, mit denen Sie Änderungen an AWS Ressourcen verwalten können AWS CloudTrail, darunter AWS Config, AWS CloudFormation, und AWS Elastic Beanstalk AWS OpsWorks, und Management Packs für Systems Center Operations Manager und System Center Virtual Machine Manager. Beachten Sie, dass Microsoft jeden Dienstag (manchmal sogar täglich) Windows-Patches veröffentlicht und alle Windows-AMIs, die von verwaltet werden, AWS innerhalb von fünf Tagen AWS aktualisiert, nachdem Microsoft einen Patch veröffentlicht hat. Daher ist es wichtig, kontinuierlich alle Basis-AMIs zu patchen, AWS CloudFormation Vorlagen und Auto

Scaling Scaling-Gruppenkonfigurationen mit den neuesten AMI-IDs zu aktualisieren und Tools zur Automatisierung des laufenden Instance-Patch-Managements zu implementieren.

Microsoft bietet verschiedene Optionen zum Verwalten von Windows-Betriebssystem- und Anwendungsänderungen. SCCM bietet beispielsweise eine vollständige Lebenszyklusabdeckung von Umgebungsänderungen. Wählen Sie Tools aus, die geschäftliche Anforderungen erfüllen und steuern, wie sich Änderungen auf Anwendungs-SLAs, Kapazität, Sicherheit und Notfallwiederherstellungsverfahren auswirken. Vermeiden Sie manuelle Änderungen und nutzen Sie stattdessen automatisierte Konfigurationsmanagement-Software oder Befehlszeilentools wie EC2 Run Command oder Windows, PowerShell um skriptbasierte, wiederholbare Änderungsprozesse zu implementieren. Um diese Anforderung zu erfüllen, verwenden Sie Bastion-Hosts mit erweiterter Protokollierung für alle Interaktionen mit Ihren Windows-Instances, um sicherzustellen, dass alle Ereignisse und Aufgaben automatisch aufgezeichnet werden.

Prüfung und Rechenschaftspflicht für Amazon EC2 Windows-Instances

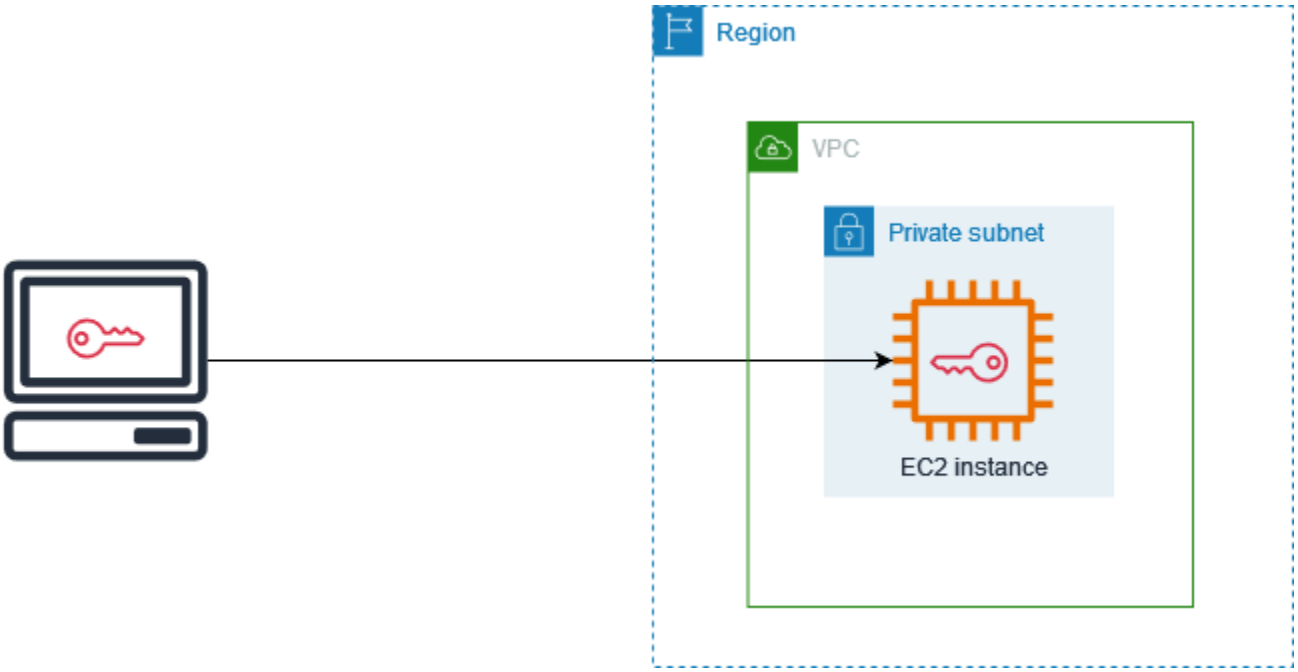
AWS CloudTrail AWS Config, und AWS-Config-Regeln bieten Audit- und Änderungsverfolgungsfunktionen für die Prüfung von AWS Ressourcenänderungen. Konfigurieren Sie Windows-Ereignisprotokolle, um lokale Protokolldateien an ein zentrales Protokollverwaltungssystem zu senden, um Protokolldaten für die Sicherheits- und Betriebsverhaltensanalyse zu führen. Microsoft System Center Operations Manager (SCOM) aggregiert Informationen zu Microsoft-Anwendungen, die auf Windows-Instances bereitgestellt werden, und wendet vorkonfigurierte und benutzerdefinierte Regelsätze basierend auf Anwendungsrollen und -services an. System Center Management Packs bauen auf SCOM auf, um anwendungsspezifische Überwachungs- und Konfigurationsrichtlinien bereitzustellen. Diese Management Packs unterstützen Windows Server Active Directory, SharePoint Server 2013, Exchange Server 2013, Lync Server 2013, SQL Server 2014 und viele weitere Server und Technologien.

Zusätzlich zu den Systemverwaltungstools von Microsoft können Kunden Amazon verwenden, CloudWatch um die CPU-Auslastung, die Festplattenleistung und die Netzwerk-I/O von Instanzen zu überwachen und Host- und Instance-Statusprüfungen durchzuführen. Die Startagenten EC2Config, EC2Launch und EC2Launch v2 bieten Zugriff auf zusätzliche, erweiterte Funktionen für Windows-Instances. Sie können beispielsweise Windows-System-, Sicherheits-, Anwendungs- und Internet Information Services (IIS) -Protokolle in Logs exportieren, die dann in CloudWatch Amazon-Metriken und -Alarme integriert werden können. CloudWatch Kunden können auch Skripts erstellen, die Windows-Leistungsindikatoren in CloudWatch benutzerdefinierte Amazon-Metriken exportieren.

Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances

Ein Schlüsselpaar, bestehend aus einem öffentlichen Schlüssel und einem privaten Schlüssel, ist ein Satz von Sicherheitsanmeldeinformationen, mit denen Sie Ihre Identität nachweisen, wenn Sie eine Verbindung zu einer Amazon EC2-Instance herstellen. Bei Linux-Instances ermöglicht Ihnen der private Schlüssel eine sichere SSH-Verbindung zu Ihrer Instance. Für Windows-Instances ist der private Schlüssel erforderlich, um das Administratorkennwort zu entschlüsseln, das Sie dann verwenden, um eine Verbindung zu Ihrer Instance herzustellen.

Amazon EC2 speichert den öffentlichen Schlüssel auf Ihrer Instance, und Sie speichern den privaten Schlüssel, wie in der folgenden Abbildung dargestellt. Es ist wichtig, dass Sie Ihren privaten Schlüssel an einem sicheren Ort aufbewahren, da jeder, der Ihren privaten Schlüssel besitzt, eine Verbindung zu Ihren Instances herstellen kann, die das key pair verwenden.



Wenn Sie eine Instance starten, können Sie ein key pair angeben, sodass Sie mit einer Methode, die ein key pair erfordert, eine Verbindung zu Ihrer Instance herstellen können. Je nachdem, wie Sie Ihre Sicherheit verwalten, können Sie dasselbe Schlüsselpaar für alle Ihre Instances angeben oder Sie können verschiedene Schlüsselpaare angeben.

Wenn Ihre Instance zum ersten Mal gestartet wird, wird bei Linux-Instances der öffentliche Schlüssel, den Sie beim Start angegeben haben, in einem Eintrag innerhalb Ihrer Linux-Instance platziert`~/.ssh/authorized_keys`. Wenn Sie über SSH eine Verbindung zu Ihrer Linux-Instance

herstellen, müssen Sie den privaten Schlüssel angeben, der dem öffentlichen Schlüssel entspricht, um sich anzumelden.

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer EC2-Instance finden Sie unterConnect zu Ihrer EC2-Instance her.

> **Important**
>
> Da Amazon EC2 keine Kopie Ihres privaten Schlüssels aufbewahrt, besteht keine Möglichkeit, einen privaten Schlüssel wiederherzustellen, wenn Sie ihn verlieren. Es kann jedoch immer noch eine Möglichkeit geben, sich mit Instances zu verbinden, für die Sie den privaten Schlüssel verloren haben. Weitere Informationen finden Sie unter Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Linux-Instance verbinden?.

Als Alternative zu Schlüsselpaaren können Sie die Verbindung AWS Systems Manager Session Managerzu Ihrer Instance über eine interaktive browserbasierte Shell mit einem Klick oder die AWS Command Line Interface () herstellen.AWS CLI

Inhalt

Erstellen Sie ein key pair für Ihre Amazon EC2 EC2-Instance

Sie können Amazon EC2 verwenden, um Ihre Schlüsselpaare zu erstellen, oder Sie können ein Drittanbieter-Tool verwenden, um Ihre Schlüsselpaare zu erstellen und sie dann in Amazon EC2 zu importieren.

Amazon EC2 unterstützt 2048-Bit-SSH-2-RSA-Schlüssel für Linux- und Windows-Instances. Amazon EC2 unterstützt auch ED25519-Schlüssel für Linux-Instances.

Anweisungen zum Herstellen einer Verbindung mit Ihrer Linux-Instance mithilfe von SSH, nachdem Sie ein key pair erstellt haben, finden Sie unterthe section called “Herstellen einer Verbindung zur Linux-Instance”.

Anweisungen zum Herstellen einer Verbindung mit Ihrer Windows-Instance mithilfe von RDP, nachdem Sie ein key pair erstellt haben, finden Sie unterthe section called “Herstellen einer Verbindung mit Ihrer -Windows-Instance”.

Inhalt

Erstellen eines Schlüsselpaars mit Amazon EC2

Wenn Sie mit Amazon EC2 ein Schlüsselpaar erstellen, wird der öffentliche Schlüssel in Amazon EC2 gespeichert und Sie speichern den privaten Schlüssel.

Sie können bis zu 5.000 Schlüsselpaare pro Region erstellen. Um eine Erhöhung zu beantragen, erstellen Sie eine Support-Anfrage. Weitere Informationen finden Sie unter Erstellen eines Support-Falls im Benutzerhandbuch von AWS Support .

Console

Schlüsselpaar mit Amazon EC2 erstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich unter Network & Security die Option Key Pairs aus.
3. Wählen Sie Create Key Pair (Schlüsselpaar erstellen) aus.
4. Geben Sie unter Name einen aussagekräftigen Namen für das Schlüsselpaar ein. Amazon EC2 ordnet den öffentlichen Schlüssel dem Namen zu, den Sie als Schlüsselnamen angeben. Ein Schlüsselname kann bis zu 255 ASCII-Zeichen enthalten. Er darf keine führenden oder nachfolgenden Leerzeichen enthalten.
5. Wählen Sie einen Schlüsselpaartyp, der für Ihr Betriebssystem geeignet ist:

   (Linux-Instances) Wählen Sie als Schlüsselpaartyp entweder RSA oder ED25519 aus.

(Windows-Instances) Wählen Sie als Schlüsselpaartyp die Option RSA aus. ED25519-Schlüssel werden für Windows-Instances nicht unterstützt.

6. Wählen Sie unter Dateiformat für den privaten Schlüssel das Format aus, in dem der private Schlüssel gespeichert werden soll. Um den privaten Schlüssel in einem Format zu speichern, das mit OpenSSH verwendet werden kann, wählen Sie pem. Um den privaten Schlüssel in einem Format zu speichern, das mit PuTTY verwendet werden kann, wählen Sie ppk.
7. Um dem öffentlichen Schlüssel ein Tag (Markierung) hinzuzufügen, wählen Sie Add Tag (Markierung hinzufügen) und geben Sie den Schlüssel und den Wert für das Tag (Markierung) ein. Wiederholen Sie diesen Schritt für jeden Tag (Markierung).
8. Wählen Sie Create Key Pair (Schlüsselpaar erstellen) aus.
9. Die private Schlüsseldatei wird von Ihrem Browser automatisch runtergeladen. Der Basisdateiname ist der Name, den Sie als Name des Schlüsselpaars angegeben haben und die Dateinamenserweiterung wird durch das ausgewählte Dateiformat bestimmt. Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort.

   > **Important**
   >
   > Dies ist die einzige Möglichkeit, die private Schlüsseldatei zu speichern.

10. (Linux-Instanzen) Wenn Sie einen SSH-Client auf einem macOS- oder Linux-Computer verwenden möchten, um eine Verbindung zu Ihrer Linux-Instance herzustellen, verwenden Sie den folgenden Befehl, um die Berechtigungen Ihrer privaten Schlüsseldatei so festzulegen, dass nur Sie sie lesen können.

    ```
    chmod 400 key-pair-name.pem
    ```

    Wenn Sie diese Berechtigungen nicht festlegen, können Sie unter Verwendung dieses Schlüsselpaars keine Verbindung zu Ihrer Instance herstellen. Weitere Informationen finden Sie unter Fehler: Ungeschützte private Schlüsseldatei.

AWS CLI

Schlüsselpaar mit Amazon EC2 erstellen

1. Verwenden Sie den create-key-pair-Befehl wie folgt, um das Schlüsselpaar zu generieren und den privaten Schlüssel in einer `.pem`-Datei zu speichern.

Für `--key-name` geben Sie einen Namen für den öffentlichen Schlüssel an. Der Name kann bis zu 255 ASCII-Zeichen enthalten.

Geben Sie für `--key-type` entweder `rsa` oder `ed25519` an. Wenn Sie den `--key-type`-Parameter nicht verwenden, wird standardmäßig ein `rsa`-Schlüssel erstellt. Hinweis: ED25519-Schlüssel werden für Windows-Instances nicht unterstützt.

Geben Sie für `--key-format` entweder `pem` oder `ppk` an. Wenn Sie den `--key-format`-Parameter nicht verwenden, wird standardmäßig eine `pem`-Datei erstellt.

`--query "KeyMaterial"` druckt das Material des privaten Schlüssels in die Ausgabe.

`--output text > my-key-pair.pem` speichert das Material des privaten Schlüssels in einer Datei mit der angegebenen Erweiterung. Die Erweiterung kann entweder `.pem` oder `.ppk` sein. Der private Schlüssel kann einen Namen haben, der sich vom Namen des öffentlichen Schlüssels unterscheidet. Verwenden Sie jedoch denselben Namen, um die Verwendung zu erleichtern.

```
aws ec2 create-key-pair \
    --key-name my-key-pair \
    --key-type rsa \
    --key-format pem \
    --query "KeyMaterial" \
    --output text > my-key-pair.pem
```

2. (Linux-Instanzen) Wenn Sie einen SSH-Client auf einem macOS- oder Linux-Computer verwenden möchten, um eine Verbindung zu Ihrer Linux-Instance herzustellen, verwenden Sie den folgenden Befehl, um die Berechtigungen Ihrer privaten Schlüsseldatei so festzulegen, dass nur Sie sie lesen können.

```
chmod 400 key-pair-name.pem
```

Wenn Sie diese Berechtigungen nicht festlegen, können Sie unter Verwendung dieses Schlüsselpaars keine Verbindung zu Ihrer Instance herstellen. Weitere Informationen finden Sie unter Fehler: Ungeschützte private Schlüsseldatei.

PowerShell

Schlüsselpaar mit Amazon EC2 erstellen

Verwenden Sie den New-EC2KeyPair AWS Tools for Windows PowerShell Befehl wie folgt, um den Schlüssel zu generieren und ihn in einer `.pem` `.ppk` OR-Datei zu speichern.

Für `-KeyName` geben Sie einen Namen für den öffentlichen Schlüssel an. Der Name kann bis zu 255 ASCII-Zeichen enthalten.

Geben Sie für `-KeyType` entweder `rsa` oder `ed25519` an. Wenn Sie den `-KeyType`-Parameter nicht verwenden, wird standardmäßig ein `rsa`-Schlüssel erstellt. Hinweis: ED25519-Schlüssel werden für Windows-Instances nicht unterstützt.

Geben Sie für `-KeyFormat` entweder `pem` oder `ppk` an. Wenn Sie den `-KeyFormat`-Parameter nicht verwenden, wird standardmäßig eine `pem`-Datei erstellt.

`KeyMaterial` druckt das Material des privaten Schlüssels in die Ausgabe.

`Out-File -Encoding ascii -FilePath` *`C:\path\my-key-pair`*`.pem` speichert das Material des privaten Schlüssels in einer Datei mit der angegebenen Erweiterung. Die Erweiterung kann `.pem` oder `.ppk` sein. Der private Schlüssel kann einen Namen haben, der sich vom Namen des öffentlichen Schlüssels unterscheidet. Verwenden Sie jedoch denselben Namen, um die Verwendung zu erleichtern.

```
PS C:\> (New-EC2KeyPair -KeyName "my-key-pair" -KeyType "rsa" -KeyFormat
 "pem").KeyMaterial | Out-File -Encoding ascii -FilePath C:\path\my-key-pair.pem
```

Erstellen Sie ein key pair mit AWS CloudFormation

Wenn Sie mit ein neues key pair erstellen AWS CloudFormation, wird der private Schlüssel im AWS Systems Manager Parameter Store gespeichert. Der Parametername hat das folgende Format:

```
/ec2/keypair/key_pair_id
```

Weitere Informationen finden Sie unter AWS Systems Manager -Parameterspeicher im Benutzerhandbuch für AWS Systems Manager .

Um ein key pair zu erstellen mit AWS CloudFormation

1. Geben Sie die AWS::EC2::KeyPairRessource in Ihrer Vorlage an.

```
Resources:
```

```
  NewKeyPair:
    Type: 'AWS::EC2::KeyPair'
    Properties:
      KeyName: new-key-pair
```

2. Verwenden Sie den describe-key-pairs-Befehl wie folgt, um die ID des Schlüsselpaars abzurufen.

```
aws ec2 describe-key-pairs --filters Name=key-name,Values=new-key-pair --query
 KeyPairs[*].KeyPairId --output text
```

Es folgt eine Beispielausgabe.

```
key-05abb699beEXAMPLE
```

3. Verwenden Sie den get-parameter-Befehl wie folgt, um den Parameter für Ihren Schlüssel abzurufen und das Schlüsselmaterial in einer `.pem`-Datei zu speichern.

```
aws ssm get-parameter --name /ec2/keypair/key-05abb699beEXAMPLE --with-decryption
 --query Parameter.Value --output text > new-key-pair.pem
```

Erforderliche IAM-Berechtigungen

Um Parameter Store-Parameter in Ihrem Namen verwalten AWS CloudFormation zu können, muss die IAM-Rolle, die von AWS CloudFormation oder Ihrem Benutzer übernommen wurde, über die folgenden Berechtigungen verfügen:

- `ssm:PutParameter` – Gewährt die Berechtigung zum Erstellen eines Parameters für das private Schlüsselmaterial.
- `ssm:DeleteParameter` – Gewährt die Berechtigung zum Löschen des Parameters, der das private Schlüsselmaterial gespeichert hat. Diese Berechtigung ist erforderlich, unabhängig davon, ob das Schlüsselpaar importiert oder von AWS CloudFormation erstellt wurde.

Wenn ein key pair AWS CloudFormation gelöscht wird, das von einem Stack erstellt oder importiert wurde, führt es eine Berechtigungsprüfung durch, um festzustellen, ob Sie berechtigt sind, Parameter zu löschen, obwohl ein Parameter nur AWS CloudFormation erstellt wird, wenn er ein key pair erstellt, nicht, wenn er ein key pair importiert. AWS CloudFormation testet anhand eines erfundenen Parameternamens, der mit keinem Parameter in Ihrem Konto übereinstimmt, die erforderliche

Berechtigung. Daher wird in der `AccessDeniedException`-Fehlermeldung möglicherweise ein fiktiver Parametername angezeigt.

Erstellen Sie ein Schlüsselpaar mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel in Amazon EC2

Linux-Instances

Anstatt Amazon EC2 zum Erstellen eines Schlüsselpaars zu verwenden, können Sie mit einem Drittanbieter-Tool ein RSA- oder ED25519-Schlüsselpaar erstellen und dann den öffentlichen Schlüssel in Amazon EC2 importieren.

Anforderungen für Schlüsselpaare

- Unterstützte Typen: RSA und ED25519. Amazon EC2 akzeptiert keine DSA-Schlüssel.
- Unterstützte Formate
  - OpenSSH-Format für öffentliche Schlüssel (das Format in `~/.ssh/authorized_keys`). Bei einer Verbindung via SSH und Verwendung der EC2 Instance Connect-API wird auch das SSH2-Format unterstützt.
  - Das private Schlüsseldateiformat von SSH muss PEM oder PPK sein
  - (Nur RSA) Base64-codiertes DER-Format
  - (Nur RSA) SSH-Dateiformat für öffentliche Schlüssel wie in RFC 4716 angegeben
- Die unterstützten Längen sind 1024, 2048 und 4096. Bei einr Verbindung via SSH und Verwendung der EC2 Instance Connect-API werden die Längen 2048 und 4096 unterstützt.

So erstellen Sie ein Schlüsselpaar mit einem Tool eines Drittanbieters

1. Generieren Sie ein Schlüsselpaar mit einem Tool eines Drittanbieters Ihrer Wahl. Beispiel: Sie können ssh-keygen (ein mit der standardmäßigen OpenSSH-Installation bereitgestelltes Tool) verwenden. Alternativ bieten Java, Ruby, Python und viele andere Programmiersprachen Standardbibliotheken, die Sie zum Erstellen eines RSA- oder ED25519-Schlüsselpaars verwenden können.

> **Important**
>
> Der private Schlüssel muss im PEM– oder PPK-Format vorliegen. Verwenden Sie zum Beispiel `ssh-keygen -m PEM`, um den OpenSSH-Schlüssel im PEM-Format zu generieren.

2. Speichern Sie den öffentlichen Schlüssel in einer lokalen Datei. Beispiel, `~/.ssh/my-key-pair.pub`. Die Dateinamenerweiterung für diese Datei ist nicht wichtig.
3. Speichern Sie den privaten Schlüssel in einer lokalen Datei mit der Erweiterung `.pem` oder `.ppk`. Zum Beispiel `~/.ssh/my-key-pair.pem` oder `~/.ssh/my-key-pair.ppk`.

> **Important**
>
> Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort. Sie müssen den Namen für Ihren öffentlichen Schlüssel beim Starten einer Instance angeben. Der entsprechende private Schlüssel muss jedes Mal angegeben werden, wenn Sie eine Verbindung mit der Instance herstellen.

Windows-Instances

Statt Ihr Schlüsselpaar mit Amazon EC2 zu erstellen, können Sie ein Drittanbietertool verwenden, um ein RSA-Schlüsselpaar zu erstellen, und den öffentlichen Schlüssel anschließend in Amazon EC2 importieren.

Anforderungen für Schlüsselpaare

- Unterstützte Typen: RSA. Amazon EC2 akzeptiert keine DSA-Schlüssel.

> **Note**
>
> ED25519-Schlüssel werden für Windows-Instances nicht unterstützt.

- Unterstützte Formate
  - OpenSSH-Format für öffentliche Schlüssel
  - Das private Schlüsseldateiformat von SSH muss PEM oder PPK sein
  - (Nur RSA) Base64-codiertes DER-Format

  - (Nur RSA) SSH-Dateiformat für öffentliche Schlüssel wie in RFC 4716 angegeben
- Die unterstützten Längen sind 1024, 2048 und 4096.

So erstellen Sie ein Schlüsselpaar mit einem Tool eines Drittanbieters

1. Generieren Sie ein Schlüsselpaar mit einem Tool eines Drittanbieters Ihrer Wahl. Beispiel: Sie können ssh-keygen (ein mit der standardmäßigen OpenSSH-Installation bereitgestelltes Tool) verwenden. Alternativ bieten Java, Ruby, Python und viele andere Programmiersprachen Standardbibliotheken, die Sie zum Erstellen eines RSA-Schlüsselpaars verwenden können.

   > **Important**
   >
   > Der private Schlüssel muss im PEM– oder PPK-Format vorliegen. Verwenden Sie zum Beispiel `ssh-keygen -m PEM`, um den OpenSSH-Schlüssel im PEM-Format zu generieren.

2. Speichern Sie den öffentlichen Schlüssel in einer lokalen Datei. Beispiel, `C:\keys\my-key-pair.pub`. Die Dateinamenerweiterung für diese Datei ist nicht wichtig.
3. Speichern Sie den privaten Schlüssel in einer lokalen Datei mit der Erweiterung `.pem` oder `.ppk`. Zum Beispiel `C:\keys\my-key-pair.pem` oder `C:\keys\my-key-pair.ppk`. Die Dateinamenerweiterung für diese Datei ist wichtig, da nur `.pem` Dateien ausgewählt werden können, wenn Sie von der EC2-Konsole aus eine Verbindung zu Ihrer Windows-Instance herstellen.

   > **Important**
   >
   > Speichern Sie die Datei mit dem privaten Schlüssel an einem sicheren Ort. Sie müssen den Namen für Ihren öffentlichen Schlüssel beim Starten einer Instance angeben. Der entsprechende private Schlüssel muss jedes Mal angegeben werden, wenn Sie eine Verbindung mit der Instance herstellen.

Nachdem Sie das Schlüsselpaar erstellt haben, verwenden Sie eine der folgenden Methoden, um den öffentlichen Schlüssel in Amazon EC2 zu importieren.

Console

Öffentlichen Schlüssel in Amazon EC2 importieren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Key Pairs aus.
3. Wählen Sie Import Key Pair (Schlüsselpaar importieren) aus.
4. Geben Sie unter Name einen aussagekräftigen Namen für den öffentlichen Schlüssel ein. Der Name kann bis zu 255 ASCII-Zeichen enthalten. Er darf keine führenden oder nachfolgenden Leerzeichen enthalten.

   > **Note**
   >
   > Wenn Sie über die EC2-Konsole eine Verbindung zu Ihrer Instance herstellen, schlägt die Konsole diesen Namen für den Namen Ihrer privaten Schlüsseldatei vor.

5. Wählen Sie entweder Browse (Durchsuchen), um zu Ihrem öffentlichen Schlüssel zu navigieren und ihn auszuwählen oder fügen Sie den Inhalt Ihres öffentlichen Schlüssels in das Feld Public key contents (Inhalt des öffentlichen Schlüssels) ein.
6. Wählen Sie Import Key Pair (Schlüsselpaar importieren) aus.
7. Stellen Sie sicher, dass der importierte öffentliche Schlüssel in der Liste der Schlüsselpaare angezeigt wird.

AWS CLI

Öffentlichen Schlüssel in Amazon EC2 importieren

Verwenden Sie den import-key-pair AWS CLI -Befehl.

So überprüfen Sie, ob das Schlüsselpaar erfolgreich importiert wurde

Verwenden Sie den describe-key-pairs AWS CLI -Befehl.

PowerShell

Öffentlichen Schlüssel in Amazon EC2 importieren

Verwenden Sie den Import-EC2KeyPair AWS Tools for Windows PowerShell -Befehl.

So überprüfen Sie, ob das Schlüsselpaar erfolgreich importiert wurde

Verwenden Sie den Get-EC2KeyPair AWS Tools for Windows PowerShell -Befehl.

Taggen eines Schlüsselpaars

Um die Schlüsselpaare, die Sie entweder mit Amazon EC2 erstellt oder in Amazon EC2 importiert haben, zu kategorisieren und zu verwalten, können Sie sie mit benutzerdefinierten Metadaten kennzeichnen. Weitere Informationen zur Funktionsweise von Tags (Markierungen) finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).

Console

So zeigen Sie ein Tag für ein key pair an, fügen es hinzu oder löschen es

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Key Pairs aus.
3. Wählen Sie einen öffentlichen Schlüssel aus und wählen Sie dann Aktionen, Tags verwalten.
4. Auf der Seite Tags verwalten werden alle Tags angezeigt, die dem öffentlichen Schlüssel zugewiesen sind.
   - Um ein Tag (Markierung) hinzuzufügen, wählen Sie Add Tags (Tags (Markierungen) hinzufügen) und geben Sie dann den Tag (Markierung)-Schlüssel und -Wert ein. Sie können Sie bis zu 50 Tags (Markierung) pro Schlüssel hinzufügen. Weitere Informationen finden Sie unter Tag (Markierung)-Einschränkungen.
   - Um ein Tag (Markierungen) zu löschen, wählen Sie Remove (Entfernen) neben dem zu löschenden Tag (Markierung).
5. Wählen Sie Save aus.

AWS CLI

Um die Tags für Ihre Schlüsselpaare anzuzeigen

Verwenden Sie den describe-tags AWS CLI -Befehl. Im folgenden Beispiel beschreiben Sie die Tags (Markierungen) für alle Ihre öffentlichen Schlüssel.

```
aws ec2 describe-tags --filters "Name=resource-type,Values=key-pair"
```

```
{
    "Tags": [
    {
        "Key": "Environment",
        "ResourceId": "key-0123456789EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    },
    {
        "Key": "Environment",
        "ResourceId": "key-9876543210EXAMPLE",
        "ResourceType": "key-pair",
        "Value": "Production"
    }]
}
```

Um die Tags für ein key pair zu beschreiben

Verwenden Sie den describe-key-pairs AWS CLI -Befehl.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789EXAMPLE
```

```
{
    "KeyPairs": [
    {
        "KeyName": "MyKeyPair",
        "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
        "KeyPairId": "key-0123456789EXAMPLE",
        "Tags": [
        {
            "Key": "Environment",
            "Value": "Production"
        }]
    }]
}
```

Um ein key pair zu taggen

Verwenden Sie den create-tags AWS CLI -Befehl. Im folgenden Beispiel wird der öffentliche Schlüssel mit `Key=Cost-Center` und `Value=CC-123` markiert.

```
aws ec2 create-tags --resources key-0123456789EXAMPLE --tags Key=Cost-
Center,Value=CC-123
```

So löschen Sie ein Tag aus einem Schlüsselpaar

Verwenden Sie den delete-tags AWS CLI -Befehl. Beispiele finden Sie unter Examples (Beispiele) in der AWS CLI -Befehlsreferenz.

PowerShell

Um Tags für Ihre Schlüsselpaare anzuzeigen

Verwenden Sie den Get-EC2Tag-Befehl.

Um die Tags für ein key pair zu beschreiben

Verwenden Sie den Get-EC2KeyPair-Befehl.

Um ein key pair zu taggen

Verwenden Sie den New-EC2Tag-Befehl.

So löschen Sie ein Tag aus einem Schlüsselpaar

Verwenden Sie den Remove-EC2Tag-Befehl.

Beschreiben Sie Ihre Schlüsselpaare

Sie können die Schlüsselpaare beschreiben, die Sie in Amazon EC2 gespeichert haben. Sie können auch das Material zum öffentlichen Schlüssel abrufen und den öffentlichen Schlüssel identifizieren, der beim Start angegeben wurde.

Themen

Beschreiben Sie Ihre Schlüsselpaare

Sie können die folgenden Informationen zu Ihren öffentlichen Schlüsseln anzeigen, die in Amazon EC2 gespeichert sind: Name des öffentlichen Schlüssels, ID, Schlüsseltyp, Fingerabdruck, Material

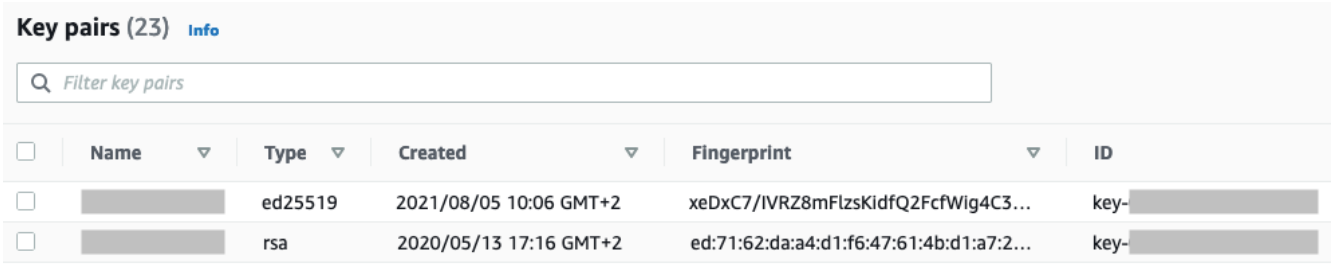
zum öffentlichen Schlüssel, Datum und Uhrzeit (UTC) der Schlüsselerstellung durch von Amazon EC2 (wenn der Schlüssel von einem Drittanbieter-Tool erstellt wurde, dann ist es das Datum und Uhrzeit, zu der der Schlüssel in Amazon EC2 importiert wurde) sowie alle Tags, die mit dem öffentlichen Schlüssel in Verbindung stehen sind.

Sie können die Amazon EC2 EC2-Konsole verwenden oder Informationen AWS CLI zu Ihren öffentlichen Schlüsseln anzeigen.

Console

Informationen über Ihre öffentlichen Schlüssel anzeigen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich Key Pairs (Schlüsselpaare) aus.
3. Sie können Informationen zu jedem öffentlichen Schlüssel in der Tabelle Key pairs (Schlüsselpaare) anzeigen.



4. Um die Tags eines öffentlichen Schlüssels anzuzeigen, aktivieren Sie das Kontrollkästchen neben dem Schlüssel und klicken dann auf Actions (Aktionen) und Manage tags (Tags verwalten).

AWS CLI

Öffentlichen Schlüssel beschreiben

Verwenden Sie den describe-key-pairs-Befehl und geben Sie den `--key-names`-Parameter an.

```
aws ec2 describe-key-pairs --key-names key-pair-name
```

Beispielausgabe

```
{
```

```
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Alternativ können Sie den öffentlichen Schlüssel anstatt mit `--key-names` mit dem Parameter `--key-pair-ids` angeben.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example
```

Um das Material zum öffentlichen Schlüssel in der Ausgabe anzuzeigen, müssen Sie den Parameter `--include-public-key` angeben.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Beispielausgabe: In der Ausgabe enthält das Feld `PublicKey` das Material zum öffentlichen Schlüssel.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Abrufen des Materials zum öffentlichen Schlüssel

Sie können mit verschiedenen Methoden Zugriff auf das Material zum öffentlichen Schlüssel erhalten. Sie können das Material des öffentlichen Schlüssels aus dem entsprechenden privaten Schlüssel auf Ihrem lokalen Computer, aus den Instance-Metadaten der Instance, die mit dem öffentlichen Schlüssel gestartet wurde, oder mithilfe des `describe-key-pairs` AWS CLI Befehls abrufen. Bei Linux-Instances kann das Material des öffentlichen Schlüssels auch aus der `authorized_keys` Datei auf der Instance abgerufen werden.

Verwenden Sie eine der folgenden Methoden, um das Material zum öffentlichen Schlüssel abzurufen.

Linux-Instances

From the private key

Material zum öffentlichen Schlüssel aus privatem Schlüssel abrufen

Sie können auf Ihrem lokalen Linux- oder macOS-Computer den Befehl ssh-keygen verwenden, um den öffentlichen Schlüssel für Ihr Schlüsselpaar abzurufen. Geben Sie den Pfad an, in den Sie Ihren privaten Schlüssel heruntergeladen haben (die `.pem`-Datei).

```
ssh-keygen -y -f /path_to_key_pair/my-key-pair.pem
```

Der Befehl gibt den öffentlichen Schlüssel zurück, wie im folgenden Beispiel gezeigt.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE
```

Falls der Befehl fehlschlägt, führen Sie den folgenden Befehl aus, um sicherzustellen, dass Sie die Berechtigungen für Ihre private Schlüsselpaardatei so geändert haben, dass nur Sie diese anzeigen können.

```
chmod 400 key-pair-name.pem
```

From the instance metadata

Sie können Instance Metadata Service Version 2 oder Instance Metadata Service Version 1 verwenden, um den öffentlichen Schlüssel aus den Instance-Metadaten abzurufen.

> **Note**
>
> Wenn Sie das Schlüsselpaar ändern, mit dem Sie eine Verbindung zur Instance herstellen, aktualisiert Amazon EC2 die Instance-Metadaten nicht, um den neuen öffentlichen Schlüssel anzuzeigen. Die Instance-Metadaten zeigen weiterhin den öffentlichen Schlüssel für das Schlüsselpaar an, das Sie beim Starten der Instance angegeben haben.

Material zum öffentlichen Schlüssel aus Instance-Metadaten abrufen

Verwenden Sie einen der folgenden Befehle über Ihre Instance.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Beispielausgabe

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Weitere Informationen zu Instance-Metadaten erhalten Sie unter Abrufen von Instance-Metadaten.

From the instance

Wenn Sie beim Starten einer Linux-Instance ein Schlüsselpaar angeben, wird der Inhalt des öffentlichen Schlüssels beim ersten Starten der Instance in einem Eintrag innerhalb von `~/.ssh/authorized_keys` auf der Instance platziert.

Material zum öffentlichen Schlüssel aus einer Instance abrufen

1. Verbinden Sie sich mit der Instance.
2. Öffnen Sie die `authorized_keys`-Datei im Terminalfenster mit Ihrem bevorzugten Texteditor (z. B. vim oder nano).

```
[ec2-user ~]$ nano ~/.ssh/authorized_keys
```

Die `authorized_keys`-Datei wird geöffnet und zeigt den öffentlichen Schlüssel gefolgt vom Namen des Schlüsselpaars an. Folgendes ist ein Beispieleintrag für das Schlüsselpaar mit der Bezeichnung *key-pair-name*.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

From describe-key-pairs

Material zum öffentlichen Schlüssel aus dem Befehl **`describe-key-pairs`** in der AWS CLI abrufen

Verwenden Sie den describe-key-pairs-Befehl und geben Sie den `--key-names`-Parameter an, um den öffentlichen Schlüssel zu identifizieren. Damit das Material zum öffentlichen Schlüssel in der Ausgabe enthalten ist, müssen Sie den Parameter `--include-public-key` angeben.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Beispielausgabe: In der Ausgabe enthält das Feld `PublicKey` das Material zum öffentlichen Schlüssel.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
```

```
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Alternativ können Sie den öffentlichen Schlüssel anstatt mit `--key-names` mit dem Parameter `--key-pair-ids` angeben.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Windows-Instances

From the private key

Material zum öffentlichen Schlüssel aus privatem Schlüssel abrufen

Sie können auf Ihrem lokalen Windows-Computer den PuTTYgen-Befehl verwenden, um den öffentlichen Schlüssel für Ihr Schlüsselpaar abzurufen.

Starten Sie PuTTYgen und wählen Sie Load (Laden) aus. Wählen Sie die private `.ppk`- oder `.pem`-Schlüsseldatei aus. PuTTYgen zeigt den öffentlichen Schlüssel unter Public key for pasting into OpenSSH authorized_keys file (Öffentliche Schlüssel zum Einfügen in die authorized_keys-Datei von OpenSSH) an. Sie können den öffentlichen Schlüssel auch anzeigen, indem Sie Save public key (Öffentlichen Schlüssel speichern) wählen, einen Namen für die Datei angeben, diese speichern und dann öffnen.

From the instance metadata

Sie können Instance Metadata Service Version 2 oder Instance Metadata Service Version 1 verwenden, um den öffentlichen Schlüssel aus den Instance-Metadaten abzurufen.

> **Note**
>
> Wenn Sie das Schlüsselpaar ändern, mit dem Sie eine Verbindung zur Instance herstellen, aktualisiert Amazon EC2 die Instance-Metadaten nicht, um den neuen öffentlichen Schlüssel anzuzeigen. Die Instance-Metadaten zeigen weiterhin den

öffentlichen Schlüssel für das Schlüsselpaar an, das Sie beim Starten der Instance angegeben haben.

Material zum öffentlichen Schlüssel aus Instance-Metadaten abrufen

Verwenden Sie einen der folgenden Befehle über Ihre Instance.

IMDSv2

```
PS C:\> [string]$token = Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token-ttl-seconds" = "21600"} -Method PUT -Uri http://169.254.169.254/latest/api/token
```

```
PS C:\> Invoke-RestMethod -Headers @{"X-aws-ec2-metadata-token" = $token} -Method
 GET -Uri http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

IMDSv1

```
PS C:\> Invoke-RestMethod -uri  http://169.254.169.254/latest/meta-data/public-keys/0/openssh-key
```

Beispielausgabe

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQClKsfkNkuSevGj3eYhCe53pcjqP3maAhDFcvBS7O6V
hz2ItxCih+PnDSUaw+WNQn/mZphTk/a/gU8jEzoOWbkM4yxyb/wB96xbiFveSFJuOp/d6RJhJOI0iBXr
lsLnBItntckiJ7FbtxJMXLvvwJryDUilBMTjYtwB+QhYXUMOzce5Pjz5/i8SeJtjnV3iAoG/cQk+0FzZ
qaeJAAHco+CY/5WrUBkrHmFJr6HcXkvJdWPkYQS3xqC0+FmUZofz221CBt5IMucxXPkX4rWi+z7wB3Rb
BQoQzd8v7yeb7OzlPnWOyN0qFU0XA246RA8QFYiCNYwI3f05p6KLxEXAMPLE key-pair-name
```

Weitere Informationen zu Instance-Metadaten erhalten Sie unter Abrufen von Instance-Metadaten.

From describe-key-pairs

Material zum öffentlichen Schlüssel aus dem Befehl **`describe-key-pairs`** in der AWS CLI abrufen

Verwenden Sie den describe-key-pairs-Befehl und geben Sie den `--key-names`-Parameter an, um den öffentlichen Schlüssel zu identifizieren. Damit das Material zum öffentlichen Schlüssel in der Ausgabe enthalten ist, müssen Sie den Parameter `--include-public-key` angeben.

```
aws ec2 describe-key-pairs --key-names key-pair-name --include-public-key
```

Beispielausgabe: In der Ausgabe enthält das Feld `PublicKey` das Material zum öffentlichen Schlüssel.

```
{
    "KeyPairs": [
        {
            "KeyPairId": "key-0123456789example",
            "KeyFingerprint":
 "1f:51:ae:28:bf:89:e9:d8:1f:25:5d:37:2d:7d:b8:ca:9f:f5:f1:6f",
            "KeyName": "key-pair-name",
            "KeyType": "rsa",
            "Tags": [],
            "PublicKey": "ssh-ed25519
 AAAAC3NzaC1lZDI1NTE5AAAAIIj7azlDjVHAsSxgcpCRZ3oWnTm0nAFM64y9jd22ioI/ my-key-pair",
            "CreateTime": "2022-04-28T11:37:26.000Z"
        }
    ]
}
```

Alternativ können Sie den öffentlichen Schlüssel anstatt mit `--key-names` mit dem Parameter `--key-pair-ids` angeben.

```
aws ec2 describe-key-pairs --key-pair-ids key-0123456789example --include-public-key
```

Identifizieren des öffentlichen Schlüssels, der beim Start angegeben wurde

Wenn Sie beim Starten einer Instance einen öffentlichen Schlüssel angeben, wird der Name des öffentlichen Schlüssels von der Instance aufgezeichnet.

Das Schlüsselpaar identifizieren, das beim Start angegeben wurde

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Auf der Registerkarte Details unter Instance-Details zeigt das Feld Beim Start zugewiesenes Schlüsselpaar den Namen des öffentlichen Schlüssels, den Sie beim Starten der Instance angegeben haben.

> **Note**
>
> Der Wert des Felds Beim Start zugewiesenes Schlüsselpaar ändert sich nicht, auch wenn Sie den öffentlichen Schlüssel in der Instance ändern oder öffentliche Schlüssel hinzufügen.

Löschen Ihres Schlüsselpaars

Sie können ein key pair löschen, wodurch der in Amazon EC2 gespeicherte öffentliche Schlüssel entfernt wird. Durch das Löschen eines key pair wird der entsprechende private Schlüssel nicht gelöscht.

Wenn Sie einen öffentlichen Schlüssel mithilfe der folgenden Methoden löschen, wird lediglich der öffentliche Schlüssel gelöscht, der in Amazon EC2 gespeichert wurde, als Sie das Schlüsselpaar erstellt oder importiert haben. Durch das Löschen eines öffentlichen Schlüssels wird der öffentliche Schlüssel nicht aus Instances entfernt, zu denen Sie ihn hinzugefügt haben, entweder beim Starten der Instance oder später. Außerdem wird der private Schlüssel dabei nicht auf Ihrem lokalen Computer gelöscht. Sie können weiterhin Verbindungen zu Instances herstellen, die Sie mit einem öffentlichen Schlüssel gestartet haben, den Sie aus Amazon EC2 gelöscht haben, solange Sie noch die Datei mit dem privaten Schlüssel (`.pem`) haben.

> **Important**
>
> Wenn Sie eine Auto-Scaling-Gruppe verwenden (z. B. in einer Elastic-Beanstalk-Umgebung), stellen Sie sicher, dass der öffentliche Schlüssel, den Sie löschen, nicht in einer verknüpften Startvorlage oder Startkonfiguration angegeben ist. Wenn Amazon EC2 Auto Scaling eine fehlerhafte Instance erkennt, startet es eine Ersatz-Instance. Der Start der Instance schlägt jedoch fehl, wenn der öffentliche Schlüssel nicht gefunden werden kann. Weitere Informationen finden Sie unter Startvorlagen im Benutzerhandbuch für Amazon EC2 Auto Scaling.

Console

Öffentlichen Schlüssel in Amazon EC2 löschen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option Key Pairs aus.

3. Wählen Sie das zu löschende Schlüsselpaar aus und wählen Sie Actions (Aktionen), Delete (Löschen).
4. Geben Sie in das Bestätigungsfeld `Delete` ein und wählen Sie dann Delete (Löschen).

AWS CLI

Öffentlichen Schlüssel in Amazon EC2 löschen

Verwenden Sie den delete-key-pair AWS CLI -Befehl.

PowerShell

Öffentlichen Schlüssel in Amazon EC2 löschen

Verwenden Sie den Remove-EC2KeyPair AWS Tools for Windows PowerShell -Befehl.

Fügen Sie einen öffentlichen Schlüssel auf Ihrer Linux-Instance hinzu oder entfernen Sie ihn

> Wenn Sie einen privaten Schlüssel verlieren, verlieren Sie den Zugriff auf alle Instances, die das key pair verwenden. Weitere Informationen zum Herstellen einer Verbindung zu einer Instance mit einem anderen key pair als dem, das Sie beim Start angegeben haben, finden Sie unter Ich habe meinen privaten Schlüssel verloren.

Sie können das Schlüsselpaar beim Starten einer Instance angeben. Wenn Sie beim Start ein Schlüsselpaar angeben, wird das Material zum öffentlichen Schlüssel, wenn Ihre Instance zum ersten Mal hochfährt, auf Ihrer Linux-Instance in einem Eintrag innerhalb von `~/.ssh/authorized_keys` platziert.

Sie können das Schlüsselpaar ändern, das für den Zugriff auf das Standard-Systemkonto Ihrer Instance verwendet wird, indem Sie einen neuen öffentlichen Schlüssel für die Instance hinzufügen oder den öffentlichen Schlüssel für die Instance ersetzen (Löschen des vorhandenen öffentlichen Schlüssels und Hinzufügen eines neuen Schlüssels). Sie können auch alle öffentlichen Schlüssel aus einer Instance entfernen. Um ein Schlüsselpaar hinzuzufügen oder zu ersetzen, müssen Sie eine Verbindung zu Ihrer Instance herstellen können.

Sie können aus den folgenden Gründen ein key pair hinzufügen oder ersetzen:

- Wenn ein Benutzer in Ihrer Organisation mithilfe eines separaten Schlüsselpaars Zugriff auf den Systembenutzer benötigt, können Sie den öffentlichen Schlüssel zu Ihrer Instance hinzufügen.
- Wenn ein Benutzer eine Kopie des privaten Schlüssels (`.pem`-Datei) besitzt und Sie verhindern möchten, dass er eine Verbindung zu Ihrer Instance herstellt (beispielsweise weil er Ihre Organisation verlassen hat), können Sie den öffentlichen Schlüssel für die Instance löschen und durch einen neuen ersetzen.
- Wenn Sie ein Linux-AMI von einer Instance erstellen, wird das Material zum öffentlichen Schlüssel von der Instance in das AMI kopiert. Wenn Sie eine Instance über das AMI starten, enthält die neue Instance den öffentlichen Schlüssel aus der ursprünglichen Instance. Um zu verhindern, dass ein Benutzer, der im Besitz des privaten Schlüssels ist, eine Verbindung zur neuen Instance herstellen kann, entfernen Sie den öffentlichen Schlüssel aus der ursprünglichen Instance, bevor Sie das AMI erstellen.

Verwenden Sie die folgenden Verfahren, um das key pair für den Standardbenutzer zu ändern, z. `ec2-user` B. Informationen zum Hinzufügen von Benutzern zu Ihrer Instance finden Sie in der Dokumentation für das Betriebssystem auf Ihrer Instance.

So fügen Sie ein Schlüsselpaar hinzu oder ersetzen es

1. Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole oder einem Tool eines Drittanbieters.
2. Rufen Sie den öffentlichen Schlüssel über Ihr neues Schlüsselpaar ab. Weitere Informationen finden Sie unter Abrufen des Materials zum öffentlichen Schlüssel.
3. Stellen Sie eine Verbindung zu Ihrer Instance mithilfe Ihres bestehenden privaten Schlüssels her.
4. Öffnen Sie die `.ssh/authorized_keys`-Datei in der Instance in einem Texteditor Ihrer Wahl. Fügen Sie die Informationen zum öffentlichen Schlüssel aus Ihrem neuen Schlüsselpaar unter den Informationen zum vorhandenen öffentlichen Schlüssel ein. Speichern Sie die Datei.
5. Trennen Sie die Verbindung zu Ihrer Instance und testen Sie, ob Sie mit der Datei des neuen privaten Schlüssels eine Verbindung zu Ihrer Instance herstellen können.
6. (Optional) Falls Sie ein vorhandenes Schlüsselpaar ersetzen, stellen Sie eine Verbindung zu Ihrer Instance her und löschen Sie die Informationen zum öffentlichen Schlüssel für Ihr ursprüngliches Schlüsselpaar aus der `.ssh/authorized_keys`-Datei.

> **Important**
>
> Wenn Sie eine Auto-Scaling-Gruppe verwenden, stellen Sie sicher, dass das Schlüsselpaar, das Sie ersetzen, nicht in Ihrer Startvorlage oder Startkonfiguration angegeben ist. Wenn Amazon EC2 Auto Scaling eine fehlerhafte Instance erkennt, startet es eine Ersatz-Instance. Der Start der Instance schlägt jedoch fehl, wenn das Schlüsselpaar nicht gefunden werden kann. Weitere Informationen finden Sie unter Startvorlagen im Benutzerhandbuch für Amazon EC2 Auto Scaling.

Öffentlichen Schlüssel von einer Instance entfernen

1. Verbinden Sie sich mit der Instance.
2. Öffnen Sie die `.ssh/authorized_keys`-Datei in der Instance in einem Texteditor Ihrer Wahl. Löschen Sie die Informationen zum öffentlichen Schlüssel und speichern Sie die Datei.

> **Warning**
>
> Nachdem Sie alle öffentlichen Schlüssel von einer Instance entfernt und die Verbindung zur Instance getrennt haben, können Sie keine neue Verbindung mehr herstellen – es sei denn, das AMI bietet eine andere Möglichkeit zur Anmeldung.

Überprüfen des Fingerabdrucks Ihres Schlüsselpaars

Um den Fingerabdruck Ihres Schlüsselpaars zu überprüfen, vergleichen Sie den Fingerabdruck, der auf der Seite Schlüsselpaare in der Amazon-EC2-Konsole angezeigt oder vom Befehl describe-key-pairs zurückgegeben wird, mit dem Fingerabdruck, den Sie mit dem privaten Schlüssel auf Ihrem lokalen Computer generiert haben. Diese Fingerabdrücke sollten übereinstimmen.

Wenn Amazon EC2 einen Fingerabdruck berechnet, wird dem Fingerabdruck möglicherweise Padding (mit =-Zeichen) angefügt. Andere Tools wie etwa ssh-keygen lassen dieses Padding unter Umständen weg.

Wenn Sie versuchen, den Fingerabdruck Ihrer Linux EC2-Instance zu verifizieren, nicht den Fingerabdruck Ihres key pair, finden Sie weitere Informationen unter Instance-Fingerabdruck abrufen.

So werden die Fingerabdrücke berechnet

Amazon EC2 verwendet verschiedene Hash-Funktionen, um die Fingerabdrücke für RSA- und ED25519-Schlüsselpaare zu berechnen. Darüber hinaus berechnet Amazon EC2 für RSA-Schlüsselpaare die Fingerabdrücke mit unterschiedlichen Hash-Funktionen unterschiedlich, je nachdem, ob das Schlüsselpaar von Amazon EC2 erstellt oder in Amazon EC2 importiert wurde.

In der folgenden Tabelle sind die Hash-Funktionen aufgeführt, die zur Berechnung der Fingerabdrücke für RSA- und ED25519 -Schlüsselpaare verwendet werden, die von Amazon EC2 erstellt und in Amazon EC2 importiert werden.

(Linux-Instances) Hash-Funktionen, die zur Berechnung von Fingerabdrücken verwendet werden

Schlüsselpaar-Quelle	RSA-Schlüsselpaare (Windows und Linux)	ED25519-Schlüsselpaare (Linux)
Erstellt von Amazon EC2	SHA-1	SHA-256
Importiert in Amazon EC2	MD5[1]	SHA-256

[1] Falls Sie einen öffentlichen RSA-Schlüssel in Amazon EC2 importieren, wird der Fingerabdruck mit einer MD5-Hash-Funktion berechnet. Dies gilt unabhängig davon, wie Sie das Schlüsselpaar erstellt haben, z. B. durch Verwendung eines Drittanbieter-Tools oder durch Generieren eines neuen öffentlichen Schlüssels aus einem vorhandenen privaten Schlüssel, der mit Amazon EC2 erstellt wurde.

Bei Verwendung des gleichen Schlüsselpaars in verschiedenen Regionen

Wenn Sie dasselbe key pair verwenden möchten, um eine Verbindung zu Instances in verschiedenen Instanzen herzustellen AWS-Regionen, müssen Sie den öffentlichen Schlüssel in alle Regionen importieren, in denen Sie ihn verwenden werden. Falls Sie Amazon EC2 zum Erstellen des Schlüsselpaars verwenden, können Sie Abrufen des Materials zum öffentlichen Schlüssel, damit Sie den öffentlichen Schlüssel in die anderen Regionen importieren können..

> **Note**
>
> - Beachten Sie, dass die importierten öffentlichen Schlüssel einen anderen Fingerabdruck haben als der ursprüngliche öffentliche Schlüssel, wenn Sie ein RSA-Schlüsselpaar mit Amazon EC2 erstellen und dann einen öffentlichen Schlüssel aus dem privaten Schlüssel

von Amazon EC2 generieren. Dies liegt daran, dass der Fingerabdruck des ursprünglichen RSA-Schlüssels, der mit Amazon EC2 erstellt wurde, mit einer SHA-1-Hash-Funktion berechnet wird, während der Fingerabdruck der importierten RSA-Schlüssel mit einer MD5-Hash-Funktion berechnet wird.

- Bei ED25519-Schlüsselpaaren sind die Fingerabdrücke identisch, egal ob sie von Amazon EC2 erstellt oder in Amazon EC2 importiert wurden, da dieselbe SHA-256-Hash-Funktion zur Berechnung des Fingerabdrucks verwendet wird.

Generieren eines Fingerabdrucks aus dem privaten Schlüssel

Generieren Sie mit einem der folgenden Befehle einen Fingerabdruck aus dem privaten Schlüssel auf Ihrem lokalen Computer.

Wenn Sie einen lokalen Windows-Computer verwenden, können Sie die folgenden Befehle mit dem Windows-Subsystem für Linux (WSL) ausführen. Installieren Sie WSL und eine Linux-Distribution mithilfe der Anleitung im Installationshandbuch für Windows 10. Mit dem in der Anleitung genannten Beispiel wird die Ubuntu-Distribution von Linux installiert, Sie können jedoch jede beliebige Distribution installieren. Sie werden zum Neustart Ihres Computers aufgefordert, damit die Änderungen wirksam werden.

- Wenn Sie das Schlüsselpaar mit Amazon EC2 erstellt haben

  Verwenden Sie die OpenSSL-Tools, um einen Fingerabdruck zu generieren, wie in den folgenden Beispielen gezeigt.

  Für RSA-Schlüsselpaare:

  ```
  openssl pkcs8 -in path_to_private_key -inform PEM -outform DER -topk8 -nocrypt |
   openssl sha1 -c
  ```

  (Linux-Instances) Für ED25519-Schlüsselpaare:

  ```
  ssh-keygen -l -f path_to_private_key
  ```

- (Nur RSA-Schlüsselpaare) Falls Sie den öffentlichen Schlüssel in Amazon EC2 importiert haben

  Dieses Verfahren können Sie unabhängig davon verwenden, wie Sie das Schlüsselpaar erstellt haben, z. B. durch Verwendung eines Drittanbieter-Tools oder durch Generieren eines neuen

öffentlichen Schlüssels aus einem vorhandenen privaten Schlüssel, der mit Amazon EC2 erstellt wurde.

Verwenden Sie die OpenSSL-Tools, um einen Fingerabdruck zu generieren, wie im folgenden Beispiel gezeigt.

```
openssl rsa -in path_to_private_key -pubout -outform DER | openssl md5 -c
```

- Wenn Sie ein OpenSSH-Schlüsselpaar mit OpenSSH 7.8 oder höher erstellt und den öffentlichen Schlüssel in Amazon EC2 importiert haben

  Verwenden Sie ssh-keygen, um einen Fingerabdruck zu generieren, wie in den folgenden Beispielen gezeigt.

  Für RSA-Schlüsselpaare:

  ```
  ssh-keygen -ef path_to_private_key -m PEM | openssl rsa -RSAPublicKey_in -outform DER
   | openssl md5 -c
  ```

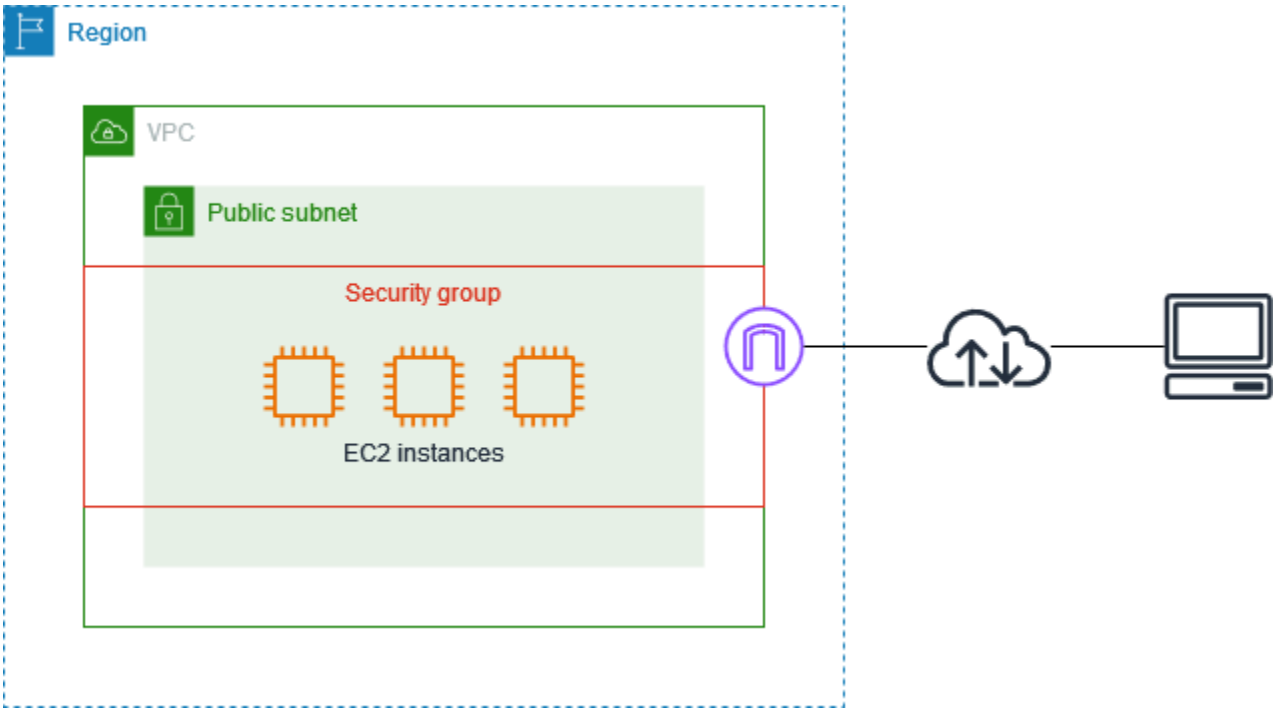
  (Linux-Instanzen) Für ED25519-Schlüsselpaare:

  ```
  ssh-keygen -l -f path_to_private_key
  ```

Amazon EC2-Sicherheitsgruppen für Ihre EC2-Instances

Eine Sicherheitsgruppe dient als virtuelle Firewall für Ihre EC2-Instances zur Steuerung von ein- und ausgehendem Datenverkehr. Eingehende Regeln steuern den eingehenden Datenverkehr zu Ihrer Instance und ausgehende Regeln steuern den ausgehenden Datenverkehr von Ihrer Instance. Wenn Sie eine Instance starten, können Sie eine oder mehrere Sicherheitsgruppen angeben. Wenn Sie keine Sicherheitsgruppe angeben, verwendet Amazon EC2 die Standard-Sicherheitsgruppe für die VPC. Sie können jeder Sicherheitsgruppe Regeln hinzufügen, die den Datenaustausch mit den zugeordneten Instances gestatten. Sie können die Regeln für eine Sicherheitsgruppe jederzeit ändern. Neue und geänderte Regeln werden automatisch auf alle Instances angewendet, die der Sicherheitsgruppe zugeordnet sind. Wenn Amazon EC2 entscheidet, ob zugelassen wird, dass der Datenverkehr eine Instance erreicht, bewertet es alle Regeln für alle Sicherheitsgruppen, die der Instance zugeordnet sind.

Das folgende Diagramm zeigt eine VPC mit einer Sicherheitsgruppe, einem Internet-Gateway und einem Subnetz. Das Subnetz enthält EC2-Instances. Die Sicherheitsgruppe ist den Instances zugewiesen. Der einzige Datenverkehr, der die Instance erreicht, ist der Datenverkehr, der nach den Sicherheitsgruppenregeln zulässig ist. Wenn die Sicherheitsgruppe beispielsweise eine Regel enthält, die SSH-Verkehr von Ihrem Netzwerk aus zulässt, können Sie von Ihrem Computer aus über SSH eine Verbindung zu Ihrer Instance herstellen. Wenn die Sicherheitsgruppe eine Regel enthält, die den gesamten Datenverkehr von den ihr zugewiesenen Ressourcen zulässt, kann jede Instanz jeglichen Datenverkehr empfangen, der von den anderen Instanzen gesendet wird.



Nach dem Start einer Instance können Sie deren Sicherheitsgruppen nicht mehr ändern. Sicherheitsgruppen sind mit Netzwerkschnittstellen verknüpft. Durch die Änderung der Sicherheitsgruppen einer Instance werden die Sicherheitsgruppen geändert, die mit der primären Netzwerkschnittstelle (eth0) der Instance verknüpft sind. Weitere Informationen finden Sie unter Ändern der Sicherheitsgruppe einer Instance. Sie können auch die Sicherheitsgruppen ändern, die mit anderen Netzwerkschnittstellen verknüpft sind. Weitere Informationen finden Sie unter Ändern der Netzwerkschnittstellenattribute.

Sicherheit ist eine gemeinsame Verantwortung zwischen Ihnen AWS und Ihnen. Weitere Informationen finden Sie unterSicherheit in Amazon EC2. AWS stellt Sicherheitsgruppen als eines der Tools zum Schutz Ihrer Instances bereit. Sie müssen sie entsprechend Ihren Sicherheitsanforderungen konfigurieren. Wenn Sie Anforderungen haben, die von

Sicherheitsgruppen nicht vollständig erfüllt werden, können Sie zusätzlich zur Verwendung von Sicherheitsgruppen eine eigene Firewall in jeder Ihrer Instances einrichten.

Für die Nutzung von Sicherheitsgruppen fallen keine zusätzlichen Gebühren an.

Inhalt

Sicherheitsgruppenregeln

Die Regeln einer Sicherheitsgruppe steuern den eingehenden Datenverkehr, der die Instances erreichen darf, die der Sicherheitsgruppe zugeordnet sind. Die Regeln steuern auch den ausgehenden Datenverkehr, der sie verlassen darf.

Es folgen die grundlegenden Merkmale von Sicherheitsgruppenregeln:

- Standardmäßig enthalten Sicherheitsgruppen ausgehende Regeln, die den gesamten ausgehenden Datenverkehr zulassen. Sie können diese Regeln löschen. Beachten Sie, dass Amazon EC2 standardmäßig Traffic auf Port 25 blockiert. Weitere Informationen finden Sie unter Einschränkung für E-Mails, die über Port 25 gesendet werden.
- Sicherheitsgruppenregeln sind stets zulassend, Sie können keine Regeln erstellen, die den Zugriff verweigern.
- Mithilfe von Sicherheitsgruppenregeln können Sie Datenverkehr basierend auf Protokollen und Portnummern filtern.
- Sicherheitsgruppen sind zustandsbehaftet — wenn Sie von Ihrer Instance eine Anforderung senden, wird der Antwortdatenverkehr für diese Anforderung zugelassen, unabhängig der für diese Sicherheitsgruppe geltenden Regeln für eingehenden Datenverkehr. Für VPC-Sicherheitsgruppen bedeutet dies auch, dass Antworten auf zulässigen eingehenden Datenverkehr ausgehen können, unabhängig von ausgehenden Regeln. Weitere Informationen finden Sie unter Verbindungsverfolgung von Sicherheitsgruppen.
- Sie können Regeln jederzeit hinzufügen oder entfernen. Ihre Änderungen werden automatisch auf die Instances angewendet, die der Sicherheitsgruppe zugeordnet sind.

Die Auswirkung einiger Regeländerungen kann davon abhängen, wie der Datenverkehr nachverfolgt wird. Weitere Informationen finden Sie unter Verbindungsverfolgung von Sicherheitsgruppen.

- Wenn Sie mehrere Sicherheitsgruppen mit einer Instance verbinden, werden die Regeln jeder Sicherheitsgruppe effektiv zu einem einzigen Regelsatz zusammengeführt. Mit diesem Regelsatz bestimmt Amazon EC2, ob der Zugriff erlaubt ist.

  Sie können einer Instance mehrere Sicherheitsgruppen zuweisen. Daher kann eine Instance Hunderte von Regeln haben, die angewendet werden. Dies kann beim Zugriff auf die Instance zu Problemen führen. Wir empfehlen, dass Sie Ihre Regeln so weit wie möglich verdichten.

> **Note**
>
> Sicherheitsgruppen können DNS-Anfragen an oder vom Route 53 Resolver, der manchmal auch als „VPC+2-IP-Adresse“ bezeichnet wird, nicht blockieren (siehe Was ist Amazon Route 53 Resolver? im Amazon Route 53 Developer Guide) oder im 'AmazonProvidedDNS' (siehe Arbeiten mit DHCP-Optionssätzen im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch). Wenn Sie DNS-Anfragen über den Route 53 Resolver filtern möchten, können Sie die Route-53-Resolver-DNS-Firewall aktivieren (Informationen unter Route-53-Resolver-DNS-Firewall im Amazon-Route-53-Entwicklerhandbuch).

Für jede Regel geben Sie Folgendes an:

- Name: Der Name für die Sicherheitsgruppe (z. B. „my-security-group“).

  Ein Name kann bis zu 255 Zeichen lang sein. Zulässige Zeichen sind a-z, A-Z, 0-9, , Leerzeichen und ._-:/()#,@[]+=;{}!$*. Wenn der Name nachgestellte Leerzeichen enthält, werden die Leerzeichen beim Speichern des Namens gekürzt. Wenn Sie beispielsweise „Sicherheitsgruppe testen“ als Namen eingeben, wird er als „Sicherheitsgruppe testen“ gespeichert.
- Protokoll: Das zulässige Protokoll. Die üblichsten Protokolle sind 6 (TCP) 17 (UDP) und 1 (ICMP).
- Portbereich: zulässiger Portbereich für TCP, UDP oder ein benutzerdefiniertes Protokoll. Sie können eine einzelne Portnummer (zum Beispiel 22) oder einen Bereich von Portnummern (zum Beispiel `7000-8000`) angeben.
- ICMP-Typ und -Code: Für ICMP der ICMP-Typ und -Code. Verwenden Sie beispielsweise Typ 8 für ICMP-Echo-Anfrage oder Typ 128 für ICMPv6-Echo-Anfrage.

- Quelle oder Ziel: Die Quelle (eingehende Regeln) oder das Ziel (ausgehende Regeln), die für den Datenverkehr zugelassen sind. Geben Sie eines der folgenden Elemente an:
  - Eine einzelne IPv4-Adresse. Sie müssen die `/32`-Präfixlänge verwenden. z. B. `203.0.113.1/32`.
  - Eine einzelne IPv6-Adresse. Sie müssen die `/128`-Präfixlänge verwenden. z. B. `2001:db8:1234:1a00::123/128`.
  - Einen Bereich von IPv4-Adressen, in CIDR-Block-Notation. z. B. `203.0.113.0/24`.
  - Einen Bereich von IPv6-Adressen, in CIDR-Block-Notation. z. B. `2001:db8:1234:1a00::/64`.
  - Die ID einer Präfixliste. z. B. `pl-1234abc1234abc123`. Weitere Informationen finden Sie unter Präfixlisten im Amazon VPC Benutzerhandbuch.
  - Die ID einer Sicherheitsgruppe (hier als angegebene Sicherheitsgruppe bezeichnet). Zum Beispiel die aktuelle Sicherheitsgruppe, eine Sicherheitsgruppe aus derselben VPC oder eine Sicherheitsgruppe für eine Peered-VPC. Dies ermöglicht Datenverkehr basierend auf den privaten IP-Adressen der Ressourcen, die der angegebenen Sicherheitsgruppe zugeordnet sind. Hierdurch werden der aktuellen Sicherheitsgruppe keine Regeln von der angegebenen Sicherheitsgruppe hinzugefügt.
- (Optional) Beschreibung: Sie können eine Beschreibung für die Regel hinzufügen, die Ihnen helfen kann, sie später zu identifizieren. Eine Beschreibung kann bis zu 255 Zeichen lang sein. Zulässige Zeichen sind a-z, A-Z, 0-9, , Leerzeichen und ._-:/()#,@[]+=;{}!$*.

Wenn Sie eine Sicherheitsgruppenregel erstellen, AWS weist Sie der Regel eine eindeutige ID zu. Sie können die ID einer Regel verwenden, wenn Sie die API oder CLI verwenden, um die Regel zu ändern oder zu löschen.

Wenn Sie eine Sicherheitsgruppe als Quelle oder Ziel für eine Regel angeben, wirkt sich die Regel auf alle Instances aus, die der Sicherheitsgruppe zugeordnet sind. Eingehender Verkehr ist basierend auf den privaten IP-Adressen der Instances erlaubt, die der Quellsicherheitsgruppe zugeordnet sind (und nicht auf den öffentlichen IP- oder Elastic IP-Adressen). Weitere Informationen über IP-Adressen finden Sie unter IP-Adressierung von Amazon EC2-Instances. Wenn Ihre Sicherheitsgruppenregel auf eine gelöschte Sicherheitsgruppe in derselben VPC oder in einer Peer-VPC verweist oder wenn sie auf eine Sicherheitsgruppe in einer Peer-VPC verweist, für die die VPC-Peering-Verbindung gelöscht wurde, wird die Regel als veraltet markiert. Weitere Informationen finden Sie unter Arbeiten mit veralteten Sicherheitsgruppenregeln im Amazon VPC Peering Guide.

Wenn mehr als eine Regel für einen bestimmten Port vorliegt, wendet Amazon EC2 die toleranteste Regel an. Wenn Sie beispielsweise über eine Regel verfügen, die den Zugriff auf TCP-Port 22 (SSH)

von der IP-Adresse 203.0.113.1 aus ermöglicht, und eine weitere Regel, die allen Benutzern den Zugriff auf TCP-Port 22 ermöglicht, dann hat jeder Zugriff auf TCP-Port 22.

Wenn Sie Regeln hinzufügen, aktualisieren oder entfernen, gelten diese Änderungen automatisch für die Instances, die der Sicherheitsgruppe zugewiesen sind.

Verbindungsverfolgung von Sicherheitsgruppen

Ihre Sicherheitsgruppen verwenden die Verbindungsverfolgung zur Nachverfolgung des Datenverkehrs zu und von der Instance. Regeln werden auf der Grundlage des Verbindungszustands des Datenverkehrs angewendet, um zu ermitteln, ob der Datenverkehr zulässig ist oder nicht. Bei diesem Ansatz sind Sicherheitsgruppen zustandsbehaftet. Das bedeutet, dass Antworten auf eingehenden Verkehr unabhängig von den Regeln für ausgehende Sicherheitsgruppen aus der Instance fließen dürfen und umgekehrt.

Angenommen, Sie initiieren einen Befehl wie „netcat“ oder ähnliches für Ihre Instances von Ihrem Heimcomputer aus und Ihre eingehenden Sicherheitsgruppenregeln lassen ICMP-Datenverkehr zu. Informationen über die Verbindung (einschließlich der Port-Informationen) werden verfolgt. Antwort-Datenverkehr von der Instance für den -Befehl wird nicht als neue Anfrage verfolgt, sondern als eingerichtete Verbindung; dieser Datenverkehr kann die Instance verlassen, selbst wenn Ihre ausgehenden Sicherheitsgruppenregeln ausgehenden ICMP-Datenverkehr beschränken.

Für andere Protokolle als TCP, UDP oder ICMP werden nur die IP-Adresse und die Protokollnummer verfolgt. Wenn Ihre Instance Datenverkehr an einen anderen Host sendet und der Host innerhalb von 600 Sekunden dieselbe Art von Datenverkehr an Ihre Instance sendet, akzeptiert die Sicherheitsgruppe für Ihre Instance diesen unabhängig von den Sicherheitsgruppen-Regeln für eingehenden Datenverkehr. Die Sicherheitsgruppe akzeptiert ihn, da er als Antwort-Datenverkehr für den ursprünglichen Datenverkehr angesehen wird.

Wenn Sie eine Sicherheitsgruppenregel ändern, werden ihre nachverfolgten Verbindungen nicht sofort unterbrochen. Die Sicherheitsgruppe lässt Pakete weiterhin zu, bis bei bestehenden Verbindungen eine Zeitüberschreitung (Timeout) auftritt. Um sicherzustellen, dass Datenverkehr sofort unterbrochen wird oder der gesamte Datenverkehr unabhängig vom Nachverfolgungsstatus den Firewall-Regeln unterliegt, können Sie eine Netzwerk-ACL für Ihr Subnetz verwenden. Netzwerk-ACLs sind zustandslos und lassen daher nicht automatisch Antwortdatenverkehr zu. Das Hinzufügen einer Netzwerk-ACL, die Datenverkehr in beide Richtungen blockiert, trennt vorhandene Verbindungen. Weitere Informationen finden Sie unter Netzwerk-ACLs im Amazon VPC Benutzerhandbuch.

> **Note**
>
> Sicherheitsgruppen haben keine Auswirkung auf den DNS-Verkehr zum oder vom Route 53 Resolver, der manchmal auch als „VPC+2-IP-Adresse“ bezeichnet wird (siehe Was ist Amazon Route 53 Resolver? im Amazon Route 53 Developer Guide) oder im 'AmazonProvidedDNS' (siehe Arbeiten mit DHCP-Optionssätzen im Amazon Virtual Private Cloud Cloud-Benutzerhandbuch). Wenn Sie DNS-Anfragen über den Route 53 Resolver filtern möchten, können Sie die Route-53-Resolver-DNS-Firewall aktivieren (Informationen unter Route-53-Resolver-DNS-Firewall im Amazon-Route-53-Entwicklerhandbuch).

Unverfolgte Verbindungen

Nicht alle Datenverkehrsflüsse werden verfolgt. Wenn eine Sicherheitsgruppenregel TCP- oder UDP-Datenflüsse für den gesamten Datenverkehr (0.0.0.0/0 oder: :/0) zulässt und es eine entsprechende Regel in der anderen Richtung gibt, die den gesamten Antwortverkehr (0.0.0.0/0 oder: :/0) für jeden Port (0-65535) zulässt, dann wird dieser Verkehrsfluss nicht verfolgt, es sei denn, er ist Teil einer automatisch verfolgten Verbindung. Der Antwort-Datenverkehr für einen nicht nachverfolgten Fluss wird anhand der Regel für ein- oder ausgehenden Datenverkehr zugelassen, die den Antwort-Datenverkehr erlaubt, und nicht anhand von Nachverfolgungsinformationen.

Ein nicht verfolgter Datenverkehrsfluss wird sofort unterbrochen, wenn die Regel, die ihn ermöglicht, entfernt oder modifiziert wird. Wenn Sie z. B. eine offene (0.0.0.0/0) ausgehende Regel haben und eine Regel entfernen, die den gesamten (0.0.0.0/0) eingehenden SSH-Verkehr (TCP-Port 22) zur Instance zulässt (oder sie so ändern, dass die Verbindung nicht mehr zulässig wäre), werden Ihre bestehenden SSH-Verbindungen zur Instance sofort gelöscht. Die Verbindung wurde zuvor nicht nachverfolgt, sodass die Änderung die Verbindung unterbricht. Wenn Sie dagegen eine restriktivere Regel für eingehende Verbindungen verwenden, die zunächst eine SSH-Verbindung zulässt (was bedeutet, dass die Verbindung nachverfolgt wurde), diese Regel aber so ändern, dass keine neuen Verbindungen von der Adresse des aktuellen SSH-Clients mehr zugelassen werden, wird die bestehende SSH-Verbindung nicht unterbrochen, weil sie nachverfolgt wird.

Automatisch nachverfolgte Verbindungen

Verbindungen, die über Folgendes hergestellt werden, werden automatisch verfolgt, auch wenn die Sicherheitsgruppenkonfiguration ansonsten keine Nachverfolgung erfordert:

- Internet-Gateways nur für ausgehenden Datenverkehr

- Accelerators von Global Accelerator
- NAT gateways (NAT-Gateways)
- Firewall-Endpunkte von Network Firewall
- Network Load Balancers
- AWS PrivateLink (Schnittstelle VPC-Endpunkte)
- AWS Lambda (Elastische Hyperplane-Netzwerkschnittstellen)

Zulagen für die Verbindungsverfolgung

Amazon EC2 definiert die maximale Anzahl von Verbindungen, die pro Instance verfolgt werden können. Nach Erreichen des Maximums werden alle gesendeten oder empfangenen Pakete verworfen, da keine neue Verbindung hergestellt werden kann. In diesem Fall können Anwendungen, die Pakete senden und empfangen, nicht ordnungsgemäß kommunizieren. Verwenden Sie die `conntrack_allowance_available`-Netzwerkleistungsmetrik, um die Anzahl der nachverfolgten Verbindungen zu bestimmen, die für diesen Instance-Typ noch verfügbar sind.

Um festzustellen, ob Pakete verworfen wurden, weil der Netzwerkverkehr für Ihre Instance die maximale Anzahl der nachverfolgbaren Verbindungen überschritten hat, verwenden Sie die `conntrack_allowance_exceeded`-Netzwerkleistungsmetrik. Weitere Informationen finden Sie unter Überwachen der Netzwerkleistung für Ihre EC2-Instance.

Wenn Sie mit Elastic Load Balancing die maximale Anzahl von Verbindungen überschreiten, die pro Instance nachverfolgt werden können, empfehlen wir, entweder die Anzahl der beim Load Balancer registrierten Instances oder die Größe der beim Load Balancer registrierten Instances zu skalieren.

Überlegungen zur Leistung der Verbindungsverfolgung

Asymmetrisches Routing, bei dem der Datenverkehr über eine Netzwerkschnittstelle in eine Instance eingeht und über eine andere Netzwerkschnittstelle wieder austritt, kann die Spitzenleistung verringern, die eine Instance erzielen kann, wenn Datenflüsse nachverfolgt werden.

Um die Spitzenleistung aufrechtzuerhalten, wenn die Verbindungsverfolgung für Ihre Sicherheitsgruppen aktiviert ist, empfehlen wir die folgende Konfiguration:

- Vermeiden Sie nach Möglichkeit asymmetrische Routing-Topologien.
- Verwenden Sie Netzwerk-ACLs, anstatt Sicherheitsgruppen zum Filtern zu verwenden.
- Wenn Sie Sicherheitsgruppen mit Verbindungsverfolgung verwenden müssen, konfigurieren Sie das kürzest mögliche Verbindungstimeout.

Weitere Informationen zur Leistungsoptimierung auf dem Nitro-System finden Sie unter. Überlegungen zum Nitro-System zur Leistungsoptimierung

Timeout für die Nachverfolgung von Leerlaufverbindungen

Die Sicherheitsgruppe verfolgt jede bestehende Verbindung nach, um sicherzustellen, dass Rückpakete wie erwartet übertragen werden. Es gibt eine maximale Anzahl von Verbindungen, die pro Instance verfolgt werden können. Im Leerlauf befindliche Verbindungen können zur Erschöpfung der Kapazität der Verbindungsnachverfolgung führen und zur Folge haben, dass Verbindungen nicht nachverfolgt und Pakete verworfen werden. Sie können das Timeout für die Nachverfolgung von Leerlaufverbindungen für eine Elastic-Network-Schnittstelle festlegen.

> **Note**
>
> Diese Funktion ist nur für Instances verfügbar, die auf dem AWS Nitro-System basieren.

Es gibt drei konfigurierbare Timeouts:

- Timeout für bestehende TCP-Verbindungen: Timeout (in Sekunden) für bestehende TCP-Verbindungen im Leerlauf. Min: 60 Sekunden. Max: 432 000 Sekunden (fünf Tage). Standard: 432 000 Sekunden. Empfohlen: Weniger als 432 000 Sekunden.
- UDP-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, bei denen Datenverkehr nur in eine Richtung oder nur in einer einzelnen Anforderung-Antwort-Transaktion übermittelt wurde. Min: 30 Sekunden. Max: 60 Sekunden. Standard: 30 Sekunden.
- UDP-Stream-Timeout: Timeout (in Sekunden) für UDP-Datenflüsse im Leerlauf, die als Streams klassifiziert sind, bei denen mehr als eine Anforderung-Antwort-Transaktion stattgefunden hat. Min: 60 Sekunden. Max: 180 Sekunden (3 Minuten) Standard: 180 Sekunden.

In folgenden Fällen empfiehlt es sich möglicherweise, die Standard-Timeouts anzupassen:

- Wenn Sie nachverfolgte Verbindungen mithilfe von Amazon-EC2-Netzwerkleistungsmetriken überwachen, ermöglichen Ihnen die Metriken conntrack_allowance_exceeded und conntrack_allowance_available die Überwachung verworfener Pakete und der nachverfolgten Verbindungsauslastung, um die EC2-Instance-Kapazität proaktiv per Hochskalierung oder horizontaler Skalierung zu verwalten und so den Bedarf an Netzwerkverbindungen zu decken, bevor Pakete verworfen werden. Wenn Sie conntrack_allowance_exceeded-Ausfälle auf

Ihren EC2-Instances beobachten, können Sie davon profitieren, ein niedrigeres TCP-Timeout festzulegen, um veraltete TCP/UDP-Sitzungen zu berücksichtigen, die von falschen Clients oder Netzwerk-Middle-Boxen verursacht werden.

- In der Regel haben Load Balancer oder Firewalls ein TCP-Etabliertes Leerlauf-Timeout im Bereich von 60 bis 90 Minuten. Wenn Sie Workloads ausführen, die voraussichtlich eine sehr hohe Anzahl von Verbindungen (mehr als 100 000) von Appliances wie Netzwerk-Firewalls verarbeiten, empfiehlt es sich, ein ähnliches Timeout für eine EC2-Netzwerkschnittstelle zu konfigurieren.
- Wenn Sie einen Workload ausführen, der eine asymmetrische Routing-Topologie verwendet, empfehlen wir Ihnen, ein TCP-Idle-Timeout von 60 Sekunden zu konfigurieren.
- Wenn Sie Workloads mit einer hohen Anzahl von Verbindungen wie DNS, SIP, SNMP, Syslog, Radius oder andere Dienste ausführen, die hauptsächlich UDP zur Verarbeitung von Anforderungen verwenden, können Sie das UDP-Stream-Timeout auf 60 Sekunden festlegen, um eine höhere Skalierung/Leistung für die vorhandene Kapazität zu erhalten und unklare Fehler zu vermeiden.
- Bei TCP/UDP-Verbindungen über Network Load Balancer (NLBs) und Elastic Load Balancer (ELB) werden alle Verbindungen nachverfolgt. Der Wert des Leerlauf-Timeouts für TCP-Datenflüsse beträgt 350 Sekunden. Für UDP-Datenflüsse beträgt er 120 Sekunden. Er unterscheidet sich somit von den Timeout-Werten auf Schnittstellenebene. Es empfiehlt sich gegebenenfalls, Timeouts auf Netzwerkschnittstellen-Ebene zu konfigurieren, um beim Timeout mehr Flexibilität zu haben als mit den Standardwerten für ELB/NLB.

Die Timeouts für die Verbindungsnachverfolgung können bei folgenden Tätigkeiten konfiguriert werden:

- Erstellen einer Netzwerkschnittstelle
- Ändern der Netzwerkschnittstellen-Attribute
- Starten einer EC2-Instance
- Erstellen einer Startvorlage für eine EC2-Instance

Beispiel

Im folgenden Beispiel hat die Sicherheitsgruppe Regeln für eingehenden Verkehr, die TCP- und ICMP-Datenverkehr zulassen, und Regeln für ausgehenden Verkehr, die allen ausgehenden Datenverkehr zulassen.

Eingehend

Protokolltyp	Port-Nummer	Quelle
TCP	22 (SSH)	203.0.113.1/32
TCP	80 (HTTP)	0.0.0.0/0
TCP	80 (HTTP)	::/0
ICMP	Alle	0.0.0.0/0

Ausgehend

Protokolltyp	Port-Nummer	Bestimmungsort
Alle	Alle	0.0.0.0/0
Alle	Alle	::/0

Bei einer direkten Netzwerkverbindung zur Instance oder Netzwerkschnittstelle sieht das Nachverfolgungsverhalten wie folgt aus:

- Ein- und ausgehender TCP-Datenverkehr auf Port 22 (SSH) wird nachverfolgt, da die Regel für eingehenden Verkehr nur Datenverkehr von 203.0.113.1/32 und nicht von allen IP-Adressen (0.0.0.0/0) zulässt.
- Ein- und ausgehender TCP-Datenverkehr auf Port 80 (HTTP) wird nicht nachverfolgt, da die Regeln für ein- und ausgehenden Verkehr Datenverkehr von allen IP-Adressen zulassen.
- ICMP-Datenverkehr wird immer nachverfolgt.

Wenn Sie die Regel für ausgehenden Verkehr für IPv4-Datenverkehr entfernen, wird der gesamte ein- und ausgehende IPv4-Datenverkehr nachverfolgt, einschließlich Datenverkehr auf Port 80 (HTTP). Gleiches gilt für IPv6-Datenverkehr, wenn Sie die Regel für ausgehenden Verkehr für IPv6-Datenverkehr entfernen.

Standard- und benutzerdefinierte Sicherheitsgruppen

Ihr AWS Konto hat automatisch eine Standardsicherheitsgruppe für die Standard-VPC in jeder Region. Wenn Sie beim Starten einer Instance keine Sicherheitsgruppe festlegen, wird die Instance automatisch der Standardsicherheitsgruppe für die VPC zugeordnet. Wenn Sie nicht wünschen, dass Ihre Instances die Standardsicherheitsgruppe verwenden, können Sie Ihre eigenen benutzerdefinierten Sicherheitsgruppen erstellen und beim Start Ihrer Instances angeben.

Inhalt

Standardsicherheitsgruppen

Jede VPC verfügt über eine Standard-Sicherheitsgruppe. Es wird empfohlen, Sicherheitsgruppen für bestimmte Instances oder Gruppen von Instances zu erstellen, anstatt die Standardeinstellung zu verwenden. Wenn Sie jedoch beim Starten einer Instance keine Sicherheitsgruppe angeben, wird die Instance der Standardeinstellung für die VPC zugeordnet.

Der Namen der Standard-Sicherheitsgruppe lautet „default“. Nachfolgend finden Sie die Standardregeln für die Standardsicherheitsgruppe.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Beschreibung
sg-1234567890abcdef0	Alle	Alle	Lässt eingehenden Datenverkehr von allen Ressourcen zu, die dieser Sicherheitsgruppe zugewiesen sind. Die Quelle ist die ID dieser Sicherheitsgruppe.

Ausgehend

Ziel	Protocol (Protokoll)	Port-Bereich	Beschreibung
0.0.0.0/0	Alle	Alle	Lässt den gesamten ausgehenden IPv4-Datenverkehr zu.
::/0	Alle	Alle	Lässt den gesamten ausgehenden IPv6-Datenverkehr zu. Diese Regel wird nur hinzugefügt, wenn Ihrer VPC ein IPv6-CIDR-Block zugeordnet ist.

Grundlagen für Standard-Sicherheitsgruppen

- Sie können die Regeln für eine Standardsicherheitsgruppe ändern.
- Sie können eine Standardsicherheitsgruppe nicht löschen. Wenn Sie versuchen, eine Standard-Sicherheitsgruppe zu löschen, wird der folgende Fehlercode zurückgegeben: `Client.CannotDelete`.

Benutzerdefinierte Sicherheitsgruppen

Sie können mehrere Sicherheitsgruppen erstellen, um die unterschiedlichen Rollen zu berücksichtigen, die Ihre Instances einnehmen, beispielsweise Webserver oder als Datenbankserver.

Wenn Sie eine Sicherheitsgruppe erstellen, müssen Sie einen Namen und eine Beschreibung dafür angeben. Namen und Beschreibungen von Sicherheitsgruppen können bis zu 255 Zeichen lang sein und dürfen nur die folgenden Zeichen enthalten:

a-z, A-Z, 0-9, Leerzeichen und ._-:/()#,@[]+=&;{}!$*

Der Name einer Sicherheitsgruppe darf nicht mit Folgendem beginnen: sg-. Der Name einer Sicherheitsgruppe muss für die VPC eindeutig sein.

Nachfolgend finden Sie die Standardregeln für eine von Ihnen erstellte Standardsicherheitsgruppe:

- Erlaubt keinen eingehenden Datenverkehr
- Erlaubt allen ausgehenden Datenverkehr

Nach der Erstellung einer Sicherheitsgruppe können Sie deren eingehende Regeln ändern, um die Art des eingehenden Datenverkehrs zu berücksichtigen, der die zugehörigen Instances erreichen soll. Sie können auch die ausgehenden Regeln ändern.

Für weitere Informationen zu den Regeln, die Sie einer Sicherheitsgruppe hinzufügen können, vgl. Sicherheitsgruppenregeln für verschiedene Anwendungsfälle.

Arbeiten mit Sicherheitsgruppen

Sie können eine Sicherheitsgruppe einer Instance zuweisen, wenn Sie die Instance starten. Wenn Sie Regeln hinzufügen oder entfernen, gelten diese Änderungen automatisch für alle Instances, denen Sie die Sicherheitsgruppe zugewiesen haben. Weitere Informationen finden Sie unter Zuordnen einer Sicherheitsgruppe zu einer Instance.

Nach dem Start einer Instance können Sie deren Sicherheitsgruppen nicht mehr ändern. Weitere Informationen finden Sie unter Ändern der Sicherheitsgruppe einer Instance.

Sie können Sicherheitsgruppen und Sicherheitsgruppenregeln mit der Amazon EC2-Konsole und den Befehlszeilentools erstellen, anzeigen, aktualisieren und löschen.

Aufgaben

- Erstellen einer Sicherheitsgruppe
- Kopieren einer Sicherheitsgruppe
- Anzeigen Ihrer Sicherheitsgruppen
- Hinzufügen von Regeln zu einer Sicherheitsgruppe
- Aktualisieren veralteter Sicherheitsgruppenregeln
- Löschen von Regeln aus einer Sicherheitsgruppe
- Löschen einer Sicherheitsgruppe
- Zuordnen einer Sicherheitsgruppe zu einer Instance
- Ändern der Sicherheitsgruppe einer Instance

Erstellen einer Sicherheitsgruppe

Auch wenn Sie die Standardsicherheitsgruppen für Ihre Instances verwenden können, ist es eventuell sinnvoll, eigene Gruppen zu erstellen, um die verschiedenen Rollen widerzuspiegeln, die die Instances in Ihrem System übernehmen.

Standardmäßig enthält jede Sicherheitsgruppe am Anfang nur eine Regel für ausgehenden Datenverkehr, die sämtlichen von der Instance ausgehenden Datenverkehr zulässt. Sie müssen Regeln hinzufügen, um eingehenden Datenverkehr zuzulassen oder den ausgehenden Datenverkehr einzuschränken.

Eine Sicherheitsgruppe kann nur in der VPC verwendet werden, für die sie erstellt wird.

Console

So erstellen Sie eine Sicherheitsgruppe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
4. Gehen Sie im Abschnitt Basic details (Grundlegende Details) wie folgt vor.
   a. Geben Sie einen beschreibenden Namen und eine kurze Beschreibung für die Sicherheitsgruppe ein. Sie können nicht bearbeitet werden, nachdem die Sicherheitsgruppe erstellt wurde. Der Name und die Beschreibung kann bis zu 255 Zeichen lang sein. Die zulässigen Zeichen sind a-z, A-Z, 0-9, Leerzeichen und ._-:/()#,@[]+=&;{}!$*.
   b. Wählen Sie unter VPC die VPC aus.
5. Sie können Regeln für eine Sicherheitsgruppe jetzt erstellen oder zu einem späteren Zeitpunkt hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Regeln zu einer Sicherheitsgruppe.
6. Sie können Tags (Markierungen) jetzt erstellen oder zu einem späteren Zeitpunkt hinzufügen. Um eine Markierung hinzuzufügen, wählen Sie Add Tags (Tags (Markierung) hinzufügen) und geben Sie dann den Markierungsschlüssel und -Wert ein.
7. Wählen Sie Sicherheitsgruppe erstellen aus.

Command line

So erstellen Sie eine Sicherheitsgruppe

Verwenden Sie einen der folgenden Befehle:

- create-security-group (AWS CLI)

- New-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Kopieren einer Sicherheitsgruppe

Sie können eine neue Sicherheitsgruppe erstellen, indem Sie eine Kopie einer vorhandenen Sicherheitsgruppe erstellen. Wenn Sie eine Sicherheitsgruppe kopieren, wird die Kopie mit den gleichen Eingangs- und Ausgangsregeln wie die ursprüngliche Sicherheitsgruppe erstellt. Wenn sich die ursprüngliche Sicherheitsgruppe in einer VPC befindet, wird die Kopie in derselben VPC erstellt, es sei denn, Sie geben eine andere an.

Die Kopie erhält eine neue eindeutige Sicherheitsgruppen-ID, und Sie müssen ihr einen Namen geben. Sie können auch eine Beschreibung hinzufügen.

Sie können eine Sicherheitsgruppe nicht von einer Region in eine andere Region kopieren.

Sie können eine Kopie Ihrer Sicherheitsgruppe mithilfe der Amazon-EC2-Konsole erstellen.

So kopieren Sie eine Sicherheitsgruppe:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die zu kopierende Sicherheitsgruppe und wählen Sie Actions (Aktionen), Copy to new security group (In neue Sicherheitsgruppe kopieren).
4. Geben Sie einen Namen und eine optionale Beschreibung an und ändern Sie bei Bedarf die VPC und Sicherheitsgruppenregeln.
5. Wählen Sie Create (Erstellen) aus.

Anzeigen Ihrer Sicherheitsgruppen

Sie können Informationen über Ihre Sicherheitsgruppen mit einer der folgenden Methoden anzeigen.

Console

So zeigen Sie Ihre Sicherheitsgruppen an:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.

3. Ihre Sicherheitsgruppen werden aufgelistet. Um die Details für eine bestimmte Sicherheitsgruppe, einschließlich ihrer eingehenden und ausgehenden Regeln, anzuzeigen, wählen Sie deren ID in der Spalte Security group ID (Sicherheitsgruppen-ID).

Command line

So zeigen Sie Ihre Sicherheitsgruppen an:

Verwenden Sie einen der folgenden Befehle.

- describe-security-groups (AWS CLI)
- describe-security-group-rules (AWS CLI)
- Get-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Amazon EC2 Global View

Sie können Amazon EC2 Global View verwenden, um Ihre Sicherheitsgruppen in allen Regionen anzuzeigen, für die Ihr AWS Konto aktiviert ist. Weitere Informationen finden Sie unter Amazon EC2 Global View.

Hinzufügen von Regeln zu einer Sicherheitsgruppe

Wenn Sie eine Regel zu einer Sicherheitsgruppe hinzufügen, wird die neue Regel automatisch auf alle Instances angewendet, die der Sicherheitsgruppe zugeordnet sind. Es kann eine kurze Verzögerung eintreten, bevor die Regel angewendet wird. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln für verschiedene Anwendungsfälle und Sicherheitsgruppenregeln.

Console

So fügen Sie eine eingehende Regel zu einer Sicherheitsgruppe hinzu:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die Sicherheitsgruppe und wählen Sie Aktionen, Eingangsregeln bearbeiten.
4. Wählen Sie für jede Regel Add rule (Regel hinzufügen) und gehen Sie wie folgt vor.

    a. Wählen Sie für Type (Typ) den Typ des zuzulassenden Protokolls aus.

- Für Benutzerdefiniertes TCP oder Benutzerdefiniertes UDP müssen Sie den Portbereich angeben, der zugelassen werden soll. z. B. `0-99`.
- Für Benutzerdefiniertes ICMP müssen Sie den ICMP-Typ unter Protokoll auswählen. Der Portbereich ist für Sie konfiguriert. Um beispielsweise ping-Befehle zu erlauben, wählen Sie Echo Anfrage aus Protocol (Protokoll).
- Für einen anderen Typ werden das Protokoll und der Portbereich für Sie konfiguriert.

b. Führen Sie für Quelle einen der folgenden Schritte aus, um Datenverkehr zuzulassen.

- Wählen Sie Custom (Benutzerdefiniert) und geben Sie dann eine IP-Adresse in CIDR-Notation, einen CIDR-Block, eine andere Sicherheitsgruppe oder eine Präfixliste eingeben.
- Wählen Sie Überall aus, um zuzulassen, dass der gesamte Datenverkehr für das angegebene Protokoll Ihre Instance erreicht. Diese Option fügt automatisch den IPv4-CIDR-Block 0.0.0.0/0 als Quelle hinzu. Wenn sich Ihre Sicherheitsgruppe in einer VPC befindet, die für IPv6 aktiviert ist, fügt diese Option automatisch eine Regel für den IPv6-CIDR-Block ::/0 hinzu.

> ⚠ Warning
>
> Wenn Sie Anywhere (Irgendwo) auswählen, aktivieren Sie alle IPv4- und IPv6-Adressen, um über das angegebene Protokoll auf Ihre Instance zuzugreifen. Wenn Sie den Ports 22 (SSH) oder 3389 (RDP) neue Regeln hinzufügen, sollten Sie nur eine bestimmte IP-Adresse bzw. einen bestimmten Adressbereich für den Zugriff auf Ihre Instance autorisieren.

- Wählen Sie My IP (Meine IP), um eingehenden Verkehr nur von der öffentlichen IPv4-Adresse Ihres lokalen Computers zuzulassen.

c. Geben Sie für Description (Beschreibung) optional eine kurze Beschreibung für die Regel an.

5. Wählen Sie Preview changes (Änderungen überprüfen), Save rules (Regeln speichern).

So fügen Sie eine ausgehende Regel zu einer Sicherheitsgruppe hinzu:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.

3. Wählen Sie die Sicherheitsgruppe und wählen Sie Aktionen, Ausgangsregeln bearbeiten.
4. Wählen Sie für jede Regel Add rule (Regel hinzufügen) und gehen Sie wie folgt vor.

   a. Wählen Sie für Type (Typ) den Typ des zuzulassenden Protokolls aus.

      - Für Benutzerdefiniertes TCP oder Benutzerdefiniertes UDP müssen Sie den Portbereich angeben, der zugelassen werden soll. z. B. `0-99`.
      - Für Benutzerdefiniertes ICMP müssen Sie den ICMP-Typ unter Protokoll auswählen. Der Portbereich ist für Sie konfiguriert.
      - Für einen anderen Typ werden das Protokoll und der Portbereich automatisch konfiguriert.

   b. Führen Sie für Destination (Ziel) einen der folgenden Schritte aus.

      - Wählen Sie Custom (Benutzerdefiniert) und geben Sie dann eine IP-Adresse in CIDR-Notation, einen CIDR-Block, eine andere Sicherheitsgruppe oder eine Präfixliste ein, für die ausgehender Verkehr zugelassen werden soll.
      - Wählen Sie Anywhere (Überall), um ausgehenden Verkehr an alle IP-Adressen zuzulassen. Diese Option fügt automatisch den IPv4-CIDR-Block 0.0.0.0/0 als Ziel hinzu.

        Wenn sich Ihre Sicherheitsgruppe in einer VPC befindet, die für IPv6 aktiviert ist, fügt diese Option automatisch eine Regel für den IPv6-CIDR-Block ::/0 hinzu.
      - Wählen Sie My IP (Meine IP), um ausgehenden Verkehr nur von der öffentlichen IPv4-Adresse Ihres lokalen Computers zuzulassen.

   c. (Optional) Geben Sie für Description (Beschreibung) eine kurze Beschreibung für die Regel an.
5. Wählen Sie Preview changes (Änderungen überprüfen), Confirm (Bestätigen).

Command line

So fügen Sie Regeln zu einer Sicherheitsgruppe hinzu:

Verwenden Sie einen der folgenden Befehle.

- authorize-security-group-ingress (AWS CLI)
- Grant-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

So fügen Sie einer Sicherheitsgruppe eine oder mehrere Ausgangsregeln hinzu:

Verwenden Sie einen der folgenden Befehle.

- authorize-security-group-egress (AWS CLI)
- Grant-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Aktualisieren veralteter Sicherheitsgruppenregeln

Sie können eine Sicherheitsgruppenregel mit einer der folgenden Methoden aktualisieren. Die aktualisierte Regel gilt automatisch für alle Instances, die der Sicherheitsgruppe zugewiesen sind.

Console

Wenn Sie das Protokoll, den Port-Bereich oder die Quelle oder das Ziel einer vorhandenen Sicherheitsgruppenregel unter Verwendung der Konsole ändern, löscht die Konsole die vorhandene Regel und fügt eine neue für Sie hinzu.

So aktualisieren Sie eine Sicherheitsgruppenregel:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die Sicherheitsgruppe aus.
4. Wählen Sie Actions (Aktionen), Edit inbound rules (Eingehende Regeln bearbeiten) aus, um eine Regel für eingehenden Datenverkehr zu aktualisieren oder Actions (Aktionen), Edit outbound rules (Ausgehende Regeln bearbeiten), um eine Regel für ausgehenden Datenverkehr zu aktualisieren.
5. Aktualisieren Sie die Regel nach Bedarf.
6. Wählen Sie Preview changes (Änderungen überprüfen), Confirm (Bestätigen).

So markieren Sie eine Sicherheitsgruppenregel

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die Sicherheitsgruppe aus.
4. Markieren Sie auf der Registerkarte Eingehende Regeln oder Ausgehende Regeln das Kontrollkästchen für die Regel und wählen Sie dann Markierungen verwalten.

5. Auf der Seite Manage Tags (Tags (Markierungen) verwalten) werden alle Tags (Markierungen) angezeigt, die der Regel zugewiesen sind. Um eine Markierung hinzuzufügen, wählen Sie Add Tags (Tags (Markierung) hinzufügen) und geben Sie den Markierungsschlüssel und -Wert ein. Um ein Tag (Markierung) zu löschen, wählen Sie Remove (Entfernen) neben dem Tag (Markierung), das Sie löschen möchten.
6. Wählen Sie Save Changes.

Command line

Sie können das Protokoll, den Portbereich, die Quelle oder das Ziel einer vorhandenen Regel nicht mit der Amazon EC2-API oder ein Befehlszeilentool ändern. Stattdessen müssen Sie die vorhandene Regel löschen und eine neue Regel hinzufügen. Sie können jedoch die Beschreibung einer vorhandenen Regel aktualisieren.

So aktualisieren Sie eine Regel

Verwenden Sie einen der folgenden Befehle.

- modify-security-group-rules (AWS CLI)

So aktualisieren Sie die Beschreibung für eine bestehende eingehende Regel:

Verwenden Sie einen der folgenden Befehle.

- update-security-group-rule-descriptions-ingress (AWS CLI)
- Update-EC2SecurityGroupRuleIngressDescription (AWS Tools for Windows PowerShell)

So aktualisieren Sie die Beschreibung für eine bestehende ausgehende Regel:

Verwenden Sie einen der folgenden Befehle.

- update-security-group-rule-descriptions-egress (AWS CLI)
- Update-EC2SecurityGroupRuleEgressDescription (AWS Tools for Windows PowerShell)

So markieren Sie eine Sicherheitsgruppenregel

Verwenden Sie einen der folgenden Befehle.

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

Löschen von Regeln aus einer Sicherheitsgruppe

Wenn Sie eine Regel aus einer Sicherheitsgruppe löschen, wird die Änderung automatisch auf alle Instances der Sicherheitsgruppe angewendet.

Sie können Regeln aus einer Sicherheitsgruppe mit einer der folgenden Methoden löschen.

Console

So löschen Sie eine Sicherheitsgruppenregel:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die zu aktualisierende Sicherheitsgruppe, wählen Sie Actions (Aktionen) und wählen Sie dann Edit inbound rules (Eingangsregeln bearbeiten), um eine Eingangsregel zu entfernen oder Edit outbound rules (Ausgangsregeln bearbeiten), um eine Ausgangsregel zu entfernen.
4. Wählen Sie die Delete (Löschen)-Schaltfläche rechts neben der zu löschenden Regel.
5. Wählen Sie Save rules (Regeln speichern) aus. Alternativ können Sie Änderungen in der Vorschau anzeigen wählen, Ihre Änderungen überprüfen und dann Bestätigen auswählen.

Command line

So entfernen Sie eine oder mehrere Eingangsregeln aus einer Sicherheitsgruppe:

Verwenden Sie einen der folgenden Befehle.

- revoke-security-group-ingress (AWS CLI)
- Revoke-EC2SecurityGroupIngress (AWS Tools for Windows PowerShell)

So entfernen Sie eine oder mehrere Ausstiegsregeln aus einer Sicherheitsgruppe:

Verwenden Sie einen der folgenden Befehle.

- revoke-security-group-egress (AWS CLI)

- Revoke-EC2SecurityGroupEgress (AWS Tools for Windows PowerShell)

Löschen einer Sicherheitsgruppe

Eine mit einer Instance verbundene Sicherheitsgruppe kann nicht gelöscht werden. Sie können die Standardsicherheitsgruppe nicht löschen. Eine Sicherheitsgruppe, auf die eine andere Sicherheitsgruppe in derselben VPC verweist, kann nicht gelöscht werden. Wenn Ihre Sicherheitsgruppe von einer ihrer eigenen Regeln referenziert wird, müssen Sie die Regel löschen, bevor Sie die Sicherheitsgruppe löschen können.

Console

Löschen Sie eine Sicherheitsgruppe wie folgt:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die Sicherheitsgruppe und dann Aktionen, Sicherheitsgruppe löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Command line

Löschen Sie eine Sicherheitsgruppe wie folgt:

Verwenden Sie einen der folgenden Befehle.

- delete-security-group (AWS CLI)
- Remove-EC2SecurityGroup (AWS Tools for Windows PowerShell)

Zuordnen einer Sicherheitsgruppe zu einer Instance

Sie können eine oder mehrere Sicherheitsgruppe(n) einer Instance zuweisen, wenn Sie die Instance starten. Sie können auch eine oder mehrere Sicherheitsgruppe(n) in einer Startvorlage angeben. Die Sicherheitsgruppen werden allen Instances zugewiesen, die mithilfe der Startvorlage gestartet werden.

- Informationen zum Zuweisen einer Sicherheitsgruppe zu einer Instance beim Starten der Instance finden Sie unter Network settings (Netzwerkeinstellungen) von Starten einer Instance mit

definierten Parametern (neue Konsole) oder Schritt 6: Konfigurieren einer Sicherheitsgruppe (alte Konsole).

- Informationen zum Angeben einer Sicherheitsgruppe in einer Startvorlage finden Sie unter Network settings (Netzwerkeinstellungen) von Erstellen Sie eine Startvorlage aus Parametern.

Ändern der Sicherheitsgruppe einer Instance

Nach dem Start einer Instance können Sie deren Sicherheitsgruppen durch das Hinzufügen oder Entfernen von Sicherheitsgruppen nicht mehr ändern.

Voraussetzungen

- Die Instance muss sich im `running`- oder `stopped`-Status befinden.
- Eine Sicherheitsgruppe ist spezifisch für eine VPC. Sie können eine Sicherheitsgruppe einer oder mehreren Instances zuweisen, die in der VPC gestartet wurden, für die Sie die Sicherheitsgruppe erstellt haben.

Console

So ändern Sie die Sicherheitsgruppen für eine Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie Ihre Instance und wähle Sie dann Actions (Aktionen), Security (Sicherheit), Change security groups (Sicherheitsgruppen ändern) aus.
4. Wählen Sie für Associated security groups (Zugehörige Sicherheitsgruppen) eine Sicherheitsgruppe aus der Liste aus und klicken Sie auf Add security group (Sicherheitsgruppe hinzufügen).

   Um eine bereits zugeordnete Sicherheitsgruppe zu entfernen, wählen Remove (Entfernen) für diese Sicherheitsgruppe.
5. Wählen Sie Save aus.

Command line

So ändern Sie die Sicherheitsgruppen für eine Instance

Verwenden Sie einen der folgenden Befehle.

- modify-instance-attribute (AWS CLI)
- Edit-EC2InstanceAttribute (AWS Tools for Windows PowerShell)

Sicherheitsgruppenregeln für verschiedene Anwendungsfälle

Sie können eine Sicherheitsgruppe erstellen und dieser Regeln hinzufügen, die die Rolle der Instance reflektieren, mit der die Sicherheitsgruppe verbunden ist. Eine Instance, die als Webserver konfiguriert ist, benötigt beispielsweise Sicherheitsgruppenregeln, die eingehenden HTTP- und HTTPS-Zugriff zulassen. Ebenso benötigt eine Datenbank-Instance Regeln, die den Zugriff für den Datenbanktyp zulassen, wie z.B. den Zugriff über Port 3306 für MySQL.

Es folgen einige Beispiele für die Arten von Regeln, die Sie für bestimmte Zugriffsarten zu Sicherheitsgruppen hinzufügen können.

Beispiele

- Webserverregeln
- Datenbankserverregeln
- Regeln für die Verbindung mit Instances von Ihrem Computer aus
- Regeln für die Verbindung mit Instances von einer Instance mit der gleichen Sicherheitsgruppe aus
- Regeln für Ping/ICMP
- DNS-Server-Regeln
- Amazon EFS-Regeln
- Elastic Load Balancing-Regeln
- VPC-Peering-Regeln

Webserverregeln

Die folgenden eingehenden Regeln erlauben den HTTP- und HTTPS-Zugriff von jeder IP-Adresse aus. Wenn Ihre VPC für IPv6 aktiviert ist, können Sie Regeln zur Steuerung des eingehenden HTTP- und HTTPS-Datenverkehrs von IPv6-Adressen hinzufügen.

Protokolltyp	Protokoll nummer	Port	Quell-IP	Hinweise
TCP	6	80 (HTTP)	0.0.0.0/0	Lässt eingehenden HTTP-Zugriff von jeder IPv4-Adresse zu
TCP	6	443 (HTTPS)	0.0.0.0/0	Lässt eingehenden HTTPS-Zugriff von jeder IPv4-Adresse zu
TCP	6	80 (HTTP)	::/0	Lässt eingehenden HTTP-Zugriff von jeder IPv6-Adresse zu
TCP	6	443 (HTTPS)	::/0	Lässt eingehenden HTTPS-Zugriff von jeder IPv6-Adresse zu

Datenbankserverregeln

Die folgenden eingehenden Regeln sind Beispiele für Regeln, die Sie für den Datenbankzugriff hinzufügen können, je nachdem, auf welcher Art von Datenbank Ihre Instance ausgeführt wird. Weitere Informationen zu Amazon RDS-Instances finden Sie im Amazon RDS-Benutzerhandbuch.

geben Sie für die Quell-IP eine der folgenden Optionen an:

- Eine bestimmte IP-Adresse oder ein Bereich von IP-Adressen (in CIDR-Block-Notation) in Ihrem On-Premises-Netzwerk
- Eine Sicherheitsgruppen-ID für eine Gruppe von Instances, die auf die Datenbank zugreifen.

Protokolltyp	Protokollnummer	Port	Hinweise
TCP	6	1433 (MS SQL)	Der Standardport für den Zugriff auf eine Microsoft SQL Server-Da

Protokolltyp	Protokollnummer	Port	Hinweise
			tenbank, beispielsweise, auf einer Amazon RDS-Instance
TCP	6	3306 (MYSQL/Aurora)	Der Standardport für den Zugriff auf eine MySQL- oder Aurora-Datenbank, beispielsweise, auf einer Amazon RDS-Instance
TCP	6	5439 (Redshift)	Der Standardport für den zugriff auf eine Amazon Redshift-Cluster-Datenbank
TCP	6	5432 (PostgreSQL)	Der Standardport für den Zugriff auf eine PostgreSQL-Datenbank, beispielsweise, auf einer Amazon RDS-Instance
TCP	6	1521 (Oracle)	Der Standardport für den Zugriff auf eine Oracle-Datenbank, beispielsweise, auf einer Amazon RDS-Instance

Sie können optional den ausgehenden Verkehr von Ihren Datenbankservern einschränken. Sie könnten zum Beispiel den Zugriff auf das Internet für Softwareupdates erlauben, aber alle anderen Arten des Datenverkehrs einschränken. Sie müssen zuerst die standardmäßige ausgehende Regel entfernen, die allen ausgehenden Datenverkehr zulässt.

Protokolltyp	Protokollnummer	Port	Ziel-IP	Hinweise
TCP	6	80 (HTTP)	0.0.0.0/0	Lässt ausgehenden HTTP-Zugriff auf jede IPv4-Adresse zu

Protokolltyp	Protokoll nummer	Port	Ziel-IP	Hinweise
TCP	6	443 (HTTPS)	0.0.0.0/0	Lässt ausgehenden HTTPS-Zugriff auf jede IPv4-Adresse zu
TCP	6	80 (HTTP)	::/0	(Nur IPv6-fähige VPC) Lässt ausgehenden HTTP-Zugriff auf jede IPv6-Adresse zu
TCP	6	443 (HTTPS)	::/0	(Nur IPv6-fähige VPC) Lässt ausgehenden HTTPS-Zugriff auf jede IPv6-Adresse zu

Regeln für die Verbindung mit Instances von Ihrem Computer aus

Um Ihre Instance zu verbinden, muss Ihre Sicherheitsgruppe über eingehende Regeln verfügen, die den SSH-Zugriff (für Linux-Instances) oder den RDP-Zugriff (für Windows-Instances) erlauben.

Protokolltyp	Protokollnummer	Port	Quell-IP
TCP	6	22 (SSH)	Die öffentliche IPv4-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen in Ihrem On-Premises-Netzwerk. Wenn Ihre VPC IPv6-fähig ist und Ihre Instance eine IPv6-Adresse hat, können Sie eine(n) IPv6-Adresse oder -Bereich eingeben.
TCP	6	3389 (RDP)	Die öffentliche IPv4-Adresse Ihres Computers bzw. ein Bereich von IP-Adressen in Ihrem On-Premises-Netzwerk. Wenn Ihre VPC IPv6-fähig ist und Ihre Instance eine IPv6-Adresse hat, können Sie eine(n) IPv6-Adresse oder -Bereich eingeben.

Regeln für die Verbindung mit Instances von einer Instance mit der gleichen Sicherheitsgruppe aus

Um zuzulassen, dass Instances, die mit derselben Sicherheitsgruppe verbunden sind, miteinander kommunizieren, müssen Sie eine ausdrückliche Regel dafür hinzufügen.

> **Note**
>
> Wenn Sie Routen konfigurieren, um den Datenverkehr zwischen zwei Instances in unterschiedlichen Subnetzen über eine Middlebox-Appliance weiterzuleiten, müssen Sie sicherstellen, dass die Sicherheitsgruppen für beide Instances den Datenverkehr zwischen den Instances zulassen. Die Sicherheitsgruppe für jede Instance muss die private IP-Adresse der anderen Instance oder den CIDR-Bereich des Subnetzes, das die andere Instance enthält, als Quelle referenzieren. Wenn Sie die Sicherheitsgruppe der anderen Instance als Quelle referenzieren, wird dadurch kein Datenverkehr zwischen den Instances möglich.

Die folgende Tabelle beschreibt die eingehende Regel für eine Sicherheitsgruppe, die zugehörigen Instances erlaubt, miteinander zu kommunizieren. Die Regel lässt alle Arten von Datenverkehr zu.

Protokolltyp	Protokollnummer	Ports	Quell-IP
-1 (All)	-1 (All)	-1 (All)	Die ID der Sicherheitsgruppe oder der CIDR-Bereich des Subnetzes , das die andere Instance enthält (siehe Hinweis).

Regeln für Ping/ICMP

Der ping-Befehl ist eine Art von ICMP-Datenverkehr. Um Ihre Instance anzupingen, müssen Sie eine der folgenden ICMP-Regeln für eingehenden Datenverkehr hinzufügen.

Typ	Protokoll	Quelle		
Benutzerdefiniertes ICMP – IPv4	Echo-Anforderung	Die öffentliche IPv4-Adresse Ihres Computers		

Typ	Protokoll	Quelle		
		, eine bestimmte IPv4-Adresse oder eine IPv4- oder IPv6-Adresse von einem beliebigen Ort.		
Alle ICMP - IPv4	IPv4 ICMP (1)	Die öffentliche IPv4-Adresse Ihres Computers, eine bestimmte IPv4-Adresse oder eine IPv4- oder IPv6-Adresse von einem beliebigen Ort.		

Zur Verwendung des ping6-Befehls zum Pinging der IPv6-Adresse für Ihre Instance müssen Sie die folgende eingehende ICMPv6-Regel hinzufügen.

Typ	Protokoll	Quelle		
Alle ICMP – IPv6	IPv6 ICMP (58)	Die IPv6-Adresse Ihres Computers, eine bestimmte IPv4-Adresse oder eine IPv4- oder IPv6-Adresse von einem beliebigen Ort.		

DNS-Server-Regeln

Wenn Sie Ihre EC2-Instance als DNS-Server eingerichtet haben, müssen Sie sicherstellen, dass TCP- und UDP-Datenverkehr Ihren DNS-Server über Port 53 erreichen kann.

geben Sie für die Quell-IP eine der folgenden Optionen an:

- Eine IP-Adresse oder ein Bereich von IP-Adressen (in CIDR-Block-Notation) in einem Netzwerk
- Eine Sicherheitsgruppen-ID für eine Gruppe von Instances in Ihrem Netzwerk, die Zugriff auf den DNS-Server benötigen

Protokolltyp	Protokollnummer	Port
TCP	6	53
UDP	17	53

Amazon EFS-Regeln

Wenn Sie ein Amazon EFS-Dateisystem mit Ihren Amazon EC2-Instances verwenden, muss die Sicherheitsgruppe, die Sie mit Ihren Amazon EFS-Mountingzielen verbinden, den Datenverkehr über das NFS-Protokoll zulassen.

Protokoll typ	Protokoll nummer	Ports	Quell-IP	Hinweise
TCP	6	2049 (NFS)	Die ID der Sicherhei tsgruppe	Erlaubt den eingehend en NFS-Zugriff von Ressourcen (einschli eßlich des Mountingziels), die mit dieser Sicherhei tsgruppe verbunden sind

Zum Mounting eines Amazon EFS-Dateisystems auf Ihrer Amazon EC2-Instance müssen Sie eine Verbindung zu Ihrer Instance herstellen. Daher muss die mit Ihrer Instance verbundene

Sicherheitsgruppe über Regeln verfügen, die den eingehenden SSH-Datenverkehr von ihrem lokalen Computer oder lokalen Netzwerk aus zulassen.

Protokolltyp	Protokollnummer	Ports	Quell-IP	Hinweise
TCP	6	22 (SSH)	Der IP-Adressbereich Ihres lokalen Computers bzw. der Bereich von IP-Adressen (in CIDR-Block-Notation) für Ihr Netzwerk.	Lässt eingehenden SSH-Zugriff von Ihrem lokalen Computer zu.

Elastic Load Balancing-Regeln

Wenn Sie einen Load Balancer verwenden, muss die mit Ihrem Load Balancer verbundene Sicherheitsgruppe über Regeln verfügen, die die Kommunikation mit Ihren Instances oder Zielen erlauben. Weitere Informationen finden Sie unter Konfigurieren von Sicherheitsgruppen für Ihren Classic Load Balancer in Benutzerhandbuch für Classic Load Balancer und Sicherheitsgruppen für Ihren Application Load Balancer in Benutzerhandbuch für Application Load Balancer.

VPC-Peering-Regeln

Sie können die eingehenden oder ausgehenden Regeln für die VPC-Sicherheitsgruppen aktualisieren, um auf Sicherheitsgruppen in der über Peering verbundenen VPC zu verweisen. Danach kann der Datenverkehr von und zu den Instances fließen, die der referenzierten Sicherheitsgruppe in der über Peering verbundenen VPC zugewiesen sind. Weitere Informationen zum Konfigurieren von Sicherheitsgruppen für VPC-Peering finden Sie unter Aktualisieren der Sicherheitsgruppen, um auf Peer-VPC-Gruppen zu verweisen.

NitroTPM

Nitro Trusted Platform Module (NitroTPM) ist ein virtuelles Gerät von AWS -Nitro-System und entspricht TPM 2.0. Es speichert sicher Artefakte (etwa Passwörter, Zertifikate oder Verschlüsselungsschlüssel), die zur Authentifizierung der Instance verwendet werden. NitroTPM kann Schlüssel generieren und sie für kryptografische Funktionen nutzen (etwa Hashing, Signieren, Verschlüsselung und Entschlüsselung).

NitroTPM bietet das sogenannte Measured Boot, einen Prozess, bei dem der Bootloader und das Betriebssystem kryptografische Hashes von jeder Bootbinärdatei erstellen und diese mit den vorherigen Werten in den internen Platform Configuration Registers (PCR) von NitroTPM kombinieren. Mit „Measured Boot“ können Sie signierte PCR-Werte von NitroTPM abrufen und diese verwenden, um gegenüber Remote-Entitäten die Integrität der Bootsoftware der Instance zu beweisen. Dieser Vorgang wird als Remote-Bescheinigung bezeichnet.

Mit NitroTPM können Schlüssel und Secrets mit einem bestimmten PCR-Wert gekennzeichnet werden. Wenn sich der Wert des PCRs und damit die Instance-Integrität ändert, kann dadurch nicht mehr auf die Schlüssel und Secrets zugegriffen werden. Diese besondere Form des bedingten Zugangs wird als Sealiung und Unsealing (etwa: Versiegeln und Entsiegeln) bezeichnet. Betriebssystemtechnologien wie z. B. können NitroTPM verwenden BitLocker, um einen Laufwerks-Entschlüsselungsschlüssel zu versiegeln, sodass das Laufwerk nur dann entschlüsselt werden kann, wenn das Betriebssystem korrekt gestartet wurde und sich in einem zweifelsfrei funktionierenden Zustand befindet.

Um NitroTPM zu verwenden, müssen Sie ein Amazon Machine Image (AMI) auswählen, das für NitroTPM-Unterstützung konfiguriert wurde, und dann das AMI verwenden, um Instances zu starten, die auf dem Nitro-System basieren. AWS Sie können eines der vorgefertigten AMIs von Amazon auswählen oder selbst eines erstellen.

Kosten

Für die Nutzung von NitroTPM fallen keine zusätzlichen Kosten an. Sie bezahlen nur für die zugrundeliegenden Ressourcen, die Sie nutzen.

Themen

Überlegungen

Die folgenden Hinweise gelten für die Verwendung von NitroTPM:

- BitLocker Volumes, die mit NitroTPM-basierten Schlüsseln verschlüsselt sind, können nur auf der ursprünglichen Instance verwendet werden.
- Der NitroTPM-Status ist nicht in Amazon EBS-Snapshots enthalten.
- Der NitroTPM-Status ist nicht in VM-Import-/Export-Images enthalten.
- Die NitroTPM-Unterstützung wird durch Angabe des Wertes von `v2.0` für `tpm-support`-Parameter beim Erstellen eines AMIs aktiviert. Nachdem Sie eine Instance mit dem AMI gestartet haben, können Sie die Attribute der Instance nicht mehr ändern. Instances mit NitroTPM unterstützen die Attribut-API nicht. ModifyInstance
- Sie können ein AMI nur mit NitroTPM erstellen, das mithilfe der RegisterImageAPI konfiguriert ist, AWS CLI und nicht mit der Amazon EC2 EC2-Konsole.
- NitroTPM wird auf Outposts nicht unterstützt.
- NitroTPM wird in lokalen Zonen und Wavelength-Zonen nicht unterstützt.

Voraussetzungen für die Aktivierung beim Start

Um eine Instanz mit aktiviertem NitroTPM zu starten, müssen die folgenden Voraussetzungen erfüllt sein.

Linux-Instances

AMI

Benötigt ein AMI mit aktiviertem NitroTPM.

Derzeit gibt es keine NitroTPM-fähigen Amazon-Linux-AMIs. Um ein unterstütztes AMI zu verwenden, müssen Sie eine Reihe von Konfigurationsschritten für Ihr eigenes Linux-AMI ausführen. Weitere Informationen finden Sie unter Erstellen eines Linux-AMIs für NitroTPM-Unterstützung.

Betriebssystem

Das AMI muss ein Betriebssystem mit einem TPM 2.0 CRB-Treiber (Command Response Buffer) enthalten. Die meisten aktuellen Betriebssysteme, wie Amazon Linux 2, enthalten einen TPM 2.0 CRB-Treiber.

UEFI-Startmodus

NitroTPM erfordert, dass eine Instance im UEFI-Boot-Modus ausgeführt wird. Dazu muss das AMI für den UEFI-Boot-Modus konfiguriert werden. Weitere Informationen finden Sie unter UEFI Secure Boot.

Windows-Instances

AMI

Benötigt ein AMI mit aktiviertem NitroTPM.

Die folgenden Windows-AMIs sind für die Aktivierung von NitroTPM und UEFI Secure Boot mit Microsoft-Schlüsseln vorkonfiguriert:

- TPM-Windows_Server-2022-English-Core-Base
- TPM-Windows_Server-2022-English-Full-Base
- TPM-Windows_Server-2022-English-Full-SQL_2022_Enterprise
- TPM-Windows_Server-2022-English-Full-SQL_2022_Standard
- TPM-Windows_Server-2019-English-Core-Base
- TPM-Windows_Server-2019-English-Full-Base
- TPM-Windows_Server-2019-English-Full-SQL_2019_Enterprise
- TPM-Windows_Server-2019-English-Full-SQL_2019_Standard
- TPM-Windows_Server-2016-English-Core-Base
- TPM-Windows_Server-2016-English-Full-Base

Derzeit wird das Importieren von Windows mit NitroTPM über den Befehl import-image nicht unterstützt.

Betriebssystem

Das AMI muss ein Betriebssystem mit einem TPM 2.0 CRB-Treiber (Command Response Buffer) enthalten. Die meisten aktuellen Betriebssysteme, wie TPM-Windows_Server-2022-English-Full-Base, enthalten einen TPM 2.0-CRB-Treiber.

UEFI-Startmodus

NitroTPM erfordert, dass eine Instance im UEFI-Boot-Modus ausgeführt wird. Dazu muss das AMI für den UEFI-Boot-Modus konfiguriert werden. Weitere Informationen finden Sie unter UEFI Secure Boot.

Instance-Typen

Sie müssen einen der folgenden virtualisierten Instanztypen verwenden:

- Allgemeiner Zweck: M5, M5a, M5ad, M5d, M5dn, M5Zn, M6a, M6i, M6id, M6idn, M6in, M7a, M7i, M7i, M7i-Flex, T3, T3a
- Für Berechnungen optimiert: C5, C5a, C5ad, C5d, C5n, C6a, C6i, C6id, C6in, C7a, C7i, C7i-Flex
- Speicheroptimiert: R5, R5a, R5ad, R5b, R5d, R5dn, R5n, R6a, R6i, R6idn, R6in, R6id, R7a, R7i, R7iz, U7i-12 TB, U7in-16 TB, U7in-24 TB, U7in-32 TB, x2IDN, X2iEDN, x2IEDN, x2iEDN, x2iEDN, x2iEDN, x2iEDN, X2iEDN, x2iEDN, x2iEDN, X2iEDN, x2iEDN, X2iEDN, x2iEDN, X2iEDN, x2iEDN, X2iEDN, x2iEDN, x2iezn, z1d
- Speicheroptimiert: D3, D3en, I3en, I4i
- Beschleunigte Datenverarbeitung: G4dn, G5, G6, Gr6, Inf1, Inf2
- Hochleistungsrechnen: HPC6a, HPC6id

> **Note**
>
> Graviton-basierte Instances, Xen-Instances, Mac-Instances und Bare-Metal-Instances werden nicht unterstützt.

Erstellen eines Linux-AMIs für NitroTPM-Unterstützung

Sie konfigurieren Ihr Linux-AMI für die NitroTPM-Unterstützung bei der Registrierung des AMIs. Sie können die NitroTPM-Unterstützung später nicht mehr konfigurieren.

Eine Liste der Windows-AMIs, die für die NitroTPM-Unterstützung vorkonfiguriert sind, finden Sie unter. Voraussetzungen für die Aktivierung beim Start

Um ein Linux-AMI für NitroTPM-Unterstützung zu registrieren

1. Starten Sie eine temporäre Instance mit Ihrem erforderlichen Linux-AMI.
2. Wenn die Instance den `running` Status erreicht hat, erstellen Sie einen Snapshot des Root-Volumes der Instance.
3. Registrieren Sie das neue AMI. Verwenden Sie den Befehl register-image. Legen Sie für `--tpm-support` die Option `v2.0` fest. Legen Sie für `--boot-mode` die Option `uefi` fest.

Und geben Sie mithilfe des Snapshots, den Sie im vorherigen Schritt erstellt haben, eine Blockgerätezuordnung für das Root-Volume an.

```
aws ec2 register-image \
    --name my-image \
    --boot-mode uefi \
    --architecture x86_64 \
    --root-device-name /dev/xvda \
    --block-device-mappings DeviceName=/dev/xvda,Ebs={SnapshotId=snapshot_id} \
    --tpm-support v2.0
```

Erwartete Ausgabe

```
{
"ImageId": "ami-0123456789example"
}
```

4. Beenden Sie die temporäre Instance, die Sie in Schritt 1 gestartet haben, falls sie nicht mehr benötigt wird.

Überprüfen des Vorhandenseins eines aktiven AMIs für NitroTPM

Sie können mit `describe-images` bzw. mit `describe-image-attributes` überprüfen, ob ein AMI für NitroTPM aktiviert ist.

Das Vorhandensein eines aktiven AMI für NitroTPM mit **`describe-images`** überprüfen

Verwenden Sie den Befehl describe-images und geben Sie die ID des AMI an.

```
aws ec2 describe-images --image-ids ami-0123456789example
```

Wenn NitroTPM für das AMI aktiviert ist, erscheint in der Ausgabe `"TpmSupport": "v2.0"`.

```
{
    "Images": [
        {
        ...
        "BootMode": "uefi",
        ...
        "TpmSupport": "v2.0"
```

```
        }
    ]
}
```

Das Vorhandensein eines aktiven AMI für NitroTPM mit **`describe-image-attribute`** überprüfen

Verwenden Sie den Befehl describe-image-attribute und geben Sie den Parameter `attribute` mit dem Wert `tpmSupport` an.

> **Note**
>
> Sie müssen der AMI-Besitzer sein, um `describe-image-attribute` abrufen zu können.

```
aws ec2 describe-image-attribute \
    --region us-east-1 \
    --image-id ami-0123456789example \
    --attribute tpmSupport
```

Wenn NitroTPM für das AMI aktiviert ist, ist der Wert für `TpmSupport` `"v2.0"`. Beachten Sie, dass `describe-image-attribute` nur die Attribute zurückgibt, die in der Anforderung angegeben sind.

```
{
    "ImageId": "ami-0123456789example",
    "TpmSupport": {
        "Value": "v2.0"
    }
}
```

Aktivieren oder Beenden der Verwendung von NitroTPM für eine Instance

Wenn Sie eine Instance von einem AMI aus starten, bei dem NitroTPM-Unterstützung aktiviert ist, wird die Instance mit aktiviertem NitroTPM gestartet. Sie können die Instance so konfigurieren, dass sie NitroTPM nicht mehr verwendet. Sie können überprüfen, ob eine Instance für NitroTPM aktiviert ist.

Themen

- Starten Sie eine Instance mit aktiviertem NitroTPM
- Beenden der Verwendung von NitroTPM für eine Instance

- Überprüfen, ob innerhalb der Instance auf NitroTPM zugegriffen werden kann

Starten Sie eine Instance mit aktiviertem NitroTPM

Wenn Sie eine Instance mit den Voraussetzungen starten, wird NitroTPM automatisch auf der Instance aktiviert. Sie können NitroTPM für eine Instance nur beim Start aktivieren. Weitere Informationen über das Starten einer Instance finden Sie unter Starten Ihrer Instance.

Beenden der Verwendung von NitroTPM für eine Instance

Nachdem Sie eine Instance mit aktiviertem NitroTPM gestartet haben, können Sie NitroTPM für die Instance nicht deaktivieren. Sie können das Betriebssystem jedoch so konfigurieren, dass es NitroTPM nicht mehr verwendet. Deaktivieren Sie dazu den TPM 2.0-Gerätetreiber für die Instance mithilfe der folgenden Tools:

- [Linux-Instanzen] Verwenden Sie tpm-tools.
- [Windows-Instanzen] Verwenden Sie die TPM-Verwaltungskonsole tpm.msc.

Weitere Informationen über das Deaktivieren des Gerätetreibers finden Sie in der Dokumentation für Ihr Betriebssystem.

Überprüfen, ob innerhalb der Instance auf NitroTPM zugegriffen werden kann

Um zu überprüfen, ob eine Instanz für die NitroTPM-Unterstützung aktiviert ist, verwenden Sie AWS CLI

Führen Sie den Befehl describe-instances AWS CLI aus und geben Sie die Instance-ID an. Derzeit zeigt die Amazon-EC2-Konsole das Feld `TpmSupport` nicht an.

```
aws ec2 describe-instances --instance-ids i-0123456789example
```

Wenn NitroTPM auf der Instance aktiviert ist, erscheint in der Ausgabe `"TpmSupport": "v2.0"`.

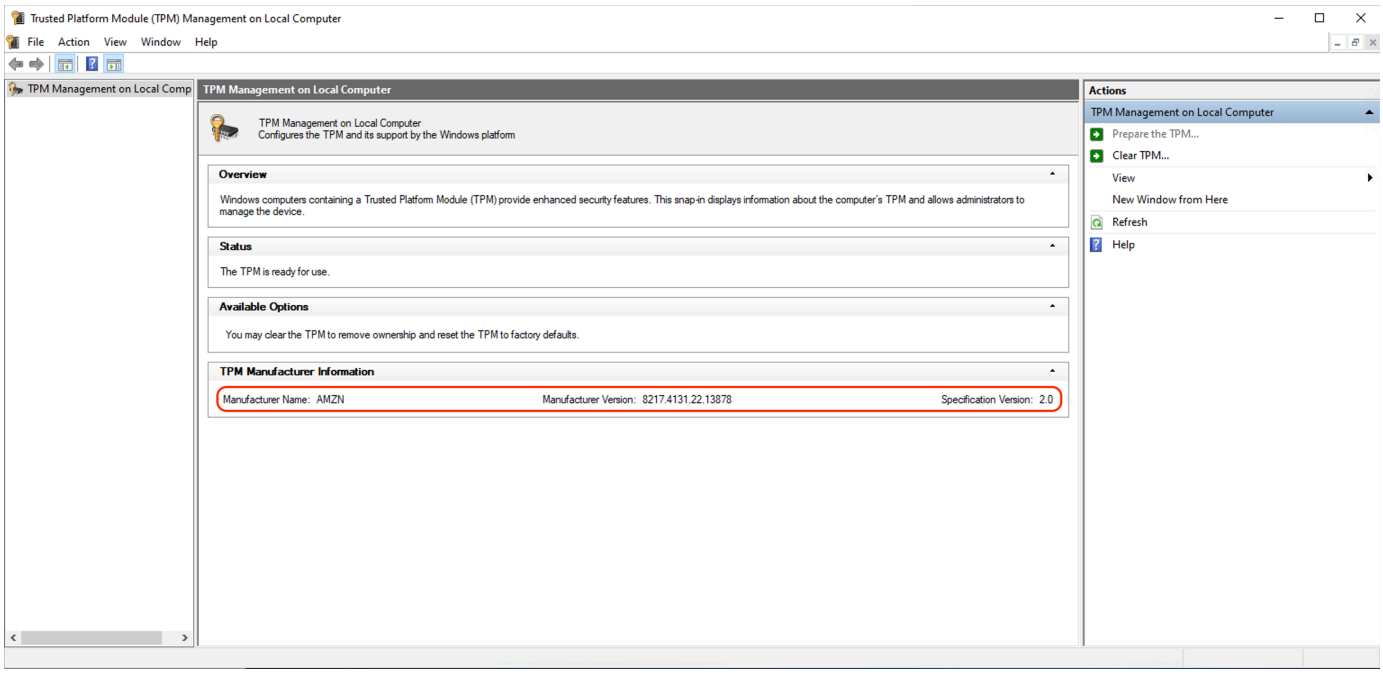
```
"Instances": {
              "InstanceId":"0123456789example",
              "InstanceType":"c5.large",
              ...
              "BootMode": "uefi",
              "TpmSupport": "v2.0"
              ...
```

```
}
```

(Windows-Instances) Um zu überprüfen, ob NitroTPM innerhalb einer Amazon EC2 EC2-Windows-Instance zugänglich ist

1. Stellen Sie eine Verbindung mit Ihrer Windows-Instance her.
2. Führen Sie in der Instance das Programm „tpm.msc“ aus.

   Das Fenster TPM Management on Local Computer (TPM-Verwaltung auf lokalem Computer) wird geöffnet.
3. Setzen Sie einen Haken bei dem Feld TPM Manufacturer Information (TPM-Herstellerinformationen). Es enthält den Namen des Herstellers und die Version von NitroTPM auf der Instance.



Rufen Sie den öffentlichen Bestätigungsschlüssel für eine Instance ab

Mit dem können Sie den öffentlichen Bestätigungsschlüssel für eine Instance jederzeit sicher abrufen. AWS CLI

Um den öffentlichen Bestätigungsschlüssel für eine Instance abzurufen

Verwenden Sie den Befehl get-instance-tpm-ek-pub AWS CLI .

Beispiel 1

Der folgende Beispielbefehl ruft beispielsweise den `rsa-2048` öffentlichen Bestätigungsschlüssel im `tpmt` Format ab. `i-01234567890abcdef`

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format tpmt \
--key-type rsa-2048
```

Das Folgende ist die Beispielausgabe.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "tpmt",
    "KeyType": "rsa-2048",
    "KeyValue": "AAEACwADALIAIINxl2dEhLEXAMPLEUal1yT9UtduBlILZPKh2hszFGmqAAYAgABDA
    EXAMPLEAAABAOiRd7WmgtdGNoV1h/AxmW+CXExblG8pEUfNm0LOLiYnEXAMPLERqApiFa/UhvEYqN4
    Z7jKMD/usbhsQaAB1gKA5RmzuhSazHQkax7EXAMPLEzDthlS7HNGuYn5eG7qnJndRcakS+iNxT8Hvf
    0S1ZtNuItMs+Yp4SO6aU28MT/JZkOKsXIdMerY3GdWbNQz9AvYbMEXAMPLEPyHfzgVO0QTTJVGdDxh
    vxtXCOu9GYf0crbjEXAMPLEd4YTbWdDdgOKWF9fjzDytJSDhrLAOUctNzHPCd/92l5zEXAMPLEOIFA
    Ss50C0/802c17W2pMSVHvCCa9lYCiAfxH/vYKovAAE="
}
```

Beispiel 2

Der folgende Beispielbefehl ruft beispielsweise `i-01234567890abcdef` den `rsa-2048` öffentlichen Bestätigungsschlüssel im `der` Format ab.

```
$ aws ec2 get-instance-tpm-ek-pub \
--instance-id i-01234567890abcdef \
--key-format der \
--key-type rsa-2048
```

Das Folgende ist die Beispielausgabe.

```
{
    "InstanceId": "i-01234567890abcdef",
    "KeyFormat": "der",
    "KeyType": "rsa-2048",
    "KeyValue": "MIIBIjANBgEXAMPLEw0BAQEFAAOCAQ8AMIIBCgKCAQEA6JF3taEXAMPLEXWH8DGZb4
    JcTFuUbykRR82bQs4uJifaKSOv5NGoEXAMPLEG8Rio3hnuMowP+6xuGxBoAHWAoDlGbO6FJrMdEXAMP
    LEnYUHvMO2GVLsc0a5ifl4buqcmd1FxqRL6I3FPwe9/REXAMPLE0yz5inhI7ppTbwxP8lmQ4qxch0x6
```

```
    tjcZ1Zs1DP0EXAMPLERUYLQ/Id/OBU7RBNMlUZ0PGG/G1cI670Zh/RytuOdx9iEXAMPLEtZ0N2A4pYX
    1+PMPK0lIOGssA5Ry03Mc8J3/3aXnOD2/ASRQ4gUBKznQLT/zTZEXAMPLEJUe8IJr2VgKIB/Ef+9gqi
    8AAQIDAQAB"
}
```

Credential Guard für Windows-Instanzen

Das AWS Nitro-System unterstützt Credential Guard für Amazon Elastic Compute Cloud (Amazon EC2) Windows-Instances. Credential Guard ist ein virtualisierungsbasiertes Windows-Sicherheitsfeature (VBS), die die Erstellung isolierter Umgebungen ermöglicht, um Sicherheitsressourcen wie Windows-Benutzeranmeldeinformationen und die Durchsetzung der Codeintegrität über den Windows-Kernelschutz hinaus zu schützen. Wenn Sie EC2-Windows-Instances ausführen, verwendet Credential Guard das AWS Nitro-System, um zu verhindern, dass Windows-Anmeldeinformationen aus dem Betriebssystemspeicher extrahiert werden.

Inhalt

Voraussetzungen

Ihre Windows-Instance muss die folgenden Voraussetzungen erfüllen, um Credential Guard verwenden zu können:

Amazon Machine Images (AMIs)

Das AMI muss vorkonfiguriert sein, um NitroTPM und UEFI Secure Boot zu aktivieren. Weitere Informationen zu unterstützten AMIs finden Sie unter. the section called “Voraussetzungen”

Speicherintegrität

Speicherintegrität, auch bekannt als Hypervisor-Protected Code Integrity (HVCI) oder Hypervisor Enforced Code Integrity, wird nicht unterstützt. Bevor Sie Credential Guard aktivieren, müssen Sie sicherstellen, dass dieses Feature deaktiviert ist. Weitere Informationen finden Sie unter Deaktivieren Sie die Speicherintegrität.

Instance-Typen

Die folgenden Instance-Typen unterstützen Credential Guard in allen Größen: `C5`, `C5d`, `C5n`, `C6i`, `C6id`, `C6in`, `M5`, `M5d`, `M5dn`, `M5n`, `M5zn`, `M6i`, `M6id`, `M6idn`, `M6in`, `R5`, `R5b`, `R5d`, `R5dn`, `R5n`, `R6i`, `R6id`, `R6idn`, `R6in`.

> **Note**
>
> NitroTPM hat zwar einige erforderliche Instance-Typen gemeinsam, aber der Instance-Typ muss einer der oben genannten sein, um Credential Guard zu unterstützen.

Starten Sie eine unterstützte Instance

Sie können die Amazon EC2 EC2-Konsole oder AWS Command Line Interface (AWS CLI) verwenden, um eine Instance zu starten, die Credential Guard unterstützt. Sie benötigen zum Starten Ihrer Instance eine kompatible AMI-ID, die für jede AWS-Region eindeutig ist.

> **Tip**
>
> Sie können den folgenden Link verwenden, um Instances mit kompatiblen, von Amazon bereitgestellten AMIs in der Amazon-EC2-Konsole zu erkennen und zu starten: https://console.aws.amazon.com/ec2/v2/home?#Images:visibility=public-images;v=3;search=:TPM-Windows_Server;ownerAlias=amazon

Amazon EC2 console

So starten Sie eine Instance mit der Amazon-EC2-Konsole

Folgen Sie den Schritten, um eine Instance zu starten, und geben Sie dabei einen unterstützten Instance-Typ und ein vorkonfiguriertes Windows-AMI an.

AWS CLI

Um eine Instance mit dem zu starten AWS CLI

Verwenden Sie den run-instances-Befehl, um eine Instance mit einem unterstützten Instance-Typ und einem vorkonfigurierten Windows-AMI zu starten.

```
aws ec2 run-instances \
    --image-id resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-
English-Full-Base \
    --instance-type c6i.large \
    --region us-east-1 \
    --subnet-id subnet-id
    --key-name key-name
```

PowerShell

Um eine Instance mit dem zu starten AWS Tools for PowerShell

Verwenden Sie den New-EC2Instance-Befehl, um eine Instance mit einem unterstützten Instance-Typ und einem vorkonfigurierten Windows-AMI zu starten.

```
New-EC2Instance `
    -ImageId resolve:ssm:/aws/service/ami-windows-latest/TPM-Windows_Server-2022-
English-Full-Base `
    -InstanceType c6i.large `
    -Region us-east-1 `
    -SubnetId subnet-id `
    -KeyName key-name
```

Deaktivieren Sie die Speicherintegrität

Sie können den Editor für lokale Gruppenrichtlinien verwenden, um die Speicherintegrität in unterstützten Szenarios zu deaktivieren. Die folgenden Hinweise können für jede Konfigurationseinstellung unter Virtualisierungsbasierter Schutz der Codeintegrität angewendet werden:

- Ohne Sperre aktiviert – Ändern Sie die Einstellung auf Deaktiviert, um die Speicherintegrität zu deaktivieren.
- Mit UEFI-Sperre aktiviert – Die Speicherintegrität wurde mit UEFI-Sperre aktiviert. Die Speicherintegrität kann nicht deaktiviert werden, nachdem sie mit der UEFI-Sperre aktiviert wurde. Wir empfehlen, eine neue Instance mit deaktivierter Speicherintegrität zu erstellen und die nicht unterstützte Instance zu beenden, wenn sie nicht verwendet wird.

So deaktivieren Sie die Speicherintegrität mit dem Editor für lokale Gruppenrichtlinien

1. Stellen Sie über das Remote Desktop Protocol (RDP) als Benutzerkonto mit Administratorrechten eine Verbindung zu Ihrer Instance her. Weitere Informationen finden Sie unter the section called “Stellen Sie mithilfe eines RDP-Clients eine Connect zu Ihrer Windows-Instanz her”.
2. Öffnen Sie das Startmenü und suchen Sie nach **cmd**, um eine Eingabeaufforderung zu starten.
3. Führen Sie den folgenden Befehl aus, um den Editor für lokale Gruppenrichtlinien zu öffnen: `gpedit.msc`
4. Wählen Sie im Editor für lokale Gruppenrichtlinien Computerkonfiguration, Administrative Vorlagen, System, Geräteschutz aus.
5. Wählen Sie Virtualisierungsbasierte Sicherheit aktivieren und dann Richtlinieneinstellung bearbeiten aus.
6. Öffnen Sie das Dropdownmenü mit den Einstellungen für Virtualisierungsbasierter Schutz der Codeintegrität, wählen Sie Deaktiviert und anschließend Anwenden.
7. Starten Sie die Instance neu, um die Änderungen zu übernehmen.

Schalten Sie Credential Guard ein

Nachdem Sie eine Windows-Instance mit einem unterstützten Instance-Typ und einem kompatiblen AMI gestartet und bestätigt haben, dass die Speicherintegrität deaktiviert ist, können Sie Credential Guard aktivieren.

> **Important**
>
> Sie benötigen Administratorrechte, um die folgenden Schritte zum Aktivieren von Credential Guard auszuführen.

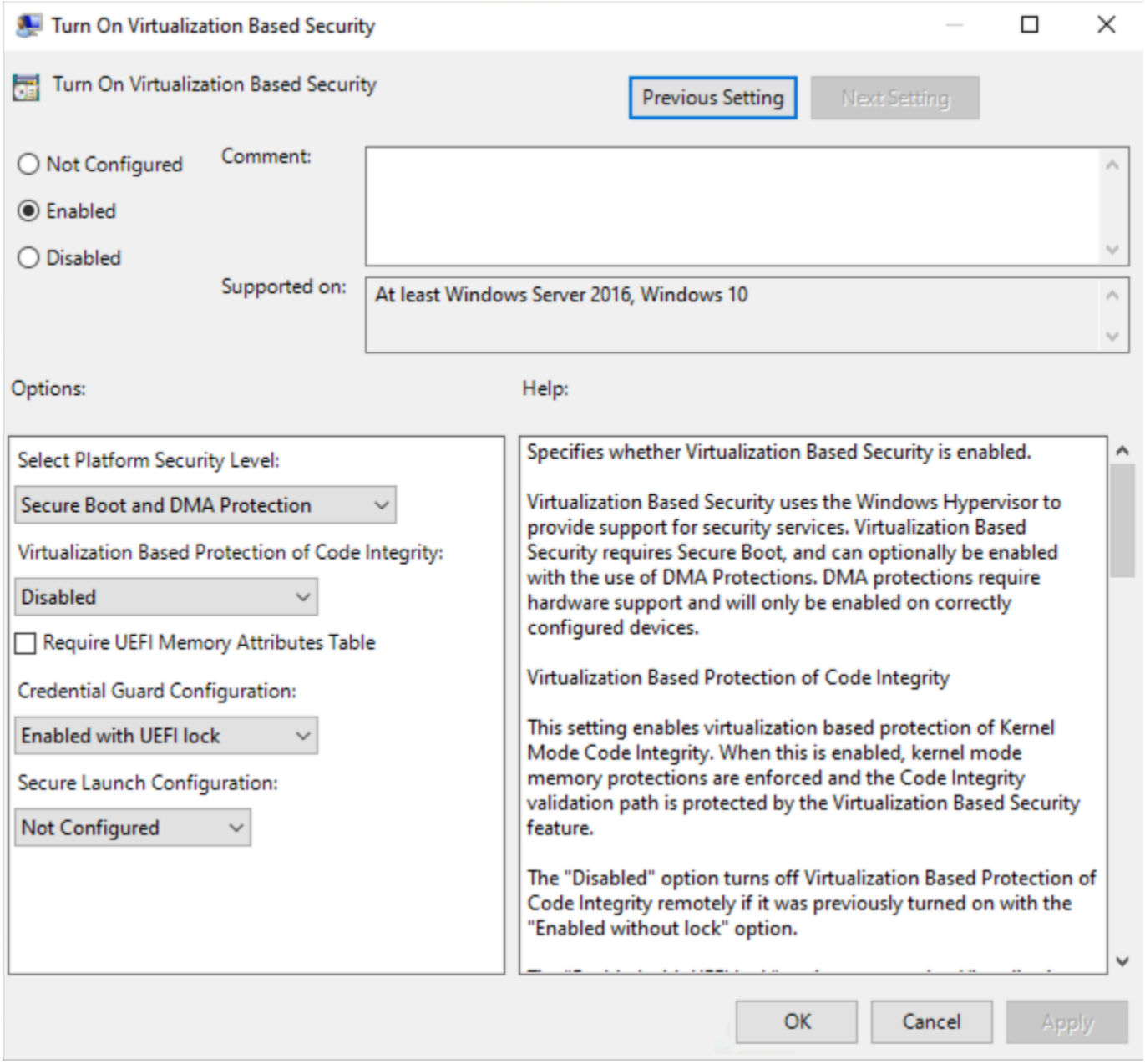
Aktivieren von Credential Guard

1. Stellen Sie über das Remote Desktop Protocol (RDP) als Benutzerkonto mit Administratorrechten eine Verbindung zu Ihrer Instance her. Weitere Informationen finden Sie unter the section called “Stellen Sie mithilfe eines RDP-Clients eine Connect zu Ihrer Windows-Instanz her”.
2. Öffnen Sie das Startmenü und suchen Sie nach **cmd**, um eine Eingabeaufforderung zu starten.

3. Führen Sie den folgenden Befehl aus, um den Editor für lokale Gruppenrichtlinien zu öffnen: `gpedit.msc`
4. Wählen Sie im Editor für lokale Gruppenrichtlinien Computerkonfiguration, Administrative Vorlagen, System, Geräteschutz aus.
5. Wählen Sie Virtualisierungsbasierte Sicherheit aktivieren und dann Richtlinieneinstellung bearbeiten aus.
6. Wählen Sie Aktiviert im Menü Virtualisierungsbasierte Sicherheit aktivieren aus.
7. Wählen Sie unter Plattformsicherheitsstufe auswählen die Optionen Sicherer Start und DMA-Schutz aus.
8. Wählen Sie für die Credential Guard-Konfiguration die Option Aktiviert mit UEFI-Sperre.

> **Note**
>
> Die verbleibenden Richtlinieneinstellungen sind nicht erforderlich, um Credential Guard zu aktivieren, und können auf Nicht konfiguriert belassen werden.

Das folgende Image zeigt die wie zuvor beschrieben konfigurierten VBS-Einstellungen:



9. Starten Sie die Instance neu, um die Einstellungen zu übernehmen.

Stellen Sie sicher, dass Credential Guard läuft

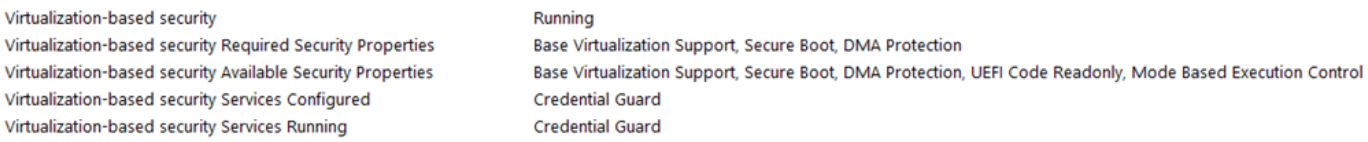
Sie können das Microsoft-Tool Systeminformationen (`Msinfo32.exe`) verwenden, um zu bestätigen, dass Credential Guard ausgeführt wird.

> **Important**
>
> Sie müssen die Instance zuerst neu starten, um die Anwendung der Richtlinieneinstellungen abzuschließen, die zum Aktivieren von Credential Guard erforderlich sind.

So überprüfen Sie, ob Credential Guard ausgeführt wird

1. Stellen Sie über das Remote Desktop Protocol (RDP) eine Verbindung zu Ihrer Instance her. Weitere Informationen finden Sie unter the section called “Stellen Sie mithilfe eines RDP-Clients eine Connect zu Ihrer Windows-Instanz her”.
2. Öffnen Sie innerhalb der RDP-Sitzung zu Ihrer Instance das Startmenü und suchen Sie nach **`cmd`**, um eine Eingabeaufforderung zu starten.
3. Öffnen Sie die Systeminformationen, indem Sie den folgenden Befehl ausführen: `msinfo32.exe`
4. Das Microsoft-Tool Systeminformationen listet die Details zur VBS-Konfiguration auf. Bestätigen Sie neben virtualisierungsbasierte Sicherheitsservices, dass Credential Guard als Wird ausgeführt angezeigt wird.

   Das folgende Image zeigt, dass VBS wie zuvor beschrieben ausgeführt wird:



Speicheroptionen für Ihre Amazon-EC2-Instances

Amazon EC2 bietet Ihnen flexible, kostengünstige easy-to-use Datenspeicheroptionen für Ihre Instances. Jede Option bietet eine einzigartige Kombination von Leistungs- und Beständigkeitsmerkmalen. Diese Speicheroptionen können Ihren Anforderungen entsprechend unabhängig voneinander oder kombiniert verwendet werden.

Amazon EBS

Amazon EBS bietet Volumes für einen dauerhaften Speicher auf Blockebene, die Sie einer Instance anfügen und von dieser trennen können. Sie können einer Instance mehrere EBS-Volumes zuordnen. Ein EBS-Volume bleibt unabhängig von der Betriebsdauer der zugeordneten Instance erhalten. Sie können Ihre EBS-Volumes verschlüsseln. Sie können eine Sicherungskopie Ihrer Daten anfertigen, indem Sie Snapshots von Ihren EBS-Volumes erstellen. Snapshots werden in Amazon S3 gespeichert. Sie können ein EBS-Volume aus einem Snapshot erstellen.

Instance-Speicher

Der Instance-Speicher stellt temporären Speicher auf Blockebene für Instances bereit. Anzahl, Größe und Typ der Instance-Speicher-Volumes werden durch den Instance-Typ und die Instance-Größe bestimmt. Die Daten auf einem Instance-Speicher-Volume bleiben nur während der Nutzungsdauer der zugewiesenen Instance erhalten; wenn Sie eine Instance anhalten, in den Ruhezustand versetzen oder beenden, gehen alle Daten auf den Instance-Speicher-Volumes verloren.

Amazon EFS(Nur Linux-Instances)

Amazon EFS bietet skalierbaren Dateispeicher für die Verwendung mit Amazon EC2. Sie können ein EFS-Dateisystem erstellen und Ihre Instances so konfigurieren, dass das Dateisystem gemountet wird. Sie können ein EFS-Dateisystem als gemeinsame Datenquelle für Workloads und Anwendungen verwenden, die jeweils auf mehr als einer Instance ausgeführt werden.

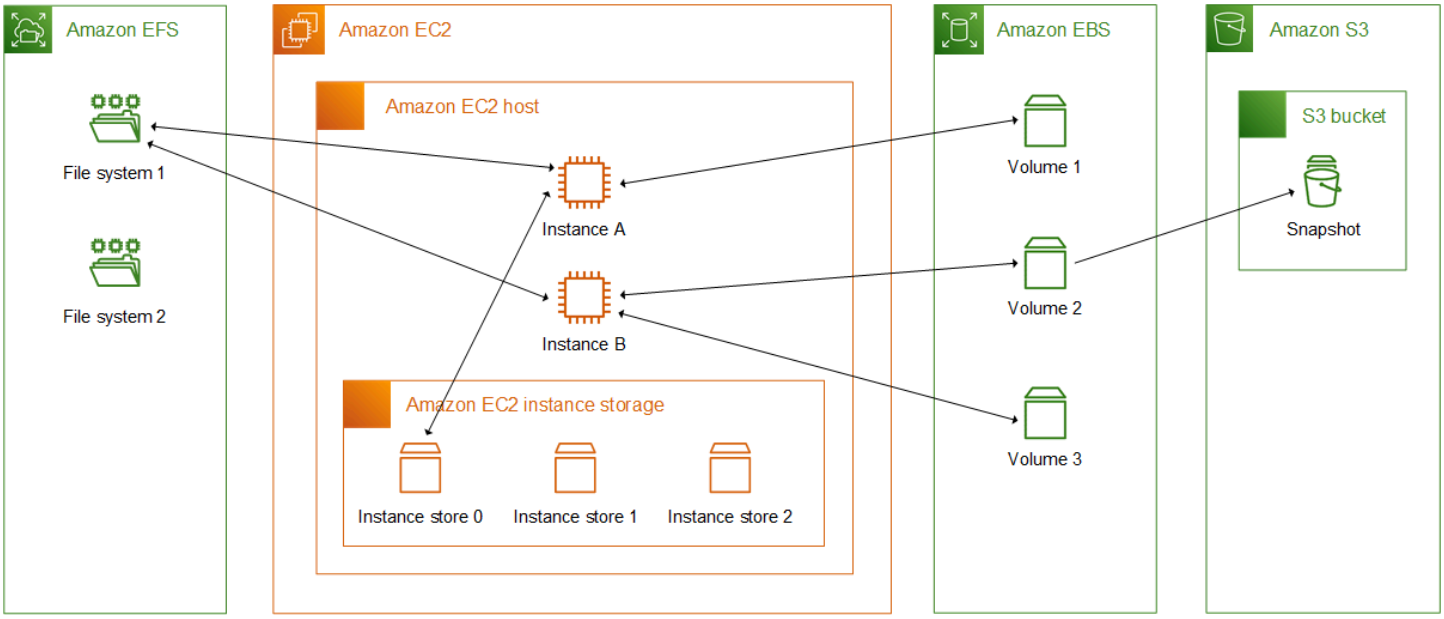
Amazon S3

Amazon S3 bietet Zugriff auf eine zuverlässige und kostengünstige Datenspeicher-Infrastruktur. Es ist darauf ausgelegt, die Webskalierung der Rechenleistung zu erleichtern, indem es Ihnen ermöglicht, jede beliebige Datenmenge jederzeit über Amazon EC2 oder das Internet zu speichern und abzurufen. Sie können Amazon S3 beispielsweise verwenden, um Backup-Kopien Ihrer Daten und Anwendungen zu speichern. Amazon EC2 verwendet Amazon S3, um EBS-Snapshots und Instance-Speicher-gestützte AMIs zu speichern.

Amazon FSx

Mit Amazon FSx können Sie leistungsstarke Dateisysteme mit hohem Featureumfang in der Cloud starten, ausführen und skalieren. Amazon FSx ist ein vollständig verwalteter Service, der eine Vielzahl von Workloads unterstützt. Sie können zwischen diesen weit verbreiteten Dateisystemen wählen: Lustre, NetApp ONTAP, OpenZFS und Windows File Server.

Im folgenden Image ist die Beziehung zwischen diesen Speicheroptionen und Ihrer Instance dargestellt.



Speicherpreise

Öffnen Sie „Preise“, scrollen Sie zu „AWS Preise für Produkte“ und wählen Sie „Speicher“ aus. AWS Wählen Sie das Speicherprodukt aus, um die entsprechende Preisseite zu öffnen.

Verwenden Sie Amazon EBS mit Amazon EC2

Amazon Elastic Block Store (Amazon EBS) bietet skalierbare, leistungsstarke Blockspeicherressourcen, die mit Amazon Elastic Compute Cloud (Amazon EC2) -Instances verwendet werden können. Mit Amazon EBS können Sie die folgenden Blockspeicherressourcen erstellen und verwalten:

- Amazon EBS-Volumes — Dies sind Speichervolumes, die Sie Amazon EC2 EC2-Instances zuordnen. Nachdem Sie ein Volume an eine Instance angehängt haben, können Sie es genauso

verwenden wie Blockspeicher. Die Instance kann mit dem Volume genauso interagieren wie mit einem lokalen Laufwerk.

- Amazon EBS-Snapshots — Dies sind point-in-time Backups von Amazon EBS-Volumes, die unabhängig vom Volume selbst bestehen bleiben. Sie können Snapshots erstellen, um die Daten auf Ihren Amazon EBS-Volumes zu sichern. Sie können dann jederzeit neue Volumes aus diesen Snapshots wiederherstellen.

Sie können Amazon EBS-Volumes während des Starts erstellen und einer Instance zuordnen, und Sie können EBS-Volumes jederzeit nach dem Start erstellen und an eine Instance anhängen. Und Sie können jederzeit nach der Erstellung Snapshots von einem Volume erstellen.

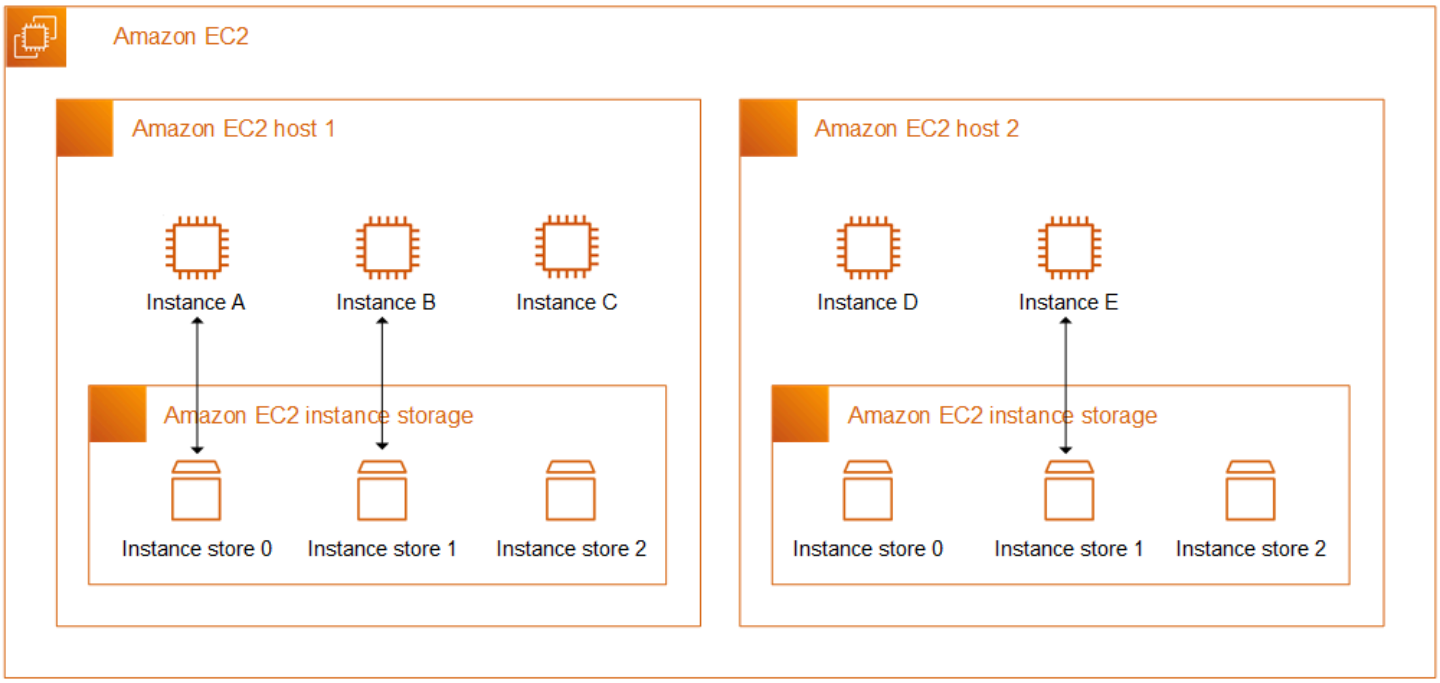
Weitere Informationen zur Arbeit mit Volumes und Snapshots finden Sie im Amazon EBS-Benutzerhandbuch.

Amazon EC2-Instance-Speicher

Ein Instance-Speicher stellt für Ihre Instance temporären Speicher auf Blockebene bereit. Dieser Speicher befindet sich auf Laufwerken, die physisch mit dem Host-Computer verbunden sind. Der Instance-Speicher ist ideal für die temporäre Speicherung von Informationen, die sich häufig ändern, wie Puffer, Caches, Arbeitsdaten und andere temporäre Inhalte. Es kann auch verwendet werden, um temporäre Daten zu speichern, die über eine Flotte von Instances, z. B. einen load balanced Pool von Webservern, repliziert werden.

Ein Instance-Speicher besteht aus einem oder mehreren Instance-Speicher-Volumes, die als Blockgeräte verfügbar gemacht werden. Die Größe eines Instance-Speichers sowie die Anzahl der verfügbaren Geräte variiert je nach Instance-Typ und Instance-Größe. Weitere Informationen finden Sie unter Instance-Speicher-Volumes.

Die virtuellen Geräte für Instance-Speicher-Volumes sind `ephemeral[0-23]`. Instance-Typen, die ein Instance-Speicher-Volume unterstützen, haben die Bezeichnung `ephemeral0`. Instance-Typen, die zwei oder mehr Instance-Speicher-Volumes unterstützen, haben die Bezeichnung `ephemeral0`, `ephemeral1` usw.



Preise für Instance-Speicher

Instance-Speicher-Volumes sind in den Nutzungskosten für die Instance enthalten.

Inhalt

Instance-Speicher-Volume und Lebensdauer der Daten

Anzahl, Größe und Typ der Instance-Speicher-Volumes werden durch den Instance-Typ und die Instance-Größe bestimmt. Weitere Informationen finden Sie unter Instance-Speicher-Volumes.

Instance-Speicher-Volumes werden nur beim Start der Instance angehängt. Sie können ein Instance-Speicher-Volume nicht an eine Instance anfügen, nachdem Sie sie gestartet haben. Sie können ein Instance-Speicher-Volume nicht von einer Instance trennen und an eine andere Instance anfügen.

Ein Instance-Speicher-Volume ist nur während der Lebensdauer der Instance, an die es angehängt ist, vorhanden. Sie können ein Instance-Speicher-Volume nicht so konfigurieren, dass es über die Nutzungsdauer der jeweiligen Instance hinaus erhalten bleibt.

Die Daten auf einem Instance-Speicher-Volume der Instance bleiben erhalten, wenn die Instance neu gestartet wird. Die Daten bleiben jedoch nicht erhalten, wenn die Instance angehalten, in den Ruhezustand versetzt oder beendet wird. Wenn die Instance angehalten, in den Ruhezustand versetzt oder beendet wird, jeder Block der Instance-Speicher-Volumes der Instance kryptografisch gelöscht.

Deshalb sollten Sie in einem Instance-Speicher keine wertvollen, langfristigen Daten ablegen. Wenn Sie die auf einem Instance-Speicher-Volume gespeicherten Daten über die Lebensdauer der Instance hinaus beibehalten müssen, müssen Sie diese Daten manuell in einen persistenteren Speicher kopieren, z. B. ein Amazon EBS-Volume, einen Amazon-S3-Bucket oder ein Amazon-EFS-Dateisystem.

Es gibt einige Ereignisse, die dazu führen können, dass Ihre Daten nicht während der gesamten Lebensdauer der Instance erhalten bleiben. Die folgende Tabelle gibt an, ob Daten auf Instance-Speicher-Volumes während bestimmter Ereignisse gespeichert werden, und zwar sowohl für virtualisierte als auch für Bare-Metal-Instances.

Ereignis	Was passiert mit Ihren Daten?
Vom Benutzer initiierte Instance-Lebenszyklusereignisse	
Die Instance wird neu gestartet	Die Daten bleiben bestehen
Die Instanz ist gestoppt	Die Daten bleiben nicht erhalten
Die Instanz befindet sich im Ruhezustand	Die Daten bleiben nicht erhalten
Die Instanz ist beendet	Die Daten bleiben nicht erhalten
Der Instanztyp wurde geändert	Die Daten bleiben nicht bestehen *
Aus der Instance wird ein EBS-gestütztes AMI erstellt	Die Daten bleiben nicht im erstellten AMI bestehen **

Ereignis	Was passiert mit Ihren Daten?
Aus der Instance wird ein durch den Instance-Speicher gestütztes AMI erstellt (Linux-Instances)	Die Daten verbleiben in dem auf Amazon S3 hochgeladenen AMI-Bundle ***
Vom Benutzer initiierte Betriebssystemereignisse	
Ein Shutdown wird eingeleitet	Die Daten bleiben nicht bestehen †
Ein Neustart wird eingeleitet	Die Daten bleiben bestehen
AWS geplante Ereignisse	
Stoppen der Instanz	Die Daten bleiben nicht erhalten
Neustart der Instanz	Die Daten bleiben bestehen
Systemneustart	Die Daten bleiben bestehen
Außerbetriebnahme der Instanz	Die Daten bleiben nicht erhalten
Ungeplante Ereignisse	
Vereinfachte automatische Wiederherstellung	Die Daten bleiben nicht erhalten
CloudWatch aktionsbasierte Wiederherstellung	Die Daten bleiben nicht erhalten
Die zugrunde liegende Festplatte fällt aus	Die Daten auf der ausgefallenen Festplatte bleiben nicht erhalten
Stromausfall	Die Daten bleiben beim Neustart erhalten

* Wenn der neue Instance-Typ Instance-Speicher unterstützt, erhält die Instance die Anzahl der Instance-Speicher-Volumes, die vom neuen Instance-Typ unterstützt werden, aber die Daten werden nicht auf die neue Instance übertragen. Wenn der neue Instance-Typ den Instance-Speicher nicht unterstützt, erhält die Instance die Instance-Speicher-Volumes nicht.

** Die Daten sind nicht im EBS-gestützten AMI enthalten und sie sind nicht in Instance-Speicher-Volumes enthalten, die an Instances angehängt sind, die von diesem AMI aus gestartet wurden.

*** Die Daten sind in dem AMI-Bündel enthalten, das auf Amazon S3 hochgeladen wird. Wenn Sie eine Instance von diesem AMI aus starten, erhält die Instance die im AMI gebündelten Instance-Speicher-Volumes mit den Daten, die sie zum Zeitpunkt der Erstellung des AMI enthielten.

† Der Terminierungsschutz und der Stoppschutz schützen Instances nicht vor Instancestopps oder -beendigungen als Folge von Shutdowns, die durch das Betriebssystem der Instance ausgelöst wurden. Daten, die auf Instance-Speicher-Volumes gespeichert sind, bleiben sowohl bei Stopp- als auch bei Terminierungsereignissen der Instance nicht erhalten.

Instance-Speicher-Volumes

Anzahl, Größe und Typ der Instance-Speicher-Volumes werden durch den Instance-Typ und die Instance-Größe bestimmt. Einige Instance-Typen wie M6, C6 und R6 unterstützen keine Instance-Speicher-Volumes, während andere Instance-Typen wie M5d, C6gd und R6gd Instance-Speicher-Volumes unterstützen. Sie können einer Instance nicht mehr Instance-Speicher-Volumes zuordnen, als von ihrem Instance-Typ unterstützt werden. Bei den Instance-Typen, die Instance-Speicher-Volumes unterstützen, variieren Anzahl und Größe der Instance-Speicher-Volumes je nach Instance-Größe. `m5d.large`Unterstützt beispielsweise 1 x 75 GB Instance-Speicher-Volume und `m5d.24xlarge` unterstützt 4 x 900 GB-Instance-Speicher-Volumes.

Bei Instance-Typen mit NVMe-Instance-Speicher-Volumes werden alle unterstützten Instance-Speicher-Volumes beim Start automatisch an die Instance angehängt. Bei Instance-Typen mit Nicht-NVMe-Instance-Speicher-Volumes, wie C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 und X1e, müssen Sie die Blockgerätezuordnungen für die Instance-Speicher-Volumes, die Sie beim Start anhängen möchten, manuell angeben. Nach dem Start der Instance müssen Sie dann die angehängten Instance-Speicher-Volumes formatieren und bereitstellen, bevor Sie sie verwenden können. Sie können ein Instance-Speicher-Volume nicht verfügbar machen, nachdem Sie die Instance gestartet haben.

Einige Instance-Typen verwenden NVMe- oder SATA-basierte SSDs, während andere SATA-basierte Festplatten-Volumes (HDD) verwenden. SSDs bieten eine hohe zufällige I/O-Leistung, wenn Sie Speicher mit sehr niedriger Latenz benötigen, die Daten aber nicht erhalten bleiben müssen, wenn die Instance beendet wird oder Sie fehlertolerante Architekturen nutzen können. Weitere Informationen finden Sie unter Instance-Speicher-Volumes auf SSD.

Die Daten auf der NVMe-Instance speichern Volumes und einige HDD-Instance-Speicher-Volumes werden im Ruhezustand verschlüsselt. Weitere Informationen finden Sie unter Datenschutz in Amazon EC2.

Verfügbare Instance-Speicher-Volumes

Der Amazon EC2 Instance Types Guide bietet Informationen zu Menge, Größe, Typ und Leistungsoptimierungen der Instance-Speicher-Volumes, die für jeden unterstützten Instance-Typ verfügbar sind. Weitere Informationen finden Sie hier:

- Spezifikationen des Instance-Speichers — Allgemeiner Zweck
- Spezifikationen des Instance-Speichers — Für Berechnungen optimiert
- Spezifikationen des Instance-Speichers — Speicheroptimiert
- Spezifikationen des Instance-Speichers — Speicheroptimiert
- Spezifikationen des Instance-Speichers — Beschleunigte Datenverarbeitung
- Spezifikationen des Instance-Speichers — Hochleistungsrechnen
- Spezifikationen des Instance-Speichers — vorherige Generation

Um Informationen zum Instance-Speicher mit dem abzurufen AWS CLI

Sie können den AWS CLI Befehl describe-instance-types verwenden, um Informationen zu einem Instance-Typ anzuzeigen, z. B. zu seinen Instance-Speicher-Volumes. Im folgenden Beispiel wird die Gesamtgröße des Instance-Speichers für alle R5-Instances mit Instance-Speicher-Volumes angezeigt.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5*" "Name=instance-storage-
supported,Values=true" \
    --query "InstanceTypes[].[InstanceType, InstanceStorageInfo.TotalSizeInGB]" \
    --output table
```

Beispielausgabe

```
---------------------------
|  DescribeInstanceTypes  |
+----------------+--------+
|  r5ad.24xlarge |  3600  |
|  r5ad.12xlarge |  1800  |
|  r5dn.8xlarge  |  1200  |
|  r5ad.8xlarge  |  1200  |
|  r5ad.large    |  75    |
|  r5d.4xlarge   |  600   |
```

```
   . . .
|  r5dn.2xlarge  |  300   |
|  r5d.12xlarge  |  1800  |
+----------------+--------+
```

Im folgenden Beispiel werden die vollständigen Instance-Speicherdetails für den angegebenen Instance-Typ angezeigt.

```
aws ec2 describe-instance-types \
    --filters "Name=instance-type,Values=r5d.4xlarge" \
    --query "InstanceTypes[].InstanceStorageInfo"
```

Die Beispielausgabe zeigt, dass dieser Instance-Typ über zwei 300 GB NVMe SSD-Volumes verfügt, für insgesamt 600 GB Instance-Speicher.

```
[
    {
        "TotalSizeInGB": 600,
        "Disks": [
            {
                "SizeInGB": 300,
                "Count": 2,
                "Type": "ssd"
            }
        ],
        "NvmeSupport": "required"
    }
]
```

Hinzufügen von Instance-Speicher-Volumes zu Ihrer EC2-Instance

Bei Instance-Typen mit NVMe-Instance-Speicher-Volumes werden alle unterstützten Instance-Speicher-Volumes beim Start automatisch an die Instance angehängt. NVMe-Instance-Speicher-Volumes werden automatisch aufgezählt und ihnen wird ein Gerätename zugeordnet.

Bei Instance-Typen mit Nicht-NVMe-Instance-Speicher-Volumes wie C1, C3, M1, M2, M3, R3, D2, H1, I2, X1 und X1e müssen Sie die Blockgerätezuordnungen für die Instance-Speicher-Volumes, die Sie beim Start anhängen möchten, manuell angeben. Blockgerätezuordnungen können in der Instance-Startanforderung oder in dem AMI, das zum Starten der Instance verwendet wird, angegeben werden. Jeder Eintrag in einer Blockgerät-Zuweisung beinhaltet einen gewählten

Namen und das Volume, dem er zugeordnet ist. Weitere Informationen finden Sie unter Blockgerät-Zuweisungen.

> **Important**
>
> Sie können Instance-Speicher-Volumes für eine Instance nur dann angeben, wenn Sie sie starten. Sie können ein Instance-Speicher-Volume nicht an eine Instance anfügen, nachdem Sie sie gestartet haben.

Nachdem Sie eine Instance gestartet haben, müssen Sie sicherstellen, dass die Instance-Speicher-Volumes für Ihre Instance formatiert und gemountet sind, bevor Sie sie verwenden. Das Root-Volume einer per Instance-Speicher gestützten Instance wird automatisch gemountet.

Berücksichtigung der Stamm-Volumes

Eine Blockgerät-Zuweisung gibt stets das Stamm-Volume für die Instance an. Das Root-Volume wird immer automatisch bereitgestellt.

Linux-Instances — Das Root-Volume ist entweder ein Amazon EBS-Volume oder ein Instance-Speicher-Volume. Bei Instances mit einem Instance-Speicher-Volume für das Stamm-Volume variiert die Größe dieses Volumes je nach AMI, aber die Maximalgröße ist 10 GB. Weitere Informationen finden Sie unter Speicher für das Root-Gerät.

Windows-Instances — Das Root-Volume muss ein Amazon EBS-Volume sein. Der Instance-Speicher wird für das Root-Volume nicht unterstützt.

Inhalt

Hinzufügen von Instance-Speicher-Volumes zu einem AMI

Sie können ein AMI mit einer Blockgerät-Zuweisung erstellen, die Instance-Speicher-Volumes enthält.

Wenn Sie eine Instance mit einem Instance-Typ starten, der non-NVMe-Instance-Speicher-Volumes unterstützt, und ein AMI, das Instance-Speicher-Volumes in seiner Blockgerät-Zuweisung

angibt, enthält die Instance diese Instance-Speicher-Volumes. Wenn die Anzahl der Instance-Speicher-Volumes in der Blockgerät-Zuweisung die für eine Instance verfügbare Anzahl an Instance-Speicher-Volumes übersteigt, werden die überzähligen Instance-Speicher-Volumes ignoriert.

Wenn Sie eine Instance mit einem Instance-Typ starten, der non-NVMe-Instance-Speicher-Volumes unterstützt, und ein AMI, das Instance-Speicher-Volumes in seiner Blockgerät-Zuweisung angibt, enthält die Instance diese Instance-Speicher-Volumes. Instances, die NVMe-Instance-Store-Volumes unterstützen, erhalten alle ihre unterstützten Instance-Speicher-Volumes, unabhängig von den Blockgerätezuordnungen, die in der Instance-Startanforderung und im AMI angegeben sind.

Überlegungen

- Bei M3-Instances spezifizieren Sie Instance-Speicher-Volumes in der Blockgerät-Zuweisung für die Instance angeben, nicht im AMI. Amazon EC2 ignoriert möglicherweise Instance-Speicher-Volumes, die nur in der Blockgerät-Zuweisung des AMI angegeben sind.
- Wenn Sie eine Instance starten, können Sie die in der AMI-Blockgerät-Zuweisung angegebenen Nicht-NVMe-Instance-Speicher-Volumes auslassen oder Instance-Speicher-Volumes hinzufügen.

New console

So fügen Sie Instance-Speicher-Volumes zu einem Amazon EBS-gestützten AMI mithilfe der Konsole hinzu

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Wählen Sie Actions (Aktionen), Image and templates (Image und Vorlagen), Create image (Image erstellen).
4. Fügen Sie im Dialogfeld Create image (Image erstellen) einen aussagekräftigen Namen und eine Beschreibung für Ihr Image hinzu.
5. Wählen Sie zum Hinzufügen jedes Instance-Speicher-Volumes Add volume (Volume hinzufügen), von Volume type (Volume-Typ) ein Instance-Speicher-Volume und aus Device (Gerät) einen Gerätenamen aus. (Weitere Informationen finden Sie unter Gerätenamen auf Amazon EC2 EC2-Instances.) Die Anzahl der verfügbaren Instance-Speicher-Volumes hängt vom Instance-Typ ab. Bei Instances mit NVMe-Instance-Speicher-Volumes hängt die Gerätezuweisung dieser Volumes von der Reihenfolge ab, in der das Betriebssystem die Volumes aufzählt.
6. Wählen Sie Create Image (Image erstellen) aus.

AWS CLI

So fügen Sie Instance-Speicher-Volumes zu einem AMI mithilfe der Befehlszeile hinzu

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- create-image oder register-image (AWS CLI)
- New-EC2Imageund Register-EC2Image(AWS Tools for Windows PowerShell)

Hinzufügen von Instance-Speicher-Volumes zu einer Instance

Wenn Sie eine Instance starten, die Non-NVMe-Instance-Speicher-Volumes unterstützt, müssen Sie Blockgerätezuordnungen für die anzuhängenden Instance-Speicher-Volumes angeben. Die Blockgerätezuordnungen müssen in der Instance-Startanforderung oder in dem AMI angegeben werden, mit dem die Instance gestartet wurde.

Wenn das AMI Blockgerätezuordnungen für die Instance-Speicher-Volumes enthält, müssen Sie Block-Gerätezuordnungen in der Instance-Startanforderung nicht angeben, es sei denn, Sie benötigen mehr Instance-Speicher-Volumes als im AMI enthalten sind.

Wenn das AMI keine Blockgerätezuordnungen enthält für Instance-Speicher-Volumes enthält, müssen Sie die Blockgerätezuordnungen in der Instance-Startanforderung angeben.

Überlegungen

- Bei M3-Instances erhalten Sie möglicherweise Instance-Speicher-Volumes auch dann, wenn Sie sie nicht in der Blockgerät-Zuweisung für die Instance angeben.

Verwenden Sie eine der folgenden Methoden, um Blockgerätezuordnungen in der Instancestartanforderung anzugeben.

Amazon EC2 console

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf dem Dashboard Launch Instance aus.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) das zu verwendende AMI aus.

4. Im Abschnitt Speicher konfigurieren werden unter dem Abschnitt Instance-Speicher-Volumes die Instance-Speicher-Volumes aufgeführt, die an die Instance angehängt werden können. Die Anzahl der verfügbaren Instance-Speicher-Volumes hängt vom Instance-Typ ab.
5. Wählen Sie für jedes anzufügende Instance-Speicher-Volume unter Gerätename den zu verwendenden Gerätenamen aus.
6. Konfigurieren Sie die übrigen Instance-Einstellungen nach Bedarf, und wählen Sie dann Instance starten.

Command line

Sie können einen der folgenden Befehle mit der entsprechenden Option verwenden.

- `--block-device-mappings` mit run-instances (AWS CLI)
- `-BlockDeviceMapping`mit New-EC2Instance(AWS Tools for Windows PowerShell)

Verfügbarmachen von Instance-Speicher-Volumes auf Ihrer Instance

Nachdem Sie eine Instance mit angefügten Instance-Speicher-Volumes gestartet haben, müssen Sie die Volumes mounten, bevor Sie auf sie zugreifen können.

> **Note**
>
> Viele Instance-Speicher-Volumes sind mit dem ext3-Dateisystem vorformatiert. SSD-basierte Instance-Speicher-Volumes, die TRIM-Befehle unterstützen, sind mit keinem Dateisystem vorformatiert. Sie können jedoch Volumes mit dem Dateisystem Ihrer Wahl formatieren, nachdem Sie Ihre Instance gestartet haben. Weitere Informationen finden Sie unter TRIM-Unterstützung für Instance-Speicher-Volumes. Bei Windows-Instances werden die Instance-Speicher-Volumes mit dem NTFS-Dateisystem neu formatiert.

Linux-Instances

Sie können die Instance-Speicher-Volumes wie im folgenden Verfahren beschrieben anzeigen und mounten.

So machen Sie ein Instance-Speicher-Volume unter Linux verfügbar

1. Stellen Sie eine Verbindung mit der Instance über einen SSH-Client her. Weitere Informationen finden Sie unter Herstellen einer Verbindung zur Linux-Instance.
2. Verwenden Sie den Befehl `df -h`, um die Volumes anzuzeigen, die formatiert und gemountet sind.

```
$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        3.8G   72K  3.8G   1% /dev
tmpfs           3.8G     0  3.8G   0% /dev/shm
/dev/nvme0n1p1  7.9G  1.2G  6.6G  15% /
```

3. Verwenden Sie den Befehl `lsblk`, um Volumes anzuzeigen, die beim Start zugeordnet, aber nicht formatiert und gemountet wurden.

```
$ lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
nvme0n1       259:1    0    8G  0 disk
##nvme0n1p1   259:2    0    8G  0 part /
##nvme0n1p128 259:3    0    1M  0 part
nvme1n1       259:0    0 69.9G  0 disk
```

4. Um ein Instance-Speicher-Volume zu formatieren und zu mounten, das nur zugeordnet wurde, gehen Sie folgendermaßen vor:

   a. Erstellen Sie mithilfe des Befehls `mkfs` ein Dateisystem auf dem Gerät.

   ```
   $ sudo mkfs -t xfs /dev/nvme1n1
   ```

   b. Erstellen Sie mithilfe des Befehls `mkdir` ein Verzeichnis, in dem das Gerät gemountet werden soll.

   ```
   $ sudo mkdir /data
   ```

   c. Mounten Sie mithilfe des Befehls `mount` das Gerät in dem neu erstellten Verzeichnis.

   ```
   $ sudo mount /dev/nvme1n1 /data
   ```

Windows-Instances

Sie können die Instance-Speicher-Volumes auch mithilfe der Windows-Datenträgerverwaltung anzeigen. Weitere Informationen finden Sie unter Auflisten von Festplatten mit Datenträgerverwaltung.

So mounten Sie ein Instance-Store-Volume manuell

1. Wählen Sie Start, wählen Sie Computer-Verwaltung und drücken Sie dann die Eingabetaste.
2. Wählen Sie im linken Bereich die Option Datenträgerverwaltung.
3. Wenn Sie aufgefordert werden, das Volume zu initialisieren, wählen Sie das zu initialisierende Volume aus, wählen Sie je nach Anwendungsfall den erforderlichen Partitionstyp aus, und wählen Sie dann OK aus.
4. Klicken Sie in der Liste der Volumes mit der rechten Maustaste auf das zu mountende Volume und wählen Sie dann Neues einfaches Volume.
5. Wählen Sie im Assistenten Weiter.
6. Wählen Sie im Bildschirm „Volume-Größe angeben“ die Option Weiter, um die maximale Volume-Größe zu verwenden. Alternativ können Sie eine Volume-Größe wählen, die zwischen dem minimalen und dem maximalen Speicherplatz liegt.
7. Führen Sie auf dem Bildschirm „Laufwerksbuchstabe oder Pfad zuweisen“ einen der folgenden Schritte aus und wählen Sie Weiter.

   - Um das Volume mit einem Laufwerksbuchstaben zu mounten, wählen Sie Den folgenden Laufwerksbuchstaben zuweisen und anschließend den zu verwendenden Laufwerksbuchstaben aus.
   - Um das Volume als Ordner bereitzustellen, wählen Sie Im folgenden leeren NTFS-Ordner mounten und anschließend Durchsuchen aus, um den zu verwendenden Ordner zu erstellen oder auszuwählen.
   - Wenn Sie das Volume ohne Laufwerksbuchstaben oder -pfad mounten möchten, wählen Sie Keinen Laufwerksbuchstaben oder Laufwerkspfad zuweisen.
8. Geben Sie im Fenster „Partition formatieren“ an, ob das Volume formatiert werden soll. Wenn Sie das Volume formatieren möchten, wählen Sie das erforderliche Dateisystem und die Einheitengröße aus und geben Sie eine Datenträgerbezeichnung an.
9. Wählen Sie Weiter, Fertigstellen.

Anweisungen zum automatischen Mounten eines angehängten Volumes nach dem Neustart finden Sie unter Automatisches Mounten eines angehängten Volumes nach dem Neustart im Amazon EBS-Benutzerhandbuch.

Instance-Speicher-Volumes auf SSD

Wie bei anderen Instance-Speicher-Volumes müssen Sie die SSD-Instance-Speicher-Volumes für Ihre Instance beim Start zuordnen. Die Daten auf einem SSD-Instance-Volume bleiben nur für die Dauer der zugehörigen Instance erhalten. Weitere Informationen finden Sie unter Hinzufügen von Instance-Speicher-Volumes zu Ihrer EC2-Instance.

NVMe-SSD-Volumes

Einige Instances stellen nicht flüchtige Memory Express (NVMe)-Solid State Drives (SSD)-Instance-Speicher-Volumes bereit. Weitere Informationen dazu, welcher Typ von Instance-Speicher-Volume von den einzelnen Instance-Typen jeweils unterstützt wird, finden Sie unter Instance-Speicher-Volumes.

Die Daten zum NVMe-Instance-Speicher sind mittels einer XTS-AES-256-Blockverschlüsselung verschlüsselt, die in einem Hardwaremodul auf der Instance implementiert ist. Die Verschlüsselungsschlüssel werden mithilfe des Hardwaremoduls erstellt und sind für jedes NVMe-Instance-Speichergerät eindeutig. Alle Verschlüsselungsschlüssel werden zerstört, wenn die Instance angehalten oder beendet wird, und können nicht wiederhergestellt werden. Sie können diese Verschlüsselung nicht deaktivieren und keine eigenen Verschlüsselungsschlüssel bereitstellen.

Linux-Instances

Für den Zugriff auf NVMe-Volumes müssen die NVMe-Treiber installiert sein. Die folgenden AMIs erfüllen diese Anforderung:

- AL2023
- Amazon Linux 2
- Amazon-Linux-AMI 2018.03 und höher
- Ubuntu 14.04 oder höher mit `linux-aws`-Kernel

> **Note**
>
> AWS Graviton-basierte Instance-Typen erfordern Ubuntu 18.04 oder höher mit Kernel `linux-aws`

- Red Hat Enterprise Linux 7.4 oder höher
- SUSE Linux Enterprise Server 12 SP2 oder höher
- CentOS 7.4.1708 oder höher
- FreeBSD 11.1 oder höher
- Debian GNU/Linux 9 oder höher

- Bottlerocket

Nachdem Sie die Verbindung mit Ihrer Instance hergestellt haben, können Sie die NVMe-Geräte mithilfe des Befehls lspci auflisten. Nachstehend finden Sie eine Beispiel-Ausgabe für eine `i3.8xlarge`-Instance, die vier NVMe-Geräte unterstützt.

```
[ec2-user ~]$ lspci
00:00.0 Host bridge: Intel Corporation 440FX - 82441FX PMC [Natoma] (rev 02)
00:01.0 ISA bridge: Intel Corporation 82371SB PIIX3 ISA [Natoma/Triton II]
00:01.1 IDE interface: Intel Corporation 82371SB PIIX3 IDE [Natoma/Triton II]
00:01.3 Bridge: Intel Corporation 82371AB/EB/MB PIIX4 ACPI (rev 01)
00:02.0 VGA compatible controller: Cirrus Logic GD 5446
00:03.0 Ethernet controller: Device 1d0f:ec20
00:17.0 Non-Volatile memory controller: Device 1d0f:cd01
00:18.0 Non-Volatile memory controller: Device 1d0f:cd01
00:19.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1a.0 Non-Volatile memory controller: Device 1d0f:cd01
00:1f.0 Unassigned class [ff80]: XenSource, Inc. Xen Platform Device (rev 01)
```

Wenn Sie ein unterstütztes Betriebssystem verwenden, aber die NVMe-Geräte nicht angezeigt werden, überprüfen Sie mit dem folgenden Befehl, ob das NVMe-Modul geladen ist.

- Amazon Linux, Amazon Linux 2, Ubuntu 14/16, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, CentOS 7

  ```
  $ lsmod | grep nvme
  nvme           48813  0
  ```

- Ubuntu 18

  ```
  $ cat /lib/modules/$(uname -r)/modules.builtin | grep nvme
  s/nvme/host/nvme-core.ko
  kernel/drivers/nvme/host/nvme.ko
  ```

```
kernel/drivers/nvmem/nvmem_core.ko
```

Die NVMe-Volumes erfüllen die Spezifikation NVMe 1.0a. Sie können die NVMe-Befehle bei Ihren NVMe-Volumes verwenden. In Amazon Linux können Sie das `nvme-cli`-Paket aus dem Repository mit dem Befehl yum install installieren. Bei anderen unterstützten Linux-Versionen können Sie das `nvme-cli`-Paket herunterladen, wenn es im Image nicht verfügbar ist.

Windows-Instances

Die neuesten AWS Windows-AMIs für die folgenden Betriebssysteme enthalten die AWS NVMe-Treiber, die für die Interaktion mit SSD-Instance-Speicher-Volumes verwendet werden, die für eine bessere Leistung als NVMe-Blockgeräte bereitgestellt werden:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

Nachdem Sie eine Verbindung mit Ihrer Instance hergestellt haben, können Sie überprüfen, ob die NVMe-Volumes in der Datenträgerverwaltung angezeigt werden. Öffnen Sie auf der Taskleiste das Kontextmenü (Rechtsklick) für das Windows-Logo und wählen Sie Datenträgerverwaltung.

Die von Amazon bereitgestellten AWS Windows-AMIs enthalten den AWS NVMe-Treiber. Wenn Sie nicht die neuesten AWS Windows-AMIs verwenden, können Sie den aktuellen AWS NVMe-Treiber installieren.

Nicht-NVMe-SSD-Volumes

Die folgenden Instances unterstützen Instance-Speicher-Volumes, die SSDs ohne NVMe verwenden, um eine hohe zufällige I/O-Leistung zu erzielen: C3, I2, M3, R3 und X1. Weitere Informationen zu den von den einzelnen Instance-Typen unterstützten Instance-Speicher-Volumes finden Sie unter Instance-Speicher-Volumes.

I/O-Leistung des SSD-basierten Instance-Speicher-Volumes

Die Anzahl der erreichten Schreib-IOPS nimmt in dem Maß ab, in dem Sie die SSD-basierten Instance-Speicher-Volumes für Ihre Instance mit Daten belegen. Der Grund dafür ist der zusätzliche Arbeitsaufwand für den SSD-Controller, der verfügbaren Speicherplatz suchen, vorhandene Daten

neu schreiben und ungenutzten Speicherplatz löschen muss, sodass er neu beschrieben werden kann. Dieser Prozess der Garbage Collection führt zu einer internen Write Amplification in der SSD; diese wird im Verhältnis der SSD-Schreibvorgänge zu den Benutzer-Schreibvorgängen ausgedrückt. Dieser Leistungsabfall ist sogar noch größer, wenn die Schreibvorgänge nicht in Vielfachen von 4 096 Byte durchgeführt oder nicht auf eine 4 096 Byte-Grenze ausgerichtet werden. Wenn eine kleinere Anzahl von Bytes oder nicht ausgerichtete Bytes geschrieben werden, muss der SSD-Controller die Daten in der Umgebung auslesen und an einem neuen Ort speichern. Dieses Muster führt zu einer erheblich größeren Write Amplification, einer höheren Latenz und zu dramatischen I/O-Leistungseinbußen.

SSD-Controller können verschiedenen Strategien anwenden, um die Auswirkungen der Write Amplification zu verringern. Eine dieser Strategien besteht darin, Speicherplatz des SSD-Instance-Speichers zu reservieren, sodass der Controller den für Schreibvorgänge verfügbaren Speicherplatz effizienter verwalten kann. Diese Methode wird als Overprovisioning (übermäßige Bereitstellung) bezeichnet. Die SSD-basierten Instance-Speicher-Volumes, die einer Instance zur Verfügung gestellt werden, haben keinen Speicherplatz, der für eine Überprovisionierung reserviert ist. Um die Schreibverstärkung zu reduzieren, empfehlen wir, 10 Prozent des Volumes unpartitioniert zu lassen, sodass der SSD-Controller es für Überprovisionierung verwenden kann. Dadurch steht zwar weniger Speicherplatz zur Verfügung, aber die Leistung wird verbessert – auch wenn der Datenträger fast vollständig belegt ist.

Speichern Sie beispielsweise Volumes, die TRIM unterstützen. Sie können den Befehl TRIM verwenden, um den SSD-Controller zu benachrichtigen, wenn Sie geschriebene Daten nicht mehr benötigen. Auf diese Weise hat der Controller mehr freien Speicherplatz zur Verfügung, wodurch die Write Amplification reduziert und die Leistung erhöht wird. Weitere Informationen finden Sie unter TRIM-Unterstützung für Instance-Speicher-Volumes.

TRIM-Unterstützung für Instance-Speicher-Volumes

Einige Instance-Typen unterstützen SSD-Volumes mit TRIM. Weitere Informationen finden Sie unter Instance-Speicher-Volumes.

> **Note**
>
> (Nur Windows-Instanzen) Instances, auf denen Windows Server 2012 R2 ausgeführt wird, unterstützen TRIM ab Version 7.3.0 des AWS PV-Treibers. Instances, die frühere Versionen von Windows Server ausführen, unterstützen TRIM nicht.

Instance-Speicher-Volumes, die TRIM unterstützen, werden vollständig gekürzt, bevor sie Ihrer Instance zugeordnet werden. Diese Volumes sind beim Start einer Instance nicht mit einem Dateisystem formatiert, deshalb müssen Sie sie formatieren, bevor sie gemountet und verwendet werden können. Um den Zugriff auf diese Volumes zu beschleunigen, sollten Sie die TRIM-Operation beim Formatieren überspringen.

(Windows-Instanzen) Verwenden Sie den `fsutil behavior set DisableDeleteNotify 1` Befehl, um die TRIM-Unterstützung während der ersten Formatierung vorübergehend zu deaktivieren. Nachdem die Formatierung abgeschlossen ist, aktivieren Sie die TRIM-Unterstützung erneut, indem Sie `fsutil behavior set DisableDeleteNotify 0`

Bei Instance-Speicher-Volumes, die TRIM unterstützen, können Sie den TRIM-Befehl dazu verwenden, dem SSD-Controller mitzuteilen, wann Sie Daten nicht mehr benötigen, die Sie geschrieben haben. Auf diese Weise hat der Controller mehr freien Speicherplatz zur Verfügung, wodurch die Write Amplification reduziert und die Leistung erhöht wird. Verwenden Sie auf Linux-Instances den `fstrim` Befehl, um das periodische TRIM zu aktivieren. Verwenden Sie auf Windows-Instances den `fsutil behavior set DisableDeleteNotify 0` Befehl, um sicherzustellen, dass die TRIM-Unterstützung während des normalen Betriebs aktiviert ist.

Instance speichert Swap-Volumes für Linux-Instances

> **Note**
>
> Dieses Thema bezieht sich nur auf Linux-Instances.

Unter Linux können Auslagerungsbereiche verwendet werden, wenn ein System mehr Speicherplatz benötigt, als ihm physisch zugeordnet ist. Wenn der Auslagerungsbereich aktiviert ist, können Linux-Systeme selten verwendete Speicherseiten aus dem physischen Speicher als Auslagerungsbereich kennzeichnen (entweder eine dedizierte Partition oder eine Auslagerungsdatei in einem bestehenden Dateisystem) und diesen Speicherplatz für Speicherseiten freigeben, die schnellen Zugriff benötigen.

> **Note**
>
> Die Verwendung des Auslagerungsbereichs für Speicherseiten ist nicht so schnell oder effizient wie die Verwendung von RAM. Wenn Ihre Workload regelmäßig Speicherplatz in den Auslagerungsbereich verschiebt, sollten Sie erwägen, zu einem größeren Instance-Typ

mit mehr RAM-Speicher zu migrieren. Weitere Informationen finden Sie unter Ändern des Instance-Typs.

Die Instance-Typen `c1.medium` und `m1.small` verfügen nur über eine begrenzte Menge an physischem Speicher und sind zum Startzeitpunkt mit einem Auslagerungsvolumen von 900 MiB ausgestattet, das als virtueller Speicher für Linux-AMIs fungiert. Obwohl der Linux-Kernel diesen Auslagerungsbereich als Partition auf dem Root-Gerät erkennt, ist er eigentlich ein separates Instance-Speicher-Volume, unabhängig vom Root-Gerätetyp.

Amazon Linux aktiviert und nutzt diesen Auslagerungsbereich automatisch, aber Ihr AMI benötigt möglicherweise einige zusätzliche Schritte, um diesen Bereich zu erkennen und zu nutzen. Verwenden Sie den Befehl swapon -s, um festzustellen, ob Ihre Instance den Auslagerungsbereich nutzt.

```
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

Bei der obigen Instance ist ein Swap-Volume mit 900 MiB angefügt und aktiviert. Wenn nach Eingabe dieses Befehls kein Swap-Volume angezeigt wird, müssen Sie möglicherweise den Auslagerungsbereich für das Gerät aktivieren. Überprüfen Sie Ihre verfügbaren Laufwerke mit dem lsblk-Befehl.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk
```

Hier ist das Swap-Volume `xvda3` für die Instance verfügbar, aber es ist nicht aktiviert (beachten Sie, dass das Feld `MOUNTPOINT` leer ist). Sie können das Swap-Volume mit dem Befehl swapon aktivieren.

> **Note**
>
> Sie müssen `/dev/` dem Gerätenamen voranstellen, der von lsblk aufgelistet wird. Möglicherweise hat Ihr Gerät eine andere Bezeichnung, beispielsweise `sda3`, `sde3` oder `xvde3`. Verwenden Sie im nachfolgenden Befehl den Gerätenamen für Ihr System.

```
[ec2-user ~]$ sudo swapon /dev/xvda3
```

Jetzt sollte der Auslagerungsbereich in der Ausgabe von lsblk und swapon -s angezeigt werden.

```
[ec2-user ~]$ lsblk
NAME  MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
xvda1 202:1    0    8G  0 disk /
xvda3 202:3    0  896M  0 disk [SWAP]
[ec2-user ~]$ swapon -s
Filename                                Type            Size    Used    Priority
/dev/xvda3                              partition       917500  0       -1
```

Sie müssen auch die Datei `/etc/fstab` bearbeiten, damit dieser Auslagerungsbereich bei jedem Starten des Systems automatisch aktiviert wird.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Hängen Sie die folgende Zeile an die Datei `/etc/fstab` an (und verwenden Sie dabei den Swap-Gerätenamen für Ihr System):

```
/dev/xvda3       none    swap    sw  0       0
```

So nutzen Sie ein Instance-Speicher-Volume als Auslagerungsbereich

Jedes Instance-Speicher-Volume kann als Auslagerungsbereich verwendet werden. Beispielsweise enthält der Instance-Typ `m3.medium` ein SSD-Instance-Speicher-Volume von 4 GB, das als Auslagerungsbereich geeignet ist. Wenn Ihr Instance-Speicher-Volume erheblich größer ist (z. B. 350 GB), können Sie das Volume in eine kleinere Auslagerungspartition von 4-8 GB und den Rest als Daten-Volume partitionieren.

> **Note**
>
> Dieses Verfahren kann nur bei Instance-Typen angewendet werden, die Instance-Speicher unterstützen. Eine Liste mit unterstützten Instance-Typen finden Sie unter Instance-Speicher-Volumes.

1. Auflisten der an Ihre Instance angefügten Blockgeräte, um den Gerätenamen für Ihr Instance-Speicher-Volume zu ermitteln.

```
[ec2-user ~]$ lsblk -p
NAME       MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
/dev/xvdb  202:16   0   4G  0 disk /media/ephemeral0
/dev/xvda1 202:1    0   8G  0 disk /
```

In diesem Beispiel ist das Instance-Speicher-Volume `/dev/xvdb`. Da dies eine Amazon Linux-Instance ist, wird das Instance-Speicher-Volume formatiert und auf `/media/ephemeral0` gemountet; nicht alle Linux-Betriebssysteme tun dies automatisch.

2. (Optional) Wenn Ihr Instance-Speicher-Volume gemountet ist (es wird ein `MOUNTPOINT` in der lsblk-Befehlsausgabe aufgeführt), müssen Sie mit dem folgenden Befehl das Mounting aufheben.

```
[ec2-user ~]$ sudo umount /dev/xvdb
```

3. Einrichten eines Linux-Auslagerungsbereichs auf dem Gerät mit dem Befehl mkswap.

```
[ec2-user ~]$ sudo mkswap /dev/xvdb
mkswap: /dev/xvdb: warning: wiping old ext3 signature.
Setting up swapspace version 1, size = 4188668 KiB
no label, UUID=b4f63d28-67ed-46f0-b5e5-6928319e620b
```

4. Aktivieren Sie den neuen Auslagerungsbereich.

```
[ec2-user ~]$ sudo swapon /dev/xvdb
```

5. Überprüfen Sie, ob der neue Auslagerungsbereich verwendet wird.

```
[ec2-user ~]$ swapon -s
Filename    Type  Size Used Priority
/dev/xvdb                               partition 4188668 0 -1
```

6. Bearbeiten Sie die Datei `/etc/fstab` so, dass dieser Auslagerungsbereich bei jedem Starten des Systems automatisch aktiviert wird.

```
[ec2-user ~]$ sudo vim /etc/fstab
```

Wenn Ihre `/etc/fstab`-Datei einen Eintrag für `/dev/xvdb` (oder `/dev/sdb`) hat, ändern Sie ihn so, dass er mit der unten stehenden Zeile übereinstimmt. Wenn die Datei keinen Eintrag für dieses Gerät hat, hängen Sie die folgende Zeile an Ihre `/etc/fstab`-Datei an (und verwenden Sie dabei den Swap-Gerätenamen für Ihr System):

```
/dev/xvdb       none    swap    sw  0       0
```

> **Important**
>
> Instance-Speicher-Volume-Daten gehen verloren, wenn eine Instance angehalten oder in den Ruhezustand versetzt wird. Dies beinhaltet auch die Formatierung des Instance-Speicher-Auslagerungsbereichs, der in Step 3 erstellt wurde. Wenn Sie eine Instance anhalten und erneut starten, die für die Verwendung eines Instance-Speicher-Auslagerungsbereichs konfiguriert wurde, müssen Sie Step 1 bis Step 5 auf dem neuen Instance-Speicher-Volume wiederholen.

Optimieren Sie die Festplattenleistung, um Volumes auf Linux-Instances zu speichern

> **Note**
>
> Dieses Thema bezieht sich nur auf Linux-Instanzen.

Wegen der Art, wie Amazon EC2 Laufwerke virtualisiert, erfolgt der erste Schreibvorgang zu einem Speicherort bei einigen Instance-Speicher-Volumes langsamer als die nachfolgenden Schreibvorgänge. Für die meisten Anwendungen ist die Amortisierung dieser Kosten während der Nutzungsdauer der Instances akzeptabel. Wenn Sie jedoch eine höhere Laufwerksleistung benötigen, empfehlen wir, dass Sie Ihre Laufwerke initialisieren, indem Sie vor dem Einsatz in der Produktion zu jedem Laufwerksspeicherort einen Schreibvorgang ausführen.

> **Note**
>
> Einige Instance-Typen mit direkt angefügten SSDs und TRIM-Unterstützung stellen ohne Initialisierung die maximale Leistung zum Startzeitpunkt bereit. Weitere Informationen über den Instance-Speicher für die einzelnen Instance-Typen finden Sie unter Instance-Speicher-Volumes.

Wenn Sie größere Flexibilität bei der Latenz oder dem Durchsatz benötigen, empfehlen wir die Verwendung von Amazon EBS.

Verwenden Sie zum Initialisieren von Instance-Speicher-Volumes die folgenden dd-Befehle, je nachdem, welchen Speicher Sie initialisieren wollen (beispielsweise `/dev/sdb` oder `/dev/nvme1n1`).

> **Note**
>
> Unmounten Sie das Laufwerk, bevor Sie diesen Befehl ausführen.
> Die Initialisierung kann lange dauern (ca. 8 Stunden bei einer sehr großen Instance).

Verwenden Sie zum Initialisieren der Instance-Speicher-Volumes die folgenden Befehle bei den Instance-Typen `m1.large`, `m1.xlarge`, `c1.xlarge`, `m2.xlarge`, `m2.2xlarge` und `m2.4xlarge`:

```
dd if=/dev/zero of=/dev/sdb bs=1M
dd if=/dev/zero of=/dev/sdc bs=1M
dd if=/dev/zero of=/dev/sdd bs=1M
dd if=/dev/zero of=/dev/sde bs=1M
```

Verwenden Sie zum gleichzeitigen Durchführen der Initialisierung bei allen Instance-Speicher-Volumes den folgenden Befehl:

```
dd if=/dev/zero bs=1M|tee /dev/sdb|tee /dev/sdc|tee /dev/sde > /dev/sdd
```

Beim Konfigurieren von Laufwerken für RAID werden diese initialisiert, indem ein Schreibvorgang zu jedem Laufwerksspeicherort durchgeführt wird. Ändern Sie beim Konfigurieren von softwarebasiertem RAID die minimale Rekonstruktionsgeschwindigkeit:

```
echo $((30*1024)) > /proc/sys/dev/raid/speed_limit_min
```

Dateispeicherung

Der Cloud-Datenspeicher ist eine Methode zur Speicherung von Daten in der Cloud, die Servern und Anwendungen den Zugriff auf Daten über gemeinsam genutzte Dateisysteme ermöglicht. Dank dieser Kompatibilität eignet sich der Cloud-Datenspeicher ideal für Workloads, die auf gemeinsam genutzten Dateisystemen basieren und ermöglicht zudem eine einfache Integration ohne Codeänderungen.

Es gibt viele Dateispeicherlösungen, angefangen von einem Dateiserver mit einem Knoten auf einer Recheninstanz, der Blockspeicher als Grundlage ohne Skalierbarkeit oder mit wenigen Redundanzen zum Schutz der Daten verwendet, über eine do-it-yourself Clusterlösung bis hin zu einer vollständig verwalteten Lösung. Im folgenden Inhalt werden einige der Speicherdienste vorgestellt, die von AWS zur Verwendung mit Amazon EC2 EC2-Instances bereitgestellt werden.

Inhalt

Verwenden von Amazon S3 mit Amazon EC2

Amazon Simple Storage Service (Amazon S3) ist ein Objektspeicherservice, der branchenführende Skalierbarkeit, Datenverfügbarkeit, Sicherheit und Leistung bietet. Sie können Amazon S3 verwenden, um beliebige Datenmengen für eine Reihe von Anwendungsfällen wie Data Lakes, Websites, Backups und Big-Data-Analysen von einer Amazon EC2 EC2-Instance oder von überall im Internet zu speichern und abzurufen. Weitere Informationen finden Sie unter Was ist Amazon S3?

Objekte sind die Grundeinheiten, die in Amazon S3 gespeichert sind. Jedes in Amazon S3 gespeicherte Objekt ist in einem Bucket enthalten. Buckets organisieren den Amazon S3-Namespace auf der höchsten Ebene und ermitteln das für die Speicherung verantwortliche Konto. Amazon-S3-Buckets sind ähnlich wie Internet-Domain-Namen. Die in den Buckets gespeicherten Objekte haben einen eindeutigen Schlüsselwert und werden über eine URL abgerufen. Wenn beispielsweise ein Objekt mit dem Schlüsselwert `/photos/mygarden.jpg` in dem Bucket `DOC-EXAMPLE-BUCKET1` gespeichert ist, kann es über die URL `https://DOC-EXAMPLE-BUCKET1.s3.amazonaws.com/photos/mygarden.jpg` abgerufen werden. Weitere Informationen finden Sie unter So funktioniert Amazon S3.

Verwendungsbeispiele

Wegen der Vorteile, die Amazon S3 bei der Speicherung hat, können Sie diesen Service zum Speichern von Dateien und Datensätzen zur Verwendung mit EC2-Instances nutzen. Es gibt verschiedene Möglichkeiten, Daten zu und von Amazon S3 zu Ihren Instances zu verschieben. Zusätzlich zu den unten dargestellten Beispielen gibt es eine Vielzahl von Tools, die von Developern verfasst wurden und die Sie dazu verwenden können, von Ihrem Computer oder Ihrer Instance auf

die in Amazon S3 gespeicherten Daten zuzugreifen. Einige der häufigsten Tools werden in den AWS -Foren diskutiert.

Wenn Sie eine entsprechende Berechtigung haben, können Sie mit einer der folgenden Methoden eine Datei zu oder von Amazon S3 und Ihrer Instance kopieren.

GET or wget (Linux)

> **Note**
>
> Diese Methode funktioniert nur für öffentliche Objekte. Wenn das Objekt nicht öffentlich ist, erhalten Sie die Meldung `ERROR 403: Forbidden`. Wenn Sie diesen Fehler erhalten, müssen Sie entweder die Amazon S3 S3-Konsole AWS CLI, AWS API, AWS SDK oder AWS Tools for Windows PowerShell, verwenden und Sie müssen über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter Identity and Access Management in Amazon S3 und Herunterladen eines Objekts im Amazon-S3-Benutzerhandbuch.

Das Dienstprogramm wget ist ein HTTP- und FTP-Client, der es ermöglicht, öffentliche Objekte von Amazon S3 herunterzuladen. Es ist standardmäßig in Amazon Linux und den meisten anderen Verteilungen installiert und bei Windows zum Download verfügbar. Verwenden Sie zum Herunterladen eines Amazon S3-Objekts den folgenden Befehl, wobei die URL des herunterzuladenden Objekts ersetzt wird.

```
[ec2-user ~]$ wget https://my_bucket.s3.amazonaws.com/path-to-file
```

AWS Tools for Windows PowerShell (Windows)

Windows-Instances haben den Vorteil eines grafischen Browsers, den Sie verwenden können, um auf die Amazon S3-Konsole direkt zuzugreifen. Zur Script-Erstellung können Windows-Benutzer jedoch auch AWS Tools for Windows PowerShell verwenden, um Objekte zu und von Amazon S3 zu verschieben.

Verwenden Sie den folgenden Befehl, um ein Amazon S3-Objekt in Ihre Windows-Instance zu kopieren.

```
PS C:\> Copy-S3Object -BucketName my_bucket -Key path-to-file -
LocalFile my_copied_file.ext
```

AWS CLI (Linux and Windows)

Das AWS Command Line Interface (AWS CLI) ist ein einheitliches Tool zur Verwaltung Ihrer AWS Services. Die AWS CLI erlaubt es Benutzern, sich zu authentifizieren und Elemente mit beschränktem Zugriff von Amazon S3 herunterzuladen sowie Elemente hochzuladen. Weitere Informationen, z. B. darüber, wie die Tools installiert und konfiguriert werden, finden Sie auf der AWS Command Line Interface -Detailseite.

Der Befehl aws s3 cp ähnelt dem Unix-Befehl cp. Sie können Dateien von Amazon S3 in Ihre Instance, von Ihrer Instance in Amazon S3 und von einem Amazon S3-Standort zu einem anderen kopieren.

Verwenden Sie den folgenden Befehl, um ein Objekt von Amazon S3 in Ihre Instance zu kopieren.

```
aws s3 cp s3://my_bucket/my_folder/my_file.ext my_copied_file.ext
```

Verwenden Sie den folgenden Befehl, um ein Objekt von Ihrer Instance zurück nach Amazon S3 zu kopieren.

```
aws s3 cp my_copied_file.ext s3://my_bucket/my_folder/my_file.ext
```

Mit dem Befehl aws s3 sync lässt sich ein ganzer Amazon S3-Bucket mit einem lokalen Verzeichnisspeicherort synchronisieren. Dies kann hilfreich sein, wenn Sie einen Datensatz herunterladen und die lokale Kopie up-to-date zusammen mit dem entfernten Datensatz behalten möchten. Wenn Sie die entsprechenden Berechtigungen für den Amazon S3-Bucket haben, können Sie Ihr lokales Verzeichnis nach Abschluss der Änderungen wieder in die Cloud verlagern, indem Sie in dem Befehl die Quell- und Zielspeicherorte vertauschen.

Verwenden Sie den folgenden Befehl, um einen ganzen Amazon S3-Bucket zu einem lokalen Verzeichnis auf Ihrer Instance herunterzuladen.

```
aws s3 sync s3://remote_S3_bucket local_directory
```

Amazon S3 API

Wenn Sie Developer sind, können Sie eine API zum Zugriff auf Daten in Amazon S3 verwenden. Sie können diese API verwenden, um Ihre Anwendung zu entwickeln und sie in andere APIs und SDKs zu integrieren. Weitere Informationen finden Sie unter Codebeispiele für Amazon S3 mit AWS SDKs im Amazon S3 S3-Benutzerhandbuch.

Verwenden Sie Amazon EFS mit Linux-Instances

> **Note**
>
> Amazon EFS wird von Windows-Instances nicht unterstützt.

Amazon EFS bietet skalierbaren Dateispeicher für die Verwendung mit Amazon EC2. Sie können ein EFS-Dateisystem als gemeinsame Datenquelle für Workloads und Anwendungen verwenden, die jeweils auf mehr als einer Instance ausgeführt werden. Weitere Informationen finden Sie auf der Amazon Elastic File System-Produktseite.

Dieses Tutorial zeigt Ihnen, wie Sie mit dem Amazon EFS Quick Create Wizard beim Instance-Start ein Amazon EFS-Dateisystem erstellen und anhängen. Ein Tutorial zum Erstellen eines Dateisystems mit der Amazon-EFS-Konsole finden Sie unter Erste Schritte mit Amazon Elastic File System im Benutzerhandbuch zu Amazon Elastic File System.

> **Note**
>
> Wenn Sie ein EFS-Dateisystem mit EFS-Quick-Create erstellen, wird das Dateisystem mit den folgenden vom Dienst empfohlenen Einstellungen erstellt:
>
> - Automatische Backups sind aktiviert.
> - Mounten Sie Ziele in jedem Standardsubnetz der ausgewählten VPC.
> - Leistungsmodus für allgemeine Zwecke.
> - Modus mit hohem Durchsatz.
> - Die Verschlüsselung von Daten im Ruhezustand wurde mit Ihrem Standardschlüssel für Amazon EFS (`aws/elasticfilesystem`) aktiviert.
> - Amazon EFS Lifecycle Management aktiviert mit einer 30-Tage-Richtlinie.

Aufgaben

- Erstellen eines EFS-Dateisystems mit Amazon EFS-Quick-Create
- Testen des EFS-Dateisystems
- Löschen des EFS-Dateisystems

Erstellen eines EFS-Dateisystems mit Amazon EFS-Quick-Create

Sie können ein EFS-Dateisystem erstellen und es in Ihrer Instance mounten, wenn Sie Ihre Instance mit dem Quick-Create-Feature von Amazon EFS des Launch Instance Wizard von Amazon EC2 starten.

Erstellen eines EFS-Dateisystems mit Amazon EFS-Quick-Create

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie Launch Instance (Instance starten) aus.
3. (Optional) Geben Sie unter Name and tags (Name und Tags) für Name einen Namen ein, um Ihre Instance zu identifizieren.
4. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) ein Linux-Betriebssystem und dann für Amazon Machine Image (AMI) ein Linux-AMI aus.
5. Wählen Sie unter Instance type (Instance-Typ) einen Instance type (Instance-Typ) aus oder behalten Sie die Standardeinstellung bei.
6. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
7. Wählen Sie unter Network settings (Netzwerkeinstellungen) Edit (Bearbeiten) (rechts) und dann für Subnet (Subnetz) ein Subnetz aus.

   > **Note**
   >
   > Sie müssen ein Subnetz auswählen, bevor Sie ein EFS-Dateisystem hinzufügen können.

8. Wählen Sie unter Configure storage (Speicher konfigurieren) die Option Edit (Bearbeiten) (unten rechts) und gehen Sie dann wie folgt vor:

   a. Stellen Sie für Dateisysteme sicher, dass EFS ausgewählt ist, und wählen Sie dann Neues gemeinsam genutztes Dateisystem erstellen aus.

   b. Geben Sie unter Dateisystemname einen Namen für das Amazon EFS-Dateisystem ein und wählen Sie dann Create file system.

   c. Geben Sie für Bereitstellungspunkt einen benutzerdefinierten Bereitstellungspunkt an, oder behalten Sie den Standardwert bei.

d. Um den Zugriff auf das Dateisystem zu ermöglichen, wählen Sie Automatically create and attach security groups (Sicherheitsgruppen automatisch erstellen und anfügen) aus. Wenn Sie dieses Kontrollkästchen aktivieren, werden die folgenden Sicherheitsgruppen automatisch erstellt und an die Instanz und die Mount-Ziele des Dateisystems angehängt:

   - Instanz-Sicherheitsgruppe — Beinhaltet eine ausgehende Regel, die Datenverkehr über den NFS 2049-Port zulässt, aber keine Regeln für eingehenden Datenverkehr enthält.
   - Sicherheitsgruppe für Mounting-Ziele für Dateisysteme – Enthält eine eingehende Regel, die den Datenverkehr über den NFS-2049-Port von der Instance-Sicherheitsgruppe (oben beschrieben) zulässt, und eine Regel für ausgehenden Datenverkehr über den NFS-2049-Port.

   > **Note**
   >
   > Alternativ können Sie die Sicherheitsgruppen manuell erstellen und anhängen. Wenn Sie die Sicherheitsgruppen manuell erstellen und anfügen möchten, deaktivieren Sie Automatically create and attach the required security groups (Erforderliche Sicherheitsgruppen automatisch erstellen und anfügen).

e. Um das gemeinsam genutzte Dateisystem beim Start der Instance automatisch zu mounten, wählen Sie Automatically mount shared file system by attaching required user data script (Gemeinsam genutztes Dateisystem automatisch mounten, indem Sie das erforderliche Benutzerdatenskript anfügen). Um die automatisch generierten Benutzerdaten anzuzeigen, erweitern Sie Advanced details (Erweiterte Details) und scrollen Sie nach unten zu User data (Benutzerdaten).

   > **Note**
   >
   > Wenn Sie Benutzerdaten hinzugefügt haben, bevor Sie dieses Kontrollkästchen aktiviert haben, werden die ursprünglichen Benutzerdaten durch die automatisch generierten Benutzerdaten überschrieben.

9. Konfigurieren Sie alle anderen Einstellungen der Instance-Konfiguration nach Bedarf.
10. Überprüfen Sie im Bereich Summary (Übersicht) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard.

Testen des EFS-Dateisystems

Sie können eine Verbindung zu Ihrer Instance herstellen und überprüfen, ob das Dateisystem in dem von Ihnen angegebenen Verzeichnis gemountet ist (z. B. /mnt/efs).

Überprüfen Sie wie folgt, ob das Dateisystem aufgespielt wurde:

1. Verbinden Sie sich mit der Instance. Weitere Informationen finden Sie unter Herstellen einer Verbindung zur Linux-Instance.
2. Führen Sie im Terminalfenster der Instance den df -T-Befehl aus, um zu überprüfen, ob das EFS-Dateisystem gemountet ist.

```
$ df -T
Filesystem     Type              1K-blocks    Used          Available Use% Mounted
 on
/dev/xvda1     ext4                8123812 1949800            6073764  25% /
devtmpfs       devtmpfs            4078468      56            4078412   1% /dev
tmpfs          tmpfs               4089312       0            4089312   0% /dev/shm
efs-dns        nfs4       9007199254740992       0   9007199254740992   0% /mnt/efs
```

   Beachten Sie, dass der Name des Dateisystems, der in der Beispielausgabe *efs-dns* lautet, das folgende Format aufweist.

```
file-system-id.efs.aws-region.amazonaws.com:/
```

3. (Optional) Erstellen Sie eine Datei im Dateisystem der Instance, und überprüfen Sie dann, ob Sie die Datei von einer anderen Instance aus anzeigen können.

   a. Führen Sie in der Instance den folgenden Befehl aus, um die Datei zu erstellen.

```
$ sudo touch /mnt/efs/test-file.txt
```

   b. Führen Sie in der anderen Instance den folgenden Befehl aus, um die Datei anzuzeigen.

```
$ ls /mnt/efs
test-file.txt
```

Löschen des EFS-Dateisystems

Sie können Ihren Dateisystem löschen, falls Sie ihn nicht mehr benötigen.

Löschen Sie das Dateisystem wie folgt:

1. Öffnen Sie die Amazon Elastic File System-Konsole unter https://console.aws.amazon.com/efs/.
2. Wählen Sie das Dateisystem aus, das Sie löschen möchten.
3. Wählen Sie Actions (Aktionen) und Delete file system (Dateisystem löschen) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie die Dateisystem-ID ein und wählen Sie Dateisystem löschen.

Verwenden von Amazon FSx mit Amazon EC2

Die Amazon-FSx-Servicefamilie erleichtert das Starten, Ausführen und Skalieren von freigegebenem Speicher, der auf gängigen kommerziellen und Open-Source-Dateisystemen basiert. Sie können den neuen Launch Instance Wizard verwenden, um beim Start automatisch die folgenden Arten von Amazon-FSx-Dateisystemen an Ihre Amazon-EC2-Instances anzufügen:

- Amazon FSx for NetApp ONTAP bietet vollständig verwalteten gemeinsamen Speicher in der AWS Cloud mit den beliebten Datenzugriffs- und Verwaltungsfunktionen von NetApp ONTAP.
- Amazon FSx for OpenZFS bietet vollständig verwalteten, kosteneffektiven freigegebenen Speicher, der auf dem beliebten OpenZFS-Dateisystem basiert.

> **Note**
>
> - Diese Funktionalität ist nur im neuen Launch Instance Wizard verfügbar. Weitere Informationen finden Sie unter Starten einer Instance mit dem neuen Launch Instance Wizard
> - Amazon-FSx-for-Windows-File-Server- und Amazon-FSx-for-Lustre-Dateisysteme können beim Start nicht bereitgestellt werden. Sie müssen diese Dateisysteme nach dem Start manuell bereitstellen.

Sie können ein vorhandenes Dateisystem bereitstellen, das Sie zuvor erstellt haben oder Sie können ein neues Dateisystem erstellen, das beim Start in einer Instance bereitgestellt werden soll.

Themen

Sicherheitsgruppen und Benutzerdatenskript

Wenn Sie ein Amazon-FSx-Dateisystem mithilfe des Launch Instance Wizard in einer Instance bereitstellen, können Sie wählen, ob die Sicherheitsgruppen, die zum Aktivieren des Zugriffs auf das Dateisystem erforderlich sind, automatisch erstellt und angefügt werden sollen, und ob die Benutzerdatenskripte, die benötigt werden, um das Dateisystem bereitzustellen und zur Nutzung verfügbar zu machen, automatisch eingeschlossen werden sollen.

Themen

Sicherheitsgruppen

Wenn Sie wählen, die Sicherheitsgruppen, die erforderlich sind, um den Zugriff auf das Dateisystem zu ermöglichen, automatisch zu erstellen, erstellt der Launch Instance Wizard zwei Sicherheitsgruppen und fügt sie an. Eine Sicherheitsgruppe wird an die Instance angefügt, die andere an das Dateisystem. Weitere Informationen zu den Anforderungen an Sicherheitsgruppen finden Sie unter Zugriffskontrolle für das FSx-for-ONTAP-Dateisystem mit Amazon VPC und Zugriffskontrolle für das FSx-for-OpenZFS-Dateisystem mit Amazon VPC.

Wir fügen das Tag `Name=instance-sg-`*`1`* der Sicherheitsgruppe hinzu, die erstellt und an die Instance angehängt wird. Der Wert im Tag wird jedes Mal, wenn der Launch Instance Wizard eine Sicherheitsgruppe für Amazon-FSx-Dateisysteme erstellt, automatisch erhöht.

Die Sicherheitsgruppe umfasst die folgenden Ausgaberegeln, jedoch keine Regeln für eingehenden Datenverkehr.

Regeln für ausgehenden Datenverkehr

Protokolltyp	Port-Nummer	Bestimmungsort
UDP	111	*`Dateisystem-Sicherheitsgruppe`*

Protokolltyp	Port-Nummer	Bestimmungsort
UDP	2001 — 2003	*Dateisystem-Sicherheitsgruppe*
UDP	4049	*Dateisystem-Sicherheitsgruppe*
UDP	2049	*Dateisystem-Sicherheitsgruppe*
UDP	635	*Dateisystem-Sicherheitsgruppe*
UDP	4045 - 4046	*Dateisystem-Sicherheitsgruppe*
TCP	4049	*Dateisystem-Sicherheitsgruppe*
TCP	635	*Dateisystem-Sicherheitsgruppe*
TCP	2049	*Dateisystem-Sicherheitsgruppe*
TCP	111	*Dateisystem-Sicherheitsgruppe*
TCP	4045 - 4046	*Dateisystem-Sicherheitsgruppe*
TCP	2001 - 2003	*Dateisystem-Sicherheitsgruppe*
Alle	Alle	*Dateisystem-Sicherheitsgruppe*

Die Sicherheitsgruppe, die erstellt und an das Dateisystem angehängt wird, ist mit `Name=fsx-sg-`*1* gekennzeichnet. Der Wert im Tag wird jedes Mal, wenn der Launch Instance Wizard zum Starten von Instance eine Sicherheitsgruppe für Amazon-FSx-Dateisysteme erstellt, automatisch erhöht.

Die Sicherheitsgruppe umfasst die folgenden Regeln.

Regeln für eingehenden Datenverkehr

Protokolltyp	Port-Nummer	Quelle
UDP	2049	*Instance-Sicherheitsgruppe*
UDP	2001 - 2003	*Instance-Sicherheitsgruppe*
UDP	4049	*Instance-Sicherheitsgruppe*

Protokolltyp	Port-Nummer	Quelle
UDP	111	*Instance-Sicherheitsgruppe*
UDP	635	*Instance-Sicherheitsgruppe*
UDP	4045 - 4046	*Instance-Sicherheitsgruppe*
TCP	4045 - 4046	*Instance-Sicherheitsgruppe*
TCP	635	*Instance-Sicherheitsgruppe*
TCP	2049	*Instance-Sicherheitsgruppe*
TCP	4049	*Instance-Sicherheitsgruppe*
TCP	2001 - 2003	*Instance-Sicherheitsgruppe*
TCP	111	*Instance-Sicherheitsgruppe*

Regeln für ausgehenden Datenverkehr

Protokolltyp	Port-Nummer	Bestimmungsort
Alle	Alle	0.0.0.0/0

Benutzerdatenskript

Wenn Sie wählen, Benutzerdatenskripte automatisch anzufügen, fügt der Launch Instance Wizard der Instance die folgenden Benutzerdaten hinzu. Dieses Skript installiert die erforderlichen Pakete, stellt das Dateisystem bereit und aktualisiert Ihre Instance-Einstellungen so, dass das Dateisystem bei jedem Neustart der Instance automatisch neu bereitgestellt wird.

```
#cloud-config
package_update: true
package_upgrade: true
runcmd:
- yum install -y nfs-utils
- apt-get -y install nfs-common
- svm_id_1=svm_id
```

```
- file_system_id_1=file_system_id
- vol_path_1=/vol1
- fsx_mount_point_1=/mnt/fsx/fs1
- mkdir -p "${fsx_mount_point_1}"
- if [ -z "$svm_id_1" ]; then printf "\n${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev
 0 0\n" >> /etc/fstab; else printf "\n${svm_id_1}.${file_system_id_1}.fsx.eu-
north-1.amazonaws.com:/${vol_path_1} ${fsx_mount_point_1} nfs4
 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,_netdev 0
 0\n" >> /etc/fstab; fi
- retryCnt=15; waitTime=30; while true; do mount -a -t nfs4 defaults; if [ $? = 0 ] ||
 [ $retryCnt -lt 1 ]; then echo File system mounted successfully; break; fi; echo File
 system not available, retrying to mount.; ((retryCnt--)); sleep $waitTime; done;
```

Bereitstellen eines Amazon-FSx-Dateisystems beim Start

Neues oder vorhandenes Amazon-FSx-Dateisystem beim Start bereitstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann Instance starten, um den Launch Instance Wizard zu öffnen.
3. Wählen Sie im Bereich Application and OS Images (Anwendungs- und Betriebssystem-Images) das zu verwendende AMI aus.
4. Wählen Sie im Bereich Instance type (Instance-Typ) den Instance-Typ aus.
5. Wählen Sie im Bereich Key pair (Schlüsselpaar) ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
6. Gehen Sie im Bereich Network settings (Netzwerkeinstellungen) wie folgt vor:

    a. Wählen Sie Bearbeiten aus.

    b. Wenn Sie ein vorhandenes Dateisystem bereitstellen möchten, wählen Sie bei Subnet (Subnetz) das bevorzugte Subnetz des Dateisystems aus. Wir empfehlen, die Instance in derselben Availability Zone zu starten wie das bevorzugte Subnetz des Dateisystems, um die Leistung zu optimieren.

    Wenn Sie ein neues Dateisystem erstellen möchten, um eine Instance zu bereitzustellen, wählen Sie bei Subnet (Subnetz) das Subnetz aus, in dem die Instance gestartet werden soll.

> **Important**
>
> Sie müssen ein Subnetz auswählen, um die Amazon-FSx-Funktionalität im neuen Launch Instance Wizard zu aktivieren. Wenn Sie kein Subnetz auswählen, können Sie kein vorhandenes Dateisystem bereitstellen oder ein neues erstellen.

7. Gehen Sie im Abschnitt Storage (Speicher) wie folgt vor:

   a. Konfigurieren Sie die Volumes nach Bedarf.

   b. Erweitern Sie den Bereich File systems (Dateisysteme) und wählen Sie FSx aus.

   c. Wählen Sie Add shared file system (Freigegebenes Dateisystem hinzufügen) aus.

   d. Wählen Sie bei File system (Dateisystem) das Dateisystem aus, das bereitgestellt werden soll.

   > **Note**
   >
   > In der Liste werden alle Amazon FSx for NetApp ONTAP- und Amazon FSx for OpenZFS-Dateisysteme in Ihrem Konto in der ausgewählten Region angezeigt.

   e. Um die Sicherheitsgruppen, die zum Aktivieren des Zugriffs auf das Dateisystem erforderlich sind, automatisch zu erstellen und anzufügen, wählen Sie Automatically create and attach security groups (Sicherheitsgruppen automatisch erstellen und anfügen) aus. Wenn Sie die Sicherheitsgruppen lieber manuell erstellen möchten, deaktivieren Sie das Kontrollkästchen. Weitere Informationen finden Sie unter Sicherheitsgruppen.

   f. Um die Benutzerdatenskripte, die zum Bereitstellen des Dateisystems erforderlich sind, automatisch anzufügen, wählen Sie Automatically mount shared file system by attaching required user data script (Freigegebenes Dateisystem automatisch bereitstellen, indem erforderliches Benutzerdatenskript angefügt wird) aus. Wenn Sie die Benutzerdatenskripte lieber manuell angeben möchten, deaktivieren Sie das Kontrollkästchen. Weitere Informationen finden Sie unter Benutzerdatenskript.

8. Konfigurieren Sie im Bereich Advanced (Erweitert) die weiteren Instance-Einstellungen nach Bedarf.

9. Wählen Sie Launch (Starten) aus.

Amazon File Cache mit Amazon EC2 verwenden

Amazon File Cache ist ein vollständig verwalteter Hochgeschwindigkeits-Cache, der zur Verarbeitung von Dateidaten verwendet wird, unabhängig davon, wo die Daten gespeichert sind. AWS Amazon File Cache dient als temporärer Hochleistungsspeicherort für Daten, die in lokalen Dateisystemen, AWS Dateisystemen und Amazon Simple Storage Service (Amazon S3) -Buckets gespeichert sind. Sie können diese Funktion nutzen, um verteilte Datensätze für dateibasierte Anwendungen in einer einheitlichen Ansicht und AWS mit hohen Geschwindigkeiten — Latenzen unter einer Millisekunde und hohem Durchsatz — verfügbar zu machen. Weitere Informationen finden Sie unter Was ist Amazon File Cache? .

Sie können von Ihren Amazon EC2 EC2-Instances aus mit dem Open-Source-Lustre-Client auf Ihren Cache zugreifen. Amazon EC2 EC2-Instances können von anderen Availability Zones innerhalb derselben Amazon Virtual Private Cloud (Amazon VPC) aus auf Ihren Cache zugreifen, sofern Ihr Netzwerk den Zugriff über Subnetze innerhalb der VPC ermöglicht. Nachdem Ihr Cache bereitgestellt wurde, können Sie mit seinen Dateien und Verzeichnissen wie mit einem lokalen Dateisystem arbeiten.

Informationen zu den ersten Schritten finden Sie unter Erste Schritte mit Amazon File Cache.

Volume-Limits für Instances

Die maximale Anzahl von Amazon-EBS-Volumes, die Sie einer Instance anfügen können, hängt vom Instance-Typ und der Instance-Größe ab. Bei der Überlegung, wie viele Volumes an Ihre Instance angefügt werden sollen, sollten Sie berücksichtigen, ob Sie eine höhere E/A-Bandbreite oder eine größere Speicherung benötigen.

Bandbreite vs. Kapazität

Verwenden Sie Amazon EBS-optimierte Instances mit Allzweck-SSD-Volumes oder bereitgestellten IOPS-SSD-Volumes für konsistente und vorhersehbare Bandbreitenanwendungen. Für maximale Leistung passen Sie die IOPS, die Sie für Ihre Volumes bereitgestellt haben, an die für Ihren Instance-Typ verfügbare Bandbreite an.

Bei RAID-Konfigurationen stellen Sie möglicherweise fest, dass Arrays mit mehr als 8 Volumes aufgrund des erhöhten E/A-Aufwands zu einem Leistungsabfall führen. Testen Sie die Leistung der einzelnen Anwendungen und nehmen Sie entsprechende Abstimmungen vor.

Themen

Volume-Limits für Instances, die auf dem Nitro-System basieren

Themen

Dediziertes Amazon-EBS-Volume-Limit

Die folgenden Nitro-Instance-Typen haben ein spezielles Amazon EBS-Volumenlimit, das je nach Instance-Größe variiert. Das Limit wird nicht mit anderen Geräteanhängen geteilt. Mit anderen Worten: Sie können eine beliebige Anzahl von Amazon-EBS-Volumes bis zum Volume-Anhangslimit anfügen, unabhängig von der Anzahl der angeschlossenen Geräte, wie z. B. NVMe-Instance-Speicher-Volumes und Netzwerkschnittstellen.

- Allgemeiner Zweck: M7a, M7i, M7i-Flex
- Für Datenverarbeitung optimiert: C7a, C7i
- Arbeitsspeicheroptimiert: R7a, R7i, R7iz

Bei diesen Instance-Typen, die dedizierte Volumenbegrenzungen unterstützen, hängen die Volumenlimits von der Instance-Größe ab. Die folgende Tabelle zeigt den Grenzwert für jede Instance-Größe.

Instance-Größe	Volume-Limit
`medium` | `large` | `xlarge` | `2xlarge` | `4xlarge` | `8xlarge` | `12xlarge`	32
`16xlarge`	48
`24xlarge`	64
`32xlarge`	88

Instance-Größe	Volume-Limit
48xlarge	128
metal-16xl | metal-24xl	39
metal-32xl | metal-48xl	79

Gemeinsames Amazon-EBS-Volume-Limit

Alle anderen Nitro-Instance-Typen (nicht aufgeführt unterDediziertes Amazon-EBS-Volume-Limit) haben ein Limit für Volumenanhänge, das von Amazon EBS-Volumes, Netzwerkschnittstellen und NVMe-Instance-Speicher-Volumes gemeinsam genutzt wird. Sie können bis zu diesem Limit eine beliebige Anzahl von Amazon-EBS-Volumes anfügen, abzüglich der Anzahl der angeschlossenen Netzwerkschnittstellen und NVMe-Instance-Speicher-Volumes. Denken Sie daran, dass jede Instance über mindestens eine Benutzeroberfläche verfügen muss und dass NVMe-Instance-Speicher automatisch beim Start angefügt werden.

Die meisten dieser Instances unterstützen maximal 28 Anhänge. Wenn Sie beispielsweise keine zusätzlichen Netzwerkschnittstellen an einer `m5.xlarge`-Instance anfügen, können Sie bis zu 27 EBS-Volumes anfügen (28 Volume-Limit – 1 Netzwerkschnittstelle). Wenn Sie über zwei zusätzliche Netzwerkschnittstellen auf einer `m5.xlarge`-Instance verfügen, können Sie bis zu 25 EBS-Volumes anfügen (28 Volume-Limit – 3 Netzwerkschnittstellen). Wenn Sie über zwei zusätzliche Benutzeroberflächen auf einer `m5d.xlarge`-Instance haben, die über 1 NVMe-Instance-Speicher-Volume verfügt, können Sie ebenfalls bis zu 24 EBS-Volumes anfügen (28 Volume-Limit – 3 Netzwerkschnittstellen – 1 NVMe-Instance-Speicher-Volume).

Die folgenden Ausnahmen für Instance-Typen mit gemeinsamen Volumenlimits:

- DL2q-Instances unterstützen maximal 19 EBS-Volumes.
- Die meisten Bare-Metal-Instances unterstützen maximal 31 EBS-Volumes.
- Virtualisierte Instances mit hoher Speicherkapazität unterstützen maximal 27 EBS-Volumes.
- Die Bare-Metal-Instances mit hoher Speicherkapazität unterstützen maximal 19 EBS-Volumes.
- `inf1.xlarge`- und `inf1.2xlarge`-Instances unterstützen maximal 26 EBS-Volumes.
- `inf1.6xlarge`-Instances unterstützen maximal 23 EBS-Volumes.

- `mac1.metal`-Instances unterstützen maximal 16 EBS-Volumes.
- `mac2.metalmac2-m2.metal`, und `mac2-m2pro.metal` Instances unterstützen maximal 10 EBS-Volumes.
- `inf1.24xlarge`-Instances unterstützen maximal 11 EBS-Volumes.
- `g5.48xlarge`-Instances unterstützen maximal 9 EBS-Volumes.
- `d3.8xlarge`- und `d3en.12xlarge`-Instances unterstützen maximal 3 EBS-Volumes.
- Bei beschleunigten Rechen-Instances werden die angefügten Beschleuniger auf das Limit für das gemeinsame genutzte Volume angerechnet. Bei `p4d.24xlarge`-Instances mit einem Limit von 28 gemeinsamen Volumes, 8 GPUs und 8 NVMe-Instance-Speicher-Volumes können Sie beispielsweise bis zu 11 Amazon-EBS-Volumes anfügen (Limit von 28 Volumes – 1 Netzwerkschnittstelle – 8 GPUs – 8 NVMe-Instance-Speicher-Volumes).

Volume-Limits für Xen-basierte Instances

Linux-Instances

Das Anfügen von mehr als 40 Volumes an eine Xen-basierte Linux-Instance kann zu Startfehlern führen. Diese Zahl umfasst das Root-Volume sowie alle angefügten Instance-Speicher-Volumes und Amazon-EBS-Volumes.

Wenn bei einer Instance mit einer großen Anzahl von Volumes Startprobleme auftreten, beenden Sie die Instance, trennen Sie alle Volumes, die für den Startvorgang nicht unbedingt erforderlich sind, starten Sie die Instance und fügen Sie die Volumes nach der Ausführung der Instance wieder an.

> **Important**
>
> Das Anfügen von mehr als 40 Volumes an eine Xen-basierte Linux-Instance wird nur nach bestem Bemühen unterstützt und kann nicht garantiert werden.

Windows-Instances

Die folgende Tabelle zeigt die Volume-Limits für Xen-basierte Windows-Instances basierend auf dem verwendeten Treiber. Diese Zahlen beinhalten das Root-Volume sowie alle angefügten Instance-Speicher-Volumes und Amazon-EBS-Volumes.

> **Important**
>
> Das Anfügen von mehr als der folgenden Anzahl von Volumes an eine Xen-basierte Windows-Instance wird nur nach bestem Bemühen unterstützt und kann nicht garantiert werden.

Treiber	Volume-Limit
AWS PV	26
Citrix PV	26
Red Hat PV	17

Wir empfehlen, nicht mehr als 26 Volumes an eine Xen-basierte Windows-Instanz mit AWS PV- oder Citrix PV-Treibern anzuhängen, da dies zu Leistungsproblemen führen kann. Informationen zur Ermittlung der PV-Treiber, die Ihre Instance verwendet, oder zum Upgrade Ihrer Windows-Instance von Red-Hat- auf Citrix-PV-Treiber finden Sie unter the section called “Upgrade für PV-Treiber”.

Weitere Informationen darüber, wie Gerätenamen mit Volumes verbunden sind, finden Sie unter Zuweisen von Datenträgern zu Volumes in Ihrer Windows-Instance.

Root-Volume der Amazon-EC2-Instance

Beim Starten einer Instance erstellen wir ein Root-Volume für die Instance. Beim Starten einer Instance enthält das Root-Volume das Image, das zum Starten der Instance verwendet wird. Jede Instance hat ein einzelnes Root-Volume. Sie können Ihren Instances während oder nach dem Start Speichervolumes hinzufügen.

Wir behalten uns bestimmte Gerätenamen für Root-Volumes vor. Weitere Informationen finden Sie unter Gerätenamen auf Amazon EC2 EC2-Instances.

Inhalt

- Ermitteln Sie den Root-Gerätetyp Ihrer Linux-Instance
- Ändern des beizubehaltenden Root-Volumes
- Ändern der Anfangsgröße des Root-Volumes
- Ersetzen Sie ein EC2-Instance-Root-Volume

Root-Volume-Typ

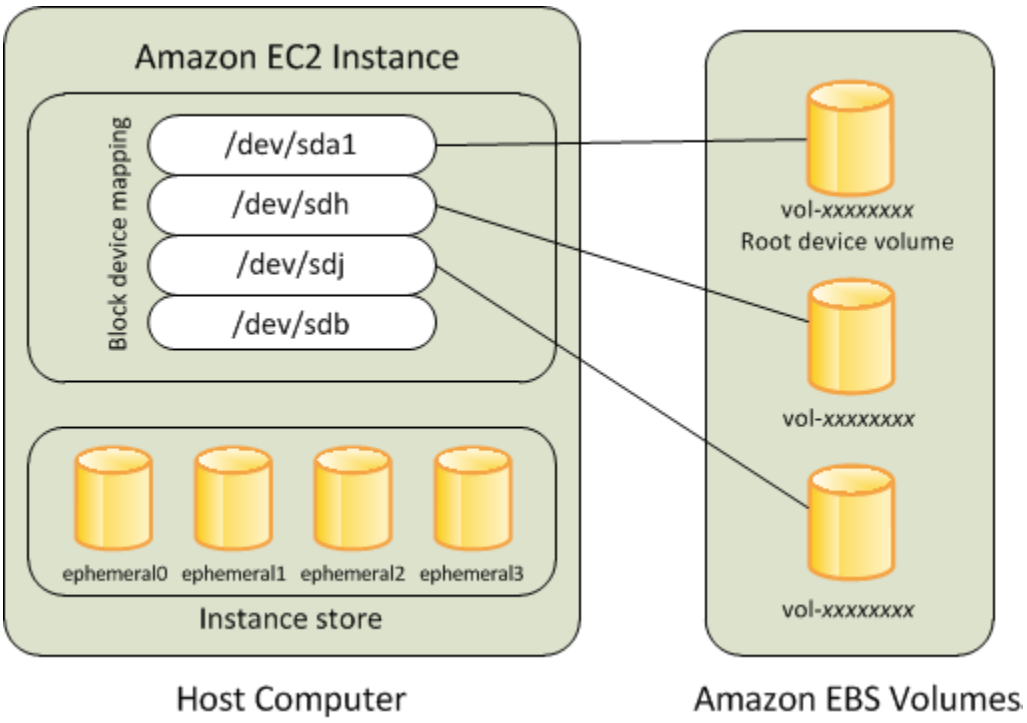
Das AMI, das Sie zum Starten einer Instance verwenden, bestimmt den Typ des Root-Volumes. Sie können eine Instance entweder von einem Amazon EBS-backed AMI (Linux- und Windows-Instances) oder einem instance store-backed AMI (nur Linux-Instances) aus starten. Es gibt erhebliche Unterschiede zwischen dem, was Sie mit den einzelnen AMI-Typen tun können. Weitere Informationen zu diesen Unterschieden erhalten Sie unter Speicher für das Root-Gerät.

Wir empfehlen Ihnen die Verwendung von Amazon EBS-gestützten AMIs, da diese Instances schneller gestartet werden und persistenten Speicher nutzen.

Amazon EBS-gestützte Instances

An Instances, die Amazon EBS für das Root-Volume verwenden, wird automatisch ein Amazon EBS-Volume angefügt. Wenn Sie eine Amazon EBS-gestützte Instance starten, erstellen wir ein Amazon EBS-Volume für jeden Amazon EBS-Snapshot, auf den von Ihrem AMI verwiesen wird. Optional können Sie je nach Instance-Typ weitere Amazon EBS-Volumes oder Instance-Speicher-Volumes nutzen.

Eine Amazon EBS-gestützte Instance kann angehalten und später neu gestartet werden, ohne dass sich dies auf die Daten auswirkt, die in den angefügten Volumes gespeichert sind. Sie können verschiedene Aufgaben für Instances und Volumes ausführen, wenn sich eine Amazon EBS-gestützte Instance im angehaltenen Zustand befindet. Sie können beispielsweise die Eigenschaften der Instance ändern, ihre Größe ändern oder den verwendeten Kernel aktualisieren oder Sie können Ihr Root-Volume an eine andere laufende Instance zum Debuggen oder zu einem anderen Zweck anhängen. Weitere Informationen finden Sie unter Amazon EBS-Volumes.



Einschränkung

Sie können `st1`- oder `sc1`-EBS-Volumes nicht als Root-Volumes verwenden.

Instance-Ausfall

Wenn eine Amazon EBS-gestützte Instance ausfällt, können Sie Ihre Sitzung mit einer der folgenden Methoden wiederherstellen:

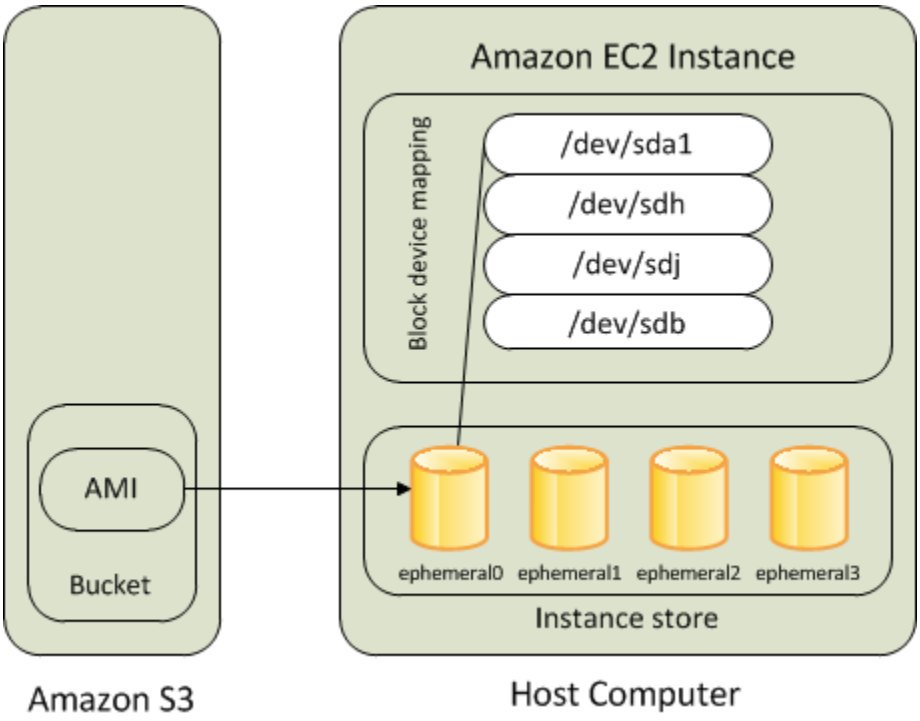
- Führen Sie das Anhalten und anschließend das erneute Starten durch. (Probieren Sie es zuerst mit dieser Methode.)
- Erstellen Sie einen automatischen Snapshot aller relevanten Volumes und erstellen Sie ein neues AMI. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.
- Fügen Sie das Volume an die neue Instance an, indem Sie die folgenden Schritte ausführen:
  1. Erstellen Sie einen Snapshot des Stamm-Volumes.
  2. Registrieren Sie ein neues AMI, indem Sie den Snapshot verwenden.
  3. Starten Sie über das neue AMI eine neue Instance.
  4. Trennen Sie die restlichen Amazon EBS-Volumes von der alten Instance.
  5. Fügen Sie die Amazon EBS-Volumes wieder an die neue Instance an.

Instances, die im Instance-Speicher unterstützt werden (nur Linux-Instances)

> **Note**
>
> Windows-Instances unterstützen keine Root-Volumes, die durch Instance-Speicher gesichert werden.

Instances, für die Instance-Speicher für das Root-Volume genutzt werden, verfügen automatisch über mindestens ein Instance-Speicher-Volume, wobei ein Volume als Root-Volume dient. Wenn eine Instance gestartet wird, wird das Image, das zum Starten der Instance verwendet wird, auf das Stamm-Volume kopiert. Beachten Sie, dass sie je nach Instance-Typ optional weitere Instance-Speicher-Volumes nutzen können.

Alle Daten auf den Instance-Speicher-Volumes werden so lange beibehalten, wie die Instance ausgeführt wird. Sie werden dann gelöscht, wenn die Instance beendet wird (für per Instance Store-Backed Instances wird die Aktion Stop (Stoppen) nicht unterstützt) oder ausfällt (bei Problemen auf einem zugrunde liegenden Laufwerk). Weitere Informationen finden Sie unter Amazon EC2-Instance-Speicher.



Anforderung

Nur die folgenden Instance-Typen unterstützen ein Instance-Speicher-Volume als Root-Volume: C3, D2, I2, M3 und R3.

Instance-Ausfall

Wenn eine per Instance-Speicher gestützte Instance ausfällt oder beendet wird, kann sie nicht wiederhergestellt werden. Wenn Sie planen, per Amazon EC2-Instance-Speicher gestützte Instances zu verwenden, empfehlen wir Ihnen dringend, die Daten auf Ihren Instance-Speichern auf mehrere Availability Zones zu verteilen. Außerdem sollten Sie regelmäßig kritische Daten von Ihren Instance-Speicher-Volumes auf persistenten Speicher sichern.

Wählen Sie ein Linux-AMI nach Root-Volume-Typ

> **Note**
>
> Alle Windows-AMIs werden von EBS unterstützt.

Anhand des AMI, das Sie beim Starten Ihrer Instance angeben, wird der Typ des Root-Gerät-Volumes Ihrer Instance ermittelt. Sie können AMIs nach Root-Gerätetyp mit einer der folgenden Methoden anzeigen.

Console

So wählen Sie mit der Konsole ein Amazon EBS-gestütztes AMI aus

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie in den Filterlisten den Image-Typ aus (z. B. Public images (Öffentliche Images)). Wählen Sie in der Suchleiste Plattform, um das Betriebssystem (z. B. Amazon Linux) auszuwählen, und Root-Gerätetyp, um den Root-Volume-Typ (ebs oder instance-store) auszuwählen.
4. (Optional) Zusätzliche Informationen zum Treffen der Auswahl erhalten Sie, indem Sie das Symbol Einstellungen auswählen, die anzuzeigenden Spalten einschalten und Schließen auswählen.
5. Wählen Sie ein AMI aus und notieren Sie sich die AMI-ID.

AWS CLI

So überprüfen Sie den Typ des Root-Gerät-Volumes eines AMI über die Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-images (AWS CLI)
- Get-EC2Image (AWS Tools for Windows PowerShell)

Ermitteln Sie den Root-Gerätetyp Ihrer Linux-Instance

> **Note**
>
> Alle Windows-Instances werden von EBS unterstützt.

Sie können den Root-Gerätetyp Ihrer Linux-Instance mit einer der folgenden Methoden anzeigen.

Console

So ermitteln Sie den Root-Gerätetyp einer Instance mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Überprüfen Sie auf der Registerkarte Speicher unter Root-Gerätedetails wie folgt den Wert des Root-Gerätetyps:
   - Wenn der Wert `EBS` lautet, ist es eine Amazon EBS-gestützte Instance.
   - Wenn der Wert `INSTANCE-STORE` lautet, ist es eine per Instance-Speicher gestützte Instance.

AWS CLI

So ermitteln Sie den Root-Gerätetyp einer Instance über die Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Ändern des beizubehaltenden Root-Volumes

Das Root-Volume für ein Amazon EBS-gestütztes AMI wird standardmäßig gelöscht, wenn die Instance beendet wird. Sie können das Standardverhalten ändern, um sicherzustellen, dass das Volume nach dem Beenden der Instance weiterhin besteht. Legen Sie das Attribut `DeleteOnTermination` auf `false` fest, indem Sie eine Blockgerät-Zuweisung verwenden, um das Standardverhalten zu ändern.

Aufgaben

- Konfigurieren des Root-Volumes für Persistenz während des Instance-Starts
- Konfigurieren des Root-Volumes für Persistenz für eine vorhandene Instance
- Bestätigen, dass ein Root-Volume für Persistenz konfiguriert ist

Konfigurieren des Root-Volumes für Persistenz während des Instance-Starts

Sie können das Root-Volume so konfigurieren, dass es beim Starten einer Instance mithilfe der Amazon EC2-Konsole oder der Befehlszeilen-Tools bestehen bleibt.

Console

So konfigurieren Sie das Root-Volume so, dass es beim Starten einer Instance über die Konsole bestehen bleibt:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und Instances starten aus.
3. Wählen Sie ein Amazon Machine Image (AMI) aus, klicken Sie auf einen Instance-Typ, wählen Sie ein Schlüsselpaar und konfigurieren Sie Ihre Netzwerkeinstellungen.
4. Wählen Sie unter Speicher konfigurieren die Option Erweitert aus.
5. Erweitern Sie das Root-Volume.
6. Für Beim Beenden löschen wählen Sie Nein aus.
7. Wenn Sie die Konfiguration Ihrer Instance abgeschlossen haben, wählen Sie Instance starten.

AWS CLI

Um das Root-Volume so zu konfigurieren, dass es beim Starten einer Instance erhalten bleibt, verwenden Sie AWS CLI

Verwenden Sie den Befehl run-instances und schließen Sie eine Blockgerät-Zuweisung ein, mit der das `DeleteOnTermination`-Attribut auf `false` festgelegt wird.

```
aws ec2 run-instances --block-device-mappings file://mapping.json ...other
 parameters...
```

Geben Sie in Folgendes a `mapping.json`.

```
[
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

Um das Root-Volume so zu konfigurieren, dass es beim Starten einer Instance erhalten bleibt, verwenden Sie die Tools für Windows PowerShell

Verwenden Sie den New-EC2InstanceBefehl und fügen Sie eine Blockgeräte-Zuordnung hinzu, die das `DeleteOnTermination` Attribut auf `false` festlegt.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsBlockDevice
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.BlockDeviceMapping
C:\> $bdm.DeviceName = "dev/xvda"
C:\> $bdm.Ebs = $ebs
C:\> New-EC2Instance -ImageId ami-0abcdef1234567890 -BlockDeviceMapping
 $bdm ...other parameters...
```

Konfigurieren des Root-Volumes für Persistenz für eine vorhandene Instance

Sie können das Root-Volume nur mit den Befehlszeilen-Tools so konfigurieren, dass es für eine ausgeführte Instance bestehen bleibt.

AWS CLI

Um das Root-Volume so zu konfigurieren, dass es für eine bestehende Instanz bestehen bleibt, verwenden Sie AWS CLI

Verwenden Sie den Befehl modify-instance-attribute mit einer Blockgerät-Zuweisung, mit der das `DeleteOnTermination`-Attribut auf `false` festgelegt wird.

```
aws ec2 modify-instance-attribute --instance-id i-1234567890abcdef0 --block-device-mappings file://mapping.json
```

Geben Sie in Folgendes a `mapping.json`.

```
[
    {
        "DeviceName": "/dev/xvda",
        "Ebs": {
            "DeleteOnTermination": false
        }
    }
]
```

Tools for Windows PowerShell

So konfigurieren Sie das Root-Volume über die AWS Tools for Windows PowerShell so, dass es für eine vorhandene Instance bestehen bleibt:

Verwenden Sie den Edit-EC2InstanceAttributeBefehl mit einer Blockgeräte-Zuordnung, die das `DeleteOnTermination` Attribut auf `false` festlegt.

```
C:\> $ebs = New-Object Amazon.EC2.Model.EbsInstanceBlockDeviceSpecification
C:\> $ebs.DeleteOnTermination = $false
C:\> $bdm = New-Object Amazon.EC2.Model.InstanceBlockDeviceMappingSpecification
C:\> $bdm.DeviceName = "/dev/xvda"
C:\> $bdm.Ebs = $ebs
```

```
C:\> Edit-EC2InstanceAttribute -InstanceId i-1234567890abcdef0 -BlockDeviceMapping
 $bdm
```

Bestätigen, dass ein Root-Volume für Persistenz konfiguriert ist

Sie können mit der Amazon EC2-Konsole oder den Befehlszeilen-Tools bestätigen, dass ein Root-Volume so konfiguriert ist, dass es bestehen bleibt.

Console

So bestätigen Sie mit der, Amazon EC2-Konsole dass ein Root-Volume so konfiguriert ist, dass es bestehen bleibt:

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und wählen Sie dann die Instance aus.
3. Suchen Sie auf der Registerkarte Speicher unter Blockgeräte den Eintrag für das Stammvolume. Wenn Bei Beendigung löschen auf No gesetzt ist, wird das Volume so konfiguriert, dass es bestehen bleibt.

AWS CLI

Um zu überprüfen, ob ein Root-Volume so konfiguriert ist, dass es fortbesteht, verwenden Sie AWS CLI

Verwenden Sie den Befehl describe-instances und stellen Sie sicher, dass das `DeleteOnTermination`-Attribut im `BlockDeviceMappings`-Antwortelement auf `false` festgelegt ist.

```
aws ec2 describe-instances --instance-id i-1234567890abcdef0
```

```
...
    "BlockDeviceMappings": [
    {
        "DeviceName": "/dev/sda1",
        "Ebs": {
            "Status": "attached",
            "DeleteOnTermination": false,
            "VolumeId": "vol-1234567890abcdef0",
            "AttachTime": "2013-07-19T02:42:39.000Z"
```

```
        }
    }
...
```

Tools for Windows PowerShell

Um zu überprüfen, ob ein Root-Volume so konfiguriert ist, dass es dauerhaft gespeichert ist, verwenden Sie AWS Tools for Windows PowerShell

Verwenden Sie den Get-EC2Instanceund stellen Sie sicher, dass das `DeleteOnTermination` Attribut im `BlockDeviceMappings` Antwortelement auf `false` gesetzt ist.

```
C:\> (Get-EC2Instance -InstanceId i-
i-1234567890abcdef0).Instances.BlockDeviceMappings.Ebs
```

Ändern der Anfangsgröße des Root-Volumes

Standardmäßig wird die Größe des Root-Volumes durch die Größe des Snapshots bestimmt. Sie können die Anfangsgröße des Root-Volumes mithilfe der Blockgerät-Zuweisung der Instance wie folgt erhöhen.

1. Bestimmen Sie den Gerätenamen des im AMI angegebenen Root-Volumes, wie unter Anzeigen der EBS-Volumes in einer AMI-Blockgerät-Zuweisung beschrieben.
2. Bestätigen Sie die Größe des Snapshots, die in der AMI-Blockgerätezuordnung angegeben ist.
3. Überschreiben Sie die Größe des Root-Volumes mithilfe der Instance-Blockgerät-Zuweisung, wie unter Aktualisieren der Blockgerät-Zuweisung beim Starten einer Instance beschrieben, und geben Sie eine Volumegröße an, die größer als die Snapshotgröße ist.

Der folgende Eintrag für die Instance-Blockgerät-Zuweisung erhöht beispielsweise die Größe des Root-Volumes `/dev/xvda` auf 100 GiB. Sie können die Snapshot-ID in der Instance-Blockgerät-Zuweisung weglassen, da die Snapshot-ID bereits in der AMI-Blockgerät-Zuweisung angegeben ist.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Weitere Informationen finden Sie unter Blockgerät-Zuweisungen.

Ersetzen Sie ein EC2-Instance-Root-Volume

Amazon EC2 ermöglicht es Ihnen, das Stamm-Amazon-EBS-Volume für eine ausgeführte Instance zu ersetzen und dabei Folgendes beizubehalten:

- In Instance-Speicher-Volumes gespeicherte Daten – Instance-Speicher-Volumes bleiben der Instance zugeordnet, nachdem das Root-Volume wiederhergestellt wurde.
- Auf Amazon-EBS-Daten-Volumes (Nicht-Stamm-Volumes) gespeicherte Daten – Nicht-Stamm-Volumes von Amazon EBS bleiben an die Instance angefügt, nachdem das Stamm-Volume wiederhergestellt worden ist.
- Netzwerkkonfiguration — Alle Netzwerkschnittstellen bleiben mit der Instance verbunden und behalten ihre IP-Adressen, Kennungen und Anhangs-IDs bei. Wenn die Instance verfügbar wird, wird der gesamte ausstehende Netzwerkverkehr gelöscht. Darüber hinaus bleibt die Instance auf demselben physischen Host, so dass sie ihre öffentlichen und privaten IP-Adressen und ihren DNS-Namen beibehält.
- IAM-Richtlinien — IAM-Profile und -richtlinien (wie Tag (Markierung)-basierte Richtlinien), die mit der Instance verknüpft sind, werden beibehalten und durchgesetzt.

Themen

Funktionsweise

Wenn Sie das Stamm-Volume für eine Instance ersetzen, wird ein neues (Ersatz-)Stamm-Volume auf eine der folgenden Arten wiederhergestellt:

- In den ursprünglichen Status beim Start – das Volume wird beim Start der Instance in seinen ursprünglichen Status zurückversetzt. Weitere Informationen finden Sie unter Wiederherstellen eines Stamm-Volumes in seinen Startzustand.
- Aus einem Snapshot aus derselben Abstammungslinie wie das aktuelle Stamm-Volume. Auf diese Weise können Sie Probleme beheben, z. B. eine Beschädigung des Stamm-Volumes oder Fehler

in der Netzwerkkonfiguration des Gastbetriebssystems. Weitere Informationen finden Sie unter Ersetzen eines Stamm-Volumes mithilfe eines Snapshots.

- Von einem AMI, das über dieselben Schlüsselattribute wie die Instance verfügt, können Sie Patches oder Erweiterungen für das Betriebssystem und die Anwendungen durchführen. Weitere Informationen finden Sie unter Ersetzen eines Stamm-Volumes mithilfe eines AMI.

Das ursprüngliche Stamm-Volume wird von der Instance abgetrennt und das neue Stamm-Volume wird an seiner Stelle an die Instance angefügt. Die Blockgerät-Zuweisung der Instance wird aktualisiert, sodass sie die ID des Ersatz-Stamm-Volumes wiedergibt. Sie können wählen, ob Sie das ursprüngliche Stamm-Volume behalten möchten oder nicht, nachdem der Ersetzungsvorgang des Stamm-Volumes abgeschlossen ist. Wenn Sie nach Abschluss des Ersetzungsvorgangs das ursprüngliche Stamm-Volume löschen, wird das ursprüngliche Stamm-Volume automatisch gelöscht und ist nicht mehr wiederherstellbar. Wenn Sie sich dafür entscheiden, das ursprüngliche Stamm-Volume nach Abschluss des Vorgangs beizubehalten, bleibt das Volume in Ihrem Konto bereitgestellt. Sie müssen es manuell löschen, wenn Sie es nicht mehr benötigen.

Wenn die Aufgabe zum Ersetzen des Stamm-Volumes fehlschlägt, wird die Instance neu gestartet und das ursprüngliche Stamm-Volume bleibt mit der Instance verbunden.

Überlegungen zum Ersetzen des Stamm-Volumes

- Die Instance muss sich im Status `running` befinden.
- Die Instance wird während des Vorgangs automatisch neu gestartet. Der Inhalt des Arbeitsspeichers (RAM) wird während des Neustarts gelöscht. Es sind keine manuellen Neustarts erforderlich.
- Sie können das Stamm-Volume nicht ersetzen, wenn es sich um ein Instance-Speicher-Volume handelt. Nur Instances mit Amazon-EBS-Stamm-Volumes werden unterstützt.
- Sie können das Stamm-Volume für alle virtualisierten Instance-Typen und Bare-Metal-Instances von EC2 Mac ersetzen. Alle anderen Bare-Metal-Instance-Typen werden nicht unterstützt.
- Sie können nur Snapshots verwenden, die zur gleichen Herkunft gehören wie eines der vorherigen Stamm-Volumes der Instance.
- Wenn Ihr Konto in der aktuellen Region standardmäßig für die Amazon-EBS-Verschlüsselung aktiviert ist, wird das Ersatz-Root-Volume, das durch die Aufgabe zum Ersetzen des Root-Volumes erstellt wird, immer verschlüsselt, unabhängig vom Verschlüsselungsstatus des angegebenen Snapshots oder des Root-Volumes des angegebenen AMI.
- In der folgenden Tabelle werden die möglichen Verschlüsselungsergebnisse zusammengefasst.

	Ursprüngliches Stamm-Volume	Angegebener Snapshot oder AMI	Standardmäßige Verschlüsselung	Stamm-Volume-Ersatz	Verschlüsselungsschlüssel, der für das Ersatz-Root-Volume verwendet wird
Wiederherstellen des Startstatus des Ersatz-Root-Volumes	Encrypted	Nicht zutreffend	Nicht berücksichtigt	Encrypted	Derselbe KMS-Schlüssel wie das ursprüngliche Root-Volume
	Unverschlüsselt	Nicht zutreffend	Disabled	Unverschlüsselt	Nicht zutreffend
	Unverschlüsselt	Nicht zutreffend	Aktiviert	Encrypted	Der Standard-KMS-Schlüssel des Kontos für die Amazon-EBS-Verschlüsselung
Wiederherstellen des Ersatz-Root-Volumes aus Snapshot oder AMI	Encrypted	Unverschlüsselt	Nicht berücksichtigt	Encrypted	Derselbe KMS-Schlüssel wie das ursprüngliche Root-Volume

	Ursprüngliches Stamm-Volume	Angegebener Snapshot oder AMI	Standardmäßige Verschlüsselung	Stamm-Volume-Ersatz	Verschlüsselungsschlüssel, der für das Ersatz-Root-Volume verwendet wird
	Encrypted	Encrypted	Nicht berücksichtigt	Encrypted	Derselbe KMS-Schlüssel wie das ursprüngliche Root-Volume
	Unverschlüsselt	Unverschlüsselt	Disabled	Unverschlüsselt	Nicht zutreffend
	Unverschlüsselt	Unverschlüsselt	Aktiviert	Encrypted	Der Standard-KMS-Schlüssel des Kontos für die Amazon-EBS-Verschlüsselung

	Ursprüngliches Stamm-Volume	Angegebener Snapshot oder AMI	Standardmäßige Verschlüsselung	Stamm-Volume-Ersatz	Verschlüsselungsschlüssel, der für das Ersatz-Root-Volume verwendet wird
	Unverschlüsselt	Encrypted	Nicht berücksichtigt	Encrypted	Wenn das AMI oder der Snapshot Eigentum des Kontos ist, wird das Ersatz-Volume mit dem KMS-Schlüssel des AMI oder Snapshots verschlüsselt. Wenn AMI oder Snapshot für das Konto freigegeben werden, wird das Ersatz-Volume mit dem Standard-KMS-Schlüssel des Kontos für die Amazon-EBS-Verschl

	Ursprüngliches Stamm-Volume	Angegebener Snapshot oder AMI	Standardmäßige Verschlüsselung	Stamm-Volume-Ersatz	Verschlüsselungsschlüssel, der für das Ersatz-Root-Volume verwendet wird
					üsselung verschlüselt.

Themen

- Wiederherstellen eines Stamm-Volumes in seinen Startzustand
- Ersetzen eines Stamm-Volumes mithilfe eines Snapshots
- Ersetzen eines Stamm-Volumes mithilfe eines AMI

Wiederherstellen eines Stamm-Volumes in seinen Startzustand

Sie können ein Ersetzen des Stamm-Volumes durchführen, bei dem das Stamm-Volume einer Instance durch ein Ersatz-Stamm-Volume ersetzt wird, das den Start-Status des ursprünglichen Stamm-Volumes wiederherstellt. Das Ersatz-Volume wird automatisch aus dem Snapshot wiederhergestellt, der zum Erstellen des ursprünglichen Volumes während des Instance-Starts verwendet wurde.

Das Ersatz-Stamm-Volume erhält denselben Typ, dieselbe Größe und dieselben Attribute zum Löschen bei Beendigung wie das ursprüngliche Stamm-Volume.

Ersetzen eines Stamm-Volumes mithilfe eines Snapshots

Sie können ein Ersetzen des Stamm-Volumes durchführen, bei dem das Stamm-Volume einer Instance durch ein Ersatz-Volume ersetzt wird, das auf einem bestimmten Snapshot wiederhergestellt wird. Auf diese Weise können Sie das Stamm-Volume für eine Instance auf einem bestimmten Snapshot wiederherstellen, den Sie zuvor von diesem Stamm-Volume erstellt haben.

Das Ersatz-Stamm-Volume erhält denselben Typ, dieselbe Größe und dieselben Attribute zum Löschen bei Beendigung wie das ursprüngliche Stamm-Volume.

Überlegungen zur Verwendung eines Snapshots

- Sie können nur Snapshots verwenden, die zur gleichen Lineage gehören wie das aktuelle Stammvolume der Instance.
- Sie können keine Snapshot-Kopien verwenden, die aus Snapshots erstellt wurden, die vom Stammvolume entnommen wurden.
- Nach dem erfolgreichen Ersetzen des Stamm-Volumes können Snapshots, die vom ursprünglichen Stamm-Volume erstellt wurden, weiterhin verwendet werden, um das neue (Ersatz-)Stamm-Volume zu ersetzen.

Ersetzen eines Stamm-Volumes mithilfe eines AMI

Sie können ein Ersetzen des Stamm-Volumes mithilfe eines AMI durchführen, das Sie besitzen oder eines AMI, das für Sie freigegeben ist. Das AMI muss über denselben Produktcode, dieselben Rechnungsinformationen, denselben Architekturtyp und denselben Virtualisierungstyp verfügen wie die Instance.

Wenn die Instance für ENA oder sriov-net aktiviert ist, müssen Sie ein AMI verwenden, das diese Funktionen unterstützt. Wenn die Instance nicht für ENA oder sriov-net aktiviert ist, können Sie entweder ein AMI auswählen, das diese Funktionen nicht unterstützt, oder Sie können automatisch Unterstützung hinzufügen, wenn Sie ein AMI auswählen, das ENA oder sriov-net unterstützt.

Wenn die Instance für NitroTPM aktiviert ist, müssen Sie ein AMI verwenden, für das NitroTPM aktiviert ist. Die NitroTPM-Unterstützung ist nicht aktiviert, wenn die Instance nicht dafür konfiguriert wurde, unabhängig vom ausgewählten AMI.

Sie können ein AMI mit einem anderen Start-Modus als dem der Instance auswählen, solange die Instance den Start-Modus des AMI unterstützt. Wenn die Instance den Start-Modus nicht unterstützt, schlägt die Anforderung fehl. Wenn die Instance den Start-Modus unterstützt, wird der neue Start-Modus an die Instance weitergegeben und ihre UEFI-Daten werden entsprechend aktualisiert. Wenn Sie die Start-Reihenfolge manuell geändert oder einen privaten UEFI-Sicherheits-Start-Schlüssel zum Laden privater Kernel-Module hinzugefügt haben, gehen die Änderungen beim Ersetzen des Stamm-Volumes verloren.

Das Ersatz-Stamm-Volume erhält denselben Volume-Typ und dasselbe Löschen-bei-Beendigung-Attribut wie das ursprüngliche Stamm-Volume und erhält die Größe der AMI-Stamm-Volume-Blockgerät-Zuweisung.

> **Note**
>
> Die Größe der AMI-Stamm-Volume-Blockgerät-Zuweisung muss der Größe des ursprünglichen Stamm-Volumes entsprechen. Wenn die Größe der Blockgerät-Zuweisung des AMI Stamm-Volumes kleiner als die Größe des ursprünglichen Stamm-Volumes ist, schlägt die Anforderung fehl.

Nachdem die Aufgabe zum Austausch des Root-Volumes abgeschlossen ist, spiegeln sich die folgenden neuen und aktualisierten Informationen wider, wenn Sie die Instance mithilfe der Konsole AWS CLI oder AWS der SDKs beschreiben:

- Neue AMI-ID
- Neue Volume-ID für das Stamm-Volume
- Aktualisierte Start-Modus-Konfiguration (sofern vom AMI geändert)
- Aktualisierte NitroTPM-Konfiguration (sofern vom AMI aktiviert)
- Aktualisierte ENA-Konfiguration (sofern vom AMI aktiviert)
- Aktualisierte sriov-net-Konfiguration (sofern vom AMI aktiviert)

Die neue AMI-ID spiegelt sich auch in den Instance-Metadaten wider.

Überlegungen zur Verwendung eines AMI:

- Wenn Sie ein AMI verwenden, das über mehrere Blockgerät-Zuweisungen verfügt, wird nur das Stamm-Volume des AMI verwendet. Die anderen (Nicht-Stamm-)Volumes werden ignoriert.
- Sie können dieses Feature nur verwenden, wenn Sie über Berechtigungen für das AMI und den zugehörigen Root-Volume-Snapshot verfügen. Sie können diese Funktion nicht mit AWS Marketplace AMIs verwenden.
- Sie können ein AMI ohne Produktcode nur verwenden, wenn die Instance über keinen Produktcode verfügt.
- Die Größe der AMI-Stamm-Volume-Blockgerät-Zuweisung muss der Größe des ursprünglichen Stamm-Volumes entsprechen. Wenn die Größe der Blockgerät-Zuweisung des AMI Stamm-Volumes kleiner als die Größe des ursprünglichen Stamm-Volumes ist, schlägt die Anforderung fehl.
- Die Instance-Identitätsdokumente für die Instance werden automatisch aktualisiert.

- Wenn die Instance NitroTPM unterstützt, werden die NitroTPM-Daten für die Instance zurückgesetzt und neue Schlüssel generiert.

Ersetzen eines Stammvolumen

Wenn Sie das Stamm-Volume für eine Instance ersetzen, wird eine Aufgabe zum Ersetzen des Stamm-Volumes erstellt. Sie können die Aufgabe zum Ersetzen des Stamm-Volumes verwenden, um den Fortschritt und das Ergebnis des Ersetzungsvorgangs zu überwachen. Weitere Informationen finden Sie unter Anzeige der Aufgaben Stammvolumenersatz.

Sie können das Stamm-Volume für eine Instance mit einer der folgenden Methoden ersetzen.

> **Note**
>
> Wenn Sie die Amazon-EC2-Konsole verwenden, ist diese Funktion nur in der neuen Konsole verfügbar.

New console

So ersetzen Sie das Stamm-Volume

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, für die das Stamm-Volume ersetzt werden soll, und wählen Sie Actions (Aktionen), Monitor and troubleshoot (Überwachen und Fehlerbehebung) und Replace root volume (Stamm-Volume ersetzen).

   > **Note**
   >
   > Die Replace root volume (Ersetzen des Root-Volumes)-Aktion ist deaktiviert, wenn sich die ausgewählte Instance nicht im Zustand `running` befindet.

4. Führen Sie auf dem Bildschirm Stamm-Volume ersetzen einen der folgenden Schritte aus:

   - Um das Ersatz-Stamm-Volume in seinen ursprünglichen Start-Status zurückzusetzen, wählen Sie Create replacement task (Ersatzaufgabe erstellen), ohne einen Snapshot auszuwählen.

- Um das Ersatz-Stamm-Volume auf einem bestimmten Snapshot wiederherzustellen, wählen Sie unter Snapshot den zu verwendenden Snapshot aus und wählen Sie dann Create replacement task (Ersatzaufgabe erstellen) aus.
- Um das Ersatz-Stamm-Volume mithilfe eines AMI wiederherzustellen, wählen Sie für AMI das zu verwendende AMI aus und wählen Sie dann Create replacement task (Ersatzaufgabe erstellen).

5. Um das ursprüngliche Stamm-Volume nach Abschluss der Ersetzungsaufgabe zu löschen, wählen Sie Delete replaced root volume (Ersetztes Stamm-Volume löschen) aus.

AWS CLI

So stellen Sie den Start-Status des Ersatz-Stamm-Volumes wieder her

Verwenden Sie den Befehl create-replace-root-volume-task. Geben Sie für `--instance-id` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Lassen Sie die Parameter `--snapshot-id` und `--image-id` aus. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `--delete-replaced-root-volume` ein und geben Sie `true` an.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--delete-replaced-root-volume true
```

So stellen Sie das Ersatz-Stamm-Volume auf einem bestimmten Snapshot wieder her

Verwenden Sie den Befehl create-replace-root-volume-task . Geben Sie für `--instance-id` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Geben Sie für `--snapshot-id` die ID des zu verwendenden Snapshots an. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `--delete-replaced-root-volume` ein und geben Sie `true` an.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-1234567890abcdef0 \
--snapshot-id snap-9876543210abcdef0 \
--delete-replaced-root-volume true
```

So stellen Sie das Ersatz-Stamm-Volume mithilfe eines AMI wieder her

Verwenden Sie den Befehl create-replace-root-volume-task. Geben Sie für `--instance-id` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Geben Sie für `--image-id` die ID des zu verwendenden AMI an. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `--delete-replaced-root-volume` ein und geben Sie `true` an.

```
$ aws ec2 create-replace-root-volume-task \
--instance-id i-01234567890abcdef \
--image-id ami-09876543210abcdef \
--delete-replaced-root-volume true
```

Tools for Windows PowerShell

So stellen Sie den Start-Status des Ersatz-Stamm-Volumes wieder her

Verwenden Sie den New-EC2ReplaceRootVolumeTask-Befehl. Geben Sie für `-InstanceId` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Lassen Sie die Parameter `-SnapshotId` und `-ImageId` aus. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `-DeleteReplacedRootVolume` ein und geben Sie `$true` an.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
DeleteReplacedRootVolume $true
```

So stellen Sie das Ersatz-Stamm-Volume auf einem bestimmten Snapshot wieder her

Verwenden Sie den New-EC2ReplaceRootVolumeTask-Befehl. Geben Sie für `--InstanceId` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Geben Sie für `-SnapshotId` die ID des zu verwendenden Snapshots an. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `-DeleteReplacedRootVolume` ein und geben Sie `$true` an.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
SnapshotId snap-9876543210abcdef0 -DeleteReplacedRootVolume $true
```

So stellen Sie das Ersatz-Stamm-Volume mithilfe eines AMI wieder her

Verwenden Sie den New-EC2ReplaceRootVolumeTask-Befehl. Geben Sie für `-InstanceId` die ID der Instance an, für die das Stamm-Volume ersetzt werden soll. Geben Sie für `-ImageId` die ID des zu verwendenden AMI an. Um das ursprüngliche Stamm-Volume zu löschen, nachdem es ersetzt wurde, schließen Sie `-DeleteReplacedRootVolume` ein und geben Sie `$true` an.

```
PS C:\> New-EC2ReplaceRootVolumeTask -InstanceId i-1234567890abcdef0 -
ImageId ami-09876543210abcdef -DeleteReplacedRootVolume $true
```

Anzeige der Aufgaben Stammvolumenersatz

Wenn Sie das Stamm-Volume für eine Instance ersetzen, wird eine Aufgabe zum Ersetzen des Stamm-Volumes erstellt. Die Aufgabe zum Ersetzen des Root-Volumes wechselt während des Vorgangs durch die folgenden Status:

- `pending` — das Ersatzvolume wird erstellt.
- `in-progress` — das ursprüngliche Volume wird gelöst und das Ersatzvolume wird angehängt.
- `succeeded` — das Ersatzvolume wurde erfolgreich an die Instance angehängt und die Instance ist verfügbar.
- `failing` — Die Ersetzungsaufgabe ist im Begriff fehlzuschlagen.
- `failed` – Die Ersetzungsaufgabe ist fehlgeschlagen, aber das ursprüngliche Stamm-Volume ist immer noch angefügt.
- `failing-detached` – Die Ersetzungsaufgabe ist im Begriff fehlzuschlagen und der Instance ist möglicherweise kein Stamm-Volume angefügt.
- `failed-detached` – Die Ersetzungsaufgabe ist fehlgeschlagen und der Instance ist kein Stamm-Volume angefügt.

Sie können die Aufgabe Stammvolumenersatz für eine Instance mit einer der folgenden Methoden anzeigen.

> **Note**
>
> Wenn Sie die Amazon-EC2-Konsole verwenden, ist diese Funktion nur in der neuen Konsole verfügbar.

Console

So zeigen Sie die Aufgaben zum Stammvolumenersatz an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.

3. Wählen Sie die Instance aus, für die Sie die Aufgaben zum Stammvolumenersatz anzeigen möchten, und wählen Sie dann die Registerkarte Storage (Speicher) .
4. Erweitern Sie auf der Registerkarte Storage (Speicher) die Letzten Aufgaben zum Stammvolumenersatz.

AWS CLI

So zeigen Sie den Status einer Aufgabe zum Stammvolumenersatz an

Verwenden Sie den Befehl describe-replace-root-volume-tasks und geben Sie die IDs der Aufgaben zum Stammvolumenersatz an, die angezeigt werden sollen.

```
$ aws ec2 describe-replace-root-volume-tasks \
--replace-root-volume-task-ids replacevol-1234567890abcdef0
```

```
{
  "ReplaceRootVolumeTasks": [
  {
    "ReplaceRootVolumeTaskId": "replacevol-1234567890abcdef0",
    "InstanceId": "i-1234567890abcdef0",
    "TaskState": "succeeded",
    "StartTime": "2020-11-06 13:09:54.0",
    "CompleteTime": "2020-11-06 13:10:14.0",
    "SnapshotId": "snap-01234567890abcdef",
    "DeleteReplacedRootVolume": "True"
  }]
}
```

Geben Sie alternativ den `instance-id`-Filter an, um die Ergebnisse nach Instances zu filtern.

```
$ aws ec2 describe-replace-root-volume-tasks \
--filters Name=instance-id,Values=i-1234567890abcdef0
```

Tools for Windows PowerShell

So zeigen Sie den Status einer Aufgabe zum Stammvolumenersatz an

Verwenden Sie den Get-EC2ReplaceRootVolumeTaskBefehl und geben Sie die IDs der Aufgaben zum Ersetzen des Stammvolumes an, die angezeigt werden sollen.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -
ReplaceRootVolumeTaskIds replacevol-1234567890abcdef0
```

Geben Sie alternativ den `instance-id`-Filter an, um die Ergebnisse nach Instances zu filtern.

```
PS C:\> Get-EC2ReplaceRootVolumeTask -Filters @{Name = 'instance-id'; Values =
 'i-1234567890abcdef0'} | Format-Table
```

Gerätenamen auf Amazon EC2 EC2-Instances

Wenn Sie an Ihre Instance ein Volume anfügen, vergeben Sie einen Gerätenamen für das Volume. Dieser Gerätename wird von Amazon EC2 verwendet. Der Blockgeräte-Treiber für die Instance weist beim Mounten des Volumes den tatsächlichen Volume-Namen zu. Dieser zugewiesene Name kann sich von dem Namen unterscheiden, den Amazon EC2 verwendet.

Die Anzahl der Volumes, die Sie Ihre Instance unterstützen kann, wird vom Betriebssystem bestimmt. Weitere Informationen finden Sie unter Volume-Limits für Instances.

Inhalt

Verfügbare Gerätenamen

Linux-Instances

Für Linux-Instances sind zwei Virtualisierungtypen verfügbar: Paravirtual (PV) und Hardware Virtual Machine (HVM). Der Virtualisierungtyp einer Instance wird durch das AMI bestimmt, das zum Starten der Instance verwendet wird. Alle Instance-Typen unterstützen HVM-AMIs. Einige Instance-Typen früherer Generationen unterstützen PV-AMIs. Notieren Sie sich den Virtualisierungstyp Ihres AMI, weil die empfohlenen und verfügbaren Gerätenamen, die Sie verwenden können, vom Virtualisierungstyp Ihrer Instance abhängig sind. Weitere Informationen finden Sie unter AMI-Virtualisierungstypen.

Die folgende Tabelle führt die verfügbaren Gerätenamen auf, die Sie in einer Blockgerätezuordnung oder beim Anhängen eines EBS-Volumes verwenden können.

Virtualisierungstyp	Verfügbar	Reserviert für Stamm-Volume	Empfohlen für EBS-Volumes	Instance-Speicher-Volumes
Paravirtual	/dev/sd[a-z] /dev/sd[a-z][1-15] /dev/hd[a-z] /dev/hd[a-z][1-15]	/dev/sda1	/dev/sd[f-p] /dev/sd[f-p][1-6]	/dev/sd[b-e]
HVM (Hardware gestützte virtuelle Maschine)	/dev/sd[a-z] /dev/xvd[a-d][a-z] /dev/xvd[e-z]	Unterschiedlich nach AMI /dev/sda1 or /dev/xvda	/dev/sd[f-p] *	/dev/sd[b-e] /dev/sd[b-h] (h1.16xlarge) /dev/sd[b-y] (d2.8xlarge) /dev/sd[b-i] (i2.8xlarge) **

*Die Gerätenamen, die Sie in einer Blockgerätezuordnung für NVMe-EBS-Volumes angeben, werden durch NVMe-Gerätenamen ersetzt (`/dev/nvme[0-26]n1`). Der Blockgerät-Treiber kann NVMe-Gerätenamen in einer anderen Reihenfolge zuweisen, als Sie es für die Volumes in der Blockgerät-Zuweisung angegeben haben.

** NVMe-Instance-Speicher-Volumes werden automatisch aufgezählt und ihnen wird ein NVMe-Gerätename zugeordnet.

Windows-Instances

Windows-AMIs verwenden einen der folgenden Treibersätze, um den Zugriff auf virtualisierte Hardware zu ermöglichen: AWS PV, Citrix PV und RedHat PV. Weitere Informationen finden Sie unter the section called “Windows PV-Treiber”.

Die folgende Tabelle führt die verfügbaren Gerätenamen auf, die Sie in einer Blockgerätezuordnung oder beim Anhängen eines EBS-Volumes verwenden können.

Treibertyp	Verfügbar	Reserviert für Stamm-Volume	Empfohlen für EBS-Volumes	Instance-Speicher-Volumes
AWS PV, Citrix PV	xvd[b-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-z] *	xvdc[a-x] xvd[a-e] **
Red Hat PV	xvd[a-z] xvd[b-c][a-z] /dev/sda1 /dev/sd[b-e]	/dev/sda1	xvd[f-p]	xvdc[a-x] xvd[a-e]

* Wenn Sie für Citrix PV und Red Hat PV ein EBS-Volume dem Namen zuordnen`xvda`, erkennt Windows das Volume nicht (das Volume ist für AWS PV oder AWS NVMe sichtbar).

** NVMe-Instance-Speicher-Volumes werden automatisch aufgezählt und ihnen wird ein Windows-Laufwerksbuchstabe zugeordnet.

Weitere Informationen zu Instance-Speicher-Volumes finden Sie unter Amazon EC2-Instance-Speicher. Weitere Informationen zu NVMe EBS-Volumes (Nitro-basierte Instances), einschließlich der Identifizierung des EBS-Geräts, finden Sie unter Amazon EBS und NVMe im Amazon EBS-Benutzerhandbuch.

Überlegungen zu Gerätenamen

Bei der Auswahl eines Gerätenamens sollten Sie Folgendes beachten:

- Obwohl Sie EBS-Volumes mit dem Gerätenamen anfügen können, der zum Anfügen von Instance-Speicher-Volumes verwendet wird, empfehlen wir dringend, dies nichts zu tun, da das Verhalten unberechenbar sein kann.
- Die Anzahl der NVMe-Instance-Speicher-Volumes für eine Instance ist abhängig von der Größe der Instance. NVMe-Instance-Speicher-Volumes werden automatisch aufgelistet und ihnen wird ein NVMe-Gerätename (Linux-Instances) oder ein Windows-Laufwerksbuchstabe (Windows-Instances) zugewiesen.
- (Windows-Instanzen) AWS Windows-AMIs werden mit zusätzlicher Software geliefert, die eine Instanz beim ersten Start vorbereitet. Dies ist entweder der EC2Config-Service (Windows-AMIs vor Windows Server 2016) oder EC2Launch (Windows Server 2016 und höher). Nachdem den Geräten Laufwerksbuchstaben zugeordnet worden sind, werden sie initialisiert und gemountet. Das Stammlaufwerk wird als `C:\` initialisiert und gemountet. Wenn ein EBS-Volume an eine Windows-Instance angefügt wird, kann es als beliebiger Laufwerksbuchstabe auf der Instance angezeigt werden. Sie können die Einstellungen ändern, um die Laufwerksbuchstaben der Volumes nach Ihren Spezifikationen anzupassen. Speichern Sie beispielsweise Volumes. Die Standardeinstellung hängt vom Treiber ab. AWS PV-Treiber und Citrix PV-Treiber weisen Instance-Speicher-Volumes Laufwerksbuchstaben von Z: bis A: zu. Red Hat-Treiber ordnen die Instance-Speicher-Volumes den Laufwerkbuchstaben von D: nach Z: zu. Weitere Informationen finden Sie unter Starteinstellungen für Amazon EC2 EC2-Windows-Instances konfigurieren und Zuweisen von Datenträgern zu Volumes in Ihrer Windows-Instance.
- (Linux-Instanzen) Je nach Blockgerätetreiber des Kernels kann das Gerät mit einem anderen Namen als dem von Ihnen angegebenen verbunden sein. Beispiel: Falls Sie einen Gerätenamen von `/dev/sdh` angeben, könnte Ihr Gerät in `/dev/xvdh` oder `/dev/hdh` umbenannt werden. In den meisten Fällen bleibt der abschließende Buchstabe gleich. In einigen Versionen von Red Hat Enterprise Linux (und deren Varianten wie z. B. CentOS) kann der abschließende Buchstabe geändert werden (`/dev/sda` kann in `/dev/xvde` geändert werden). In diesen Fällen wird jeder abschließende Buchstabe entsprechend fortgeschrieben. Beispiel: Wenn `/dev/sdb` in `/dev/xvdf` umbenannt wird, dann wird `/dev/sdc` in `/dev/xvdg` umbenannt. Amazon Linux erstellt einen symbolischen Link für den Namen, den Sie für das umbenannte Gerät angegeben haben. Andere Betriebssysteme könnten sich anders verhalten.
- (Linux-Instances) HVM-AMIs unterstützen die Verwendung von nachfolgenden Zahlen in Gerätenamen nicht, mit Ausnahme von`/dev/sda1`, das für das Root-Gerät reserviert ist, und. `/dev/sda2` Obwohl es möglich ist, `/dev/sda2` zu verwenden, wird die Nutzung dieser Gerätezuweisung mit HVM-Instances nicht empfohlen.

- (Linux-Instances) Bei der Verwendung von PV-AMIs können Sie keine Volumes anhängen, die dieselben Gerätebuchstaben verwenden, sowohl mit als auch ohne nachstehende Ziffern. Wenn Sie beispielsweise ein Volume als `/dev/sdc` und ein anderes als `/dev/sdc1` anfügen, ist nur `/dev/sdc` für die Instance sichtbar. Um nachfolgende Stellen in Gerätenamen zu verwenden, müssen Sie bei allen Gerätenamen nachfolgende Stellen verwenden, die dieselben Grundbuchstaben haben (beispielsweise `/dev/sdc1`, `/dev/sdc2`, `/dev/sdc3`).
- (Linux-Instances) Für einige benutzerdefinierte Kernel gelten möglicherweise Einschränkungen, die die Verwendung auf `/dev/sd[f-p]` oder beschränken. `/dev/sd[f-p][1-6]` Wenn Probleme bei der Verwendung von `/dev/sd[q-z]` oder `/dev/sd[q-z][1-6]` auftreten, versuchen Sie es mit `/dev/sd[f-p]` oder `/dev/sd[f-p][1-6]`.

Bevor Sie den von Ihnen ausgewählten Gerätenamen angeben, stellen Sie sicher, dass er verfügbar ist. Andernfalls erhalten Sie eine Fehlermeldung, dass der Gerätename bereits verwendet wird. Um die Festplattengeräte und ihre Bereitstellungspunkte anzuzeigen, verwenden Sie den lsblk Befehl (Linux-Instanzen), das Festplattenverwaltungsprogramm oder den diskpart Befehl (Windows-Instanzen).

Blockgerät-Zuweisungen

Jede gestartete Instance hat einen zugehörigen Root-Gerät-Volume, entweder ein Amazon EBS-Volume oder ein Instance-Speicher-Volume. Sie können mit der Blockgerät-Zuweisung zusätzliche EBS-Volumes oder Instance-Speicher-Volumes an eine Instance anfügen, wenn diese gestartet wird. Sie können auch zusätzliche EBS-Volumes an eine laufende Instance anhängen. Die einzige Möglichkeit zum Anfügen von Instance-Speicher-Volumes an eine Instance ist die Blockgerät-Zuweisung, um die Volumes beim Start der Instance anzufügen.

Inhalt

Konzepte der Blockgerät-Zuweisung

Ein Blockgerät ist ein Speichergerät, das Daten in Byte- bzw. Bit-Blöcken verschiebt. Diese Geräte unterstützen zufälligen Zugriff und verwenden im Allgemeinen I/O-Puffer. Beispiele sind Festplatten,

CD-ROM-Laufwerke und Flashlaufwerke. Ein Blockgerät kann physisch mit einem Computer verbunden oder per Remotezugriff verwendet werden, so als ob es physikalisch mit dem Computer verbunden wäre.

Amazon EC2 unterstützt zwei Arten von Blockgeräten:

- Instance-Speicher-Volumes (virtuelle Geräte, deren physikalische Hardware mit dem Host-Computer für die Instance verbunden ist)
- EBS-Volumes (Remotespeichergeräte)

Eine Blockgerät-Zuweisung definiert die Blockgeräte (Instance-Speicher-Volumes und EBS-Volumes) zum Anfügen an eine Instance. Sie können eine Blockgerät-Zuweisung als Teil der Erstellung eines AMI angeben, sodass die Zuweisung von allen Instances verwendet wird, die vom AMI gestartet werden. Alternativ können Sie eine Blockgerät-Zuweisung zum Starten einer Instance angeben. Diese Zuweisung gilt dann statt der im AMI angegebenen, von der aus die Instance gestartet wurde. Beachten Sie, dass alle von einem Instance-Typ unterstützen NVMe-Instance-Speicher-Volumes automatisch aufgezählt und beim Starten der Instance einem Gerätenamen zugeordnet werden. Die Aufnahme in Ihre Blockgerät-Zuweisung hat keine Auswirkung.

Inhalt

Blockgerät-Zuweisungseinträge

Wenn Sie eine Blockgerät-Zuweisung erstellen, geben Sie die folgenden Informationen für jedes Blockgerät an, das der Instance angefügt werden soll:

- Der in Amazon EC2 verwendete Gerätename. Der Blockgerätetreiber für die Instance weist den tatsächlichen Volume-Namen beim Einbinden des Volumes zu. Der zugewiesene Name kann vom Namen abweichen, der von Amazon EC2 empfohlen wird. Weitere Informationen finden Sie unter Gerätenamen auf Amazon EC2 EC2-Instances.

Für Instance-Speichervolumes können Sie auch die folgenden Informationen angeben:

- Das virtuelle Gerät: `ephemeral[0-23]`. Die Anzahl und Größe der verfügbaren Instance-Speicher-Volumes für die Instance hängt vom Instance-Typ ab.

Für NVMe-Instance-Speichervolumes gelten auch die folgenden Informationen:

- Diese Volumes werden automatisch aufgezählt und beim Starten der Instance einem Gerätenamen zugeordnet. Die Aufnahme in Ihre Blockgerät-Zuweisung hat keine Auswirkung.

Für EBS-Volumes geben Sie auch die folgenden Informationen an:

- Die ID des zu verwendenden Snapshots zur Erstellung des Blockgeräts (snap-xxxxxxxx). Der Wert ist optional, sofern eine Volumengröße angegeben wird. Sie können die ID eines archivierten Snapshots nicht angeben.
- Die Größe des Volumes in GiB Die angegebene Größe muss größer oder genauso groß wie der angegebene Snapshot sein.
- Ob das Volume bei Beendigung der Instance gelöscht wird (`true` oder `false`). Der Standardwert ist `true` für den Root-Gerät-Volume und `false` für angefügte Volumes. Wenn Sie ein AMI erstellen, erbt die Blockgerät-Zuweisung die Einstellung von der Instance. Wenn Sie eine Instance starten, erbt sie die Einstellung vom AMI.
- Der Volume-Typ. Dieser kann bei Allzweck-SSD `gp2` und `gp3`, bei SSD mit bereitgestellten IOPS `io1` und `io2`, bei durchsatzoptimierten HDD `st1`, bei Cold-HDD `sc1` und bei Magnetfestplatten `standard` sein.
- Die Anzahl der Ein/Ausgangs-Vorgänge pro Sekunde (IOPS), die das Volume unterstützt. (Wird nur mit `io1`- und `io2`-Volumes verwendet.)

Blockgerät-Zuweisung – Instance-Speicher-Einschränkungen

Beim Starten von Instances mit AMIs mit Instance-Speicher-Volumes in ihren Blockgerät-Zuweisungen müssen einige Einschränkungen beachtet werden.

- Einige Instance-Typen enthalten mehr Instance-Speicher-Volumes als andere und bestimmte Instance-Typen enthalten überhaupt keine Instance-Speicher-Volumes. Wenn der Instance-Typ ein Instance-Speicher-Volume unterstützt und das AMI Zuweisungen für zwei Instance-Speicher-Volumes aufweist, wird die Instance mit einem Instance-Speicher-Volume gestartet.
- Instance-Speicher-Volumes können ausschließlich zum Startzeitpunkt zugewiesen werden. Sie können Instances nicht ohne Instance-Speicher-Volumes anhalten (z. B. `t2.micro`), die Instance

zu einem Typ ändern, der Instance-Speicher-Volumes unterstützt, und anschließend die Instance mit Instance-Speicher-Volumes neustarten. Allerdings können Sie ein AMI aus der Instance erstellen, dieses mit einem Instance-Typ starten, der Instance-Speicher-Volumes unterstützt, und anschließend die Instance-Speicher-Volumes der Instance zuweisen.

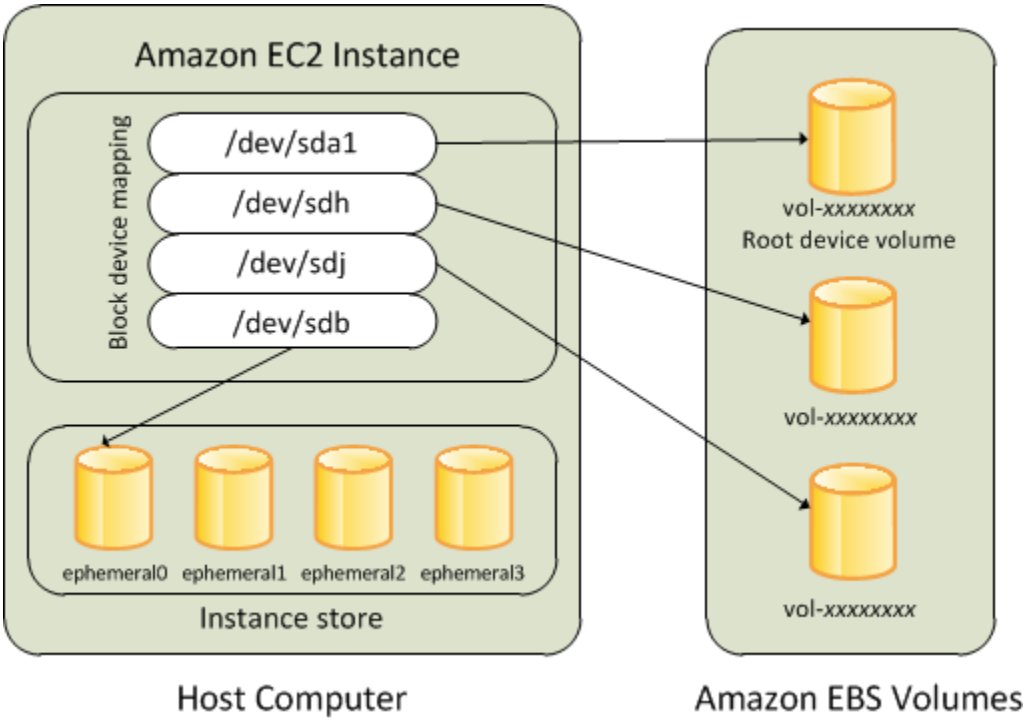
- Wenn Sie eine Instance mit zugewiesenen Instance-Speicher-Volumes starten, anschließend die Instance anhalten und zu einem Instance-Typ mit weniger Instance-Speicher-Volumes ändern und neustarten, werden die Instance-Speicher-Volume-Zuweisungen in den Instance-Metadaten angezeigt. Allerdings ist nur die Höchstanzahl der unterstützten Instance-Speicher-Volumes für den Instance-Typ für die Instance verfügbar.

  > **Note**
  >
  > Wenn eine Instance angehalten wird, gehen alle Daten auf den Instance-Speicher-Volumes verloren.

- Je nach Instance-Speicher-Kapazität zum Startzeitpunkt können M3-Instances AMI-Instance-Speicher-Blockgerät-Zuweisungen beim Start ignorieren, sofern sie nicht beim Start angegeben werden. Geben Sie Instance-Speicher-Blockgerät-Zuweisungen zum Startzeitpunkt an, selbst wenn beim gestarteten AMI die Instance-Speicher-Volumes im AMI zugewiesen sind, um sicherzustellen, dass die Instance-Speicher-Volumes beim Starten der Instance verfügbar sind.

Beispiel einer Blockgerät-Zuweisung

Diese Abbildung zeigt ein Beispiel für eine Blockgerät-Zuweisung für eine EBS-Backed-Instance. Sie weist `/dev/sdb` zu `ephemeral0` und zwei EBS-Volumes zu: eines zu `/dev/sdh` und ein weiteres zu `/dev/sdj`. Es zeigt außerdem das EBS-Volume, das der Root-Gerät-Volume ist, `/dev/sda1`.



Hinweis: Dieses Beispiel für Blockgerät-Zuweisung wird in den Beispielbefehlen und APIs in diesem Thema verwendet. Beispielbefehle und APIs zur Erstellung von Blockgerät-Zuweisungen finden Sie in Angeben einer Blockgerät-Zuweisung für ein AMI und Aktualisieren der Blockgerät-Zuweisung beim Starten einer Instance.

Bereitstellung von Geräten im Betriebssystem

Gerätenamen wie `/dev/sdh` und `xvdh` werden von Amazon EC2 zum Beschreiben von Blockgeräten verwendet. Die Blockgerät-Zuweisung dient in Amazon EC2 zum Angeben der Blockgeräte zum Hinzufügen zu einer EC2 Instance. Nach dem Anfügen eines Blockgeräts zu einer Instance muss es vom Betriebssystem aufgespielt werden, bevor Sie auf das Speichergerät zugreifen können. Wenn ein Blockgerät von einer Instance getrennt wird, wird die Bereitstellung vom Betriebssystem aufgehoben und Sie können nicht mehr auf das Speichergerät zugreifen.

Linux-Instances — Die in der Blockgerätezuordnung angegebenen Gerätenamen werden den entsprechenden Blockgeräten zugeordnet, wenn die Instance zum ersten Mal gestartet wird. Die Instance-Typen bestimmen, welche Instance-Speicher-Volumes standardmäßig formatiert und aufgespielt werden. Sie können zusätzliche Instance-Speicher-Volumes zum Startzeitpunkt aufspielen, sofern die Anzahl der für den Instance-Typ verfügbaren Instance-Speicher-Volumes nicht überschritten wird. Weitere Informationen finden Sie unter Amazon EC2-Instance-Speicher. Der Blockgerät-Treiber für die Instance bestimmt, welche Geräte beim Formatieren und Aufspielen der Volumes verwendet werden.

Windows-Instanzen — Die in der Blockgerätezuordnung angegebenen Gerätenamen werden den entsprechenden Blockgeräten zugeordnet, wenn die Instanz zum ersten Mal gestartet wird. Anschließend initialisiert und mountet der Ec2Config-Dienst die Laufwerke. Der Root-Gerät-Volume wird als `C:\` aufgespielt. Die Instance-Speicher-Volumes werden als `Z:\`, `Y:\` aufgespielt usw. Zum Aufspielen eines EBS-Volume kann ein beliebiger verfügbarer Laufwerkbuchstabe verwendet werden. Sie können jedoch konfigurieren, wie Laufwerksbuchstaben EBS-Volumes zugewiesen werden. Weitere Informationen finden Sie unter. the section called “Konfigurieren Sie Windows-Startagenten”

AMI-Blockgerät-Zuweisung

Jedes AMI weist eine Blockgerät-Zuweisung auf, die die Blockgeräte angibt, die einer Instance beim Start des AMI angefügt werden sollen. Um einem AMI mehr Blockgeräte hinzuzufügen, müssen Sie Ihr eigenes AMI erstellen.

Inhalt

Angeben einer Blockgerät-Zuweisung für ein AMI

Beim Erstellen eines AMI können Volumes zusätzlich zum Root-Volume auf zwei Arten angegeben werden. Wenn Sie bereits Volumes einer ausgeführten Instance vor dem Erstellen eines AMI von der Instance angefügt haben, enthält die Blockgerät-Zuweisung für das AMI dieselben Volumes. Im Fall von EBS-Volumes werden die bestehenden Daten in einem neuen Snapshot gespeichert. Dieser neue Snapshot wird dann in der Blockgerät-Zuweisung angegeben. Im Fall von Instance-Speicher-Volumes werden die Daten nicht gespeichert.

Im Fall von EBS-Backed AMIs können Sie EBS-Volumes und Instance-Speicher-Volumes mit Blockgerät-Zuweisung hinzufügen. Im Fall von Instance Store-Backed AMIs können Sie Instance-Speicher-Volumes nur durch Änderung der Blockgerät-Zuweisungs-Einträge in der Image-Manifestdatei beim Registrieren des Images hinzufügen.

> **Note**
>
> Geben Sie für M3-Instances die Instance-Speicher-Volumes in der Blockgerät-Zuweisung für die Instance an, wenn Sie diese starten. Wenn Sie eine M3-Instance starten, werden in der

Blockgerät-Zuweisung für das AMI angegebene Instance-Speicher-Volumes möglicherweise ignoriert, wenn sie nicht als Teil der Instance-Blockgerät-Zuweisung angegeben werden.

Console

Hinzufügen von Volumes zu einem AMI mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie eine Instance und anschließend Actions (Aktionen), Image and templates (Image und Vorlagen), Create Image (Image erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für das neue Image ein.
5. Die Instance-Volumes werden unter Instance volumes (Instance-Volumes) angezeigt. Um ein weiteres Volume hinzuzufügen, wählen Sie Add volume (Volume hinzufügen).
6. Wählen Sie unter Volume type (Volume-Type) den Volume-Typen aus. Wählen Sie für Device (Gerät) den Gerätenamen aus. Für ein EBS-Volume können Sie zusätzliche Details wie einen Snapshot, eine Volume-Größe, einen Volume-Typ, IOPS und einen Verschlüsselungsstatus angeben.
7. Wählen Sie Create Image (Image erstellen) aus.

Command line

Hinzufügen von Volumes zu einem AMI mit der Befehlszeile

Verwenden Sie den AWS CLI Befehl create-image, um eine Blockgerätezuordnung für ein EBS-gestütztes AMI anzugeben. Verwenden Sie den AWS CLI Befehl register-image, um eine Blockgerätezuordnung für ein durch einen instance store-backed AMI anzugeben.

Geben Sie die Blockgerät-Zuweisung mit dem `--block-device-mappings`-Parameter an. Argumente, die in JSON kodiert sind, können entweder direkt in der Befehlszeile oder durch einen Verweis auf eine Datei bereitgestellt werden:

```
--block-device-mappings [mapping, ...]
--block-device-mappings [file://mapping.json]
```

Verwenden Sie das folgende Mapping, um ein Instance-Speicher-Volume hinzuzufügen.

```
{
    "DeviceName": "device_name",
    "VirtualName": "ephemeral0"
}
```

Verwenden Sie das folgende Mapping, um ein leeres 100 GiB-gp2-Volume hinzuzufügen:

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Verwenden Sie das folgende Mapping, um ein EBS-Volume basierend auf einem Snapshot hinzuzufügen.

```
{
    "DeviceName": "device_name",
    "Ebs": {
      "SnapshotId": "snap-xxxxxxxx"
    }
}
```

Um das Mapping für ein Gerät auszulassen, verwenden Sie das folgende Mapping.

```
{
    "DeviceName": "device_name",
    "NoDevice": ""
}
```

Alternativ können Sie den `-BlockDeviceMapping`-Parameter mit den folgenden Befehlen verwenden (AWS Tools for Windows PowerShell):

- New-EC2Image
- Register-EC2Image

Anzeigen der EBS-Volumes in einer AMI-Blockgerät-Zuweisung

Sie können die EBS-Volumes in der Blockgerät-Zuweisung für ein AMI leicht aufzählen.

Console

Anzeigen der EBS-Volumes für ein AMI mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie im Navigationsbereich die Option AMIs.
3. Wählen Sie EBS images (EBS-Images) in der Liste Filter aus, um eine Liste der EBS-Backed AMIs abzurufen.
4. Wählen Sie das gewünschte AMI aus und rufen Sie die Registerkarte Details auf. Für das Root-Gerät sind mindestens die folgenden Informationen verfügbar:

   - Root Device Type (Root-Gerätetyp (`ebs`)
   - Root Device Name (Root-Gerätename) (Beispiel: `/dev/sda1`)
   - Block Devices (Blockgeräte) (z. B. `/dev/sda1=snap-1234567890abcdef0:8:true`)

   Wenn das AMI mit zusätzlichen EBS-Volumes mit einer Blockgerät-Zuweisung erstellt wurde, wird im Feld Block Devices (Blockgeräte) ebenfalls die Zuweisung für diese zusätzlichen Volumes angezeigt. (Dieser Bildschirm zeigt keine Instance-Speicher-Volumes an.)

Command line

Anzeigen der EBS-Volumes für ein AMI mithilfe der Befehlszeile

Verwenden Sie den Befehl describe-images (AWS CLI) oder den Befehl Get-EC2Image(AWS Tools for Windows PowerShell), um die EBS-Volumes in der Blockgerätezuordnung für ein AMI aufzulisten.

Instance-Blockgerät-Zuweisung

Standardmäßig enthält eine gestartete Instance ein in der Blockgerät-Zuweisung der AMI, in der die Instance gestartet wurde, angegebenes Speichergerät. Alternativ können Sie Änderungen an der Blockgerät-Zuweisung für eine Instance bei deren Start angeben. Diese Aktualisierungen überschreiben dann die Blockgerät-Zuweisung der AMI bzw. werden in diese integriert.

Einschränkungen

- Im Fall des Root-Volumes kann ausschließlich Folgendes geändert werden: Volume-Größe, Volume-Typ und das Bei Beendigung löschen-Flag.
- Wenn Sie ein EBS-Volume ändern, können Sie dessen Größe verringern. Geben Sie deshalb einen Snapshot an, dessen Größe der in der Blockgerät-Zuweisung des AMI angegebenen entspricht bzw. größer als diese ist.

Inhalt

Aktualisieren der Blockgerät-Zuweisung beim Starten einer Instance

Sie können EBS-Volumes und Instance-Speicher-Volumes beim Starten zu einer Instance hinzufügen. Hinweis: Durch das Aktualisieren der Blockgerät-Zuweisung für eine Instance wird die Blockgerät-Zuweisung des AMI, von der sie gestartet wurde, nicht dauerhaft geändert.

Console

Hinzufügen von Volumes zu einer Instance mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole.
2. Wählen Sie auf dem Dashboard Launch Instance aus.
3. Wählen Sie auf der Seite Choose an Amazon Machine Image (AMI) (Amazon Machine Image (AMI) wählen) das gewünschte AMI und dann die Option Select (Auswählen).
4. Befolgen Sie im Assistenten die Anweisungen zu den Seiten Choose an Instance Type (Instance-Typ auswählen) und Configure Instance Details (Instance-Details konfigurieren).
5. Auf der Seite Add Storage (Speicher hinzufügen) können Sie das Root-Volume, EBS-Volumes und Instance-Speicher-Volumes wie folgt ändern:

   - Gehen Sie wie folgt vor, um die Größe des Root-Volumes zu ändern: Suchen Sie nach dem Volume Root unter der Spalte Type (Typ) und ändern Sie den Wert im Feld Size (Größe).

- Um ein EBS-Volume zu unterdrücken, das von der Blockgerät-Zuweisung des AMI angegeben wurde, mit dem die Instance gestartet wurde, klicken Sie auf das Symbol Delete (Löschen) des Volume.
- Um ein EBS-Volume hinzuzufügen, klicken Sie auf Add New Volume (Neues Volume hinzufügen), wählen Sie EBS in der Liste Type (Typ) und füllen Sie die Felder aus, u. a. Device (Gerät) und Snapshot.
- Um ein Instance-Speicher-Volume zu unterdrücken, das von der Blockgerät-Zuweisung des AMI angegeben wurde, mit dem die Instance gestartet wurde, klicken Sie auf das Symbol Delete (Löschen) des Volumes.
- Wählen Sie zum Hinzufügen eines Instance-Speicher-Volumes Add New Volume (Neues Volume hinzufügen), Instance Store (Instance-Speicher) in der Liste Type (Typ) und anschließend einen Gerätenamen unter Device (Gerät) aus.

6. Führen Sie die Schritte für die restlichen Seiten des Assistenten aus und wählen Sie anschließend die Option Launch (Start) aus.

Command line

Um Volumes zu einer Instance hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie den AWS CLI Befehl run-instances mit der `--block-device-mappings` Option, um beim Start eine Blockgerätezuordnung für eine Instance anzugeben.

Nehmen wir beispielsweise an, dass ein EBS-gestütztes AMI die folgende Blockgerätezuordnung für eine Linux-Instance spezifiziert:

- `/dev/sdb` = `ephemeral0`
- `/dev/sdh` = `snap-1234567890abcdef0`
- `/dev/sdj` = `100`

Verwenden Sie das folgende Mapping, damit `/dev/sdj` keiner von diesem AMI gestarteten Instance angefügt wird.

```
{
    "DeviceName": "/dev/sdj",
    "NoDevice": ""
}
```

Um die Größe von auf `/dev/sdh` zu erhöhen`300 GiB`, geben Sie die folgende Zuordnung an. Hinweis: Sie brauchen keine Snapshot-ID für `/dev/sdh` anzugeben, da die Angabe des Gerätenamens zur Bestimmung des Volumes ausreicht.

```
{
    "DeviceName": "/dev/sdh",
    "Ebs": {
      "VolumeSize": 300
    }
}
```

Um die Größe des Root-Volumes beim Start der Instance zu erhöhen, rufen Sie zuerst describe-images mit der ID des AMI auf, um den Gerätenamen des Root-Volumes zu überprüfen. Beispiel, `"RootDeviceName": "/dev/xvda"`. Um die Größe des Root-Volumes zu überschreiben, geben Sie den Gerätenamen des vom AMI verwendeten Root-Geräts und die neue Volume-Größe an.

```
{
    "DeviceName": "/dev/xvda",
    "Ebs": {
      "VolumeSize": 100
    }
}
```

Verwenden Sie das folgende Mapping, um ein Instance-Speicher-Volume, `/dev/sdc`, hinzuzufügen: Wenn der Instance-Typ nicht mehrere Instance-Speicher-Volumes unterstützt, hat das Mapping keine Wirkung. Wenn die Instance NVMe-Instance-Speicher-Volumes unterstützt, werden diese automatisch aufgelistet und es wird ein NVMe-Gerätename zugewiesen.

```
{
    "DeviceName": "/dev/sdc",
    "VirtualName": "ephemeral1"
}
```

Um einer Instance Volumes hinzuzufügen, verwenden Sie AWS Tools for Windows PowerShell

Verwenden Sie den `-BlockDeviceMapping` Parameter mit dem New-EC2InstanceBefehl (AWS Tools for Windows PowerShell).

Aktualisieren der Blockgerät-Zuweisung einer ausgeführten Instance

Sie können den AWS CLI Befehl modify-instance-attribute verwenden, um die Blockgeräte-Zuordnung einer laufenden Instance zu aktualisieren. Die Instance muss vor Änderung dieses Attributs nicht angehalten werden.

```
aws ec2 modify-instance-attribute --instance-id i-1a2b3c4d --block-device-mappings
 file://mapping.json
```

Beispiel: Um das Root-Volume beim Beenden der Instance zu speichern, geben Sie Folgendes in `mapping.json` an.

```
[
  {
    "DeviceName": "/dev/sda1",
    "Ebs": {
      "DeleteOnTermination": false
    }
  }
]
```

Alternativ können Sie den `-BlockDeviceMapping` Parameter mit dem Befehl () verwenden. Edit-EC2InstanceAttributeAWS Tools for Windows PowerShell

Anzeigen der EBS-Volumes in einer Instance-Blockgerät-Zuweisung

Sie können die EBS-Volumes, die einer Instance zugewiesen sind, leicht aufzählen.

> **Note**
>
> Bei Instances, die vor der Veröffentlichung der API vom 31.10.2009 gestartet wurden, AWS kann die Blockgeräte-Zuordnung nicht angezeigt werden. Sie müssen die Volumes trennen und wieder anhängen, damit die Blockgeräte-Zuordnung angezeigt AWS werden kann.

Console

Anzeigen der EBS-Volumes für eine Instance mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole.

2. Wählen Sie im Navigationsbereich Instances aus.
3. Geben Sie in das Suchfeld Root device type (Root-Gerätetyp) ein und wählen Sie EBS aus. Eine Liste mit EBS-Backed Instances wird angezeigt.
4. Wählen Sie die gewünschte Instance aus und zeigen Sie die Registerkarte Storage (Speicher) an. Für das Root-Gerät sind mindestens die folgenden Informationen verfügbar:

   - Root device type (Root-Gerätetyp) (zum Beispiel EBS)
   - Root device name (Root-Gerätename) (Beispiel: `/dev/xvda`)
   - Block devices (Blockgeräte) (z. B. `/dev/xvda`, `/dev/sdf` und `/dev/sdj`)

   Wenn die Instance mit zusätzlichen EBS-Volumes unter Verwendung einer Blockgeräte-Zuweisung gestartet wurde, werden diese unter Block devices (Blockgeräte) angezeigt. Auf dieser Registerkarte werden keine Instance-Speicher-Volumes angezeigt.
5. Um zusätzliche Informationen zu einem EBS-Volume anzuzeigen, wählen Sie seine Volume-ID aus, um zur Volume-Seite zu gelangen.

Command line

Anzeigen der EBS-Volumes für eine Instance mithilfe der Befehlszeile

Verwenden Sie den Befehl describe-instances (AWS CLI) oder den Befehl Get-EC2Instance(AWS Tools for Windows PowerShell), um die EBS-Volumes in der Blockgerätezuordnung für eine Instance aufzulisten.

Anzeigen der Instance-Blockgerät-Zuweisung für Instance-Speicher-Volumes

Der Instance-Typ bestimmt die Anzahl und den Typ der Instance-Speicher-Volumes, die für die Instance verfügbar sind. Wenn die Anzahl der Instance-Speicher-Volumes in einer Blockgerät-Zuweisung die für eine Instance verfügbare Anzahl an Instance-Speicher-Volumes übersteigt, werden die überzähligen Volumes ignoriert. Um die Instance-Speicher-Volumes für Ihre Instance anzuzeigen, führen Sie den lsblk Befehl aus (Linux-Instances) oder öffnen Sie die Windows-Datenträgerverwaltung (Windows-Instances). Informationen darüber, wie viele Instance-Speicher-Volumes von jedem Instance-Typ unterstützt werden, finden Sie in den Amazon EC2 EC2-Instance-Typspezifikationen.

Wenn Sie die Blockgerät-Zuweisung für die Instance anzeigen, werden ausschließlich die EBS-Volumes und nicht die Instance-Speicher-Volumes angezeigt. Welche Methode Sie verwenden, um die Instance-Speicher-Volumes für die Instance anzuzeigen, hängt vom Volume-Typ ab.

NVMe-Instance-Speicher-Volumes

Linux-Instances

Sie können das NVMe-Befehlszeilenpaket nvme-cli verwenden, um die Speichervolumes der NVMe-Instance in der Blockgerätezuordnung abzufragen. Laden Sie das Paket herunter, installieren Sie es auf Ihrer Instance und führen Sie dann den folgenden Befehl aus.

```
[ec2-user ~]$ sudo nvme list
```

Nachstehend finden Sie eine Beispielausgabe für eine Instance. Der Text in der Spalte Modell gibt an, ob das Volume ein EBS-Volume oder ein Instance-Speicher-Volume ist. In diesem Beispiel sind sowohl `/dev/nvme1n1` als auch `/dev/nvme2n1` Instance-Speicher-Volumes.

```
Node             SN                   Model
 Namespace
---------------- -------------------- ----------------------------------------
 ---------
/dev/nvme0n1     vol06afc3f8715b7a597 Amazon Elastic Block Store              1

/dev/nvme1n1     AWS2C1436F5159EB6614 Amazon EC2 NVMe Instance Storage        1

/dev/nvme2n1     AWSB1F4FF0C0A6C281EA Amazon EC2 NVMe Instance Storage        1
  ...
```

Windows-Instances

Sie können Disk Management oder verwenden, PowerShell um sowohl EBS- als auch Instance-Speicher-NVMe-Volumes aufzulisten. Weitere Informationen finden Sie unter the section called “Auflisten von NVMe-Volumes”.

HDD- oder SSD-Instance-Speicher-Volumes

Sie können Instance-Metadaten verwenden, um HDD- oder SSD-Instance-Speicher-Volumes in der Blockgerät-Zuweisung abzufragen. NVMe-Instance-Speicher-Volumes sind in der Blockgerät-Zuweisung nicht enthalten.

Die Basis-URI für alle Instance-Metadaten-Anfragen ist `http://169.254.169.254/latest/`. Weitere Informationen finden Sie unter Arbeiten mit Instance-Metadaten.

Linux-Instances

Stellen Sie zunächst eine Verbindung mit der ausgeführten Instance her. Rufen Sie von dieser Instance aus mithilfe der Abfrage die Blockgerät-Zuweisung ab.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/
```

Die Antwort enthält die Namen der Blockgeräte für die Instance. Die Ausgabe für eine Instance–Speicher basierte `m1.small`-Instance sieht beispielsweise folgendermaßen aus.

```
ami
ephemeral0
root
swap
```

Das `ami`-Gerät ist das Root-Gerät wie es von der Instance erfasst wird. Die Instance-Speicher-Volumes werden nach dem Schema `ephemeral[0-23]` benannt. Das `swap`-Gerät ist für die Seitendatei. Wenn Sie ebenfalls EBS-Volumes zugewiesen haben, werden sie als `ebs1`, `ebs2` usw. aufgeführt.

Um Details zu einzelnen Blockgeräten in der Blockgerät-Zuweisung abzurufen, hängen Sie den Namen wie hier gezeigt an die vorherige Abfrage an.

IMDSv2

```
[ec2-user ~]$ TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
```

```
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

IMDSv1

```
[ec2-user ~]$ curl http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Windows-Instances

Stellen Sie zunächst eine Verbindung mit der ausgeführten Instance her. Rufen Sie von dieser Instance aus mithilfe der Abfrage die Blockgerät-Zuweisung ab.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/
```

Die Antwort enthält die Namen der Blockgeräte für die Instance. Die Ausgabe für eine Instance–Speicher basierte `m1.small`-Instance sieht beispielsweise folgendermaßen aus.

```
ami
ephemeral0
root
swap
```

Das `ami`-Gerät ist das Root-Gerät wie es von der Instance erfasst wird. Die Instance-Speicher-Volumes werden nach dem Schema `ephemeral[0-23]` benannt. Das `swap`-Gerät ist für die Seitendatei. Wenn Sie ebenfalls EBS-Volumes zugewiesen haben, werden sie als `ebs1`, `ebs2` usw. aufgeführt.

Um Details zu einzelnen Blockgeräten in der Blockgerät-Zuweisung abzurufen, hängen Sie den Namen wie hier gezeigt an die vorherige Abfrage an.

```
PS C:\> Invoke-RestMethod -uri http://169.254.169.254/latest/meta-data/block-device-mapping/ephemeral0
```

Zuweisen von Datenträgern zu Volumes in Ihrer Windows-Instance

> **Note**
>
> Dieses Thema bezieht sich nur auf Windows-Instanzen.

Ihre Windows-Instance verfügt über ein EBS-Volume, das als Root-Volume dient. Wenn Ihre Windows-Instanz AWS PV- oder Citrix PV-Treiber verwendet, können Sie optional bis zu 25 Volumes hinzufügen, was insgesamt 26 Volumes ergibt. Weitere Informationen finden Sie unter Volume-Limits für Instances.

Je nach dem vorliegenden Instance-Typ können Sie Ihrer Instance zwischen 0 und 24 Instance-Speicher-Volumes zuordnen. Sie können die in einer Instance verfügbaren Instance-Speicher-Volumes verwenden, wenn Sie sie bei der Erstellung des entsprechenden AMIs oder beim Start der Instance angeben. Außerdem können Sie bei der Erstellung des entsprechenden AMIs oder beim Start der Instance weitere EBS-Volumes hinzufügen oder Sie ordnen sie zu, während die Instance ausgeführt wird.

Wenn Sie einer Instance ein Volume hinzufügen, geben Sie den Gerätenamen an, den Amazon EC2 verwendet. Weitere Informationen finden Sie unter Gerätenamen auf Amazon EC2 EC2-Instances. AWS Windows Amazon Machine Images (AMIs) enthalten eine Reihe von Treibern, mit denen Amazon EC2 dem Instance-Speicher und den EBS-Volumes Windows-Datenträger und -Laufwerkbuchstaben zuweist. Wenn Sie eine Instance von einem Windows-AMI aus starten, das AWS PV- oder Citrix PV-Treiber verwendet, können Sie die auf dieser Seite beschriebenen Beziehungen verwenden, um Ihre Windows-Festplatten Ihrem Instance-Speicher und Ihren EBS-Volumes zuzuordnen. Wenn das Windows-AMI Red Hat PV-Treiber verwendet, können Sie ein Upgrade Ihrer Instance auf Citrix-Treiber durchführen. Weitere Informationen finden Sie unter the section called “Upgrade für PV-Treiber”.

Inhalt

Auflisten von NVMe-Volumes

Sie können die Datenträger in Ihrer Windows-Instances auch mithilfe der Datenträgerverwaltung oder Powershell anzeigen.

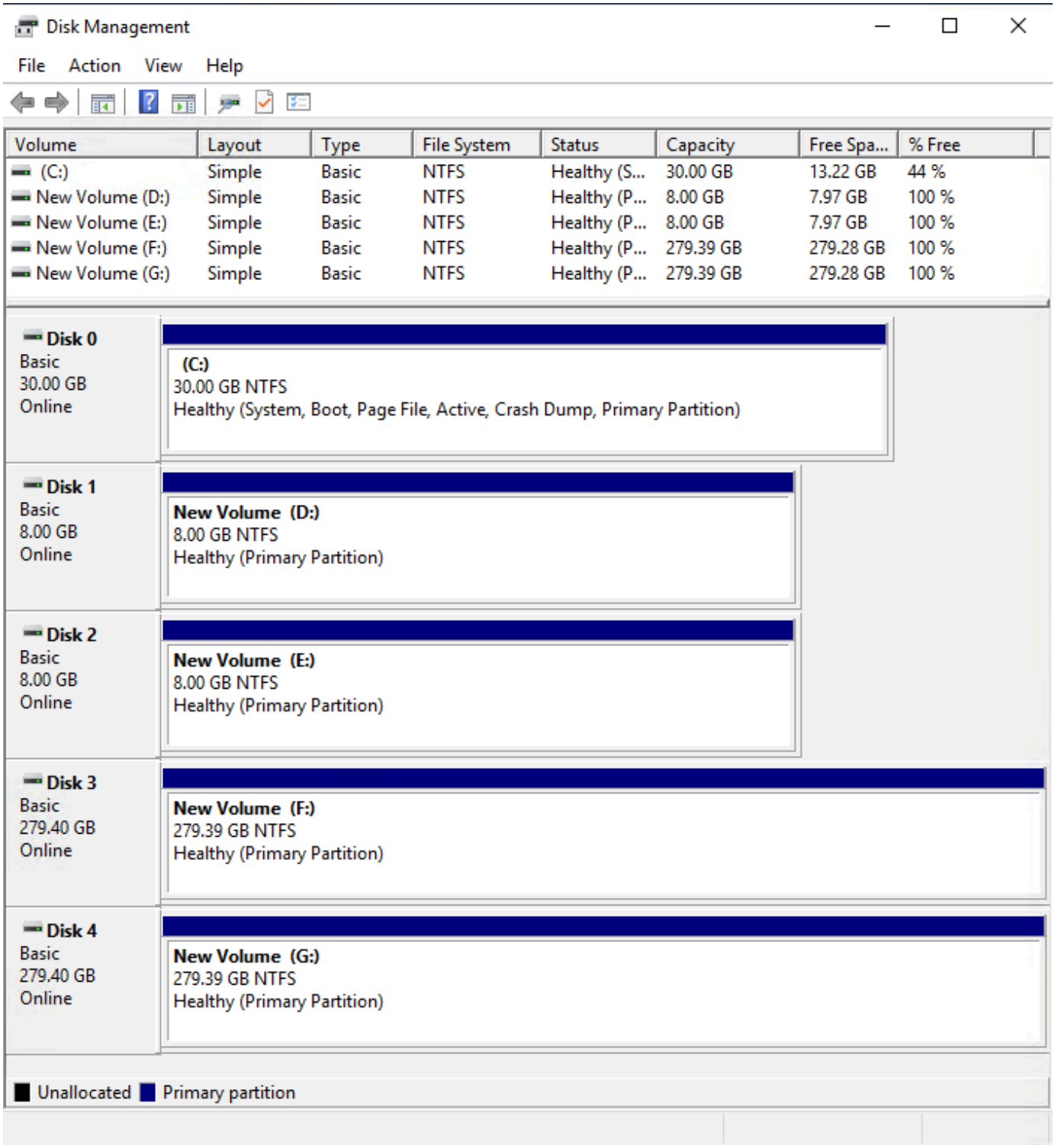
Auflisten von NVMe-Festplatten mit Datenträgerverwaltung

Sie können die Datenträger in Ihrer Windows-Instances auch mithilfe der Datenträgerverwaltung anzeigen.

So zeigen Sie die Datenträger in Ihrer Windows-Instance an

1. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer -Windows-Instance.
2. Starten Sie das Dienstprogramm für die Datenträgerverwaltung.
3. Überprüfen Sie die Datenträger. Das Root-Volume ist ein EBS-Volume, das unter `C:\` gemountet ist. Wenn keine weiteren Datenträger angezeigt werden, haben Sie keine zusätzlichen Volumes angegeben, als Sie das AMI erstellt bzw. die Instance gestartet haben.

   Das folgende Beispiel zeigt die verfügbaren Datenträger beim Start einer `r5d.4xlarge`-Instance mit zwei zusätzlichen EBS-Volumes.


Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (S... 30.00 GB 13.22 GB 44 %
New Volume (D:) Simple Basic NTFS Healthy (P... 8.00 GB 7.97 GB 100 %
New Volume (E:) Simple Basic NTFS Healthy (P... 8.00 GB 7.97 GB 100 %
New Volume (F:) Simple Basic NTFS Healthy (P... 279.39 GB 279.28 GB 100 %
New Volume (G:) Simple Basic NTFS Healthy (P... 279.39 GB 279.28 GB 100 %
Disk 0
Basic
30.00 GB
Online
(C:)
30.00 GB NTFS
Healthy (System, Boot, Page File, Active, Crash Dump, Primary Partition)
Disk 1
Basic
8.00 GB
Online
New Volume (D:)
8.00 GB NTFS
Healthy (Primary Partition)
Disk 2
Basic
8.00 GB
Online
New Volume (E:)
8.00 GB NTFS
Healthy (Primary Partition)
Disk 3
Basic
279.40 GB
Online
New Volume (F:)
279.39 GB NTFS
Healthy (Primary Partition)
Disk 4
Basic
279.40 GB
Online
New Volume (G:)
279.39 GB NTFS
Healthy (Primary Partition)
Unallocated
Primary partition

NVMe-Festplatten auflisten mit PowerShell

Das folgende PowerShell Skript listet jede Festplatte sowie den entsprechenden Gerätenamen und das entsprechende Volume auf. Es ist für die Verwendung mit Instances vorgesehen, die auf dem AWS Nitro-System basieren und NVMe EBS und Instance-Speicher-Volumes verwenden.

Connect zu Ihrer Windows-Instanz her und führen Sie den folgenden Befehl aus, um die PowerShell Skriptausführung zu aktivieren.

```
Set-ExecutionPolicy RemoteSigned
```

Kopieren Sie das folgende Skript und speichern Sie es unter Ihrer Windows-Instance als `mapping.ps1`.

```
# List the disks for NVMe volumes

function Get-EC2InstanceMetadata {
    param([string]$Path)
    (Invoke-WebRequest -Uri "http://169.254.169.254/latest/$Path").Content
}

function GetEBSVolumeId {
    param($Path)
    $SerialNumber = (Get-Disk -Path $Path).SerialNumber
    if($SerialNumber -clike 'vol*'){
        $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("vol","vol-")
    }
    else {
       $EbsVolumeId = $SerialNumber.Substring(0,20).Replace("AWS","AWS-")
    }
    return $EbsVolumeId
}

function GetDeviceName{
    param($EbsVolumeId)
    if($EbsVolumeId -clike 'vol*'){

        $Device  = ((Get-EC2Volume -VolumeId $EbsVolumeId ).Attachment).Device
        $VolumeName = ""
    }
     else {
        $Device = "Ephemeral"
```

```
        $VolumeName = "Temporary Storage"
    }
    Return $Device,$VolumeName
}

function GetDriveLetter{
    param($Path)
    $DiskNumber =  (Get-Disk -Path $Path).Number
    if($DiskNumber -eq 0){
        $VirtualDevice = "root"
        $DriveLetter = "C"
        $PartitionNumber = (Get-Partition -DriveLetter C).PartitionNumber
    }
    else
    {
        $VirtualDevice = "N/A"
        $DriveLetter = (Get-Partition -DiskNumber $DiskNumber).DriveLetter
        if(!$DriveLetter)
        {
            $DriveLetter = ((Get-Partition -DiskId $Path).AccessPaths).Split(",")[0]
        }
        $PartitionNumber = (Get-Partition -DiskId $Path).PartitionNumber
    }

    return $DriveLetter,$VirtualDevice,$PartitionNumber

}

$Report = @()
foreach($Path in (Get-Disk).Path)
{
    $Disk_ID = ( Get-Partition -DiskId $Path).DiskId
    $Disk = ( Get-Disk -Path $Path).Number
    $EbsVolumeId  = GetEBSVolumeId($Path)
    $Size =(Get-Disk -Path $Path).Size
    $DriveLetter,$VirtualDevice, $Partition = (GetDriveLetter($Path))
    $Device,$VolumeName = GetDeviceName($EbsVolumeId)
    $Disk = New-Object PSObject -Property @{
      Disk          = $Disk
      Partitions    = $Partition
      DriveLetter   = $DriveLetter
      EbsVolumeId   = $EbsVolumeId
      Device        = $Device
      VirtualDevice = $VirtualDevice
```

```
      VolumeName= $VolumeName
    }
 $Report += $Disk
}

$Report | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions,
 DriveLetter, EbsVolumeId, Device, VirtualDevice, VolumeName
```

Führen Sie das Skript wie folgt aus:

```
PS C:\> .\mapping.ps1
```

Im Folgenden finden Sie eine Beispielausgabe für eine Instance mit einem Root-Volume, zwei EBS-Volumes und zwei Instance-Speicher-Volumes.

```
Disk Partitions DriveLetter EbsVolumeId           Device    VirtualDevice VolumeName
---- ---------- ----------- -----------           ------    ------------- ----------
   0          1 C           vol-03683f1d861744bc7 /dev/sda1 root
   1          1 D           vol-082b07051043174b9 xvdb      N/A
   2          1 E           vol-0a4064b39e5f534a2 xvdc      N/A
   3          1 F           AWS-6AAD8C2AEEE1193F0 Ephemeral N/A           Temporary
 Storage
   4          1 G           AWS-13E7299C2BD031A28 Ephemeral N/A           Temporary
 Storage
```

Wenn Sie Ihre Anmeldeinformationen für Tools für Windows PowerShell auf der Windows-Instance nicht konfiguriert haben, kann das Skript die EBS-Volume-ID nicht abrufen und verwendet N/A in der `EbsVolumeId` Spalte.

Zuordnen von NVMe-EBS-Volumes

Bei Instances, die auf dem AWS Nitro-System basieren, werden EBS-Volumes als NVMe-Geräte bereitgestellt. Mit dem Befehl Get-Disk können Sie EBS-Volume-IDs Windows-Disknummern zuordnen.

```
PS C:\> Get-Disk
Number Friendly Name Serial Number                   HealthStatus
 OperationalStatus      Total Size Partition

                     Style
------ ------------ -------------                   ------------
 -----------------      ---------- ----------
```

```
3      NVMe Amazo... AWS6AAD8C2AEEE1193F0_00000001.   Healthy            Online
             279.4 GB MBR
4      NVMe Amazo... AWS13E7299C2BD031A28_00000001.   Healthy            Online
             279.4 GB MBR
2      NVMe Amazo... vol0a4064b39e5f534a2_00000001.   Healthy            Online
               8 GB MBR
0      NVMe Amazo... vol03683f1d861744bc7_00000001.   Healthy            Online
              30 GB MBR
1      NVMe Amazo... vol082b07051043174b9_00000001.   Healthy            Online
               8 GB MBR
```

Sie können auch den Befehl ebsnvme-id ausführen, um die NVMe-Datenträgernummern EBS-Volume-IDs und Gerätenamen zuzuordnen.

```
PS C:\> C:\PROGRAMDATA\Amazon\Tools\ebsnvme-id.exe
Disk Number: 0
Volume ID: vol-03683f1d861744bc7
Device Name: sda1

Disk Number: 1
Volume ID: vol-082b07051043174b9
Device Name: xvdb

Disk Number: 2
Volume ID: vol-0a4064b39e5f534a2
Device Name: xvdc
```

Auflisten von Volumes

Sie können die Datenträger in Ihrer Windows-Instances auch mithilfe der Datenträgerverwaltung oder Powershell anzeigen.

Auflisten von Festplatten mit Datenträgerverwaltung

Sie können die Datenträger in Ihrer Windows-Instances auch mithilfe der Datenträgerverwaltung anzeigen.

So zeigen Sie die Datenträger in Ihrer Windows-Instance an

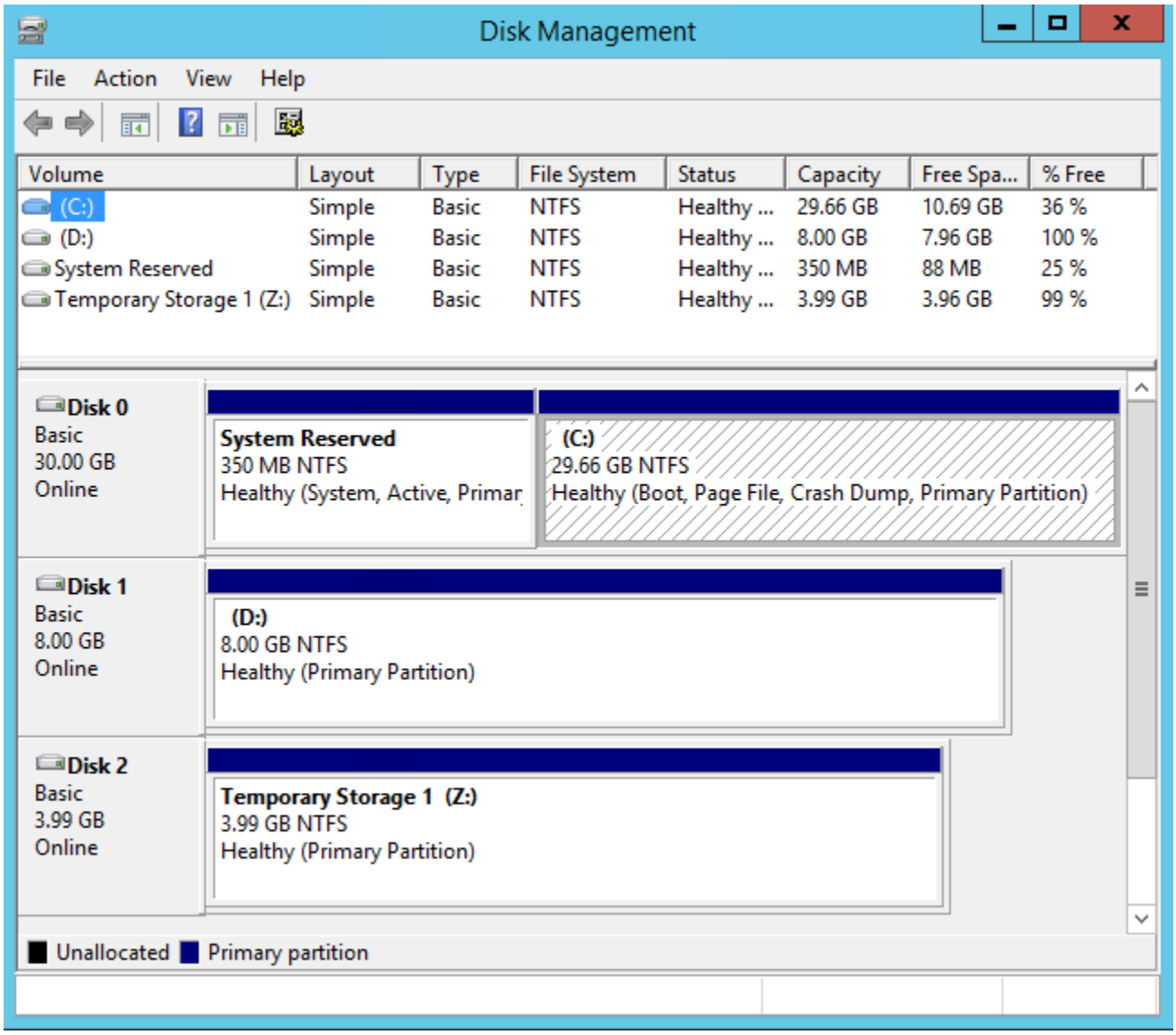
1. Melden Sie sich per Remotedesktop an Ihrer Windows-Instance an. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer -Windows-Instance.

2. Starten Sie das Dienstprogramm für die Datenträgerverwaltung.

   Klicken Sie in der Taskleiste mit der rechten Maustaste auf das Windows-Logo und wählen Sie dann Disk Management.

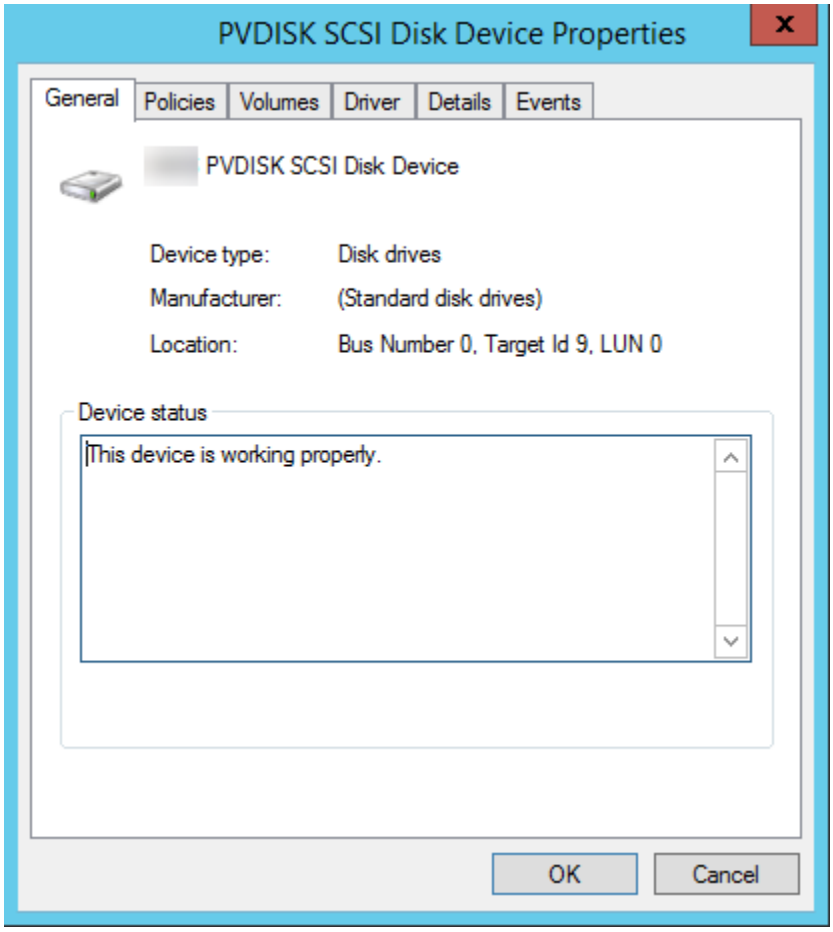
3. Überprüfen Sie die Datenträger. Das Root-Volume ist ein EBS-Volume, das unter `C:\` gemountet ist. Wenn keine weiteren Datenträger angezeigt werden, haben Sie keine zusätzlichen Volumes angegeben, als Sie das AMI erstellt bzw. die Instance gestartet haben.

   Das folgende Beispiel zeigt die verfügbaren Datenträger beim Start einer `m3.medium`-Instance mit einem Instance-Speicher-Volume (Disk 2) und einem zusätzlichen EBS Volume (Disk 1).



4. Klicken Sie mit der rechten Maustaste auf den grauen Bereich mit der Bezeichnung "Datenträger 1" und wählen Sie dann die Option Eigenschaften. Notieren Sie sich den Wert unter Location (Speicherort) und schlagen Sie ihn in den Tabellen unter Zuordnen von Datenträgergeräten

an Gerätenamen nach. Für den folgenden Datenträger wird als Speicherort z. B. der Wert„Bus Number 0, Target Id 9, LUN 0” angezeigt. Laut der Tabelle für EBS-Volumes lautet der Gerätename für diesen Speicherort `xvdj`.



Zuordnen von Datenträgergeräten an Gerätenamen

Der Blockgerät-Treiber für die Instance weist die tatsächlichen Volume-Namen beim Aufspielen der Volumes zu.

Mappings

- Instance-Speicher-Volumes
- EBS-Datenträger

Instance-Speicher-Volumes

In der folgenden Tabelle wird beschrieben, wie die Citrix PV- und AWS PV-Treiber Windows-Volumes, die keine NVMe-Instanzspeicher sind, zuordnen. Die Anzahl der verfügbaren Instance-

Speicher-Volumes wird von dem jeweiligen Instance-Typ bestimmt. Weitere Informationen finden Sie unter Instance-Speicher-Volumes.

Ort	Gerätename
Bus Number 0, Target ID 78, LUN 0	xvdca
Bus Number 0, Target ID 79, LUN 0	xvdcb
Bus Number 0, Target ID 80, LUN 0	xvdcc
Bus Number 0, Target ID 81, LUN 0	xvdcd
Bus Number 0, Target ID 82, LUN 0	xvdce
Bus Number 0, Target ID 83, LUN 0	xvdcf
Bus Number 0, Target ID 84, LUN 0	xvdcg
Bus Number 0, Target ID 85, LUN 0	xvdch
Bus Number 0, Target ID 86, LUN 0	xvdci
Bus Number 0, Target ID 87, LUN 0	xvdcj
Bus Number 0, Target ID 88, LUN 0	xvdck
Bus Number 0, Target ID 89, LUN 0	xvdcl

EBS-Datenträger

In der folgenden Tabelle wird beschrieben, wie die Citrix PV- und AWS PV-Treiber Nicht-NVMe-EBS-Volumes Windows-Volumes zuordnen.

Ort	Gerätename
Bus Number 0, Target ID 0, LUN 0	/dev/sda1
Bus Number 0, Target ID 1, LUN 0	xvdb

Ort	Gerätename
Bus Number 0, Target ID 2, LUN 0	xvdc
Bus Number 0, Target ID 3, LUN 0	xvdd
Bus Number 0, Target ID 4, LUN 0	xvde
Bus Number 0, Target ID 5, LUN 0	xvdf
Bus Number 0, Target ID 6, LUN 0	xvdg
Bus Number 0, Target ID 7, LUN 0	xvdh
Bus Number 0, Target ID 8, LUN 0	xvdi
Bus Number 0, Target ID 9, LUN 0	xvdj
Bus Number 0, Target ID 10, LUN 0	xvdk
Bus Number 0, Target ID 11, LUN 0	xvdl
Bus Number 0, Target ID 12, LUN 0	xvdm
Bus Number 0, Target ID 13, LUN 0	xvdn
Bus Number 0, Target ID 14, LUN 0	xvdo
Bus Number 0, Target ID 15, LUN 0	xvdp
Bus Number 0, Target ID 16, LUN 0	xvdq
Bus Number 0, Target ID 17, LUN 0	xvdr
Bus Number 0, Target ID 18, LUN 0	xvds
Bus Number 0, Target ID 19, LUN 0	xvdt
Bus Number 0, Target ID 20, LUN 0	xvdu
Bus Number 0, Target ID 21, LUN 0	xvdv

Ort	Gerätename
Bus Number 0, Target ID 22, LUN 0	xvdw
Bus Number 0, Target ID 23, LUN 0	xvdx
Bus Number 0, Target ID 24, LUN 0	xvdy
Bus Number 0, Target ID 25, LUN 0	xvdz

Listet Festplatten auf mit PowerShell

Das folgende PowerShell Skript listet alle Festplatten sowie den zugehörigen Gerätenamen und das entsprechende Volume auf.

Anforderungen und Einschränkungen

- Erfordert Windows Server 2012 oder höher.
- Erfordert Anmeldedaten, um die EBS-Volume-ID zu erhalten Sie können ein Profil mit den Tools für PowerShell konfigurieren oder der Instanz eine IAM-Rolle zuweisen.
- Unterstützt keine NVMe-Volumes.
- Unterstützt keine dynamischen Festplatten.

Connect zu Ihrer Windows-Instanz her und führen Sie den folgenden Befehl aus, um die PowerShell Skriptausführung zu aktivieren.

```
Set-ExecutionPolicy RemoteSigned
```

Kopieren Sie das folgende Skript und speichern Sie es unter Ihrer Windows-Instance als `mapping.ps1`.

```
# List the disks
function Convert-SCSITargetIdToDeviceName {
  param([int]$SCSITargetId)
  If ($SCSITargetId -eq 0) {
    return "sda1"
  }
  $deviceName = "xvd"
  If ($SCSITargetId -gt 25) {
```

```
    $deviceName += [char](0x60 + [int]($SCSITargetId / 26))
  }
  $deviceName += [char](0x61 + $SCSITargetId % 26)
  return $deviceName
}

[string[]]$array1 = @()
[string[]]$array2 = @()
[string[]]$array3 = @()
[string[]]$array4 = @()

Get-WmiObject Win32_Volume | Select-Object Name, DeviceID | ForEach-Object {
  $array1 += $_.Name
  $array2 += $_.DeviceID
}

$i = 0
While ($i -ne ($array2.Count)) {
  $array3 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).SerialNumber) -
replace "_[^ ]*$" -replace "vol", "vol-"
  $array4 += ((Get-Volume -Path $array2[$i] | Get-Partition | Get-Disk).FriendlyName)
  $i ++
}

[array[]]$array = $array1, $array2, $array3, $array4

Try {
  $InstanceId = Get-EC2InstanceMetadata -Category "InstanceId"
  $Region = Get-EC2InstanceMetadata -Category "Region" | Select-Object -ExpandProperty
 SystemName
}
Catch {
  Write-Host "Could not access the instance Metadata using AWS Get-EC2InstanceMetadata
 CMDLet.
Verify you have AWSPowershell SDK version '3.1.73.0' or greater installed and Metadata
 is enabled for this instance." -ForegroundColor Yellow
}
Try {
  $BlockDeviceMappings = (Get-EC2Instance -Region $Region -Instance
 $InstanceId).Instances.BlockDeviceMappings
  $VirtualDeviceMap = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").GetEnumerator() | Where-Object { $_.Key -ne "ami" }
}
Catch {
```

```
  Write-Host "Could not access the AWS API, therefore, VolumeId is not available.
Verify that you provided your access keys or assigned an IAM role with adequate
 permissions." -ForegroundColor Yellow
}

Get-disk | ForEach-Object {
  $DriveLetter = $null
  $VolumeName = $null
  $VirtualDevice = $null
  $DeviceName = $_.FriendlyName

  $DiskDrive = $_
  $Disk = $_.Number
  $Partitions = $_.NumberOfPartitions
  $EbsVolumeID = $_.SerialNumber -replace "_[^ ]*$" -replace "vol", "vol-"
  if ($Partitions -ge 1) {
    $PartitionsData = Get-Partition -DiskId $_.Path
    $DriveLetter = $PartitionsData.DriveLetter | Where-object { $_ -notin @("",
 $null) }
    $VolumeName = (Get-PSDrive | Where-Object { $_.Name -in
 @($DriveLetter) }).Description | Where-object { $_ -notin @("", $null) }
  }
  If ($DiskDrive.path -like "*PROD_PVDISK*") {
    $BlockDeviceName = Convert-SCSITargetIdToDeviceName((Get-WmiObject -Class
 Win32_Diskdrive | Where-Object { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" +
 $DiskDrive.Number) }).SCSITargetId)
    $BlockDeviceName = "/dev/" + $BlockDeviceName
    $BlockDevice = $BlockDeviceMappings | Where-Object { $BlockDeviceName -like "*" +
 $_.DeviceName + "*" }
    $EbsVolumeID = $BlockDevice.Ebs.VolumeId
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
 $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON_EC2_NVME*") {
    $BlockDeviceName = (Get-EC2InstanceMetadata -Category
 "BlockDeviceMapping").ephemeral((Get-WmiObject -Class Win32_Diskdrive | Where-Object
 { $_.DeviceID -eq ("\\.\PHYSICALDRIVE" + $DiskDrive.Number) }).SCSIPort - 2)
    $BlockDevice = $null
    $VirtualDevice = ($VirtualDeviceMap.GetEnumerator() | Where-Object { $_.Value -eq
 $BlockDeviceName }).Key | Select-Object -First 1
  }
  ElseIf ($DiskDrive.path -like "*PROD_AMAZON*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
```

```
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
$EbsVolumeID }).DeviceName
  }
  ElseIf ($DiskDrive.path -like "*NETAPP*") {
    if ($DriveLetter -match '[^a-zA-Z0-9]') {
      $i = 0
      While ($i -ne ($array3.Count)) {
        if ($array[2][$i] -eq $EbsVolumeID) {
          $DriveLetter = $array[0][$i]
          $DeviceName = $array[3][$i]
        }
        $i ++
      }
    }
    $EbsVolumeID = "FSxN Volume"
    $BlockDevice = ""
    $BlockDeviceName = ($BlockDeviceMappings | Where-Object { $_.ebs.VolumeId -eq
$EbsVolumeID }).DeviceName
  }
  Else {
    $BlockDeviceName = $null
    $BlockDevice = $null
  }
  New-Object PSObject -Property @{
    Disk          = $Disk;
    Partitions    = $Partitions;
    DriveLetter   = If ($DriveLetter -eq $null) { "N/A" } Else { $DriveLetter };
    EbsVolumeId   = If ($EbsVolumeID -eq $null) { "N/A" } Else { $EbsVolumeID };
    Device        = If ($BlockDeviceName -eq $null) { "N/A" } Else
{ $BlockDeviceName };
    VirtualDevice = If ($VirtualDevice -eq $null) { "N/A" } Else { $VirtualDevice };
    VolumeName    = If ($VolumeName -eq $null) { "N/A" } Else { $VolumeName };
    DeviceName    = If ($DeviceName -eq $null) { "N/A" } Else { $DeviceName };
  }
```

```
} | Sort-Object Disk | Format-Table -AutoSize -Property Disk, Partitions, DriveLetter,
 EbsVolumeId, Device, VirtualDevice, DeviceName, VolumeName
```

Führen Sie das Skript wie folgt aus:

```
PS C:\> .\mapping.ps1
```

Es folgt eine Beispielausgabe.

```
Disk  Partitions  DriveLetter   EbsVolumeId             Device      VirtualDevice
 DeviceName              VolumeName
----  ----------  -----------   -----------             ------      -------------
 ----------              ----------
   0           1            C   vol-0561f1783298efedd   /dev/sda1   N/A
 NVMe Amazon Elastic B   N/A
   1           1            D   vol-002a9488504c5e35a   xvdb        N/A
 NVMe Amazon Elastic B   N/A
   2           1            E   vol-0de9d46fcc907925d   xvdc        N/A
 NVMe Amazon Elastic B   N/A
```

Wenn Sie Ihre Anmeldeinformationen für die Windows-Instance nicht angegeben haben, kann das Skript die EBS-Volume-ID nicht erhalten und verwendet N/A in der `EbsVolumeId`-Spalte.

Anwendungskonsistente Windows VSS-basierte Amazon EBS-Snapshots

> **Note**
>
> Anwendungskonsistente Windows VSS-basierte Snapshots werden nur mit Windows-Instances unterstützt.

Mit Run Command können Sie anwendungskonsistente Snapshots aller Amazon EBS-Volumes erstellen, die an Ihre Amazon EC2 EC2-Windows-Instances angehängt sind.AWS Systems Manager Der Snapshot-Vorgang erstellt mit dem Windows Volume Shadow Copy Service (VSS) Backups VSS-fähiger Anwendungen auf EBS-Volume-Ebene. Dazu gehören auch Daten von schwebenden Transaktionen zwischen diesen Anwendungen und dem Datenträger. Sie müssen Ihre Instances

nicht herunterfahren oder trennen, wenn Sie ein Backup aller angefügten Volumes durchführen möchten.

Für die Verwendung von VSS-basierten EBS-Snapshots fallen keine zusätzlichen Kosten an. Sie zahlen nur für die EBS-Snapshots, die durch den Backup-Vorgang erstellt werden. Weitere Informationen finden Sie unter Wie werden mir meine Amazon EBS EBS-Snapshots in Rechnung gestellt?

Inhalt

Was ist -VSS?

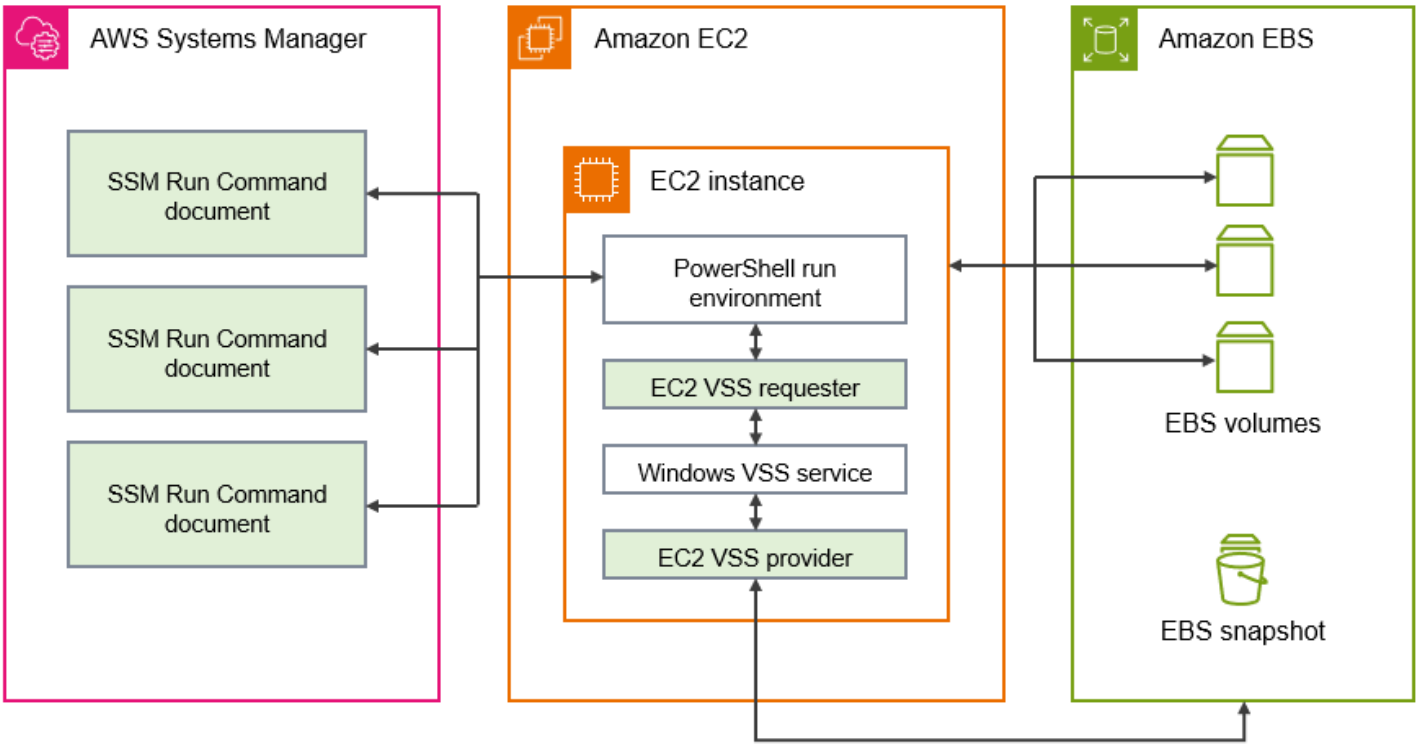
Volume Snapshot Copy Service (VSS) ist eine Backup- und Wiederherstellungstechnologie, die in Microsoft Windows enthalten ist. Es kann Backup-Kopien oder Snapshots von Computerdateien oder Volumes erstellen, während diese verwendet werden. Weitere Informationen finden Sie unter Volume Shadow Copy Service.

Die folgenden Softwarekomponenten sind an der Erstellung eines anwendungskonsistenten Snapshots beteiligt.

- VSS-Service – Teil des Windows-Betriebssystems
- VSS-Anforderer – Die Software, die die Erstellung von Schattenkopien anfordert
- VSS-Writer – Wird in der Regel als Teil einer Anwendung, wie z. B. SQL Server, bereitgestellt, um einen konsistenten Datensatz für das Backup sicherzustellen
- VSS-Anbieter – Die Komponente, die die Schattenkopien der zugrunde liegenden Volumes erstellt

Die auf Windows VSS basierende Amazon EBS-Snapshot-Lösung besteht aus mehreren Systems Manager (SSM) Run Command-Dokumenten, die die Erstellung von Backups erleichtern, und einem Systems Manager Distributor-Paket namens`AwsVssComponents`, das einen EC2-VSS-Requester

und einen EC2-VSS-Anbieter umfasst. Das Paket `AwsVssComponents` muss auf EC2-Windows-Instances installiert werden, um anwendungskonsistente Snapshots von EBS-Volumes erstellen zu können. Die folgende Abbildung zeigt die Beziehung zwischen diesen Softwarekomponenten.



So funktioniert die VSS-basierte Amazon EBS-Snapshot-Lösung

Der Prozess zur Erstellung anwendungskonsistenter, VSS-basierter EBS-Snapshot-Skripts besteht aus den folgenden Schritten.

1. Arbeiten Sie Voraussetzungen durch.
2. Geben Sie Parameter für das SSM-Dokument `AWSEC2-VssInstallAndSnapshot` ein und führen Sie dieses Dokument mit Run Command aus. Weitere Informationen finden Sie unter Führen Sie das AWSEC VssInstallAndSnapshot 2-Befehlsdokument aus (empfohlen).
3. Der Windows VSS-Service auf Ihrer Instance koordiniert alle laufenden I/O-Vorgänge für laufende Anwendungen.
4. Das System bereinigt alle I/O-Puffer und hält alle I/O-Vorgänge vorübergehend an. Die Unterbrechung dauert maximal zehn Sekunden.
5. Während der Unterbrechung erstellt das System Snapshots aller Volumes, die an die Instance angehängt sind.
6. Die Unterbrechung wird aufgehoben und der I/O-Vorgang fortgesetzt.

7. Das System fügt alle neu erstellten Snapshots zu der Liste der EBS-Snapshots hinzu. Das System kennzeichnet alle VSS-fähigen EBS-Snapshots, die durch diesen Prozess erfolgreich erstellt wurden, mit:true. AppConsistent
8. Falls Sie eine Wiederherstellung von einem Snapshot aus vornehmen müssen, können Sie hierfür den EBS-Standardvorgang zum Erstellen eines Volumes aus einem Snapshot verwenden oder alle Volumes in einer Instance wiederherstellen, indem Sie ein Beispielskript verwenden. Dieses Verfahren wird in Wiederherstellen von EBS-Volumes von VSS-fähigen EBS-Snapshots beschrieben.

Voraussetzungen

Sie können VSS-basierte EBS-Snapshots mit Systems Manager Run Command oder Amazon Data AWS Backup Lifecycle Manager erstellen. Die folgenden Voraussetzungen gelten für alle Lösungen.

Voraussetzungen

- Systemanforderungen
- IAM-Berechtigungen
- VSS-Komponenten

Systemanforderungen

Installieren Sie den Systems Manager Agent

VSS wird vom AWS Systems Manager (Systems Manager) unter Verwendung von orchestriert. PowerShell Auf Ihrer EC2-Instance muss die SSM-Agent-Version `3.0.502.0` oder höher installiert sein. Wenn Sie bereits eine ältere Version von SSM-Agent verwenden, aktualisieren Sie diese mithilfe von Run Command. Weitere Informationen finden Sie unter Einrichtung von Systems Manager für Amazon EC2-Instances und Arbeiten mit SSM-Agent auf Amazon-EC2-Instances für Windows Server im AWS Systems Manager -Benutzerhandbuch.

Amazon EC2-Windows Instance-Anforderungen

VSS-basierte EBS-Snapshots werden für Instanzen unterstützt, auf denen Windows Server 2012 und höher ausgeführt wird. Informationen zu älteren Versionen von Windows finden Sie in der Tabelle zur Unterstützung von Windows-Versionen unter AWS Versionsverlauf der VSS-Lösung.

.NET Framework-Version

Das `AwsVssComponents`-Paket erfordert .NET Framework der Version `4.6` oder höher. Windows-Betriebssystemversionen vor Windows Server 2016 verwenden standardmäßig eine frühere Version von.NET Framework. Wenn Ihre Instanz eine frühere Version von.NET Framework verwendet, müssen Sie Version `4.6` oder höher mit Windows Update installieren.

AWS Tools for Windows PowerShell Version

Stellen Sie sicher, dass auf Ihrer Instance AWS Tools for Windows PowerShell Version `3.3.48.0` oder höher ausgeführt wird. Um Ihre Version zu überprüfen, führen Sie den folgenden Befehl im PowerShell Terminal der Instance aus.

```
C:\> Get-AWSPowerShellVersion
```

Wenn Sie AWS Tools for Windows PowerShell auf Ihrer Instance ein Update durchführen müssen, finden Sie weitere Informationen unter Installation von AWS Tools for Windows PowerShell im AWS Tools for Windows PowerShell Benutzerhandbuch.

PowerShell Windows-Version

Stellen Sie sicher, dass auf Ihrer Instance die PowerShell Windows-Hauptversion`3`,`4`, oder ausgeführt wird`5`. Um Ihre Version zu überprüfen, führen Sie den folgenden Befehl in einem PowerShell Terminal auf der Instance aus.

```
C:\> $PSVersionTable.PSVersion
```

PowerShell Sprachmodus

Stellen Sie sicher, dass für Ihre Instanz der PowerShell Sprachmodus auf eingestellt ist`FullLanguage`. Weitere Informationen finden Sie unter about_Language_Modes in der Microsoft-Dokumentation.

IAM-Berechtigungen

Die IAM-Rolle, die Ihrer Amazon EC2 EC2-Windows-Instance zugeordnet ist, muss über die Berechtigung verfügen, anwendungskonsistente Snapshots mit VSS zu erstellen. Um die erforderlichen Berechtigungen zu gewähren, können Sie die Richtlinie an Ihr Instance-Profil anhängen. `AWSEC2VssSnapshotPolicy`

Die Richtlinie ermöglicht es Systems Manager, die folgenden Aktionen durchzuführen:

- EBS-Snapshots erstellen und taggen
- Amazon Machine Images (AMIs) erstellen und taggen
- Hängen Sie Metadaten wie die Geräte-ID an die von VSS erstellten Standard-Snapshot-Tags an.

Themen

Hängen Sie die VSS-fähige Snapshot-Richtlinie an Ihr Instanzprofil an

Um Berechtigungen für VSS-fähige Snapshots für Ihre Instance zu gewähren, fügen Sie die AWSEC2VssSnapshotPolicy verwaltete Richtlinie wie folgt Ihrer Instanzprofilrolle hinzu. Es ist wichtig sicherzustellen, dass Ihre Instanz alle Anforderungen erfüllt. Systemanforderungen

> **Note**
>
> Um die verwaltete Richtlinie verwenden zu können, muss auf Ihrer Instanz die `AwsVssComponents` Paketversion `2.3.1` oder eine neuere Version installiert sein. Informationen zum Versionsverlauf finden Sie unterAwsVssComponents Paketversionen. Wenn Sie eine frühere Version des `AwsVssComponents` Pakets auf Ihrer Instanz installiert haben, finden Sie weitere Informationen unterLegacy-Richtlinie.

1. Öffnen Sie die IAM-Konsole unter https://console.aws.amazon.com/iam/.
2. Wählen Sie im Navigationsbereich Rollen aus, um eine Liste der IAM-Rollen anzuzeigen, auf die Sie Zugriff haben.
3. Wählen Sie den Link Rollenname für die Rolle aus, die Ihrer Instance zugeordnet ist. Dadurch wird die Seite mit den Rollendetails geöffnet.
4. Um die verwaltete Richtlinie anzuhängen, wählen Sie in der oberen rechten Ecke des Listenfensters die Option Berechtigungen hinzufügen aus. Wählen Sie dann in der Dropdownliste die Option Richtlinien anhängen aus.
5. Um die Ergebnisse zu optimieren, geben Sie den Richtliniennamen in die Suchleiste ein ()`AWSEC2VssSnapshotPolicy`.

6. Aktivieren Sie das Kontrollkästchen neben dem Namen der Richtlinie, die angehängt werden soll, und wählen Sie Berechtigungen hinzufügen aus.

Verwaltete Richtlinie zum Erstellen von VSS-Snapshots

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die Amazon AWS seinen Kunden anbietet. AWS verwaltete Richtlinien dienen dazu, Berechtigungen für allgemeine Anwendungsfälle zu gewähren. Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Sie können die Richtlinie jedoch kopieren und als Grundlage für eine vom Kunden verwaltete Richtlinie verwenden, die für Ihren Anwendungsfall spezifisch ist.

Weitere Informationen zu AWS verwalteten Richtlinien finden Sie im IAM-Benutzerhandbuch unter AWS Verwaltete Richtlinien.

Um die verwaltete AWSEC2VssSnapshotPolicyRichtlinie zu verwenden, können Sie sie der IAM-Rolle zuordnen, die Ihren EC2-Windows-Instances zugewiesen ist. Diese Richtlinie ermöglicht es der EC2 VSS-Lösung, Tags zu Amazon Machine Images (AMIs) und EBS-Snapshots zu erstellen und hinzuzufügen. Informationen zum Anhängen der Richtlinie finden Sie unter. Hängen Sie die VSS-fähige Snapshot-Richtlinie an Ihr Instanzprofil an

Berechtigungen vonAWSEC2VssSnapshotPolicy

Die AWSEC2VssSnapshotPolicyRichtlinie umfasst die folgenden Amazon EC2 EC2-Berechtigungen:

- ec2: CreateTags — Fügen Sie Tags zu EBS-Snapshots und AMIs hinzu, um die Ressourcen leichter identifizieren und kategorisieren zu können.
- ec2: DescribeInstance Attribut — Ruft die EBS-Volumes und die entsprechenden Blockgerätezuordnungen ab, die an die Ziel-Instance angehängt sind.
- ec2: CreateSnapshots — Erstellen Sie Snapshots von EBS-Volumes.
- ec2: CreateImage — Erstellen Sie ein AMI aus einer laufenden EC2-Instance.
- ec2: DescribeImages — Ruft die Informationen für EC2-AMIs und -Snapshots ab.
- ec2: DescribeSnapshots — Ermitteln Sie die Erstellungszeit und den Status von Snapshots, um die Anwendungskonsistenz zu überprüfen.

Beispiel für eine Richtlinie

Im Folgenden finden Sie ein Beispiel für die AWSEC2VssSnapshotPolicy Richtlinie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DescribeInstanceInfo",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstanceAttribute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AwsVssConfig": "*"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsAccessInstance",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
```

```
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
            }
        },
        {
            "Sid": "CreateSnapshotsAccessVolume",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSnapshots"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ]
        },
        {
            "Sid": "CreateImageWithTag",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:RequestTag/AwsVssConfig": "*"
                }
            }
        },
        {
            "Sid": "CreateImageAccessInstance",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateImage"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:SourceInstanceARN": "*${ec2:InstanceId}"
                }
```

```
            }
        },
        {
            "Sid": "CreateTagsOnResourceCreation",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": [
                        "CreateImage",
                        "CreateSnapshots"
                    ]
                }
            }
        },
        {
            "Sid": "CreateTagsAfterResourceCreation",
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": [
                "arn:aws:ec2:*:*:snapshot/*",
                "arn:aws:ec2:*:*:image/*"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/AwsVssConfig": "*"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "AppConsistent",
                        "Device"
                    ]
                }
            }
        },
        {
            "Sid": "DescribeImagesAndSnapshots",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImages",
```

```
                "ec2:DescribeSnapshots"
            ],
            "Resource": "*"
        }
    ]
}
```

Optimieren Sie die Berechtigungen für bestimmte Anwendungsfälle (fortgeschritten)

Die `AWSEC2VssSnapshotPolicy` verwaltete Richtlinie umfasst Berechtigungen für alle Möglichkeiten, wie Sie VSS-fähige Snapshots erstellen können. Sie können eine benutzerdefinierte Richtlinie erstellen, die nur die Berechtigungen enthält, die Sie benötigen.

Anwendungsfall: AMI erstellen, Anwendungsfall: AWS Backup Dienst verwenden

Wenn Sie ausschließlich `CreateAmi` diese Option verwenden oder wenn Sie VSS-fähige Snapshots nur über den AWS Backup Service erstellen, können Sie die Richtlinienangaben wie folgt optimieren.

- Lassen Sie die durch die folgenden Statement IDs (SIDs) identifizierten Richtlinienaussagen weg:
  - `CreateSnapshotsWithTag`
  - `CreateSnapshotsAccessInstance`
  - `CreateSnapshotsAccessVolume`
- Passen Sie die `CreateTagsOnResourceCreation` Aussage wie folgt an:
  - `arn:aws:ec2:*:*:snapshot/*`Aus den Ressourcen entfernen.
  - `CreateSnapshots`Aus dem `ec2:CreateAction` Zustand entfernen.
- Passen Sie die `CreateTagsAfterResourceCreation` Aussage an, um sie `arn:aws:ec2:*:*:snapshot/*` aus den Ressourcen zu entfernen.
- Passen Sie die `DescribeImagesAndSnapshots` Aussage an, um sie `ec2:DescribeSnapshots` aus der Aktion zu entfernen.

Anwendungsfall: Nur Snapshot

Wenn Sie die `CreateAmi` Option nicht verwenden, können Sie die Richtlinienerklärungen wie folgt vereinfachen.

- Lassen Sie die durch die folgenden Statement IDs (SIDs) identifizierten Richtlinienaussagen weg:
  - `CreateImageAccessInstance`

  - `CreateImageWithTag`
- Passen Sie die `CreateTagsOnResourceCreation` Aussage wie folgt an:
  - `arn:aws:ec2:*:*:image/*`Aus den Ressourcen entfernen.
  - `CreateImage`Aus dem `ec2:CreateAction` Zustand entfernen.
- Passen Sie die `CreateTagsAfterResourceCreation` Aussage an, um sie `arn:aws:ec2:*:*:image/*` aus den Ressourcen zu entfernen.
- Passen Sie die `DescribeImagesAndSnapshots` Aussage an, um sie `ec2:DescribeImages` aus der Aktion zu entfernen.

> **Note**
>
> Um sicherzustellen, dass Ihre benutzerdefinierte Richtlinie erwartungsgemäß funktioniert, empfehlen wir Ihnen, die verwaltete Richtlinie regelmäßig zu überprüfen und Aktualisierungen daran vorzunehmen.

Legacy-Richtlinie (nicht mehr unterstützt)

Die Legacy-Richtlinie, die Berechtigungen für VSS-fähige Snapshots gewährt, umfasst die IAM-Berechtigungen, die vor der Veröffentlichung der verwalteten Richtlinie empfohlen wurden. `AWSEC2VssSnapshotPolicy`

Wenn Sie eine Instanzrolle mit der Legacy-Richtlinie konfiguriert haben, können Sie sie weiterhin verwenden. Um jedoch sicherzustellen, dass Ihre Richtlinie stets auf dem neuesten Stand der bewährten Methoden für IAM ist und den Geltungsbereich der Richtlinienerklärungen entsprechend berücksichtigt, empfehlen wir Ihnen, die alte Richtlinie durch die `AWSEC2VssSnapshotPolicy` verwaltete Richtlinie zu ersetzen.

Beispiel für eine Richtlinie

Das folgende Richtlinienbeispiel verwendet die`ec2:DescribeInstanceAttribute`, die in den `AwsVssComponents` Paketversionen 2.2.1 und höher unterstützt wird. Wenn Sie eine ältere Version des `AwsVssComponents` Pakets installiert haben, sollten Sie diese durch die `ec2:DescribeInstances` Aktion ersetzen.

```
{
```

```
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "ec2:CreateTags",
   "Resource": [
    "arn:aws:ec2:*::snapshot/*",
    "arn:aws:ec2:*::image/*"
   ]
  },
  {
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstanceAttribute",
    "ec2:CreateSnapshot",
    "ec2:CreateSnapshots",
    "ec2:CreateImage",
    "ec2:DescribeImages",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  }
 ]
}
```

Weitere Informationen zu verwalteten IAM-Richtlinien finden Sie unter AWS Verwaltete Richtlinien im IAM-Benutzerhandbuch.

VSS-Komponenten

Um anwendungskonsistente Snapshots auf Windows-Betriebssystemen zu erstellen, muss das Paket `AwsVssComponents` auf der Instance installiert sein. Das Paket enthält einen On-Instance-EC2-VSS-Agent, der als VSS-Anforderer und EC2-VSS-Anbieter für EBS-Volumes fungiert.

Es gibt verschiedene Möglichkeiten, wie Sie die Komponente auf einer vorhandenen Instance installieren können:

- (Empfohlen) Führen Sie das AWSEC VssInstallAndSnapshot 2-Befehlsdokument aus (empfohlen). Dies wird bei jeder Ausführung automatisch installiert oder bei Bedarf aktualisiert.
- VSS-Komponenten manuell auf einer Instance installieren.
- VSS-Komponenten auf Ihren Instances nach einem Zeitplan aktualisieren.

Sie können auch ein AMI mit EC2 Image Builder erstellen, das die verwaltete Komponente `aws-vss-components-windows` verwendet, um das `AwsVssComponents`-Paket für das Image zu installieren. Die verwaltete Komponente verwendet AWS Systems Manager Distributor, um das Paket zu installieren. Nachdem Image Builder das Image erstellt hat, wird auf jeder Instance, die Sie über das zugehörige AMI starten, das VSS-Paket installiert. Weitere Informationen dazu, wie Sie ein AMI mit dem installierten VSS-Paket erstellen können, finden Sie unter Vom Verteilerpaket verwaltete Komponenten für Windows im Benutzerhandbuch für EC2 Image Builder.

Inhalt

VSS-Komponenten manuell auf einer Instance installieren

Auf Ihrer EC2-Windows-Instance müssen VSS-Komponenten installiert sein, bevor Sie mit Systems Manager anwendungskonsistente Snapshots erstellen können. Wenn Sie das `AWSEC2-VssInstallAndSnapshot`-Befehlsdokument nicht ausführen, um das Paket jedes Mal automatisch zu installieren oder zu aktualisieren, wenn Sie anwendungskonsistente Snapshots erstellen, müssen Sie das Paket manuell installieren.

Sie müssen die Installation auch manuell durchführen, wenn Sie eine der folgenden Methoden verwenden möchten, um anwendungskonsistente Snapshots von Ihrer EC2-Instance zu erstellen.

- Erstellen Sie VSS-Snapshots mit AWS Backup
- VSS-Snapshots mit Amazon Data Lifecycle Manager erstellen

Wenn Sie eine manuelle Installation durchführen müssen, empfehlen wir Ihnen, das neueste AWS VSS-Komponentenpaket zu verwenden, um die Zuverlässigkeit und Leistung anwendungskonsistenter Snapshots auf Ihren EC2-Windows-Instances zu verbessern.

> **Note**
>
> Um das Paket `AwsVssComponents` automatisch zu installieren oder zu aktualisieren, wenn Sie anwendungskonsistente Snapshots erstellen, empfehlen wir, dass Sie Systems Manager verwenden, um das Dokument `AWSEC2-VssInstallAndSnapshot` auszuführen. Weitere Informationen finden Sie unter Führen Sie das AWSEC VssInstallAndSnapshot 2-Befehlsdokument aus (empfohlen).

Befolgen Sie die Schritte für Ihre bevorzugte Umgebung, um die VSS-Komponenten auf einer Amazon-EC2-Windows-Instance zu installieren.

Console

So installieren Sie die VSS-Komponenten mit SSM-Distributor

1. Öffnen Sie die Konsole unter https://console.aws.amazon.com/systems-manager/. AWS Systems Manager
2. Wählen Sie im Navigationsbereich Run Command aus.
3. Wählen Sie Run Command (Befehl ausführen) aus.
4. Wählen Sie für das Befehlsdokument die Schaltfläche neben AWSPackageAWS-Configure.
5. Führen Sie unter Command parameters (Befehlsparameter) die folgenden Schritte aus:
   a. Stellen Sie sicher, dass Action (Aktion) auf Install (Installieren) festgelegt ist.
   b. Geben Sie unter Name `AwsVssComponents` ein.
   c. Geben Sie für Version eine Version ein oder lassen Sie das Feld leer, sodass Systems Manager die neueste Version installiert.
6. Identifizieren für Targets (Ziele) die Instances, in denen Sie diese Operation ausführen möchten, indem Sie Tags angeben oder Instances manuell auswählen.

   > **Note**
   >
   > Wenn Sie entscheiden, Instances manuell auszuwählen, und eine von Ihnen erwartete Instance nicht in der Liste enthalten ist, finden Sie Tipps zur Fehlerbehebung unter Einige meiner Instances fehlen im Benutzerhandbuch zu AWS Systems Manager .

7. Für Other parameters (Weitere Parameter):
   - (Optional) Geben Sie für Comment (Kommentar) Informationen zu diesem Befehl ein.
   - Geben Sie für Timeout (seconds) (Timeout (Sekunden)) in Sekunden an, wie lange gewartet werden soll, bis für die gesamte Befehlsausführung ein Fehler auftritt.
8. (Optional) Für Rate control (Ratenregelung):
   - Geben Sie unter Concurrency (Gleichzeitigkeit) entweder eine Zahl oder einen Prozentsatz für die Instances an, auf denen der Befehl gleichzeitig ausgeführt werden soll.

> **Note**
>
> Wenn Sie Ziele anhand von Amazon-EC2-Tags (Markierungen) ausgewählt haben und noch nicht sicher sind, von wie vielen Instances die ausgewählten Tags (Markierungen) verwendet werden, sollten Sie die Anzahl von Instances für die gleichzeitige Ausführung des Dokuments beschränken, indem Sie einen Prozentsatz angeben.

- Geben Sie unter Error threshold (Schwellenwert-Fehler) an, wann die Ausführung des Befehls auf anderen Instances beendet werden soll, nachdem dafür entweder auf einer bestimmten Anzahl oder einem Prozentsatz von Instances ein Fehler aufgetreten ist. Falls Sie beispielsweise drei Fehler angeben, sendet Systems Manager keinen Befehl mehr, wenn der vierte Fehler empfangen wird. Von Instances, auf denen der Befehl noch verarbeitet wird, werden unter Umständen ebenfalls Fehler gesendet.

9. (Optional) Wenn Sie im Abschnitt Ouput options (Ausgabeoptionen) die Befehlsausgabe in einer Datei speichern möchten, aktivieren Sie das Kontrollkästchen neben Enable writing to a S3 bucket (Schreiben in einen S3-Bucket aktivieren). Geben Sie den Bucket und (optional) die Präfixnamen (Ordner) an.

   > **Note**
   >
   > Die S3-Berechtigungen zum Schreiben von Daten in einen S3-Bucket sind die Berechtigungen des der Instance zugewiesenen Instance-Profils und nicht diejenigen des -Benutzers, der diese Aufgabe ausführt. Weitere Informationen finden Sie unter Erstellen eines IAM-Instance-Profils für Systems Manager im Benutzerhandbuch zu AWS Systems Manager .

10. (Optional) Geben Sie Optionen für SNS notifications (SNS-Benachrichtigungen) an.

    Weitere Informationen über das Konfigurieren von Amazon SNS-Benachrichtigungen für Run Command finden Sie unter Konfigurieren von Amazon SNS-Benachrichtigungen für AWS Systems Manager.

11. Wählen Sie Ausführen aus.

AWS CLI

Gehen Sie wie folgt vor, um mithilfe von Run Command über die `AwsVssComponents` das AWS CLI-Paket herunterzuladen und auf Ihren Instances zu installieren. Das Paket installiert zwei Komponenten: einen VSS-Anforderer und einen VSS-Anbieter. Das System kopiert diese Komponenten in ein Verzeichnis auf der Instance und registriert die Anbieter-DLL als VSS-Anbieter.

Um das VSS-Paket zu installieren, verwenden Sie AWS CLI

- Führen Sie den folgenden Befehl aus, um die erforderlichen VSS-Komponenten für Systems Manager herunterzuladen und zu installieren.

```
aws ssm send-command \
  --document-name "AWS-ConfigureAWSPackage" \
  --instance-ids "i-01234567890abcdef" \
  --parameters '{"action":["Install"],"name":["AwsVssComponents"]}'
```

PowerShell

Gehen Sie wie folgt vor, um das `AwsVssComponents` Paket herunterzuladen und auf Ihren Instanzen zu installieren, indem Sie Run Command in den Tools für Windows PowerShell verwenden. Das Paket installiert zwei Komponenten: einen VSS-Anforderer und einen VSS-Anbieter. Das System kopiert diese Komponenten in ein Verzeichnis auf der Instance und registriert die Anbieter-DLL als VSS-Anbieter.

Um das VSS-Paket mit dem zu installieren AWS Tools for Windows PowerShell

- Führen Sie den folgenden Befehl aus, um die erforderlichen VSS-Komponenten für Systems Manager herunterzuladen und zu installieren.

```
Send-SSMCommand -DocumentName AWS-ConfigureAWSPackage -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'action'='Install';'name'='AwsVssComponents'}
```

Überprüfen Sie die Signatur der AWS VSS-Komponenten

Gehen Sie wie folgt vor, um die Signatur für das `AwsVssComponents`-Paket zu überprüfen.

1. Herstellen einer Verbindung mit Ihrer Windows-Instance. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer -Windows-Instance.
2. Navigieren Sie zu C:\Program Files\ Amazon\ AwsVss Components.
3. Öffnen Sie das Kontextmenü (rechte Maustaste) für `ec2-vss-agent.exe` und wählen Sie dann Eigenschaften.
4. Navigieren Sie zur Registerkarte Digitale Signaturen und stellen Sie sicher, dass der Name des Signierers „Amazon Web Services Inc.“ lautet.
5. Überprüfen Sie mit den vorherigen Schritten auch die Signatur für `Ec2VssInstaller` und `Ec2VssProvider.dll`.

VSS-Komponenten auf Ihren Instances nach einem Zeitplan aktualisieren

Wir empfehlen, die VSS-Komponenten immer auf die neueste empfohlene Version zu aktualisieren. Es gibt verschiedene Möglichkeiten, wie Sie Komponenten aktualisieren können, wenn eine neue Version des Pakets `AwsVssComponents` veröffentlicht wird.

Update-Methoden

- Sie können die unter beschriebenen Schritte wiederholenVSS-Komponenten manuell auf einer Instance installieren, wenn eine neue Version der AWS VSS-Komponenten veröffentlicht wird.
- Sie können eine Systems-Manager-State-Manager-Zuordnung so konfigurieren, dass neue VSS-Komponenten automatisch heruntergeladen und installiert werden, sobald das Paket `AwsVssComponents` verfügbar ist.
- Sie können das Paket `AwsVssComponents` automatisch installieren oder aktualisieren, wenn Sie anwendungskonsistente Snapshots erstellen und den Systems Manager verwenden, um das Dokument `AWSEC2-VssInstallAndSnapshot` auszuführen.

> **Note**
>
> Wir empfehlen, dass Sie Systems Manager verwenden, um das Dokument mit dem Befehl `AWSEC2-VssInstallAndSnapshot` auszuführen, wodurch das Paket `AwsVssComponents` automatisch installiert oder aktualisiert wird, bevor die anwendungskonsistenten Snapshots erstellt werden. Weitere Informationen finden Sie unter Führen Sie das AWSEC VssInstallAndSnapshot 2-Befehlsdokument aus (empfohlen).

Um eine Systems-Manager-State-Manager-Zuordnung zu erstellen, folgen Sie den Schritten für Ihre bevorzugte Umgebung.

Console

So erstellen Sie eine State Manager-Zuordnung mit der Konsole

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Statusmanager aus.

   Oder, wenn die Systems Manager-Startseite zuerst geöffnet wird, öffnen Sie den Navigationsbereich und wählen Sie dann State Manager aus.
3. Wählen Sie Create association (Zuordnung erstellen) aus.
4. Geben Sie im Feld Name einen aussagekräftigen Namen ein.
5. Wählen Sie in der Dokumentenliste AWSPackage AWS-Configure aus.
6. Wählen Sie im Abschnitt Parameters (Parameter) die Option Install (Installieren) aus der Liste Action (Aktion) aus.
7. Wählen Sie für Installation type (Art der Installation) Uninstall and reinstall (Deinstallieren und neu installieren).
8. Geben Sie im Feld Name `AwsVssComponents` ein. Sie können die Felder Version und Additional Arguments leer lassen.
9. Wählen Sie im Abschnitt Targets (Ziele) eine Option aus.

   > **Note**
   >
   > Wenn Sie Ziel-Instances mittels Tags auswählen und Tags angeben, die Linux-Instances zugeordnet sind, ist die Zuordnung zwar auf der Windows-Instance erfolgreich, schlägt jedoch auf den Linux-Instances fehl. Der Gesamtstatus der Zuordnung zeigt Failed (Fehler) an.
10. Wählen Sie im Abschnitt Specify schedule eine Option.
11. Wählen Sie im Abschnitt Advanced options (Erweiterte Optionen) für Compliance severity (Compliance-Schweregrad) einen Schweregrad für die Zuordnung aus. Weitere Informationen finden Sie unter About State Manager association compliance. Wählen Sie für

Änderungskalender einen vorkonfigurierten Änderungskalender aus. Weitere Informationen finden Sie unter AWS Systems Manager -Change Calendar.

12. Gehen Sie für Ratenkontrolle wie folgt vor:

    - Geben Sie unter Concurrency (Nebenläufigkeit) entweder eine Zahl oder einen Prozentsatz der verwalteten Knoten an, auf denen der Befehl gleichzeitig ausgeführt werden soll.
    - Geben Sie unter Error threshold (Fehlerschwellenwert) an, wann die Ausführung des Befehls auf anderen verwalteten Knoten beendet werden soll, nachdem dafür entweder auf einer bestimmten Anzahl oder einem Prozentsatz von Knoten ein Fehler aufgetreten ist.

13. (Optional) Wenn Sie im Abschnitt Ausgabeoptionen die Befehlsausgabe in einer Datei speichern möchten, wählen Sie Schreiben der Ausgabe in S3 aktivieren aus. Geben Sie die Namen für den Bucket und das Präfix (Ordner) in die Textfelder ein.
14. Wählen Sie Create association (Zuordnung erstellen) und dann Close (Schließen) aus. Das System versucht, die Zuordnung auf den Instances zu erstellen und den Status sofort anzuwenden.

> **Note**
>
> Wenn EC2-Instances für Windows Server den Status Fehlgeschlagen anzeigen, stellen Sie sicher, dass der SSM-Agent auf der Instance ausgeführt wird, und stellen Sie sicher, dass die Instance mit einer AWS Identity and Access Management (IAM-) Rolle für Systems Manager konfiguriert ist. Weitere Informationen finden Sie unter Einrichtung. AWS Systems Manager

AWS CLI

Sie können den AWS CLI Befehl create-association ausführen, um ein Verteilerpaket nach einem Zeitplan zu aktualisieren, ohne die zugehörige Anwendung offline zu nehmen. Nur neue oder aktualisierte Dateien im Paket werden ersetzt.

Um eine State Manager-Zuordnung mit dem AWS CLI

1. Installieren und konfigurieren Sie den AWS CLI, falls Sie dies noch nicht getan haben. Weitere Informationen finden Sie unter Installieren oder Aktualisieren der neuesten Version von AWS CLI.

2. Führen Sie den folgenden Befehl aus, um eine Zuordnung zu erstellen. Der Wert für `--name`, d. h. der Name des Dokuments, ist stets `AWS-ConfigureAWSPackage`. Der folgende Befehl verwendet den Schlüssel `InstanceIds` zur Angabe von Ziel-Instances.

```
aws ssm create-association \
 --name "AWS-ConfigureAWSPackage" \
 --parameters '{"action":["Install"],"installationType":["Uninstall and
 reinstall"],"name":["AwsVssComponents"]}' \
 --targets [{\"Key\":\"InstanceIds\",\"Values\":[\"i-01234567890abcdef\",
\"i-000011112222abcde\"]}]
```

Informationen zu anderen Optionen, die Sie mit dem `create-association` Befehl verwenden können, finden Sie unter create-association im AWS Systems Manager Abschnitt der AWS CLI Befehlsreferenz.

Erstellen von VSS-fähigen EBS-Snapshots

Dieser Abschnitt beschreibt die Schritte zur Erstellung von VSS-fähigen EBS-Snapshots.

Sie können VSS-fähige EBS-Snapshots von EBS-Volumes erstellen, die mit Ihren EC2-Instances verknüpft sind. Bevor Sie versuchen, einen VSS-fähigen Snapshot zu erstellen, stellen Sie sicher, dass die Voraussetzungen erfüllt sind.

Themen

- VSS-Snapshots mit AWS Systems Manager -Befehlsdokumenten erstellen
- Erstellen Sie VSS-Snapshots mit AWS Backup
- VSS-Snapshots mit Amazon Data Lifecycle Manager erstellen

VSS-Snapshots mit AWS Systems Manager -Befehlsdokumenten erstellen

Sie können AWS Systems Manager Befehlsdokumente verwenden, um VSS-fähige Snapshots zu erstellen. Im Folgenden werden die verfügbaren Befehlsdokumente und die Laufzeitparameter vorgestellt, die die Dokumente zur Erstellung Ihrer Snapshots verwenden.

Bevor Sie eines der Befehlsdokumente von Systems Manager verwenden, stellen Sie sicher, dass Sie alle Anforderungen von Voraussetzungen erfüllt haben.

Themen

Parameter für VSS-Snapshot-Dokumente von Systems Manager

Die Systems-Manager-Dokumente, die VSS-Snapshots erstellen, verwenden alle die folgenden Parameter, sofern nicht anders angegeben:

ExcludeBootVolumen (Zeichenfolge, optional)

Mit dieser Einstellung werden Boot-Volumes aus dem Sicherungsvorgang ausgeschlossen, wenn Sie Snapshots erstellen. Um Startvolumes aus Ihren Snapshots auszuschließen, legen Sie ExcludeBootVolume auf und CreateAmito `True` `False` fest.

Wenn Sie ein AMI für Ihr Backup erstellen, sollte dieser Parameter auf `False` gesetzt werden. Der Standardwert für diesen Parameter ist `False`.

NoWriters(Zeichenfolge, optional)

Um Anwendungs-VSS-Writer vom Snapshot-Vorgang auszuschließen, setzen Sie diesen Parameter auf `True`. Anwendungs-VSS-Writer auszuschließen kann Ihnen helfen, Konflikte mit VSS-Backup-Komponenten von Drittanbietern zu lösen. Der Standardwert für diesen Parameter ist `False`.

CopyOnly(Zeichenfolge, optional)

Wenn Sie zusätzlich zu AWS VSS die systemeigene SQL Server-Sicherung verwenden, verhindert die Ausführung einer reinen Kopiersicherung, dass AWS VSS die systemeigene differenzielle Sicherungskette unterbricht. Um einen Copy-only-Backup-Vorgang durchzuführen, setzen Sie diesen Parameter auf `True`.

Der Standardwert für diesen Parameter ist`False`, was dazu führt, dass AWS VSS einen vollständigen Sicherungsvorgang durchführt.

CreateAmi(Zeichenfolge, optional)

Um ein VSS-fähiges Amazon Machine Image (AMI) zum Sichern Ihrer Instance zu erstellen, setzen Sie diesen Parameter auf `True`. Der Standardwert für diesen Parameter ist `False`, wodurch Ihre Instance stattdessen mit einem EBS-Snapshot gesichert wird.

Weitere Informationen zum Erstellen einer AMI von einer Instance finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

AmiName(Zeichenfolge, optional)

Wenn die CreateAmiOption auf gesetzt ist`True`, geben Sie den Namen des AMI an, das das Backup erstellt.

description (Zeichenfolge, optional)

Geben Sie eine Beschreibung für die Snapshots oder das Image an, das dieser Prozess erstellt.

tags (Zeichenfolge, optional)

Wir empfehlen Ihnen, Ihre Snapshots und Images mit Tags zu versehen, damit Sie Ihre Ressourcen leichter finden und verwalten können, z. B. um Volumes aus einer Liste von Snapshots wiederherzustellen. Das System fügt den `Name` Schlüssel mit einem leeren Wert hinzu, in dem Sie den Namen angeben können, den Sie auf Ihre ausgegebenen Schnappschüsse oder Bilder anwenden möchten.

Wenn Sie zusätzliche Tags angeben möchten, trennen Sie die Tags durch ein Semikolon dazwischen. z. B. `Key=Environment,Value=Test;Key=User,Value=TestUser1`.

Standardmäßig fügt das System die folgenden reservierten Tags für VSS-fähige Snapshots und Bilder hinzu.

- Gerät — Bei VSS-fähigen Snapshots ist dies der Gerätename des EBS-Volumes, das der Snapshot erfasst.
- AppConsistent— Dieses Tag weist auf die erfolgreiche Erstellung eines VSS-fähigen Snapshots oder AMIs hin.
- AwsVssConfig — Identifiziert Snapshots und AMIs, die mit aktiviertem VSS erstellt wurden. Das Tag enthält Metainformationen wie die `AwsVssComponents` Version.

> **Warning**
>
> Wenn Sie eines dieser reservierten Tags in Ihrer Parameterliste angeben, wird ein Fehler verursacht.

executionTimeout (Zeichenfolge, optional)

Geben Sie die maximale Zeit in Sekunden an, um den Snapshot-Erstellungsprozess auf der Instance auszuführen oder ein AMI aus der Instance zu erstellen. Wenn Sie dieses Timeout

erhöhen, kann der Befehl länger warten, bis VSS mit dem Einfrieren beginnt und die Markierung der von ihm erstellten Ressourcen abgeschlossen hat. Dieses Timeout gilt nur für die Schritte zur Snapshot- oder AMI-Erstellung. Der erste Schritt zur Installation oder Aktualisierung des Pakets `AwsVssComponents` ist nicht im Timeout enthalten.

CollectDiagnosticProtokolle (Zeichenfolge, optional)

Um während der Schritte zur Snapshot- und AMI-Erstellung weitere Informationen zu sammeln, setzen Sie diesen Parameter auf "`True`“. Der Standardwert für diesen Parameter ist "`False`“. Konsolidierte Diagnoseprotokolle werden als `.zip` Formatarchiv am folgenden Speicherort auf Ihrer Instance gespeichert:

`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`

VssVersion(Zeichenfolge, optional)

Sie können nur für das `AWSEC2-VssInstallAndSnapshot`-Dokument den Parameter `VssVersion` angeben, um eine bestimmte Version des `AwsVssComponents`-Pakets auf Ihrer Instance zu installieren. Lassen Sie diesen Parameter leer, um die empfohlene Standardversion zu installieren.

Wenn die angegebene Version des Pakets `AwsVssComponents` bereits installiert ist, überspringt das Skript den Installationsschritt und fährt mit dem Backup-Schritt fort. Eine Liste der `AwsVssComponents`-Paketversionen und der Betriebsunterstützung finden Sie unter AWS Versionsverlauf der VSS-Lösung.

VSS-Snapshot-Befehlsdokumente im Systems Manager ausführen

Sie können VSS-fähige EBS-Snapshots mit AWS Systems Manager Befehlsdokumenten wie folgt erstellen.

Führen Sie das AWSEC VssInstallAndSnapshot 2-Befehlsdokument aus (empfohlen)

Wenn Sie AWS Systems Manager das `AWSEC2-VssInstallAndSnapshot` Dokument ausführen, führt das Skript die folgenden Schritte aus.

1. Das Skript installiert oder aktualisiert zuerst das Paket `AwsVssComponents` auf Ihrer Instance, je nachdem, ob es bereits installiert ist.
2. Das Skript erstellt die anwendungskonsistenten Snapshots, nachdem der erste Schritt abgeschlossen ist.

Folgen Sie den Schritten für Ihre bevorzugte Umgebung, um das Dokument `AWSEC2-VssInstallAndSnapshot` auszuführen.

Console

VSS-fähige EBS-Snapshots über die Konsole erstellen

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Befehl ausführen. Hier wird gegebenenfalls eine Liste der Befehle angezeigt, die derzeit in Ihrem Konto ausgeführt werden.
3. Wählen Sie Run Command (Befehl ausführen) aus. Dadurch wird eine Liste von Befehlsdokumenten geöffnet, auf die Sie Zugriff haben.
4. Wählen Sie `AWSEC2-VssInstallAndSnapshot` aus der Liste der Befehlsdokumente aus. Um die Ergebnisse zu optimieren, können Sie den Dokumentnamen ganz oder teilweise eingeben. Sie können auch nach dem Eigentümer, nach Plattformtypen oder nach Tags filtern.

   Wenn Sie ein Befehlsdokument auswählen, werden die Details unter der Liste angezeigt.
5. Wählen Sie `Default version at runtime` aus der Liste der Dokumentversionen.
6. Konfigurieren Sie die Befehlsparameter, um zu definieren, wie `AWSEC2-VssInstallAndSnapshot` das Paket `AwsVssComponents` installieren und mit VSS-Snapshots oder einem AMI sichern soll. Einzelheiten zu den Parametern finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.
7. Geben Sie für Zielauswahl Tags an oder wählen Sie Instances manuell, um die Instances zu identifizieren, in denen Sie diesen Vorgang ausführen möchten.

   > **Note**
   >
   > Wenn Sie entscheiden, Instances manuell auszuwählen, und eine von Ihnen erwartete Instance nicht in der Liste enthalten ist, finden Sie Tipps zur Fehlersuche unter Wo sind meine Instances?.
8. Für zusätzliche Parameter zur Definition des Verhaltens von Systems Manager Run Command, wie z. B. die Ratensteuerung, geben Sie Werte ein, wie unter Befehle von der Konsole ausführen beschrieben.
9. Wählen Sie Run (Ausführen) aus.

Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach `AppConsistent` suchen. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die Systems Manager-Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren. Wenn der Befehl erfolgreich abgeschlossen wurde, ein bestimmtes Volume-Backup jedoch fehlgeschlagen ist, können Sie in der Liste der EBS-Volumes nach Informationen zur Problembehebung suchen.

AWS CLI

Sie können die folgenden Befehle in der ausführen, AWS CLI um VSS-fähige EBS-Snapshots zu erstellen und den Status Ihrer Snapshot-Erstellung abzurufen.

Erstellen von VSS-fähigen EBS-Snapshots

Führen Sie den folgenden Befehl aus, um VSS-fähige EBS-Snapshots zu erstellen. Um die Snapshots zu erstellen, müssen Sie die Instances mit dem `--instance-ids`-Parameter identifizieren. Weitere Informationen zu andere Parameter, die Sie verwenden können, finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-VssInstallAndSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"],"VssVersion":[""]}'
```

Bei Erfolg füllt das Befehlsdokument die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach `AppConsistent` suchen. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

Abrufen des Befehlsstatus

Um den aktuellen Status der Snapshots abzurufen, führen Sie den folgenden Befehl mit der Befehls-ID aus, die von send-command zurückgegeben wurde.

```
aws ssm get-command-invocation
```

```
 --instance-ids "i-01234567890abcdef" \
 --command-id "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
 --plugin-name "CreateVssSnapshot"
```

PowerShell

Führen Sie die folgenden Befehle mit aus AWS Tools for Windows PowerShell , um VSS-fähige EBS-Snapshots zu erstellen und den aktuellen Laufzeitstatus für die Erstellung Ihrer Ausgabe abzurufen. Geben Sie die in der vorherigen Liste beschriebenen Parameter an, um das Verhalten des Snapshot-Prozesses zu ändern.

Erstellen Sie VSS-fähige EBS-Snapshots mit Tools für Windows PowerShell

Führen Sie den folgenden Befehl aus, um VSS-fähige EBS-Snapshots oder AMIs zu erstellen.

```
Send-SSMCommand -DocumentName "AWSEC2-VssInstallAndSnapshot" -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value';'VssVersion'=''}
```

Abrufen des Befehlsstatus

Um den aktuellen Status der Snapshots abzurufen, führen Sie den folgenden Befehl mit der Befehls-ID aus, die von Send-SSMCommand zurückgegeben wurde.

```
Get-SSMCommandInvocationDetail -InstanceId "i-01234567890abcdef" -CommandId
 "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" -PluginName "CreateVssSnapshot"
```

Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach `AppConsistent` suchen. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

Führen Sie das Dokument mit den Befehlen 2 aus AWSEC CreateVssSnapshot

Folgen Sie den Schritten für Ihre bevorzugte Umgebung, um das Dokument `AWSEC2-CreateVssSnapshot` auszuführen.

Console

VSS-fähige EBS-Snapshots über die Konsole erstellen

1. Öffnen Sie die AWS Systems Manager Konsole unter https://console.aws.amazon.com/systems-manager/.
2. Wählen Sie im Navigationsbereich Befehl ausführen. Hier wird gegebenenfalls eine Liste der Befehle angezeigt, die derzeit in Ihrem Konto ausgeführt werden.
3. Wählen Sie Run Command (Befehl ausführen) aus. Dadurch wird eine Liste von Befehlsdokumenten geöffnet, auf die Sie Zugriff haben.
4. Wählen Sie `AWSEC2-CreateVssSnapshot` aus der Liste der Befehlsdokumente aus. Um die Ergebnisse zu optimieren, können Sie den Dokumentnamen ganz oder teilweise eingeben. Sie können auch nach dem Eigentümer, nach Plattformtypen oder nach Tags filtern.

   Wenn Sie ein Befehlsdokument auswählen, werden die Details unter der Liste angezeigt.
5. Wählen Sie `Default version at runtime` aus der Liste der Dokumentversionen.
6. Konfigurieren Sie die Befehlsparameter, um zu definieren, wie `AWSEC2-CreateVssSnapshot` mit VSS-Snapshots oder einem AMI gesichert werden soll. Einzelheiten zu den Parametern finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.
7. Geben Sie für Zielauswahl Tags an oder wählen Sie Instances manuell, um die Instances zu identifizieren, in denen Sie diesen Vorgang ausführen möchten.

   > **Note**
   >
   > Wenn Sie entscheiden, Instances manuell auszuwählen, und eine von Ihnen erwartete Instance nicht in der Liste enthalten ist, finden Sie Tipps zur Fehlersuche unter Wo sind meine Instances?.
8. Für zusätzliche Parameter zur Definition des Verhaltens von Systems Manager Run Command, wie z. B. die Ratensteuerung, geben Sie Werte ein, wie unter Befehle von der Konsole ausführen beschrieben.
9. Wählen Sie Run (Ausführen) aus.

   Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen

Tags (Markierungen) oder nach `AppConsistent` suchen. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die Systems Manager-Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren. Wenn der Befehl erfolgreich abgeschlossen wurde, ein bestimmtes Volume-Backup jedoch fehlgeschlagen ist, können Sie in der Liste der EBS-Volumes nach Informationen zur Problembehebung suchen.

AWS CLI

Sie können den folgenden Befehl in der ausführen, AWS CLI um VSS-fähige EBS-Snapshots zu erstellen.

Erstellen von VSS-fähigen EBS-Snapshots

Führen Sie den folgenden Befehl aus, um VSS-fähige EBS-Snapshots zu erstellen. Um die Snapshots zu erstellen, müssen Sie die Instances mit dem `--instance-ids`-Parameter identifizieren. Weitere Informationen zu andere Parameter, die Sie verwenden können, finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.

```
aws ssm send-command \
 --document-name "AWSEC2-CreateVssSnapshot" \
 --instance-ids "i-01234567890abcdef" \
 --parameters '{"ExcludeBootVolume":["False"],"description":["Description"],"tags":
["Key=key_name,Value=tag_value"]}'
```

Bei Erfolg füllt das Befehlsdokument die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach `AppConsistent` suchen. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren.

PowerShell

Führen Sie den folgenden Befehl mit aus, um VSS-fähige AWS Tools for Windows PowerShell EBS-Snapshots zu erstellen.

Erstellen Sie VSS-fähige EBS-Snapshots mit Tools für Windows PowerShell

Führen Sie den folgenden Befehl aus, um VSS-fähige EBS-Snapshots zu erstellen. Um die Snapshots zu erstellen, müssen Sie die Instances mit dem `InstanceId`-Parameter identifizieren. Sie können mehr als eine Instance angeben, für die Snapshots erstellt werden. Weitere

Informationen zu andere Parameter, die Sie verwenden können, finden Sie unter Parameter für VSS-Snapshot-Dokumente von Systems Manager.

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-01234567890abcdef" -Parameter
 @{'ExcludeBootVolume'='False';'description'='a_description'
 ;'tags'='Key=key_name,Value=tag_value'}
```

Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach `AppConsistent` suchen. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren. Wenn der Befehl erfolgreich abgeschlossen wurde, ein bestimmtes Volume-Backup jedoch fehlgeschlagen ist, können Sie in der Liste der EBS-Snapshots nach Informationen zur Problembehebung suchen.

Führen Sie Befehlsdokumente für einen Windows-Failover-Cluster mit gemeinsam genutztem EBS-Speicher aus

Sie können jedes der im vorherigen Abschnitt beschriebenen Befehlszeilenverfahren verwenden, um einen VSS-fähigen Snapshot zu erstellen. Das Befehlsdokument (`AWSEC2-VssInstallAndSnapshot` oder `AWSEC2-CreateVssSnapshot`) muss auf dem Primärknoten in Ihrem Cluster ausgeführt werden. Das Dokument schlägt auf den sekundären Knoten fehl, da sie keinen Zugriff auf die gemeinsam genutzten Festplatten haben. Wenn sich Ihr primärer und sekundärer Knoten dynamisch ändern, können Sie das Dokument „Befehl AWS Systems Manager ausführen“ auf mehreren Knoten ausführen, wobei Sie davon ausgehen, dass der Befehl auf dem primären Knoten erfolgreich ist und auf sekundären Knoten fehlschlägt.

Führen Sie das AWSEC ManageVss 2-IO SSM-Befehlsdokument aus

Sie können das folgende Skript und das vordefinierte SSM-Dokument `AWSEC2-ManageVssIO` verwenden, um I/O-Vorgänge vorübergehend zu unterbrechen, VSS-fähige EBS-Snapshots zu erstellen und die I/O-Vorgänge erneut zu starten. Dieser Vorgang wird im Kontext des Benutzers ausgeführt, der den Befehl ausführt. Wenn der Benutzer über ausreichende Rechte zum Erstellen und Markieren von Snapshots verfügt, AWS Systems Manager kann er VSS-fähige EBS-Snapshots erstellen und taggen, ohne dass die zusätzliche IAM-Snapshot-Rolle auf der Instance erforderlich ist.

Im Gegensatz dazu erfordert das Befehlsdokument (`AWSEC2-VssInstallAndSnapshot` or `AWSEC2-CreateVssSnapshot`), dass Sie die IAM-Snapshot-Rolle jeder Instance zuweisen, für

die EBS-Snapshots erstellt werden sollen. Wenn Sie aufgrund der Richtlinie oder aus Compliance-Gründen keine weiteren IAM-Berechtigungen für Ihre Instances bereitstellen möchten, können Sie das folgende Skript verwenden.

Bevor Sie beginnen

Beachten Sie die folgenden wichtigen Details zu diesem Vorgang:

- Dieser Prozess verwendet ein PowerShell Skript (`CreateVssSnapshotAdvancedScript.ps1`), um Snapshots aller Volumes auf den von Ihnen angegebenen Instances zu erstellen, mit Ausnahme der Root-Volumes. Wenn Sie Snapshots von Stamm-Volumes erstellen möchten, müssen Sie das SSM-Dokument `AWSEC2-CreateVssSnapshot` verwenden.
- Das Skript ruft das Dokument `AWSEC2-ManageVssIO` zweimal auf. Beim ersten Mal ist der Parameter `Action` dabei auf `Freeze` gesetzt. Dadurch werden alle I/O-Vorgänge auf den Instances angehalten. Beim zweiten Mal ist der Parameter `Action` auf `Thaw` gesetzt. Dadurch wird der I/O-Vorgang fortgesetzt.
- Versuchen Sie nicht, das `AWSEC2-ManageVssIO` Dokument ohne das CreateVssSnapshotAdvancedScript .ps1-Skript zu verwenden. Das VSS-Framework von Microsoft verlangt, dass der Aufruf der Aktionen `Freeze` und `Thaw` im Abstand von höchstens zehn Sekunden erfolgt. Ein manueller Aufruf dieser Aktionen ohne das Skript könnte zu Fehlern führen.

VSS-fähige EBS-Snapshots mithilfe des SSM-Dokuments **`AWSEC2-ManageVssIO`** erstellen

1. Laden Sie die Datei CreateVssSnapshotAdvancedScript.zip herunter und extrahieren Sie den Inhalt der Datei.
2. Öffnen Sie `CreateVssSnapshotAdvancedScript.ps1` in einem Texteditor, bearbeiten Sie den Beispielaufruf am Ende des Skripts mit einer gültigen EC2-Instanz-ID, einer Snapshot-Beschreibung und den gewünschten Tag-Werten, und führen Sie das Skript dann von aus aus PowerShell.

Bei Erfolg füllt der Befehl die Liste der EBS-Snapshots mit den neuen Snapshots. Sie können diese Snapshots in der Liste der EBS-Snapshots suchen, indem Sie nach den angegebenen Tags (Markierungen) oder nach `AppConsistent` suchen. Wenn die Befehlsausführung fehlgeschlagen ist, zeigen Sie die -Befehlsausgabe an, um nähere Informationen zum Grund hierfür zu erfahren. Wenn der Befehl erfolgreich abgeschlossen wurde, ein bestimmtes Volume-Backup jedoch fehlgeschlagen ist, können Sie in der Liste der EBS-Volumes nach Informationen zur Problembehebung suchen.

> **Note**
>
> Um Backups zu automatisieren, können Sie eine Aufgabe im AWS Systems Manager Wartungsfenster erstellen, die das `AWSEC2-VssInstallAndSnapshot` Dokument verwendet. Weitere Informationen finden Sie unter Arbeiten mit Wartungsfenstern (Konsole) im Benutzerhandbuch für AWS Systems Manager .

Erstellen Sie VSS-Snapshots mit AWS Backup

Sie können bei der Verwendung ein VSS-Backup erstellen, AWS Backup indem Sie VSS in der Konsole oder CLI aktivieren. Stellen Sie sicher, dass Sie die Voraussetzungen erfüllt haben, bevor Sie den VSS-fähigen Backup-Plan erstellen. Weitere Informationen finden Sie unter Creating Windows VSS backups im AWS Backup -Entwicklerhandbuch.

> **Note**
>
> AWS Backup installiert das `AwsVssComponents` Paket nicht automatisch auf Ihrer Instanz. Sie müssen in Ihrer Instance eine manuelle Installation durchführen. Weitere Informationen finden Sie unter VSS-Komponenten manuell auf einer Instance installieren.

VSS-Snapshots mit Amazon Data Lifecycle Manager erstellen

Sie können VSS-Snapshots mit Amazon Data Lifecycle Manager erstellen, indem Sie Vor- und Nach-Skripte in Ihren Snapshot-Lebenszyklusrichtlinien aktivieren. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/ebs/latest/userguide/automate-app-consistent-backups.html.

> **Note**
>
> Amazon Data Lifecycle Manager installiert das `AwsVssComponents`-Paket nicht automatisch auf Ihrer Instance. Sie müssen in Ihrer Instance eine manuelle Installation durchführen. Weitere Informationen finden Sie unter VSS-Komponenten manuell auf einer Instance installieren.

Problembehandlung bei Windows VSS-basierten EBS-Snapshots

Bevor Sie andere Schritte zur Fehlerbehebung ausprobieren, empfehlen wir Ihnen, die folgenden Details zu überprüfen.

- Stellen Sie sicher, dass Sie alle Voraussetzungen erfüllt haben.
- Stellen Sie sicher, dass Sie das neueste Support von Windows-Betriebssystemversionen des `AwsVssComponents`-Pakets für Ihr Betriebssystem verwenden. Das von Ihnen beobachtete Problem wurde möglicherweise in neueren Versionen behoben.

Themen

Überprüfen Sie die Protokolldateien

Wenn beim Erstellen von VSS-fähigen EBS-Snapshots Probleme auftreten oder Fehlermeldungen angezeigt werden, können Sie die Befehlsausgabe in der Systems Manager Manager-Konsole anzeigen.

Für Systems Manager Manager-Dokumente, die VSS-Snapshots erstellen, können Sie den `CollectDiagnosticLogs` Parameter zur Laufzeit auf "`True`" setzen. Wenn der `CollectDiagnosticLogs` Parameter auf "`True`" gesetzt ist, sammelt VSS zusätzliche Protokolle, um das Debuggen zu erleichtern. Weitere Informationen finden Sie unter Sammeln Sie zusätzliche Diagnoseprotokolle.

Wenn Sie Diagnoseprotokolle sammeln, speichert das Systems Manager Manager-Dokument sie auf Ihrer Instanz am folgenden Ort:`C:\ProgramData\Amazon\AwsVss\Logs\`*`timestamp`*`.zip`. Die Standardeinstellung für den `CollectDiagnosticLogs` Parameter ist "`False`“.

> **Note**
>
> Wenn Sie zusätzliche Hilfe beim Debuggen benötigen, können Sie die `.zip` Datei an AWS Support senden.

Die folgenden zusätzlichen Protokolle sind verfügbar, unabhängig davon, ob Sie Diagnoseprotokolle sammeln oder nicht:

- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stdout`
- `%ProgramData%\Amazon\SSM\InstanceData\`*`InstanceID`*`\document\orchestration\`*`SSMCommandID`*`\awsrunPowerShellScript\runPowerShellScript\stderr`

Sie können auch die Windows-Anwendung Event Viewer öffnen und Windows Logs (Windows-Protokolle), Application (Anwendung) auswählen, um zusätzliche Protokolle anzuzeigen. Um Ereignisse speziell vom EC2 Windows VSS Provider und dem Volume Shadow Copy Service anzuzeigen, filtern Sie nach Source (Quelle) nach den Begriffen **`Ec2VssSoftwareProvider`** und **`VSS`**.

Wenn Sie Systems Manager mit VPC-Endpunkten verwenden und die Systems Manager SendCommandManager-API-Aktion (Befehl ausführen in der Konsole) fehlgeschlagen ist, stellen Sie sicher, dass Sie den folgenden Endpunkt korrekt konfiguriert haben: com.amazonaws.***region .ec2.***

Wenn der Amazon EC2 EC2-Endpunkt nicht definiert ist, schlägt der Aufruf zur Aufzählung angehängter EBS-Volumes fehl, was dazu führt, dass der Systems Manager Manager-Befehl fehlschlägt. Weitere Informationen zum Einrichten von VPC-Endpunkten mit Systems Manager finden Sie unter Erstellen eines Virtual Private Cloud-Endpunkts im Benutzerhandbuch für AWS Systems Manager .

Sammeln Sie zusätzliche Diagnoseprotokolle

Um zusätzliche Diagnoseprotokolle zu sammeln, wenn Sie den Befehl send von Systems Manager verwenden, um das VSS-Snapshot-Dokument auszuführen, setzen Sie den `CollectDiagnosticLogs` Eingabeparameter zur Laufzeit auf `True` "". Wir empfehlen, diesen Parameter bei der Problembehandlung auf "`True`" zu setzen.

Um ein Befehlszeilenbeispiel zu sehen, wählen Sie eine der folgenden Registerkarten aus.

AWS CLI

Im folgenden Beispiel wird das `AWSEC2-CreateVssSnapshot` Systems Manager Manager-Dokument ausgeführt in AWS CLI:

```
aws ssm send-command \
--document-name "AWSEC2-CreateVssSnapshot" \
--instance-ids "i-1234567890abcdef0" \
--parameters '{"description":["Example - create diagnostic logs at
 runtime."],"tags":["Key=tag_name,Value=tag_value"],"CollectDiagnosticLogs":
["True"]}'
```

PowerShell

Im folgenden Beispiel wird das `AWSEC2-CreateVssSnapshot` Systems Manager Manager-Dokument ausgeführt in PowerShell:

```
Send-SSMCommand -DocumentName AWSEC2-CreateVssSnapshot -InstanceId
 "i-1234567890abcdef0" -Parameter @{'description'='Example - create diagnostic logs
 at runtime.';'tags'='Key=tag_name,Value=tag_value';'CollectDiagnosticLogs'='True'}
```

Verwenden Sie VSS auf Instanzen, für die der Proxy konfiguriert ist

Wenn beim Erstellen von VSS-fähigen EBS-Snapshots in Instances, die einen Proxy zum Erreichen von EC2-Endpunkten verwenden, Probleme auftreten, stellen Sie Folgendes sicher:

- Der Proxy ist so konfiguriert, dass die EC2-Dienstendpunkte in der Region und im IMDS der Instance erreichbar AWS Tools for Windows PowerShell sind, wenn er als SYSTEM ausgeführt wird.
- `AwsVssComponents`-Version 2.0.1 oder höher ist installiert. Ab `AwsVssComponents`-Version 2.0.1 unterstützt der EC2 VSS-Anbieter die Verwendung des konfigurierten WinHTTP-Proxys des Systems. Weitere Informationen zum Konfigurieren des WinHTTP-Proxys finden Sie unter Netsh-Befehle für Windows Hypertext Transfer Protocol (WINHTTP) auf der Microsoft-Website.

Fehler: Zeitüberschreitung bei der Thaw-Pipe-Verbindung, Fehler beim Thaw, Zeitüberschreitung beim Warten auf VSS Freeze oder andere Zeitüberschreitungsfehler

Der EC2 Windows VSS Provider kann aufgrund von Aktivitäten oder Diensten auf der Instance, die verhindert, dass VSS-fähige Snapshots rechtzeitig ausgeführt werden, die Zeit überschreiten. Das Windows VSS Framework bietet ein nicht konfigurierbares 10-Sekunden-Fenster, in dem die Kommunikation mit dem Dateisystem unterbrochen wird. Während dieser Zeit erstellt `AWSEC2-CreateVssSnapshot` Snapshots Ihrer Volumes.

Die folgenden Probleme können dazu führen, dass der EC2 Windows VSS Provider während eines Snapshots auf Zeitlimits stößt:

- Übermäßiger I/O für ein Volume
- Langsame Reaktion der EC2-API auf der Instance
- Fragmentierte Volumes
- Inkompatibilität mit einigen Antivirensoftwares
- Probleme mit einem VSS Application Writer
- Wenn die Modulprotokollierung für eine große Anzahl von PowerShell Modulen aktiviert ist, kann dies dazu führen, dass PowerShell Skripts langsam ausgeführt werden

Die meisten Zeitüberschreitungsprobleme, die bei der Ausführung des `AWSEC2-CreateVssSnapshot`-Befehlsdokuments auftreten, hängen damit zusammen, dass die Workload auf der Instance zum Zeitpunkt der Sicherung zu hoch ist. Die folgenden Aktionen können Ihnen dabei helfen, einen erfolgreichen Snapshot zu erstellen:

- Wiederholen Sie den Befehl `AWSEC2-CreateVssSnapshot`, um zu sehen, ob der Snapshot-Versuch erfolgreich ist. Wenn der Wiederholungsversuch in einigen Fällen erfolgreich ist, kann das Reduzieren der Instance-Last Snapshots erfolgreicher machen.
- Warten Sie eine Weile, bis der Workload der Instance abnimmt, und wiederholen Sie den Befehl `AWSEC2-CreateVssSnapshot`. Alternativ können Sie Snapshots versuchen, wenn bekannt ist, dass die Instance unter geringem Stress steht.
- Versuchen Sie VSS-Snapshots, wenn die Antivirensoftware auf dem System ausgeschaltet ist. Wenn das Problem dadurch behoben wird, lesen Sie die Anweisungen der Antivirensoftware und konfigurieren Sie sie so, dass VSS-Snapshots zulässig sind.

- Wenn Ihr Konto in derselben Region, in der Sie einen Snapshot ausführen, eine große Anzahl von Amazon-EC2-API-Aufrufen enthält, kann die API-Drosselung Snapshot-Vorgänge verzögern. Um die Auswirkungen der Drosselung zu reduzieren, verwenden Sie das neueste `AwsVssComponents`-Paket (Version 2.1.0 und höher, mit den erforderlichen Berechtigungen). Dieses Paket verwendet die EC2-API-Aktion `CreateSnapshots`, um die Anzahl mutierender Aktionen wie das Erstellen und Taggen von Snapshots pro Volume zu reduzieren.
- Wenn Sie mehrere `AWSEC2-CreateVssSnapshot`-Befehlsskripte gleichzeitig ausführen, können Sie die folgenden Schritte unternehmen, um Gleichzeitigkeitsprobleme zu verringern.
  - Erwägen Sie die Planung von Snapshots in Zeiten geringerer API-Aktivität.
  - Wenn Sie Run Command in der Systems-Manager-Konsole (oder SendCommand in der API) verwenden, um das Befehlsskript auszuführen, können Sie die Systems-Manager-Ratensteuerung verwenden, um die Gleichzeitigkeit zu reduzieren.

    Sie können auch Systems Manager-Ratensteuerungen verwenden, um die Parallelität von Diensten wie AWS Backup denen zu reduzieren, die Systems Manager zur Ausführung des Befehlsskripts verwenden.
- Führen Sie den Befehl `vssadmin list writers` in einer Shell aus und prüfen Sie, ob er Fehler im Feld Last error (Letzter Fehler) für alle Autoren auf dem System meldet. Wenn Autoren einen time out (Timeout)-Fehler melden, sollten Sie Snapshots erneut versuchen, Snapshots erneut zu versuchen, wenn die Instance weniger belastet ist.
- Wenn Sie kleinere Instance-Typen wie *`t2 | t3 | t3a`*.nano oder *`t2 | t3 | t3a`*.micro verwenden, kann es aufgrund von Speicher- und CPU-Einschränkungen zu Timeouts kommen. Die folgenden Aktionen können dazu beitragen, Timeout-Probleme zu reduzieren.
  - Versuchen Sie, speicher- oder CPU-intensive Anwendungen zu schließen, bevor Sie Snapshots erstellen.
  - Versuchen Sie, Snapshots in Zeiten mit geringerer Instance-Aktivität zu erstellen.

Fehler: Methode kann nicht aufgerufen werden. Der Methodenaufruf wird in diesem Sprachmodus nur für Kerntypen unterstützt.

Dieser Fehler tritt auf, wenn der PowerShell Sprachmodus nicht auf `FullLanguage` eingestellt ist. Die Dokumente `AWSEC2-CreateVssSnapshot` und `AWSEC2-ManageVssIo` SSM PowerShell müssen für den `FullLanguage` Modus konfiguriert werden.

Um den Sprachmodus zu überprüfen, führen Sie den folgenden Befehl auf der Instanz in einer PowerShell Konsole aus:

```
$ExecutionContext.SessionState.LanguageMode
```

Weitere Informationen über Sprachmodi finden Sie unter about_Language_Modes in der Microsoft-Dokumentation.

Wiederherstellen von EBS-Volumes von VSS-fähigen EBS-Snapshots

Sie können das Skript `RestoreVssSnapshotSampleScript.ps1` zum Wiederherstellen von Volumes auf einer Instance von VSS-fähigen EBS-Snapshots verwenden. Dieses Skript führt die folgenden Aufgaben aus:

- Anhalten einer Instance
- Entfernen aller vorhandenen Laufwerke aus der Instance (mit Ausnahme des Stamm-Volumes, wenn es ausgeschlossen wurde)
- Erstellen neuer Volumes von den Snapshots
- Anfügen der Volumes an die Instance mithilfe des Geräte-ID-Tags (Markierung) auf dem Snapshot
- Neustart der Instance

> **Important**
>
> Das folgende Skript trennt alle Volumes ab, die einer Instance angefügt sind, und erstellt dann neue Volumes von einem Snapshot. Stellen Sie sicher, dass Sie die Instance ordnungsgemäß gesichert haben. Die alten Volumes werden nicht gelöscht. Wenn Sie möchten, können Sie das Skript bearbeiten, um die alten Volumes zu löschen.

So stellen Sie Volumes von VSS-fähigen EBS-Snapshots wieder her

1. Laden Sie die Datei RestoreVssSnapshotSampleScript.zip herunter und extrahieren Sie den Inhalt der Datei.
2. Öffnen Sie das Skript `RestoreVssSnapshotSampleScript.ps1` in einem Texteditor und bearbeiten Sie den Beispielaufruf am Ende des Skripts mit einer gültigen EC2-Instanz-ID und einer EBS-Snapshot-ID. Führen Sie dann das Skript von aus. PowerShell

AWS Versionsverlauf der VSS-Lösung

Themen

AwsVssComponents Paketversionen

In der folgenden Tabelle werden die veröffentlichten Versionen des AWS VSS-Komponentenpakets beschrieben.

Version	Details	Datum der Veröffentlichung
2.3.2	Es wurde ein Fall behoben, bei dem die VSS-Anbieterregistrierung bei der Deinstallation nicht entfernt wurde.	9. Mai 2024
2.3.1	Es wurde ein neues Standard-Tag `AwsVssConfig` zur Identifizierung von Snapshots und AMIs hinzugefügt, die von AWS VSS erstellt wurden.	7. März 2024
2.2.1	• Unterstützung für die Verwendung der `DescribeInstanceAttribute` API hinzugefügt. • Fehlerbehebungen und verbesserte Zuverlässigkeit. • Veraltete Unterstützung für Windows Server 2012 und 2012 R2. AWS Die Installation der Version 2.2.1 der VSS-Komponenten auf Windows Server 2012 und 2012 R2 schlägt fehl. AWS Die Version 2.1.0 der VSS-Komponenten ist die letzte Version, die Windows Server 2012 und 2012 R2 unterstützt.	18. Januar 2024
2.1.0		6. November 2023

Version	Details	Datum der Veröffentlichung
	Unterstützung für die Verwendung der `CreateSnapshots` API hinzugefügt.	
2.0.1	Unterstützung für die Verwendung der WinHTTP-Proxy-Einstellungen hinzugefügt.	26. Oktober 2023
2.0.0	Der AWS VSS-Komponente wurde die Möglichkeit hinzugefügt, Snapshots und AMIs zu erstellen, was die Kompatibilität mit PowerShell Modulprotokollierung, Skriptblockprotokollierung und Transkriptionsfunktionen ermöglicht.	28. April 2023
1.3.2.0	Es wurde ein Fall behoben, bei dem ein Installationsfehler nicht korrekt gemeldet wurde.	10. Mai 2022
1.3.1.0	• Snapshots, die auf Domain-Controllern im Zusammenhang mit einem NTDS-VSS Schreiber-Protokollierungsfehler fehlgeschlagen sind, wurden behoben. • Es wurde ein VSS-Agent-Fehler beim Deinstallieren von Version 1.0 des VSS-Anbieters behoben.	6. Februar 2020

Version	Details	Datum der Veröffentlichung
1.3.00	• Verbesserte Protokollierung durch Reduzierung unerwünschter Ausführlichkeit. • Es wurden Regionalisierungsprobleme während der Installation behoben. • Es wurden Rückgabecodes für einige Anbieter-Registrierungsfehlerbedingungen korrigiert. • Es wurden verschiedene Installationsprobleme behoben.	19. März 2019
1.2.00	• Dem Agenten wurden Befehlszeilenparameter `-nw` (no-writers) und `-copy` (copy-only) hinzugefügt. • EventLog Fehler behoben, die durch unsachgemäße Aufrufe zur Speicherzuweisung verursacht wurden.	15. November 2018
1.1	AWS VSS-Komponenten wurden behoben, die fälschlicherweise als standardmäßiger Windows-Backup- und Wiederherstellungsanbieter verwendet wurden.	12. Dezember 2017
1,0	Erstversion.	20. November 2017

Support von Windows-Betriebssystemversionen

Die folgende Tabelle zeigt, welche Versionen der AWS VSS-Lösung Sie auf jeder Version von Windows Server auf Amazon EC2 ausführen sollten.

Windows Server Version	AwsVssComponents Version	AWSEC2-VssInstallAndSnapshotVersionsname	AWSEC2-CreateVssSnapshotVersionsname	AWSEC2-Namder ManageVssIO-Version
Windows Server 202	default	default	default	default
Windows Server 201	default	default	default	default
Windows Server 201	default	default	default	default
Windows Server 2012 R2	2.1.0	Nicht unterstützt	2012R2	2012R2
Windows Server 201	2.1.0	Nicht unterstützt	2012R2	2012R2
Windows Server 2008 R2	1.3.1.0	Nicht unterstützt	2008R2	2008R2

Verhinderung von Schreibfehlern für Linux-Instances

> **Note**
>
> Der Schutz vor Schreibfehlern wird nur für Linux-Instances unterstützt.

Die Verhinderung von Schreibfehlern ist eine Blockspeicherfunktion, die entwickelt wurde AWS , um die Leistung Ihrer I/O-intensiven relationalen Datenbank-Workloads zu verbessern und die Latenz zu

reduzieren, ohne die Datenstabilität negativ zu beeinflussen. Relationale Datenbanken, die InnoDB oder XtraDB als Datenbank-Engine verwenden, wie MySQL und MariaDB, profitieren von Torn-Write-Prävention.

In der Regel verwenden relationale Datenbanken, die Seiten verwenden, die größer sind als die Stromausfall-Atomizität des Speichergeräts, Datenprotokollierungsmechanismen, um sich vor fehlerhaften Schreibvorgängen zu schützen. MariaDB und MySQL verwenden einen Doublewrite-Puffer, um Daten zu protokollieren, bevor sie in Datentabellen geschrieben werden. Bei unvollständigen oder unterbrochenen Schreibvorgängen aufgrund von Betriebssystemabstürzen oder Stromausfällen während Schreibtransaktionen kann die Datenbank die Daten aus dem Doublewrite-Puffer wiederherstellen. Der zusätzliche I/O-Overhead, der mit dem Schreiben in den Doublewrite-Puffer verbunden ist, wirkt sich auf die Datenbankleistung und die Anwendungslatenz aus und reduziert die Anzahl der Transaktionen, die pro Sekunde verarbeitet werden können. Weitere Informationen zu Doublewrite Buffer finden Sie in der Dokumentation zu MariaDB und MySQL.

Mit Torn-Write-Prävention werden Daten in Alles-oder-Nichts-Schreibtransaktionen in den Speicher geschrieben, sodass der Doublewrite-Puffer nicht mehr verwendet werden muss. Dadurch wird verhindert, dass bei Betriebssystemabstürzen oder Stromausfällen während Schreibtransaktionen teilweise oder aufgespaltete Daten in den Speicher geschrieben werden. Die Anzahl der pro Sekunde verarbeiteten Transaktionen kann um bis zu 30 Prozent erhöht und die Schreiblatenz um bis zu 50 Prozent verringert werden, ohne die Resilienz Ihrer Workloads zu beeinträchtigen.

Preisgestaltung

Für die Verwendung von Torn-Write-Prävention fallen keine zusätzlichen Kosten an.

Unterstützte Blockgrößen und Blockgrenzausrichtungen

Torn-Write-Prävention unterstützt Schreiboperationen für Datenblöcke von 4 KiB, 8 KiB und 16 KiB. Die Startadresse des Datenblocks (Logical Block Address, LBA) muss auf die jeweilige Blockgrenzengröße von 4 KiB, 8 KiB oder 16 KiB ausgerichtet sein. Beispielsweise muss für 16-KiB-Schreibvorgänge der Datenblockstart LBA auf eine Blockgrenzgröße von 16 KiB ausgerichtet werden.

Die folgende Tabelle zeigt die Unterstützung für verschiedene Speicher- und Instance-Typen.

	4-KiB-Blöcke	8-KiB-Blöcke	16-KiB-Blöcke
Instance-Speicher-Volumes	Alle NVMe-Instance-Speichervolumes, die an Instances der I-Familie der aktuellen Generation angefügt sind.	i4I-, IM4GN- und IS4Gen-Instances, die von Nitro SSD unterstützt werden. AWS	
Amazon-EBS-Volumes	Alle Amazon EBS-Volumes, die an Instances angehängt sind, die auf dem AWS Nitro-System basieren.		

Um zu überprüfen, ob Ihre Instance und Ihr Volume Torn-Write-Prävention unterstützen, prüfen Sie, ob die Instance Torn-Write-Prävention unterstützt und überprüfen Sie weitere Details wie unterstützte Block- und Grenzgrößen. Weitere Informationen finden Sie unter Überprüfen der Unterstützung und Konfiguration von Torn-Write-Prävention.

Voraussetzungen

Damit Torn-Write-Prävention ordnungsgemäß funktioniert, muss ein I/O-Vorgang die Anforderungen an Größe, Ausrichtung und Grenzen erfüllen, wie in den Feldern `NTWPU`, `NTWGU` und `NTWBU` angegeben. Sie müssen Ihr Betriebssystem so konfigurieren, dass das spezifische Speichersubsystem (Dateisystem, LVM, RAID usw.) keine I/O-Eigenschaften im Speicherstapel verändert, einschließlich Blockzusammenführungen, Splits oder Blockadressverschiebungen, bevor sie an das Gerät übermittelt werden.

Torn-Write-Prävention wurde mit der folgenden Konfiguration getestet:

- Ein Instance-Typ und ein Speichertyp, der die erforderliche Blockgröße unterstützt.
- Amazon Linux 2 mit Kernel-Version 5.10 oder höher.
- ext4 mit `bigalloc` aktiviert und einer Clustergröße von 16 KiB sowie die neuesten ext4-Hilfsprogramme (e2fsprogs 1.46.5 oder höher).
- `O_DIRECT`-Dateizugriffsmodus zur Umgehung des Linux-Kernel-Puffercaches.

> **Note**
>
> Sie müssen die I/O-Zusammenführung für MySQL- und MariaDB-Workloads nicht deaktivieren.

Überprüfen der Unterstützung und Konfiguration von Torn-Write-Prävention

Verwenden Sie den folgenden Befehl, um zu überprüfen, ob Ihre Instance und Ihr Volume Torn-Write-Prävention unterstützen, und um die herstellerspezifischen NVMe-Namespace-Daten einzusehen, die Informationen zur Verhinderung von Torn-Write-Prävention enthalten.

```
$ sudo nvme id-ns -v device_name
```

> **Note**
>
> Der Befehl gibt die herstellerspezifischen Informationen in Hexadezimalform mit ASCII-Interpretation zurück. Möglicherweise müssen Sie ein ähnliches Tool wie `ebsnvme-id` in Ihre Anwendungen einbauen, das die Ausgabe lesen und analysieren kann.

Der folgende Befehl gibt beispielsweise die herstellerspezifischen NVMe-Namespace-Daten zurück, die Informationen zu Torn-Write-Prävention für `/dev/nvme1n1` enthalten.

```
$ sudo nvme id-ns -v /dev/nvme1n1
```

Wenn Ihre Instance und Ihr Volume die Verhinderung von fehlerhaftem Schreiben unterstützen, werden die folgenden Informationen zur Verhinderung von AWS Schreibfehlern in den herstellerspezifischen NVMe-Namespace-Daten zurückgegeben.

> **Note**
>
> Die Bytes in der folgenden Tabelle stellen den Abstand in Bytes vom Anfang der herstellerspezifischen NVMe-Namespace-Daten dar.

Bytes	Beschreibung
`0:31`	Der Name des Befestigungspunkts des Geräts, z. B. `/dev/xvda` . Sie geben dies bei der Anforderung eines Volumenanhangs an und es kann von der Amazon-EC2-Instance verwendet werden, um einen Symlink zum NVMe-Blockgerät (`nvmeXn1`) zu erstellen.
`32:63`	Die Volume-ID. z. B. `vol01234567890abcdef` . Dieses Feld kann verwendet werden, um das NVMe-Gerät dem angeschlossenen Volume zuzuordnen.
`64:255`	Für die spätere Verwendung reserviert.
`256:257`	Größe der Namespace-Torn-Write-Prävention-Einheit (NTWPU, Namespace Torn Write Prevention Unit). Dieses Feld gibt die namespace-spezifischen Größe des Schreibvorgangs an, die bei einem Stromausfall oder einer Fehlerbedingung garantiert automatsch in den NVM geschrieben werden. Dieses Feld ist in logischen Blöcken angegeben, die in Nullwerten dargestellt werden.
`258:259`	Granularitätsgröße von Namespace Torn Write Prevention (NTWPG). Dieses Feld gibt die namespace-spezifischen Größeninkremente unter `NTWPU` des Schreibvorgangs an, die bei einem Stromausfall oder einer Fehlerbedingung garantiert atomar in den NVM geschrieben werden. Das heißt, die Größe sollte bei `NTWPG * n <= NTWPU` liegen, wobei n eine positive Ganzzahl ist. Der Schreibvorgang „LBA-Offset“ muss ebenfalls an dieses Feld angepasst werden. Dieses Feld ist in logischen Blöcken angegeben, die in Nullwerten dargestellt werden.
`260:263`	Größe der Namespace-Torn-Write-Prävention-Grenze (NTWPB, Namespace Torn Write Prevention Boundary). Dieses Feld gibt die atomare Grenzgröße für diesen Namespace für den Wert `NTWPU` an. Es ist nicht garantiert, dass Schreibvorgänge in diesen Namespace , die atomare Grenzen überschreiten, bei einem Stromausfall oder einem Fehler automatsch auf die NVM geschrieben werden. Ein Wert von `0`h gibt an, dass es keine atomaren Grenzen für Stromausfall- oder Fehlerbedingungen gibt. Alle anderen Werte geben eine Größe in

Bytes	Beschreibung
	Form logischer Blöcke an, die dieselbe Kodierung wie das NTWPU-Feld verwenden.

Konfigurieren Ihres Software-Stacks für Torn-Write-Prävention

Torn-Write-Prävention ist standardmäßig auf unterstützten Instance-Typen mit unterstützten Volumes aktiviert. Sie müssen keine zusätzlichen Einstellungen aktivieren, um Ihr Volume oder Ihre Instance für Torn-Write-Prävention zu aktivieren.

> **Note**
>
> Es gibt keine Auswirkungen auf die Leistung von Workloads, die Torn-Write-Prävention nicht unterstützen. Sie müssen keine Änderungen für diese Workloads vornehmen. Workloads, die Torn-Write-Prävention unterstützen, aber nicht dafür konfiguriert sind, verwenden weiterhin den Doublewrite-Puffer und erhalten keine Leistungsvorteile.

Gehen Sie wie folgt vor, um Ihren MySQL- oder MariaDB-Softwarestack so zu konfigurieren, dass der Doublewrite-Puffer deaktiviert und Torn-Write-Prävention verwendet wird:

1. Konfigurieren Sie Ihr Volume für die Verwendung des ext4-Dateisystems mit der BigAlloc Option und legen Sie die Clustergröße auf 4 KiB, 8 KiB oder 16 KiB fest. Die Verwendung BigAlloc mit einer Clustergröße von 4 KiB, 8 KiB oder 16 KiB stellt sicher, dass das Dateisystem Dateien zuordnet, die an der jeweiligen Grenze ausgerichtet sind.

   ```
   $  mkfs.ext4 -O bigalloc -C 4096|8192|16384 device_name
   ```

   > **Note**
   >
   > Für MySQL und MariaDB müssen Sie `-C 16384` verwenden, um die Seitengröße der Datenbank anpassen. Wenn Sie die Zuweisungsgranularität auf einen anderen Wert als ein Vielfaches der Seitengröße festlegen, kann dies zu Zuordnungen führen, die möglicherweise nicht mit den Grenzen des Speichergeräts zur Verhinderung von fehlerhaften Schreibvorgängen übereinstimmen.

Beispielsweise:

```
$  mkfs.ext4 -O bigalloc -C 16384 /dev/nvme1n1
```

2. Konfigurieren Sie InnoDB so, dass es die `O_DIRECT`-Flushing-Methode verwendet, und schalten Sie InnoDB-Doublewrite aus. Verwenden Sie Ihren bevorzugten Texteditor, um `/etc/my.cnf` zu öffnen und die `innodb_flush_method`- und `innodb_doublewrite`-Parameter wie folgt zu aktualisieren:

```
innodb_flush_method=O_DIRECT
innodb_doublewrite=0
```

> **Important**
>
> Wenn Sie den Logical Volume Manager (LVM) oder eine andere Speichervirtualisierungsschicht verwenden, stellen Sie sicher, dass die Startoffsets der Volumes auf ein Vielfaches von 16 KiB ausgerichtet sind. Dies bezieht sich auf den zugrunde liegenden NVMe-Speicher, um die von der Speichervirtualisierungsebene verwendeten Metadaten-Header und Superblöcke zu berücksichtigen. Wenn Sie dem physischen LVM-Volume einen Offset hinzufügen, kann dies zu einer Fehlausrichtung zwischen den Dateisystemzuordnungen und den Offsets des NVMe-Geräts führen, was die Verhinderung von fehlerhaften Schreibvorgängen zunichte machen würde. Weitere Informationen finden Sie unter `--dataalignmentoffset` in der Linux-Handbuchseite.

Ressourcen und Tags (Markierungen)

Amazon EC2 stellt mehrere Ressourcen bereit, die Sie erstellen und verwenden können. Manche dieser Ressourcen umfassen Images, Instances, Volumes und Snapshots. Wenn Sie eine Ressource erstellen, weisen wir der Ressource eine eindeutige Ressourcen-ID zu.

Manche Ressourcen können mit Werten markiert werden, die Sie definieren, um sie organisieren und identifizieren zu können.

In den folgenden Themen werden Ressourcen und Tags (Markierungen) beschrieben, und wie Sie mit ihnen arbeiten können.

Inhalt

Papierkorb

Der Papierkorb ist ein Datenwiederherstellungsfeature, mit dem Sie versehentlich gelöschte Amazon-EBS-Snapshots und EBS-gestützte AMIs wiederherstellen können. Wenn Sie den Papierkorb verwenden, werden Ressourcen nach dem Löschen für einen von Ihnen angegebenen Zeitraum im Papierkorb aufbewahrt, bevor sie endgültig gelöscht werden.

Sie können eine Ressource vor Ablauf des Aufbewahrungszeitraums jederzeit aus dem Papierkorb wiederherstellen. Nachdem Sie eine Ressource aus dem Papierkorb wiederhergestellt haben, wird die Ressource aus dem Papierkorb entfernt und Sie können sie genauso wie jede andere Ressource dieses Typs in Ihrem Konto verwenden. Wenn der Aufbewahrungszeitraum abläuft und die Ressource nicht wiederhergestellt wird, wird die Ressource dauerhaft aus dem Papierkorb gelöscht und kann nicht mehr wiederhergestellt werden.

Durch die Verwendung des Papierkorbs wird die Geschäftskontinuität gewährleistet, indem Ihre geschäftskritischen Daten vor versehentlichem Löschen geschützt werden.

Themen

Funktionsweise

Um den Papierkorb zu aktivieren und zu verwenden, müssen Sie Aufbewahrungsregeln in den AWS Regionen erstellen, in denen Sie Ihre Ressourcen schützen möchten. Die Aufbewahrungsregeln umfassen Folgendes:

- Der Ressourcentyp, der geschützt werden soll.
- Die Ressourcen, die im Papierkorb aufbewahrt werden sollen, wenn sie gelöscht werden.
- Der Aufbewahrungszeitraum, für den Ressourcen im Papierkorb vor dem dauerhaften Löschen aufbewahrt werden sollen.

Sie können zwei Arten von Aufbewahrungsregeln für den Papierkorb erstellen:

- Tag-level retention rules (Aufbewahrungsregeln auf Tag-Ebene) – Diese Aufbewahrungsregel auf Tag-Ebene verwendet Ressourcen-Tags, um die Ressourcen zu identifizieren, die im Papierkorb aufbewahrt werden sollen. Für jede Aufbewahrungsregel geben Sie einen oder mehrere Tag-Schlüssel/Wert-Paare an. Ressourcen des spezifizierten Typs, die mit mindestens einem der Tag-Schlüssel/Wert-Paare markiert sind, die in der Aufbewahrungsregel angegeben sind, werden beim Löschen automatisch im Papierkorb aufbewahrt. Verwenden Sie diese Art von

Aufbewahrungsregel, wenn Sie bestimmte Ressourcen in Ihrem Konto basierend auf ihren Tags schützen möchten.

- Region-level retention rules (Aufbewahrungsregeln auf Regionsebene) – Für eine Aufbewahrungsregel auf Regionsebene sind keine Ressourcen-Tags angegeben. Sie gilt für alle Ressourcen des angegebenen Typs in der Region, in der die Regel erstellt wird, auch wenn die Ressourcen nicht markiert sind. Verwenden Sie diese Art von Aufbewahrungsregel, wenn Sie alle Ressourcen eines bestimmten Typs in einer bestimmten Region schützen möchten.

Während sich eine Ressource im Papierkorb befindet, können Sie sie jederzeit zur Verwendung wiederherstellen.

Die Ressource verbleibt im Papierkorb, bis eines der folgenden Ereignisse eintritt:

- Sie stellen den Snapshot manuell wieder her, um ihn zu verwenden. Wenn Sie eine Ressource aus dem Papierkorb wiederherstellen, wird sie aus dem Papierkorb entfernt und kann sofort verwendet werden. Sie können wiederhergestellte Ressourcen genauso wie jede andere Ressource dieses Typs in Ihrem Konto verwenden.
- Der Aufbewahrungszeitraum läuft ab. Wenn der Aufbewahrungszeitraum abläuft und die Ressource nicht wiederhergestellt wurde, wird die Ressource dauerhaft aus dem Papierkorb gelöscht und sie kann nicht mehr angezeigt oder wiederhergestellt werden.

Unterstützte Ressourcen

Der Papierkorb unterstützt das Erstellen der folgenden Ressourcentypen:

- Amazon-EBS-Snapshots

> **Important**
>
> Die Aufbewahrungsregeln für den Papierkorb gelten auch für archivierte Snapshots auf der Archivspeicherebene. Wenn Sie einen archivierten Snapshot löschen, der einer Aufbewahrungsregel entspricht, wird dieser archivierte Snapshot für den in der Aufbewahrungsregel festgelegten Archivierungszeitraum im Papierkorb beibehalten. Archivierte Snapshots werden mit dem Satz für archivierte Snapshots abgerechnet, während sie sich im Papierkorb befinden.

- Amazon-EBS-gestützte Amazon Machine Images (AMIs)

> **Note**
>
> Aufbewahrungsregeln gelten auch für deaktivierte AMIs.

Überlegungen

Bei der Arbeit mit Papierkorb und Aufbewahrungsregeln gelten die folgenden Überlegungen.

Allgemeine Überlegungen

- > **Important**
  >
  > Wenn Sie Ihre erste Aufbewahrungsregel erstellen, kann es bis zu 30 Minuten dauern, bis die Regel aktiv ist und Ressourcen aufbewahrt werden. Nachdem Sie die erste Aufbewahrungsregel erstellt haben, werden nachfolgende Aufbewahrungsregeln aktiv und bewahren fast umgehend Ressourcen auf.

- Wenn eine Ressource mehreren Aufbewahrungsregeln entspricht, wenn er gelöscht wird, hat die Aufbewahrungsregel mit dem längsten Aufbewahrungszeitraum Vorrang.
- Sie können eine Ressource nicht manuell aus dem Papierkorb löschen. Die Ressource wird automatisch gelöscht, wenn sein Aufbewahrungszeitraum abläuft.
- Während sich eine Ressource im Papierkorb befindet, können Sie sie nur anzeigen, wiederherstellen oder ihre Tags ändern. Bevor Sie die Ressource auf andere Weise verwenden können, müssen Sie ihn zuerst wiederherstellen.
- Wenn eine Ressource AWS-Service, wie AWS Backup oder Amazon Data Lifecycle Manager, löscht, die einer Aufbewahrungsregel entspricht, wird diese Ressource automatisch im Papierkorb aufbewahrt.
- Wenn eine Ressource in den Papierkorb gesendet wird, wird der Ressource das folgende vom System generierte Tag zugewiesen:
  - Tag-Schlüssel – `aws:recycle-bin:resource-in-bin`
  - Tag-Wert – `true`

  Sie können dieses Tag nicht manuell bearbeiten oder löschen. Wenn die Ressource aus dem Papierkorb wiederhergestellt wird, wird das Tag automatisch entfernt.

Überlegungen zu Snapshots

- **Important**

  Wenn Sie über Aufbewahrungsregeln für AMIs und die zugehörigen Snapshots verfügen, sollten Sie den Aufbewahrungszeitraum für die Snapshots gleich oder länger als den Aufbewahrungszeitraum für die AMIs festlegen. Dadurch löscht der Papierkorb die mit einem AMI verknüpften Snapshots nicht, bevor das AMI selbst gelöscht wird, da das AMI ansonsten nicht wiederhergestellt werden könnte.

- Wenn ein Snapshot für die schnelle Snapshot-Wiederherstellung aktiviert ist, wenn er gelöscht wird, wird die schnelle Snapshot-Wiederherstellung kurz nach dem Verschieben des Snapshots in den Papierkorb automatisch deaktiviert.
  - Wenn Sie den Snapshot wiederherstellen, bevor die schnelle Snapshot-Wiederherstellung für den Snapshot deaktiviert wird, bleibt er aktiviert.
  - Wenn Sie den Snapshot wiederherstellen, nachdem die schnelle Snapshot-Wiederherstellung deaktiviert wurde, bleibt er deaktiviert. Bei Bedarf müssen Sie die schnelle Snapshot-Wiederherstellung manuell wieder aktivieren.
- Wenn ein Snapshot freigegeben ist, wenn er gelöscht wird, wird die Freigabe automatisch aufgehoben, wenn er in den Papierkorb verschoben wird. Wenn Sie den Snapshot wiederherstellen, werden alle vorherigen Freigabeberechtigungen automatisch wiederhergestellt.
- Wenn ein Snapshot, der von einem anderen AWS Service erstellt wurde, z. B. in den Papierkorb geschickt AWS Backup wird und Sie diesen Snapshot später aus dem Papierkorb wiederherstellen, wird er nicht mehr von dem AWS Service verwaltet, der ihn erstellt hat. Sie müssen den Snapshot manuell löschen, wenn er nicht mehr länger benötigt wird.

Überlegungen für AMIs

- Es werden nur Amazon-EBS-gestützte AMIs unterstützt.
- **Important**

  Wenn Sie über Aufbewahrungsregeln für AMIs und die zugehörigen Snapshots verfügen, sollten Sie den Aufbewahrungszeitraum für die Snapshots gleich oder länger als den Aufbewahrungszeitraum für die AMIs festlegen. Dadurch löscht der Papierkorb die mit

einem AMI verknüpften Snapshots nicht, bevor das AMI selbst gelöscht wird, da das AMI ansonsten nicht wiederhergestellt werden könnte.

- Wenn ein AMI freigegeben ist, wenn es gelöscht wird, wird die Freigabe automatisch aufgehoben, wenn es in den Papierkorb verschoben wird. Wenn Sie das AMI wiederherstellen, werden alle vorherigen Freigabeberechtigungen automatisch wiederhergestellt.
- Bevor Sie ein AMI aus dem Papierkorb wiederherstellen können, müssen Sie zuerst alle zugehörigen Snapshots aus dem Papierkorb wiederherstellen und sicherstellen, dass sie sich im Zustand `available` befinden.
- Wenn die Snapshots, die mit dem AMI verknüpft sind, aus dem Papierkorb gelöscht werden, kann das AMI nicht mehr wiederhergestellt werden. Das AMI wird nach Ablauf der Aufbewahrungsfrist gelöscht.
- Wenn ein AMI, das von einem anderen AWS Dienst wie AWS Backup erstellt wurde, in den Papierkorb gesendet wird und Sie dieses AMI später aus dem Papierkorb wiederherstellen, wird es nicht mehr von dem AWS Dienst verwaltet, der es erstellt hat. Sie müssen das letzte AMI manuell löschen, wenn es nicht mehr benötigt wird.

Überlegungen zu den Snapshot-Richtlinien von Amazon Data Lifecycle Manager

- Wenn der Amazon Data Lifecycle Manager einen Snapshot löscht, der einer Aufbewahrungsregel entspricht, wird dieser Snapshot automatisch im Papierkorb beibehalten.
- Wenn Amazon Data Lifecycle Manager einen Snapshot löscht und ihn an den Papierkorb sendet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, und Sie den Snapshot manuell aus dem Papierkorb wiederherstellen, müssen Sie diesen Snapshot manuell löschen, wenn er nicht mehr benötigt wird. Amazon Data Lifecycle Manager verwaltet den Snapshot nicht mehr.
- Wenn Sie einen Snapshot, der von einer Richtlinie erstellt wurde, manuell löschen und sich dieser Snapshot im Papierkorb befindet, wenn der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, löscht Amazon Data Lifecycle Manager den Snapshot nicht. Amazon Data Lifecycle Manager verwaltet die Snapshots nicht, während sie im Papierkorb gespeichert sind.

  Wenn der Snapshot aus dem Papierkorb wiederhergestellt wird, bevor der Aufbewahrungsschwellenwert der Richtlinie erreicht wird, löscht Amazon Data Lifecycle Manager den Snapshot, sobald der Aufbewahrungsschwellenwert der Richtlinie erreicht wird.

  Wenn der Snapshot aus dem Papierkorb wiederhergestellt wird, nachdem der Aufbewahrungsschwellenwert der Richtlinie erreicht wurde, löscht Amazon Data Lifecycle Manager

den Snapshot nicht mehr. Sie müssen den Snapshot manuell löschen, wenn er nicht mehr benötigt wird.

Überlegungen zum AWS Backup

- Wenn AWS Backup einen Snapshot löscht, der einer Aufbewahrungsregel entspricht, wird dieser Snapshot automatisch im Papierkorb aufbewahrt.

Überlegungen zu archivierten Snapshots

- Die Aufbewahrungsregeln für den Papierkorb gelten auch für archivierte Snapshots auf der Archivspeicherebene. Wenn Sie einen archivierten Snapshot löschen, der einer Aufbewahrungsregel entspricht, wird dieser archivierte Snapshot für den in der Aufbewahrungsregel festgelegten Archivierungszeitraum im Papierkorb beibehalten.

  Archivierte Snapshots werden mit dem Satz für archivierte Snapshots abgerechnet, während sie sich im Papierkorb befinden.

  Wenn eine Aufbewahrungsregel einen archivierten Snapshot vor Ablauf der Mindestarchivierungsdauer von 90 Tagen aus dem Papierkorb löscht, werden Ihnen die verbleibenden Tage in Rechnung gestellt. Weitere Informationen finden Sie unter Preise und Abrechnung archivierter Snapshots im Amazon EBS-Benutzerhandbuch.

  Um einen archivierten Snapshot zu verwenden, der sich im Papierkorb befindet, müssen Sie den Snapshot zunächst aus dem Papierkorb wiederherstellen und ihn dann von der Archivstufe auf die Standardstufe zurückbringen.

Kontingente

Die folgenden Kontingente gelten für den Papierkorb.

Kontingent	Standardkontingent			
Aufbewahrungsregeln pro Region	250			

Kontingent	Standardkontingent			
Tag-Schlüssel/Wert-Paare pro Aufbewahrungsregel	50			

Zugehörige Services

Der Papierkorb funktioniert in Verbindung mit den folgenden Services:

- AWS CloudTrail – Ermöglicht es Ihnen, Ereignisse aufzuzeichnen, die im Papierkorb erfolgen. Weitere Informationen finden Sie unter Papierkorb überwachen mit AWS CloudTrail.

Preisgestaltung

Ressourcen im Papierkorb werden zu ihren Standardsätzen abgerechnet. Für die Verwendung des Papierkorbs und von Aufbewahrungsregeln fallen keine zusätzlichen Gebühren an. Weitere Informationen finden Sie unter Amazon EBS – Preise.

> **Note**
>
> Einige Ressourcen werden möglicherweise noch für kurze Zeit in der Papierkorb-Konsole oder in der AWS CLI API-Ausgabe angezeigt, nachdem ihre Aufbewahrungsfristen abgelaufen sind und sie dauerhaft gelöscht wurden. Diese Ressourcen werden Ihnen nicht in Rechnung gestellt. Die Abrechnung endet, sobald der Aufbewahrungszeitraum abgelaufen ist.

Bei der Verwendung können Sie die folgenden AWS generierten Kostenzuordnungs-Tags für die Kostenverfolgung und -zuweisung verwenden AWS Billing and Cost Management.

- Schlüssel: `aws:recycle-bin:resource-in-bin`
- Wert: `true`

Weitere Informationen finden Sie unter Von AWS generierte Kostenzuordnungs-Tags im AWS Billing and Cost Management -Benutzerhandbuch.

Erforderliche IAM-Berechtigungen

Standardmäßig verfügen Benutzer nicht über die Berechtigung, mit dem Papierkorb, mit Aufbewahrungsregeln oder mit Ressourcen, die sich im Papierkorb befinden, zu arbeiten. Damit Benutzer mit diesen Ressourcen arbeiten können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Nutzung bestimmter Ressourcen und API-Aktionen gewähren. Nachdem die Richtlinien erstellt wurden, müssen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzufügen.

Themen

Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln

Um mit Papierkorb- und Aufbewahrungsregeln arbeiten zu können, benötigen Benutzer die folgenden Berechtigungen.

- `rbin:CreateRule`
- `rbin:UpdateRule`
- `rbin:GetRule`
- `rbin:ListRules`
- `rbin:DeleteRule`
- `rbin:TagResource`
- `rbin:UntagResource`
- `rbin:ListTagsForResource`
- `rbin:LockRule`
- `rbin:UnlockRule`

Um die Papierkorb-Konsole verwenden zu können, benötigen Benutzer die `tag:GetResources`-Berechtigung.

Es folgt eine IAM-Beispielrichtlinie, die die `tag:GetResources`-Berechtigung für Konsolenbenutzer enthält. Werden einige Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": [
            "rbin:CreateRule",
            "rbin:UpdateRule",
            "rbin:GetRule",
            "rbin:ListRules",
            "rbin:DeleteRule",
            "rbin:TagResource",
            "rbin:UntagResource",
            "rbin:ListTagsForResource",
            "rbin:LockRule",
            "rbin:UnlockRule",
            "tag:GetResources"
        ],
        "Resource": "*"
    }]
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Berechtigungen zum Arbeiten mit Ressourcen im Papierkorb

Weitere Informationen zu den IAM-Berechtigungen, die für die Arbeit mit Ressourcen im Papierkorb erforderlich sind, finden Sie im folgenden Abschnitt:

- Berechtigungen zum Arbeiten mit Snapshots im Papierkorb
- Berechtigungen zum Arbeiten mit AMIs im Papierkorb

Bedingungsschlüssel für den Papierkorb

Der Papierkorb definiert die folgenden Bedingungsschlüssel, die Sie im `Condition`-Element einer IAM-Richtlinie zur Kontrolle der Bedingungen, unter denen die Richtlinienanweisung angewendet wird, verwenden können. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.

Themen

- rbin:Request/ResourceType-Bedingungsschlüssel
- rbin:Attribute/ResourceType-Bedingungsschlüssel

`rbin:Request/ResourceType`-Bedingungsschlüssel

Der `rbin:Request/ResourceType` Bedingungsschlüssel kann verwendet werden, um ListRulesZugriffe CreateRuleund Anfragen auf der Grundlage des für den `ResourceType` Anforderungsparameter angegebenen Werts zu filtern.

Beispiel 1 — CreateRule

Die folgende Beispiel-IAM-Richtlinie ermöglicht es IAM-Prinzipalen, CreateRuleAnfragen nur zu stellen, wenn der für den `ResourceType` Anforderungsparameter angegebene Wert oder ist. `EBS_SNAPSHOT` `EC2_IMAGE` Dies ermöglicht es dem Prinzipal, neue Aufbewahrungsregeln nur für Snapshots und AMIs zu erstellen.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:CreateRule"
```

```
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Beispiel 2 — ListRules

Die folgende Beispiel-IAM-Richtlinie ermöglicht es IAM-Prinzipalen, ListRulesAnfragen nur zu stellen, wenn der für den `ResourceType` Anforderungsparameter angegebene Wert lautet. `EBS_SNAPSHOT` Dies ermöglicht es dem Prinzipal, Aufbewahrungsregeln nur für Snapshots aufzulisten, und verhindert, dass er Aufbewahrungsregeln für jeden anderen Ressourcentyp auflisten kann.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:ListRules"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Request/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

`rbin:Attribute/ResourceType`-Bedingungsschlüssel

Der `rbin:Attribute/ResourceType` Bedingungsschlüssel kann verwendet werden, um den Zugriff auf DeleteRule,, GetRule, UpdateRule, LockRuleUnlockRuleTagResourceUntagResource, und ListTagsForResourceAnfragen basierend auf dem Wert des Attributs der Aufbewahrungsregel zu filtern. `ResourceType`

Beispiel 1 — UpdateRule

Das folgende Beispiel für eine IAM-Richtlinie ermöglicht es IAM-Prinzipalen, UpdateRuleAnfragen nur zu stellen, wenn das `ResourceType` Attribut der angeforderten Aufbewahrungsregel oder lautet. `EBS_SNAPSHOT` `EC2_IMAGE` Dies ermöglicht es dem Prinzipal, Aufbewahrungsregeln nur für Snapshots und AMIs zu aktualisieren.

```
{
    "Version" : "2012-10-17",
    "Statement" : [
        {
            "Effect" : "Allow",
            "Action" :[
                "rbin:UpdateRule"
            ],
            "Resource" : "*",
            "Condition" : {
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : ["EBS_SNAPSHOT", "EC2_IMAGE"]
                }
            }
        }
    ]
}
```

Beispiel 2 — DeleteRule

Das folgende Beispiel für eine IAM-Richtlinie ermöglicht es IAM-Prinzipalen, DeleteRuleAnfragen nur zu stellen, wenn das `ResourceType` Attribut der angeforderten Aufbewahrungsregel `EBS_SNAPSHOT` Dies ermöglicht es dem Prinzipal, Aufbewahrungsregeln nur für Snapshots zu löschen.

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

```
                "StringEquals" : {
                    "rbin:Attribute/ResourceType" : "EBS_SNAPSHOT"
                }
            }
        }
    ]
}
```

Arbeit mit Aufbewahrungsregeln

Um den Papierkorb zu aktivieren und zu verwenden, müssen Sie Aufbewahrungsregeln in den AWS Regionen erstellen, in denen Sie Ihre Ressourcen schützen möchten. Die Aufbewahrungsregeln umfassen Folgendes:

- Der Ressourcentyp, der geschützt werden soll.
- Die Ressourcen, die im Papierkorb aufbewahrt werden sollen, wenn sie gelöscht werden.
- Der Aufbewahrungszeitraum, für den Ressourcen im Papierkorb vor dem dauerhaften Löschen aufbewahrt werden sollen.

Sie können zwei Arten von Aufbewahrungsregeln für den Papierkorb erstellen:

- Tag-level retention rules (Aufbewahrungsregeln auf Tag-Ebene) – Diese Aufbewahrungsregel auf Tag-Ebene verwendet Ressourcen-Tags, um die Ressourcen zu identifizieren, die im Papierkorb aufbewahrt werden sollen. Für jede Aufbewahrungsregel geben Sie einen oder mehrere Tag-Schlüssel/Wert-Paare an. Ressourcen des spezifizierten Typs, die mit mindestens einem der Tag-Schlüssel/Wert-Paare markiert sind, die in der Aufbewahrungsregel angegeben sind, werden beim Löschen automatisch im Papierkorb aufbewahrt. Verwenden Sie diese Art von Aufbewahrungsregel, wenn Sie bestimmte Ressourcen in Ihrem Konto basierend auf ihren Tags schützen möchten.
- Region-level retention rules (Aufbewahrungsregeln auf Regionsebene) – Für eine Aufbewahrungsregel auf Regionsebene sind keine Ressourcen-Tags angegeben. Sie gilt für alle Ressourcen des angegebenen Typs in der Region, in der die Regel erstellt wird, auch wenn die Ressourcen nicht markiert sind. Verwenden Sie diese Art von Aufbewahrungsregel, wenn Sie alle Ressourcen eines bestimmten Typs in einer bestimmten Region schützen möchten.

Nachdem Sie eine Aufbewahrungsregel erstellt haben, werden Ressourcen, die ihren Kriterien entsprechen, automatisch für den angegebenen Aufbewahrungszeitraum im Papierkorb aufbewahrt, nachdem sie gelöscht werden.

Themen

Erstellen einer Aufbewahrungsregel

Beim Erstellen einer Aufbewahrungsregel müssen Sie die folgenden erforderlichen Parameter angeben:

- Der Ressourcentyp, der durch die Aufbewahrungsregel geschützt werden soll.
- Die Ressourcen, welche durch die Aufbewahrungsregel geschützt werden sollen. Sie können Aufbewahrungsregeln auf Tag-Ebene und Regionsebene erstellen.
  - Um eine Aufbewahrungsregel auf Tag-Ebene zu erstellen, geben Sie die Ressourcen-Tags an, die die zu schützenden Ressourcen identifizieren. Sie können bis zu 50 Tags für jede Regel angeben und dasselbe Tag-Schlüssel/Wert-Paare zu maximal fünf Aufbewahrungsregeln hinzufügen.
  - Um eine Aufbewahrungsregel auf Regionsebene zu erstellen, geben Sie keine Tag-Schlüssel/Wert-Paare an. In diesem Fall sind alle Ressourcen des angegebenen Typs geschützt.
- Der Zeitraum, für den Ressourcen nach dem Löschen im Papierkorb beibehalten werden sollen. Der Zeitraum kann bis zu 1 Jahr (365 Tage) betragen.

Sie können auch die folgenden optionalen-Parameter angeben:

- Ein Name für die Aufbewahrungsregel (optional). Er kann bis zu 255 Zeichen lang sein.
- Eine optionale Beschreibung der Aufbewahrungsregel. Die Beschreibung kann bis zu 255 Zeichen lang sein.

> **Note**
>
> Wir empfehlen, dass Sie keine personenbezogenen, vertraulichen oder sensiblen Informationen in die Beschreibung der Aufbewahrungsregel aufnehmen.

- Optionale Aufbewahrungsregel-Tags zur Identifizierung und Organisation Ihrer Aufbewahrungsregeln. Sie können jeder Regel bis zu 50 Tags zuweisen.

Sie können optional auch Aufbewahrungsregeln bei der Erstellung sperren. Wenn Sie eine Aufbewahrungsregel bei der Erstellung sperren, müssen Sie auch den Zeitraum für die Verzögerung beim Entsperren angeben, der 7 bis 30 Tage betragen kann. Aufbewahrungsregeln bleiben standardmäßig entsperrt, sofern Sie sie nicht ausdrücklich sperren.

Aufbewahrungsregeln funktionieren nur in den Regionen, in denen sie erstellt wurden. Wenn Sie den Papierkorb in anderen Regionen verwenden möchten, müssen Sie in diesen Regionen zusätzliche Aufbewahrungsregeln erstellen.

Sie können mit einer der folgenden Methoden eine Aufbewahrungsregel für den Papierkorb erstellen.

Recycle Bin console

So erstellen Sie eine Aufbewahrungsregel:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) und dann Create retention rule (Aufbewahrungsregel erstellen) aus.
3. Gehen Sie im Abschnitt Regeldetails wie folgt vor:
   a. (Optional) Geben Sie im Feld Retention rule name (Name der Aufbewahrungsregel) einen aussagekräftigen Namen für die Aufbewahrungsregel ein.
   b. (Optional) Geben Sie im Feld Retention rule description (Beschreibung der Aufbewahrungsregel) eine kurze Beschreibung für die Aufbewahrungsregel ein.
4. Gehen Sie im Abschnitt Rule settings (Regeleinstellungen) wie folgt vor:

a. Bei Resource type (Ressourcentyp) wählen Sie den Ressourcentyp für die zu schützende Aufbewahrungsregel aus. Die Aufbewahrungsregel behält nur Ressourcen dieses Typs im Papierkorb bei.

b. Führen Sie eine der folgenden Aktionen aus:

- Um eine Aufbewahrungsregel auf Regionsebene zu erstellen, die allen gelöschten Ressourcen des festgelegten Typs in der Region entspricht, wählen Sie Apply to all resources (Auf alle Ressourcen anwenden) aus. Beim Löschen behält die Aufbewahrungsregel alle gelöschten festgelegten Ressourcen im Papierkorb bei, auch wenn die Ressourcen keine Tags haben.
- Um eine Aufbewahrungsregel auf Tag-Ebene zu erstellen, geben Sie für Resource tags to match (Zuzuordnende Ressourcen-Tags) die Tag-Schlüssel/Wert-Paare ein, die verwendet werden sollen, um im Papierkorb aufzubewahrende Ressourcen des festgelegten Typs zu identifizieren. Nur Ressourcen des festgelegten Typs, die mindestens eines der angegebenen Tag-Schlüssel/Wert-Paare haben, werden von der Aufbewahrungsregel aufbewahrt.

c. Geben Sie für Retention period (Aufbewahrungszeitraum) die Anzahl der Tage ein, für die die Aufbewahrungsregel Ressourcen im Papierkorb beibehalten soll.

5. (Optional) Um die Aufbewahrungsregel zu sperren, wählen Sie unter Rule lock settings (Regelsperreinstellungen) die Option Lock (Sperren) aus und geben Sie dann für Unlock delay period (Verzögerungszeitraum entsperren) den Zeitraum für die Entsperrung in Tagen an. Eine gesperrte Aufbewahrungsregel kann nicht geändert oder gelöscht werden. Um die Regel zu ändern oder zu löschen, müssen Sie sie zuerst entsperren und dann warten, bis der Zeitraum für die Verzögerung beim Entsperren abgelaufen ist. Weitere Informationen finden Sie unter Sperren von Aufbewahrungsregeln.

   Um die Aufbewahrungsregel entsperrt zu lassen, behalten Sie für die Rule lock settings (Regelsperreinstellungen) die Option Unlock (Entsperren) bei. Eine entsperrte Aufbewahrungsregel kann jederzeit geändert oder gelöscht werden. Weitere Informationen finden Sie unter Entsperren von Aufbewahrungsregeln.

6. (Optional) Gehen Sie im Abschnitt Tags wie folgt vor:

   - Um die Regel mit benutzerdefinierten Tags zu versehen, wählen Sie Tag hinzufügen und geben Sie dann das Tag-Schlüssel/Wert-Paar ein.

7. Klicken Sie auf Create retention rule (Aufbewahrungsregel erstellen).

AWS CLI

So erstellen Sie eine Aufbewahrungsregel:

Verwenden Sie den AWS CLI -Befehl create-rule. Geben Sie für `--retention-period` die Anzahl der Tage an, die gelöschte Snapshots im Papierkorb aufbewahrt werden sollen. Für `--resource-type` geben Sie `EBS_SNAPSHOT` für Snapshots oder `EC2_IMAGE` für AMIs an. Um eine Aufbewahrungsregel auf Tag-Ebene zu erstellen, geben Sie für `--resource-tags` die Tags an, die zum Identifizieren der aufzubewahrenden Snapshots verwendet werden sollen. Um eine Aufbewahrungsregel auf Regionsebene zu erstellen, lassen Sie `--resource-tags` aus. Um eine Aufbewahrungsregel zu sperren, geben Sie den Zeitraum für die Entsperrung in Tagen an und geben Sie `--lock-configuration` an.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description" \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=unlock_delay_in_days}' \
--resource-tags ResourceTagKey=tag_key,ResourceTagValue=tag_value
```

Beispiel 1

Der folgende Beispielbefehl erstellt eine entsperrte Aufbewahrungsregel auf Regionsebene, die alle gelöschten Snapshots für einen Zeitraum von 7 Tagen beibehalten.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots"
```

Beispiel 2

Der folgende Beispielbefehl erstellt eine Regel auf Tag-Ebene, die gelöschte Snapshots, die mit `purpose=production` gekennzeichnet sind, für einen Zeitraum von 7 Tagen aufbewahrt.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match snapshots with a specific tag" \
```

```
--resource-tags ResourceTagKey=purpose,ResourceTagValue=production
```

Beispiel 3

Der folgende Beispielbefehl erstellt eine gesperrte Aufbewahrungsregel auf Regionsebene, die alle gelöschten Snapshots für einen Zeitraum von 7 Tagen beibehalten. Die Aufbewahrungsregel ist mit einer Freigabeverzögerung von 7 Tagen gesperrt.

```
aws rbin create-rule \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Match all snapshots" \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=7}'
```

Aufbewahrungsregeln für den Papierkorb anzeigen

Sie können die Aufbewahrungsregeln für den Papierkorb mit einer der folgenden Methoden anzeigen.

Recycle Bin console

So zeigen Sie Aufbewahrungsregeln an:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Das Raster listet alle Aufbewahrungsregeln für die ausgewählte Region auf. Um weitere Informationen zu einer bestimmten Aufbewahrungsregel anzuzeigen, markieren Sie sie im Raster.

AWS CLI

So zeigen Sie alle Ihre Aufbewahrungsregeln an:

Verwenden Sie den Befehl list-rules AWS CLI und für `--resource-type` geben Sie `EBS_SNAPSHOT` für Snapshots oder `EC2_IMAGE` für AMIs an.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT|EC2_IMAGE
```

Beispiel

Der folgende Beispielbefehl enthält alle Aufbewahrungsregeln für Snapshots.

```
aws rbin list-rules --resource-type EBS_SNAPSHOT
```

So zeigen Sie Informationen für eine bestimmte Aufbewahrungsregel an:

Verwenden Sie den Befehl get-rule AWS CLI .

```
aws rbin get-rule --identifier rule_ID
```

Beispiel

Mit dem folgenden Beispielbefehl rufen Sie Informationen zur Aufbewahrungsregel `pwxIkFcvge4` ab.

```
aws rbin get-rule --identifier pwxIkFcvge4
```

Aktualisieren von Aufbewahrungsregeln

Sie können Beschreibung, Ressourcen-Tags und den Aufbewahrungszeitraum einer entsperrten Aufbewahrungsregel jederzeit aktualisieren, nachdem sie erstellt wurde. Sie können den Ressourcentyp oder den Entsperrzeitraum einer Aufbewahrungsregel nicht aktualisieren, selbst wenn die Aufbewahrungsregel entsperrt ist.

Sie können eine gesperrte Aufbewahrungsregel in keiner Weise aktualisieren. Wenn Sie eine gesperrte Aufbewahrungsregel ändern müssen, müssen Sie sie zunächst entsperren und warten, bis der Zeitraum für die Verzögerung beim Entsperren abgelaufen ist.

Wenn Sie den Zeitraum für die Entsperrverzögerung für eine gesperrte Aufbewahrungsregel ändern müssen, müssen Sie die Aufbewahrungsregel entsperren und warten, bis der aktuelle Entsperrverzögerungszeitraum abläuft. Wenn der Zeitraum für die Entsperrung abgelaufen ist, müssen Sie die Aufbewahrungsregel erneut sperren und den neuen Zeitraum für die Entsperrverzögerung angeben.

> **Note**
>
> Wir empfehlen, dass Sie keine personenbezogenen, vertraulichen oder sensiblen Informationen in die Beschreibung der Aufbewahrungsregel aufnehmen.

Nachdem Sie eine Aufbewahrungsregel aktualisiert haben, gelten die Änderungen nur für neue Ressourcen, die damit beibehalten werden. Die Änderungen wirken sich nicht auf Ressourcen aus, die zuvor an den Papierkorb gesendet wurden. Wenn Sie beispielsweise den Aufbewahrungszeitraum einer Aufbewahrungsregel aktualisieren, werden nur Snapshots, die nach der Aktualisierung gelöscht werden, für den neuen Aufbewahrungszeitraum beibehalten. Snapshots, die vor dem Update an den Papierkorb gesendet wurden, werden weiterhin für die Dauer des vorherigen (alten) Aufbewahrungszeitraums beibehalten.

Sie können eine Aufbewahrungsregel mit einer der folgenden Methoden aktualisieren.

Recycle Bin console

So aktualisieren Sie eine Aufbewahrungsregel:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie im Raster die zu aktualisierende Aufbewahrungsregel aus und wählen Sie dann Aktionen, Edit retention rule (Aufbewahrungsregel bearbeiten).
4. Aktualisieren Sie im Abschnitt Regeldetails den Namen der Aufbewahrungsregel und die Beschreibung der Aufbewahrungsregel nach Bedarf.
5. Aktualisieren Sie im Abschnitt Rule settings (Regeleinstellungen) die Angaben für Resource type (Ressourcentyp), Resource tags to match (Zuzuordnende Ressourcen-Tags) und Retention period (Aufbewahrungszeitraum) nach Bedarf.
6. Fügen Sie im Abschnitt Tags nach Bedarf Tags für Aufbewahrungsregeln hinzu oder entfernen Sie sie.
7. Klicken Sie auf Save retention rule (Aufbewahrungsregel speichern).

AWS CLI

So aktualisieren Sie eine Aufbewahrungsregel:

Verwenden Sie den AWS CLI -Befehl update-rule. Für `--identifier` geben Sie die ID der zu aktualisierenden Aufbewahrungsregel an. Für `--resource-types` geben Sie `EBS_SNAPSHOT` für Snapshots oder `EC2_IMAGE` für AMIs an.

```
aws rbin update-rule \
--identifier rule_ID \
--retention-period RetentionPeriodValue=number_of_days,RetentionPeriodUnit=DAYS \
```

```
--resource-type EBS_SNAPSHOT|EC2_IMAGE \
--description "rule_description"
```

Beispiel

Der folgende Beispielbefehl aktualisiert die Aufbewahrungsregel `6lsJ2Fa9nh9`, um alle Snapshots für 7 Tage aufzubewahren, und aktualisiert ihre Beschreibung.

```
aws rbin update-rule \
--identifier 6lsJ2Fa9nh9 \
--retention-period RetentionPeriodValue=7,RetentionPeriodUnit=DAYS \
--resource-type EBS_SNAPSHOT \
--description "Retain for three weeks"
```

Sperren von Aufbewahrungsregeln

Mit dem Papierkorb können Sie die Aufbewahrungsregeln auf Regionsebene jederzeit sperren.

> **Note**
>
> Aufbewahrungsregeln auf Tag-Ebene können nicht gesperrt werden.

Eine gesperrte Aufbewahrungsregel kann nicht geändert oder gelöscht werden, auch nicht von Benutzern, die über die erforderlichen IAM-Berechtigungen verfügen. Aufbewahrungsregeln können gesperrt werden, um sie vor versehentlichen oder böswilligen Änderungen und Löschungen zu schützen.

Beim Sperren einer Aufbewahrungsregel müssen Sie einen Entsperrverzögerungszeitraum angeben. Dies ist der Zeitraum, den Sie nach dem Entsperren der Aufbewahrungsregel warten müssen, bevor Sie sie ändern oder löschen können. Sie können die Aufbewahrungsregel während des Zeitraums der Entsperrverzögerung nicht ändern oder löschen. Sie können die Aufbewahrungsregel erst ändern oder löschen, wenn die Verzögerungszeit für die Entsperrung abgelaufen ist.

Sie können den Zeitrahmen für die Entsperrung nach dem Sperren der Aufbewahrungsregel nicht mehr ändern. Wenn Ihre Kontoberechtigungen beeinträchtigt wurden, haben Sie durch die Verzögerung der Entsperrung zusätzliche Zeit, um Sicherheitsbedrohungen zu erkennen und darauf zu reagieren. Die Dauer dieses Zeitraums sollte länger sein als die Zeit, die Sie benötigen, um Sicherheitsverstöße zu erkennen und darauf zu reagieren. Um die richtige Dauer festzulegen, können

Sie frühere Sicherheitsvorfälle sowie die Zeit überprüfen, die zur Identifizierung und Behebung einer Kontoverletzung benötigt wurde.

Wir empfehlen Ihnen, die EventBridge Amazon-Regeln zu verwenden, um Sie über Änderungen des Sperrstatus der Aufbewahrungsregeln zu informieren. Weitere Informationen finden Sie unter Überwachen Sie den Papierkorb mit Amazon EventBridge.

Überlegungen

- Sie können nur Aufbewahrungsregeln auf Regionsebene sperren.
- Sie können eine entsperrte Aufbewahrungsregel jederzeit sperren.
- Die Verzögerung beim Entsperren muss 7 bis 30 Tage betragen.
- Sie können eine Aufbewahrungsregel während der Dauer der Entsperrverzögerung erneut sperren. Durch das erneute Sperren der Aufbewahrungsregel wird der Zeitraum für die Entsperrverzögerung zurückgesetzt.

Sie können mit einer der folgenden Methoden eine Aufbewahrungsregel auf Regionsebene sperren.

Recycle Bin console

So sperren Sie eine Aufbewahrungsregel

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Aufbewahrungsregeln aus.
3. Wählen Sie im Raster die zu sperrende Aufbewahrungsregel aus und wählen Sie dann Actions (Aktionen), Edit retention rule (Aufbewahrungsregel bearbeiten) aus.
4. Wählen Sie im Bildschirm „Sperrung der Aufbewahrungsregel bearbeiten“ die Option Lock (Sperren) und geben Sie dann unter Unlock delay period (Verzögerungszeit für die Entsperrung) die Verzögerungszeit für die Entsperrung in Tagen an.
5. Aktivieren Sie das Kontrollkästchen I acknowledge that locking the retention rule will prevent it from being modified or deleted (Ich bin mir bewusst, dass das Sperren der Aufbewahrungsregel verhindert, dass sie geändert oder gelöscht wird) und wählen Sie dann Save (Speichern).

AWS CLI

So sperren Sie eine entsperrte Aufbewahrungsregel

Verwenden Sie den AWS CLI -Befehl lock-rule. Geben Sie für `--identifier` die ID der zu sperrenden Aufbewahrungsregel an. Geben Sie für `--lock-configuration` den Zeitraum der Entsperrverzögerung in Tagen an.

```
aws rbin lock-rule \
--identifier rule_ID \
--lock-configuration
 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=number_of_days}'
```

Beispiel

Der folgende Beispielbefehl sperrt die Aufbewahrungsregel `6lsJ2Fa9nh9` und legt den Zeitraum für die Verzögerung beim Entsperren auf 15 Tage fest.

```
aws rbin lock-rule \
--identifier 6lsJ2Fa9nh9 \
--lock-configuration 'UnlockDelay={UnlockDelayUnit=DAYS,UnlockDelayValue=15}'
```

Entsperren von Aufbewahrungsregeln

Sie können eine gesperrte Aufbewahrungsregel nicht löschen oder ändern. Wenn Sie eine gesperrte Aufbewahrungsregel ändern müssen, müssen Sie sie zunächst entsperren. Nachdem Sie die Aufbewahrungsregel entsperrt haben, müssen Sie warten, bis der Zeitraum für die Verzögerung beim Entsperren abgelaufen ist, bevor Sie sie ändern oder löschen. Sie können eine Aufbewahrungsregel während des Zeitraums der Entsperrverzögerung nicht ändern oder löschen.

Eine entsperrte Aufbewahrungsregel kann jederzeit von einem Benutzer geändert und gelöscht werden, der über die erforderlichen IAM-Berechtigungen verfügt. Wenn Sie Ihre Aufbewahrungsregeln nicht sperren, können sie versehentlich oder böswillig geändert oder gelöscht werden.

Überlegungen

- Sie können eine Aufbewahrungsregel während der Dauer der Entsperrverzögerung erneut sperren.
- Sie können eine Aufbewahrungsregel erneut sperren, nachdem die Frist für die Entsperrung abgelaufen ist.
- Sie können die Entsperrverzögerung nicht umgehen.
- Sie können die Zeitdauer der Entsperrung nach der ersten Sperre nicht mehr ändern.

Wir empfehlen Ihnen, die EventBridge Amazon-Regeln zu verwenden, um Sie über Änderungen des Sperrstatus der Aufbewahrungsregeln zu informieren. Weitere Informationen finden Sie unter Überwachen Sie den Papierkorb mit Amazon EventBridge.

Sie können mit einer der folgenden Methoden eine gesperrte Aufbewahrungsregel auf Regionsebene entsperren.

Recycle Bin console

So entsperren Sie eine Aufbewahrungsregel

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Aufbewahrungsregeln aus.
3. Wählen Sie im Raster die zu gesperrte Aufbewahrungsregel aus und wählen Sie dann zum entsperren Actions (Aktionen), Edit retention rule (Aufbewahrungsregel bearbeiten).
4. Wählen Sie im Bildschirm „Sperrung der Aufbewahrungsregel bearbeiten“ die Option Unlock (Entsperren) und dann Save (Speichern).

AWS CLI

So entsperren Sie eine gesperrte Aufbewahrungsregel

Verwenden Sie den AWS CLI -Befehl unlock-rule. Geben Sie für `--identifier` die ID der zu entsperrenden Aufbewahrungsregel an.

```
aws rbin unlock-rule \
--identifier rule_ID
```

Beispiel

Der folgende Beispielbefehl entsperrt die Aufbewahrungsregel `6lsJ2Fa9nh9`

```
aws rbin unlock-rule \
--identifier 6lsJ2Fa9nh9
```

Zuweisen von Tags zu Aufbewahrungsregeln

Sie können Ihren Aufbewahrungsregeln benutzerdefinierte Tags zuweisen, um sie auf unterschiedliche Weise zu kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Auf diese

Weise können Sie basierend auf den von Ihnen zugewiesenen benutzerdefinierten Tags effizient eine bestimmte Aufbewahrungsregel finden.

Gehen Sie wie folgt vor, um einer Aufbewahrungsregel ein Tag zuzuweisen.

Recycle Bin console

So weisen Sie einer Aufbewahrungsregel ein Tag zu:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie die Aufbewahrungsregel aus, der Sie das Tag zuweisen möchten, und wählen Sie dann die Registerkarte Tags und dann Tags verwalten aus.
4. Wählen Sie Add tag. Geben Sie für Key (Schlüssel) den Tag-Schlüssel ein. Geben Sie für Value (Wert) den Tag-Wert ein.
5. Wählen Sie Save (Speichern) aus.

AWS CLI

So weisen Sie einer Aufbewahrungsregel ein Tag zu:

Verwenden Sie den Befehl tag-resource AWS CLI . Geben Sie für `--resource-arn` den Amazon-Ressourcennamen (ARN) der Aufbewahrungsregel an, die mit Tags versehen werden soll, und für `--tags` das Tag-Schlüssel/Wert-Paar.

```
aws rbin tag-resource \
--resource-arn retention_rule_arn \
--tags key=tag_key,value=tag_value
```

Beispiel

Der folgende Beispielbefehl weist der Aufbewahrungsregel `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3` das Tag `purpose=production` zu.

```
aws rbin tag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3 \
--tags key=purpose,value=production
```

Anzeigen von Tags für Aufbewahrungsregeln

Gehen Sie wie folgt vor, um die Tags anzuzeigen, die einer Aufbewahrungsregel zugewiesen sind.

Recycle Bin console

So zeigen Sie die Tags einer Aufbewahrungsregel an:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie die Aufbewahrungsregel aus, für die Tags angezeigt werden sollen, und wählen Sie die Registerkarte Tags aus.

AWS CLI

So zeigen Sie die Tags an, die einer Aufbewahrungsregel zugewiesen sind:

Verwenden Sie den AWS CLI -Befehl list-tags-for-resource. Geben Sie für `--resource-arn` den ARN der Aufbewahrungsregel an.

```
aws rbin list-tags-for-resource \
--resource-arn retention_rule_arn
```

Beispiel

Der folgende Beispielbefehl listet die Tags für die Aufbewahrungsregel `arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3` auf.

```
aws rbin list-tags-for-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/n0oSBBtItF3
```

Entfernen von Tags von Aufbewahrungsregeln

Sie können Tags mithilfe einer der folgenden Methoden aus einer Aufbewahrungsregel entfernen.

Recycle Bin console

So entfernen Sie ein Tag aus einer Aufbewahrungsregel:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/

2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie die Aufbewahrungsregel aus, aus der das Tag entfernt werden soll, wählen Sie die Registerkarte Tags und dann Tags verwalten aus.
4. Wählen Sie neben dem zu entfernenden Tag Entfernen aus.
5. Wählen Sie Save (Speichern) aus.

AWS CLI

So entfernen Sie ein Tag aus einer Aufbewahrungsregel:

Verwenden Sie den AWS CLI -Befehl untag-resource. Geben Sie für `--resource-arn` den ARN der Aufbewahrungsregel an. Geben Sie für `--tagkeys` die Tag-Schlüssel der zu entfernenden Tags an.

```
aws rbin untag-resource \
--resource-arn retention_rule_arn \
--tagkeys tag_key
```

Beispiel

Der folgende Beispielbefehl entfernt Tags mit dem Tag-Schlüssel `purpose` aus der Aufbewahrungsregel `arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3`.

```
aws rbin untag-resource \
--resource-arn arn:aws:rbin:us-east-1:123456789012:rule/nOoSBBtItF3 \
--tagkeys purpose
```

Löschen von Aufbewahrungsregeln für den Papierkorb

Sie können eine Aufbewahrungsregel jederzeit löschen. Wenn Sie eine Aufbewahrungsregel löschen, werden im Papierkorb keine neuen Ressourcen mehr aufbewahrt, nachdem sie gelöscht wurden. Ressourcen, die vor dem Löschen der Aufbewahrungsregel an den Papierkorb gesendet wurden, werden gemäß dem Aufbewahrungszeitraum, der in der Aufbewahrungsregel festgelegt ist, weiterhin im Papierkorb aufbewahrt. Wenn der Zeitraum abläuft, wird die Ressource dauerhaft aus dem Papierkorb gelöscht.

Sie können eine Aufbewahrungsregel mit einer der folgenden Methoden löschen.

Recycle Bin console

So löschen Sie eine Aufbewahrungsregel:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Retention rules (Aufbewahrungsregeln) aus.
3. Wählen Sie im Raster die zu löschende Aufbewahrungsregel aus und wählen Sie Actions (Aktionen), Delete retention rule (Aufbewahrungsregel löschen) aus.
4. Geben Sie die Bestätigungsnachricht ein, wenn Sie dazu aufgefordert werden, und wählen Sie Delete retention rule (Aufbewahrungsregel löschen).

AWS CLI

So löschen Sie eine Aufbewahrungsregel:

Verwenden Sie den AWS CLI -Befehl delete-rule. Geben Sie für `--identifier` die ID der zu löschenden Aufbewahrungsregel an.

```
aws rbin delete-rule --identifier rule_ID
```

Beispiel

Der folgende Beispielbefehl löscht die Aufbewahrungsregel `6lsJ2Fa9nh9`.

```
aws rbin delete-rule --identifier 6lsJ2Fa9nh9
```

Arbeiten mit Ressourcen im Papierkorb

Der Papierkorb unterstützt das Erstellen der folgenden Ressourcentypen:

- Amazon-EBS-Snapshots
- Amazon-EBS-gestützte Amazon Machine Images (AMIs)

Aufgaben

- Wiederherstellen von Snapshots aus dem Papierkorb
- Wiederherstellen von AMIs aus dem Papierkorb

Wiederherstellen von Snapshots aus dem Papierkorb

Der Papierkorb ist ein Datenwiederherstellungsfeature, mit dem Sie versehentlich gelöschte Amazon-EBS-Snapshots und EBS-gestützte AMIs wiederherstellen können. Wenn Sie den Papierkorb verwenden, werden Ressourcen nach dem Löschen für einen von Ihnen angegebenen Zeitraum im Papierkorb aufbewahrt, bevor sie endgültig gelöscht werden.

Sie können eine Ressource vor Ablauf des Aufbewahrungszeitraums jederzeit aus dem Papierkorb wiederherstellen. Nachdem Sie eine Ressource aus dem Papierkorb wiederhergestellt haben, wird die Ressource aus dem Papierkorb entfernt und Sie können sie genauso wie jede andere Ressource dieses Typs in Ihrem Konto verwenden. Wenn der Aufbewahrungszeitraum abläuft und die Ressource nicht wiederhergestellt wird, wird die Ressource dauerhaft aus dem Papierkorb gelöscht und kann nicht mehr wiederhergestellt werden.

Snapshots im Papierkorb werden mit demselben Satz in Rechnung gestellt wie normale Snapshots in Ihrem Konto. Für die Verwendung des Papierkorbs und von Aufbewahrungsregeln fallen keine zusätzlichen Gebühren an. Weitere Informationen finden Sie unter Amazon EBS – Preise.

Weitere Informationen finden Sie unter Papierkorb.

Themen

- Berechtigungen zum Arbeiten mit Snapshots im Papierkorb
- Anzeigen von Snapshots im Papierkorb
- Wiederherstellen von Snapshots aus dem Papierkorb

Berechtigungen zum Arbeiten mit Snapshots im Papierkorb

Standardmäßig verfügen Benutzer nicht über die Berechtigung zum Arbeiten mit Snapshots, die sich im Papierkorb befinden. Damit Benutzer mit diesen Ressourcen arbeiten können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Nutzung bestimmter Ressourcen und API-Aktionen gewähren. Nachdem die Richtlinien erstellt wurden, müssen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzufügen.

Um Snapshots im Papierkorb anzuzeigen und wiederherzustellen, müssen Benutzer über die folgenden Berechtigungen verfügen:

- `ec2:ListSnapshotsInRecycleBin`
- `ec2:RestoreSnapshotFromRecycleBin`

Zum Verwalten von Tags für Schnappschüsse im Papierkorb benötigen Benutzer die folgenden zusätzlichen Berechtigungen.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Um die Papierkorb-Konsole verwenden zu können, benötigen Benutzer die `ec2:DescribeTags`-Berechtigung.

Es folgt eine IAM-Beispielrichtlinie. Sie umfasst die `ec2:DescribeTags`-Berechtigung für Konsolenbenutzer und enthält die `ec2:CreateTags`- und `ec2:DeleteTags`-Berechtigungen zum Verwalten von Tags. Werden die Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListSnapshotsInRecycleBin",
            "ec2:RestoreSnapshotFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region:account-id:snapshot/*"
      },

    ]
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.
- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Weitere Informationen zu den Berechtigungen, die zur Verwendung des Papierkorbs erforderlich sind, finden Sie unter Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln.

Anzeigen von Snapshots im Papierkorb

Während sich ein Snapshot im Papierkorb befindet, können Sie beschränkte Informationen darüber anzeigen. Hier einige Beispiele:

- Die ID des Snapshots.
- Die Beschreibung des Snapshots.
- Die ID des Volumes, aus dem der Snapshot erstellt wurde.
- Das Datum und die Uhrzeit, zu der der Snapshot gelöscht und in den Papierkorb verschoben wurde.
- Das Datum und die Uhrzeit, zu der der Aufbewahrungszeitraum abläuft. Der Snapshot wird nun dauerhaft aus dem Papierkorb entfernt.

Sie haben mehrere Möglichkeiten, um die Snapshots im Papierkorb anzuzeigen.

Recycle Bin console

So zeigen Sie Snapshots im Papierkorb mit der Konsole an:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/

2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.
3. Im Raster werden alle Snapshots aufgelistet, die sich derzeit im Papierkorb befinden. Um die Details für einen bestimmten Snapshot anzuzeigen, wählen Sie ihn im Raster aus und wählen Sie Aktionen, Details anzeigen.

AWS CLI

Um Schnappschüsse im Papierkorb anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den Befehl AWS CLI list-snapshots-in-recycle-bin. Schließen Sie die Option `--snapshot-id` ein, um einen bestimmten Snapshot anzuzeigen. Oder lassen Sie die `--snapshot-id`-Option weg, um alle Snapshots im Papierkorb anzuzeigen.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snapshot_id
```

Der folgende Befehl bietet beispielsweise Informationen zum Snapshot `snap-01234567890abcdef` im Papierkorb.

```
aws ec2 list-snapshots-in-recycle-bin --snapshot-id snap-01234567890abcdef
```

Beispielausgabe:

```
{
    "SnapshotRecycleBinInfo": [
        {
            "Description": "Monthly data backup snapshot",
            "RecycleBinEnterTime": "2021-12-01T13:00:00.000Z",
            "RecycleBinExitTime": "2021-12-15T13:00:00.000Z",
            "VolumeId": "vol-abcdef09876543210",
            "SnapshotId": "snap-01234567890abcdef"
        }
    ]
}
```

Wiederherstellen von Snapshots aus dem Papierkorb

Solange sich ein Snapshot im Papierkorb befindet, können Sie ihn auf keine Weise verwenden. Um den Snapshot verwenden zu können, müssen Sie ihn zuerst wiederherstellen. Wenn Sie einen Snapshot aus dem Papierkorb wiederherstellen, kann er sofort verwendet werden und wird aus dem

Papierkorb entfernt. Sie können einen wiederhergestellten Snapshot genauso verwenden wie jeden anderen Snapshot in Ihrem Konto.

Sie haben mehrere Möglichkeiten, um einen Snapshot aus dem Papierkorb wiederherzustellen.

Recycle Bin console

So stellen Sie einen Snapshot mit der Konsole aus dem Papierkorb wieder her:

1. Öffnen Sie die Papierkorb-Konsole unter https://console.aws.amazon.com/rbin/home/
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.
3. Im Raster werden alle Snapshots aufgelistet, die sich derzeit im Papierkorb befinden. Wählen Sie den wiederherzustellenden Snapshot aus und wählen Sie Wiederherstellen.
4. Wählen Sie Wiederherstellen, wenn Sie dazu aufgefordert werden.

AWS CLI

Um einen gelöschten Snapshot aus dem Papierkorb wiederherzustellen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl AWS CLI restore-snapshot-from-recycle-bin. Geben Sie für `--snapshot-id` die ID des wiederherzustellenden Snapshots an.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snapshot_id
```

Mit dem folgenden Befehl wird beispielsweise der Snapshot `snap-01234567890abcdef` aus dem Papierkorb wiederhergestellt.

```
aws ec2 restore-snapshot-from-recycle-bin --snapshot-id snap-01234567890abcdef
```

Beispielausgabe:

```
{
    "SnapshotId": "snap-01234567890abcdef",
    "Description": "Monthly data backup snapshot",
    "Encrypted": false,
    "OwnerId": "111122223333",
    "Progress": "100%",
    "StartTime": "2021-12-01T13:00:00.000000+00:00",
    "State": "recovering",
```

```
    "VolumeId": "vol-ffffffff",
    "VolumeSize": 30
}
```

Wiederherstellen von AMIs aus dem Papierkorb

Der Papierkorb ist ein Datenwiederherstellungsfeature, mit dem Sie versehentlich gelöschte Amazon-EBS-Snapshots und EBS-gestützte AMIs wiederherstellen können. Wenn Sie den Papierkorb verwenden, werden Ressourcen nach dem Löschen für einen von Ihnen angegebenen Zeitraum im Papierkorb aufbewahrt, bevor sie endgültig gelöscht werden.

Sie können eine Ressource vor Ablauf des Aufbewahrungszeitraums jederzeit aus dem Papierkorb wiederherstellen. Nachdem Sie eine Ressource aus dem Papierkorb wiederhergestellt haben, wird die Ressource aus dem Papierkorb entfernt und Sie können sie genauso wie jede andere Ressource dieses Typs in Ihrem Konto verwenden. Wenn der Aufbewahrungszeitraum abläuft und die Ressource nicht wiederhergestellt wird, wird die Ressource dauerhaft aus dem Papierkorb gelöscht und kann nicht mehr wiederhergestellt werden.

Es fallen keine zusätzlichen Gebühren für AMIs im Papierkorb an.

Weitere Informationen finden Sie unter Papierkorb.

Themen

- Berechtigungen zum Arbeiten mit AMIs im Papierkorb
- Anzeigen von AMIs im Papierkorb
- Wiederherstellen von AMIs aus dem Papierkorb

Berechtigungen zum Arbeiten mit AMIs im Papierkorb

Standardmäßig verfügen Benutzer nicht über die Berechtigung zum Arbeiten mit AMIs, die sich im Papierkorb befinden. Damit Benutzer mit diesen Ressourcen arbeiten können, müssen Sie IAM-Richtlinien erstellen, die die Berechtigung zur Nutzung bestimmter Ressourcen und API-Aktionen gewähren. Nachdem die Richtlinien erstellt wurden, müssen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzufügen.

Um AMIs, die sich im Papierkorb befinden, anzeigen und wiederherstellen zu können, müssen Benutzer über die folgenden Berechtigungen verfügen:

- `ec2:ListImagesInRecycleBin`

- `ec2:RestoreImageFromRecycleBin`

Zur Verwaltung von Tags für AMIs im Papierkorb, müssen Benutzer über die folgenden zusätzlichen Berechtigungen verfügen.

- `ec2:CreateTags`
- `ec2:DeleteTags`

Um die Papierkorb-Konsole verwenden zu können, benötigen Benutzer die `ec2:DescribeTags`-Berechtigung.

Es folgt eine IAM-Beispielrichtlinie. Sie umfasst die `ec2:DescribeTags`-Berechtigung für Konsolenbenutzer und enthält die `ec2:CreateTags`- und `ec2:DeleteTags`-Berechtigungen zum Verwalten von Tags. Werden die Berechtigungen nicht benötigt, können Sie sie aus der Richtlinie entfernen.

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
            "ec2:ListImagesInRecycleBin",
            "ec2:RestoreImageFromRecycleBin"
        ],
        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags"
        ],
        "Resource": "arn:aws:ec2:Region::image/*"
      }
    ]
}
```

Um Zugriff zu gewähren, fügen Sie Ihren Benutzern, Gruppen oder Rollen Berechtigungen hinzu:

- Benutzer und Gruppen in AWS IAM Identity Center:

  Erstellen Sie einen Berechtigungssatz. Befolgen Sie die Anweisungen unter Erstellen eines Berechtigungssatzes im AWS IAM Identity Center -Benutzerhandbuch.

- Benutzer, die in IAM über einen Identitätsanbieter verwaltet werden:

  Erstellen Sie eine Rolle für den Identitätsverbund. Befolgen Sie die Anweisungen unter Erstellen einer Rolle für einen externen Identitätsanbieter (Verbund) im IAM-Benutzerhandbuch.

- IAM-Benutzer:
  - Erstellen Sie eine Rolle, die Ihr Benutzer annehmen kann. Folgen Sie den Anweisungen unter Erstellen einer Rolle für einen IAM-Benutzer im IAM-Benutzerhandbuch.
  - (Nicht empfohlen) Weisen Sie einem Benutzer eine Richtlinie direkt zu oder fügen Sie einen Benutzer zu einer Benutzergruppe hinzu. Befolgen Sie die Anweisungen unter Hinzufügen von Berechtigungen zu einem Benutzer (Konsole) im IAM-Benutzerhandbuch.

Weitere Informationen zu den Berechtigungen, die zur Verwendung des Papierkorbs erforderlich sind, finden Sie unter Berechtigungen zum Arbeiten mit dem Papierkorb und Aufbewahrungsregeln.

Anzeigen von AMIs im Papierkorb

Wenn sich ein AMI im Papierkorb befindet, können Sie eingeschränkte Informationen dazu anzeigen, unter anderem:

- Name, Beschreibung und eindeutige ID des AMI
- Datum und Uhrzeit, zu der das AMI gelöscht und in den Papierkorb verschoben wurde
- Das Datum und die Uhrzeit, zu der der Aufbewahrungszeitraum abläuft. Das AMI wird zu diesem Zeitpunkt dauerhaft gelöscht.

Sie haben mehrere Möglichkeiten, um die AMIs im Papierkorb anzuzeigen.

Recycle Bin console

Gelöschte AMIs im Papierkorb über die Konsole anzeigen

1. Öffnen Sie die Papierkorb-Konsole unter console.aws.amazon.com/rbin/home/.
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.

3. Im Raster werden alle Ressourcen aufgelistet, die sich derzeit im Papierkorb befinden. Um Details zu einem bestimmten AMI anzuzeigen, wählen Sie es im Raster aus und wählen dann Actions (Aktionen), View details (Details anzeigen) aus.

AWS CLI

Um gelöschte AMIs im Papierkorb anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den Befehl list-images-in-recycle-bin AWS CLI . Um bestimmte AMIs anzuzeigen, schließen Sie die `--image-id`-Option ein und geben Sie die IDs der anzuzeigenden AMIs an. Sie können bis zu 20 IDs in einer einzigen Anforderung angeben.

Um alle AMIs im Papierkorb anzuzeigen, lassen Sie die `--image-id`-Option weg. Wenn Sie keinen Wert für `--max-items` angeben, gibt der Befehl standardmäßig 1 000 Elemente pro Seite zurück. Weitere Informationen finden Sie unter Paginierung in der Amazon-EC2-API-Referenz.

```
aws ec2 list-images-in-recycle-bin --image-id ami_id
```

Der folgende Befehl bietet beispielsweise Informationen über das AMI `ami-01234567890abcdef` im Papierkorb.

```
aws ec2 list-images-in-recycle-bin --image-id ami-01234567890abcdef
```

Beispielausgabe:

```
{
    "Images": [
        {
            "ImageId": "ami-0f740206c743d75df",
            "Name": "My AL2 AMI",
            "Description": "My Amazon Linux 2 AMI",
            "RecycleBinEnterTime": "2021-11-26T21:04:50+00:00",
            "RecycleBinExitTime": "2022-03-06T21:04:50+00:00"
        }
    ]
}
```

> **Important**
>
> Wenn Sie die folgende Fehlermeldung erhalten, müssen Sie möglicherweise Ihre AWS CLI Version aktualisieren. Weitere Informationen finden Sie unter Befehl nicht gefunden-Fehlermeldungen.
>
> ```
> aws.exe: error: argument operation: Invalid choice, valid choices are: ...
> ```

Wiederherstellen von AMIs aus dem Papierkorb

Solange sich ein AMI im Papierkorb befindet, können Sie es in keiner Weise verwenden. Um das AMI verwenden zu können, müssen Sie es zuerst wiederherstellen. Wenn Sie ein AMI aus dem Papierkorb wiederherstellen, kann es sofort verwendet werden und wird aus dem Papierkorb entfernt. Sie können ein wiederhergestelltes AMI genauso verwenden wie jedes andere AMI in Ihrem Konto.

Sie haben mehrere Möglichkeiten, ein AMI aus dem Papierkorb wiederherzustellen.

Recycle Bin console

AMI aus dem Papierkorb über die Konsole wiederherstellen

1. Öffnen Sie die Papierkorb-Konsole unter console.aws.amazon.com/rbin/home/.
2. Wählen Sie im Navigationsbereich Recycle Bin (Papierkorb) aus.
3. Im Raster werden alle Ressourcen aufgelistet, die sich derzeit im Papierkorb befinden. Wählen Sie das wiederherzustellende AMI aus und wählen Sie dann Recover (Wiederherstellen).
4. Wählen Sie Wiederherstellen, wenn Sie dazu aufgefordert werden.

AWS CLI

Um ein gelöschtes AMI aus dem Papierkorb wiederherzustellen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl restore-image-from-recycle-bin AWS CLI . Geben Sie für `--image-id` die ID des wiederherzustellenden AMI an.

```
aws ec2 restore-image-from-recycle-bin --image-id ami_id
```

Mit dem folgenden Befehl wird beispielsweise das AMI `ami-01234567890abcdef` aus dem Papierkorb wiederhergestellt.

```
aws ec2 restore-image-from-recycle-bin --image-id ami-01234567890abcdef
```

Wenn der Befehl erfolgreich ausgeführt wird, wird keine Ausgabe zurückgegeben.

> **Important**
>
> Wenn Sie die folgende Fehlermeldung erhalten, müssen Sie möglicherweise Ihre AWS CLI Version aktualisieren. Weitere Informationen finden Sie unter Befehl nicht gefunden-Fehlermeldungen.
>
> ```
> aws.exe: error: argument operation: Invalid choice, valid choices are: ...
> ```

Überwachen des Papierkorbs

Sie können die folgenden Funktionen zur Überwachung des Papierkorbs verwenden.

Themen

- Überwachen Sie den Papierkorb mit Amazon EventBridge
- Papierkorb überwachen mit AWS CloudTrail

Überwachen Sie den Papierkorb mit Amazon EventBridge

Der Papierkorb sendet Ereignisse an Amazon EventBridge für Aktionen, die im Rahmen der Aufbewahrungsregeln ausgeführt wurden. Mit können Sie Regeln festlegen EventBridge, die als Reaktion auf diese Ereignisse programmatische Aktionen auslösen. Sie können beispielsweise eine EventBridge Regel erstellen, die eine Benachrichtigung an Ihre E-Mail-Adresse sendet, wenn eine Aufbewahrungsregel entsperrt wird und ihre Sperrverzögerung eintritt. Weitere Informationen finden Sie unter EventBridge Amazon-Regeln erstellen, die auf Ereignisse reagieren.

Ereignisse in EventBridge werden als JSON-Objekte dargestellt. Die Felder, die für das Ereignis einzigartig sind, sind im Abschnitt `detail` des JSON-Objekt enthalten. Im Feld `event` ist der Name des Ereignisses enthalten. Das Feld `result` enthält den vollständigen Status der Aktion, die zur

Auslösung des Ereignisses führte. Weitere Informationen finden Sie unter Amazon EventBridge Event Patterns im EventBridge Amazon-Benutzerhandbuch.

Weitere Informationen zu Amazon EventBridge finden Sie unter Was ist Amazon EventBridge? im EventBridge Amazon-Benutzerhandbuch.

Ereignisse

- RuleLocked
- RuleChangeVersucht
- RuleUnlockGeplant
- RuleUnlockingHinweis
- RuleUnlocked

RuleLocked

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das der Papierkorb generiert, wenn eine Aufbewahrungsregel erfolgreich gesperrt wurde. Dieses Ereignis kann durch CreateRuleund LockRuleAnfragen generiert werden. Die API, die das Ereignis generiert hat, ist im `api-name`-Feld vermerkt.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Locked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "CreateRule"
  }
```

```
}
```

RuleChangeVersucht

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das der Papierkorb für erfolglose Versuche, eine gesperrte Regel zu ändern oder zu löschen, generiert. Dieses Ereignis kann durch DeleteRuleund UpdateRule-Anfragen generiert werden. Die API, die das Ereignis generiert hat, ist im `api-name`-Feld vermerkt.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Change Attempted",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "api-name": "DeleteRule"
  }
}
```

RuleUnlockGeplant

Im Folgenden sehen Sie ein Beispiel für ein Ereignis, das der Papierkorb erzeugt, wenn eine Aufbewahrungsregel entsperrt wird und die Verzögerungszeit für die Entsperrung beginnt.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlock Scheduled",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z",
  }
}
```

RuleUnlockingHinweis

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das der Papierkorb täglich generiert, während sich eine Aufbewahrungsregel in ihrer Entsperrungsverzögerung befindet, bis zum Tag vor dem Ablauf der Entsperrungsverzögerung.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocking Notice",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

RuleUnlocked

Im Folgenden finden Sie ein Beispiel für ein Ereignis, das der Papierkorb generiert, wenn die Frist für die Entsperrung einer Aufbewahrungsregel abläuft und die Aufbewahrungsregel geändert oder gelöscht werden kann.

```
{
  "version": "0",
  "id": "exampleb-b491-4cf7-a9f1-bf370example",
  "detail-type": "Recycle Bin Rule Unlocked",
  "source": "aws.rbin",
  "account": "123456789012",
  "time": "2022-08-10T16:37:50Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:rbin:us-west-2:123456789012:rule/a12345abcde"
  ],
  "detail":
  {
    "detail-version": " 1.0.0",
    "rule-id": "a12345abcde",
    "rule-description": "locked account level rule",
    "unlock-delay-period": "30 days",
    "scheduled-unlock-time": "2022-09-10T16:37:50Z"
  }
}
```

Papierkorb überwachen mit AWS CloudTrail

Der Papierkorb-Service ist in integriert AWS CloudTrail. CloudTrail ist ein Dienst, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Dienst ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe, die im Papierkorb ausgeführt werden, als Ereignisse. Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon Simple Storage Service (Amazon S3) -Bucket aktivieren. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Verwaltungsereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der gesammelten Informationen können Sie ermitteln, welche Anfrage CloudTrail an den Papierkorb gestellt wurde, von welcher IP-Adresse aus die Anfrage gestellt wurde, wer die Anfrage gestellt hat, wann sie gestellt wurde, und weitere Informationen.

Weitere Informationen zu CloudTrail finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen zum Papierkorb finden Sie in CloudTrail

CloudTrail ist in Ihrem AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn die Aktivität unterstützter Ereignisse im Papierkorb stattfindet, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung der Ereignisse in Ihrem AWS Konto, einschließlich der Ereignisse für den Papierkorb, erstellen Sie einen Trail. Ein Trail ermöglicht die CloudTrail Übermittlung von Protokolldateien an einen S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen Regionen in der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie unter Übersicht zum Erstellen eines Trails im AWS CloudTrail -Benutzerhandbuch.

Unterstützte API-Aktionen

Für den Papierkorb können Sie CloudTrail die folgenden API-Aktionen als Verwaltungsereignisse protokollieren.

- CreateRule
- UpdateRule
- GetRules
- ListRule
- DeleteRule
- TagResource
- UntagResource
- ListTagsForResource
- LockRule
- UnlockRule

Weitere Informationen zur Protokollierung von Verwaltungsereignissen finden Sie im CloudTrail Benutzerhandbuch unter Protokollieren von Verwaltungsereignissen für Trails.

Informationen zur Identität

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Anmeldeinformationen des Root-Benutzers oder des Benutzers gestellt wurde.
- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen erhalten Sie beim CloudTrail Benutzer IdentityElement.

Auswerten der Papierkorb-Protokolldateieinträge

Ein Trail ist eine Konfiguration, die die Übermittlung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Im Folgenden finden CloudTrail Sie Beispiele für Protokolleinträge.

CreateRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
```

```
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:22Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "CreateRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": {
    "identifier": "jkrnexample"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


GetRule


```
{
  "eventVersion": "1.08",
```

```
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:45:33Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "GetRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
```

```
}
```

ListRules

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:44:37Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListRules",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "resourceTags": [
      {
        "resourceTagKey": "test",
        "resourceTagValue": "test"
      }
    ]
  },
  "responseElements": null,
```

```
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

UpdateRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:03Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UpdateRule",
  "awsRegion": "us-west-2",
```

```
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample",
    "retentionPeriod": {
      "retentionPeriodValue": 365,
      "retentionPeriodUnit": "DAYS"
    },
    "description": "Match all snapshots",
    "resourceType": "EBS_SNAPSHOT"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


DeleteRule


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
```

```
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-02T21:43:38Z"
      }
    }
  },
  "eventTime": "2021-08-02T21:46:25Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "DeleteRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.9 Python/3.6.14
 Linux/4.9.230-0.1.ac.224.84.332.metal1.x86_64 botocore/1.21.9",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": null,
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


TagResource


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
```

```
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:43:15Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tags": [
      {
        "key": "purpose",
        "value": "production"
      }
    ]
  },
  "responseElements": null,
  "requestID": "examplee-7962-49ec-8633-795efexample",
  "eventID": "example4-6826-4c0a-bdec-0bab1example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
```

```
  }
}
```

UntagResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:44:16Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UntagResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234",
    "tagKeys": [
      "purpose"
    ]
  },
  "responseElements": null,
  "requestID": "example7-6c1e-4f09-9e46-bb957example",
```

```
  "eventID": "example6-75ff-4c94-a1cd-4d5f5example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

ListTagsForResource

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-10-22T21:38:34Z"
      }
    }
  },
  "eventTime": "2021-10-22T21:42:31Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "ListTagsForResource",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
```

```
  "userAgent": "aws-cli/1.20.26 Python/3.6.14
 Linux/4.9.273-0.1.ac.226.84.332.metal1.x86_64 botocore/1.21.26",
  "requestParameters": {
    "resourceArn": "arn:aws:rbin:us-west-2:123456789012:rule/ABCDEF01234"
  },
  "responseElements": null,
  "requestID": "example8-10c7-43d4-b147-3d9d9example",
  "eventID": "example2-24fc-4da7-a479-c9748example",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "123456789012",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

LockRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
```

```
    }
  },
  "eventTime": "2022-10-25T00:45:19Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "LockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    }
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EBS_SNAPSHOT",
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "locked"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
```

```
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```

UnlockRule

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "123456789012",
    "arn": "arn:aws:iam::123456789012:root",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:role/Admin",
        "accountId": "123456789012",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2022-10-25T00:45:11Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2022-10-25T00:46:17Z",
  "eventSource": "rbin.amazonaws.com",
  "eventName": "UnlockRule",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "123.123.123.123",
  "userAgent": "python-requests/2.25.1",
  "requestParameters": {
    "identifier": "jkrnexample"
  },
  "responseElements": {
    "identifier": "jkrnexample",
    "description": "",
    "resourceType": "EC2_IMAGE",
```

```
    "retentionPeriod": {
      "retentionPeriodValue": 7,
      "retentionPeriodUnit": "DAYS"
    },
    "resourceTags": [],
    "status": "available",
    "lockConfiguration": {
      "unlockDelay": {
        "unlockDelayValue": 7,
        "unlockDelayUnit": "DAYS"
      }
    },
    "lockState": "pending_unlock",
    "lockEndTime": "Nov 1, 2022, 12:46:17 AM"
  },
  "requestID": "ex0577a5-amc4-pl4f-ef51-50fdexample",
  "eventID": "714fafex-2eam-42pl-913e-926d4example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.2",
    "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
    "clientProvidedHostHeader": "rbin.us-west-2.amazonaws.com"
  }
}
```


Ressourcenstandorte

Amazon EC2 EC2-Ressourcen sind spezifisch für die AWS Region oder Availability Zone, in der sie sich befinden.

Ressource	Typ	Beschreibung
Amazon EC2-Ressourcen-IDs	Regional	Jede Ressourcen-ID, z. B. eine AMI-ID, Instance-ID, EBS-Volume-ID oder EBS-Snapshot-ID, ist an ihre Region gebunden und kann nur in der Region

Ressource	Typ	Beschreibung
		verwendet werden, in der Sie die Ressource erstellt haben.
Vom Benutzer angegebene Ressourcennamen	Regional	Jeder Ressourcenname, z. B. ein Sicherheitsgruppenname oder ein Schlüsselpaarname, ist an seine Region gebunden und kann nur in der Region verwendet werden, in der Sie die Ressource erstellt haben. Sie können zwar Ressourcen mit demselben Namen in mehreren Regionen erstellen, aber diese sind nicht miteinander verwandt.
AMIs	Regional	Ein AMI ist an die Region gebunden, in der seine Dateien in Amazon S3 gespeichert sind. Sie können ein AMI von einer Region in eine andere kopieren. Weitere Informationen finden Sie unter Kopieren eines AMI.
EBS-Snapshots	Regional	Ein EBS-Snapshot ist an seine Region gebunden und kann nur verwendet werden, um Volumes in derselben Region zu erstellen. Sie können einen Snapshot von einer Region in eine andere kopieren.
EBS-Datenträger	Availability Zone	Ein Amazon EBS-Volume ist an seine Availability Zone gebunden und kann nur einer Instance innerhalb derselben Availability Zone zugeordnet werden.
Elastic IP-Adressen	Regional	Eine Elastic IP-Adresse ist an eine Region gebunden und kann nur einer Instance in derselben Region zugewiesen werden.
Instances	Availability Zone	Eine Instance ist an die Availability Zones gebunden, in denen Sie sie gestartet haben. Ihre Instance-ID ist jedoch an die Region gebunden.

Ressource	Typ	Beschreibung
Schlüsselpaare	Global oder regional	Die Schlüsselpaare, die Sie mit Amazon EC2 erstellen, sind an die Region gebunden, in der Sie sie erstellt haben. Sie können ein eigenes RSA-Schlüsselpaar erstellen und in die Region hochladen, in der Sie es verwenden möchten; d. h. Sie können Ihr Schlüsselpaar global verfügbar machen, indem Sie es in jede Region hochladen. Weitere Informationen finden Sie unter Amazon EC2 EC2-Schlüsselpaare und Amazon EC2 EC2-Instances.
Sicherheitsgruppen	Regional	Eine Sicherheitsgruppe ist an eine Region gebunden und kann nur Instances in derselben Region zugewiesen werden. Sie können einer Instance die Kommunikation mit einer Instance außerhalb ihrer Region nicht mithilfe von Sicherheitsgruppenregeln ermöglichen. Der Datenverkehr von einer Instance in eine andere Region wird als WAN-Bandbreite betrachtet.

Ressourcen-IDs

Wenn Sie eine Ressource erstellen, weisen wir jeder Ressource eine eindeutige Ressourcen-ID zu. Eine Ressourcen-ID besteht aus einer Ressourcenkennung (z. B. `snap` für einen Snapshot), gefolgt von einem Bindestrich und einer eindeutigen Kombination aus Buchstaben und Zahlen.

Jede Ressourcen-ID, z. B. eine AMI-ID, Instance-ID, EBS-Volume-ID oder EBS-Snapshot-ID, ist an ihre Region gebunden und kann nur in der Region verwendet werden, in der Sie die Ressource erstellt haben.

Sie können Ressourcen-IDs verwenden, um Ihre Ressourcen in der Amazon EC2-Konsole zu suchen. Wenn Sie ein Befehlszeilen-Tool oder die Amazon EC2-API für die Arbeit mit Amazon EC2 verwenden, sind Ressourcen-IDs für bestimmte Befehle erforderlich. Wenn Sie beispielsweise den

AWS CLI Befehl stop-instances verwenden, um eine Instance zu stoppen, müssen Sie die Instance-ID im Befehl angeben.

Länge der Ressourcen-ID

Vor Januar 2016 wurden für die IDs, die neu erstellten Ressourcen bestimmter Ressourcentypen zugewiesen wurden, 8 Zeichen nach dem Bindestrich verwendet (z. B. i-1a2b3c4d). Von Januar 2016 bis Juni 2018 änderten wir die IDs dieser Ressourcentypen so, dass nach dem Bindestrich 17 Zeichen verwendet werden (z. B, `i-1234567890abcdef0`). Je nachdem, wann Ihr Konto erstellt wurde, verfügen Sie möglicherweise über einige Ressourcen mit kurzen IDs, jedoch erhalten alle neuen Ressourcen die längeren IDs.

Auflisten und Filtern Ihrer Ressourcen

Sie erhalten eine Liste einiger Ressourcentypen, die die Amazon EC2-Konsole verwenden. Sie erhalten eine Liste für jeden Ressourcentyp mit dem entsprechenden Befehl oder einer API-Aktion. Falls Sie über viele Ressourcen verfügen, können Sie die Ergebnisse so filtern, dass sie nur die Ressourcen enthalten oder ausschließen, die bestimmten Kriterien entsprechen.

Inhalt

Auflisten und Filtern von Ressourcen über die Konsole

Inhalt

Auflisten von Ressourcen mithilfe der Konsole

Sie können die gängigsten Amazon EC2-Ressourcentypen mit der Konsole auflisten. Zum Anzeigen zusätzlicher Ressourcen verwenden Sie die Befehlszeilenschnittstelle oder die API-Aktionen.

So listen Sie EC2-Ressourcen mit der Konsole auf

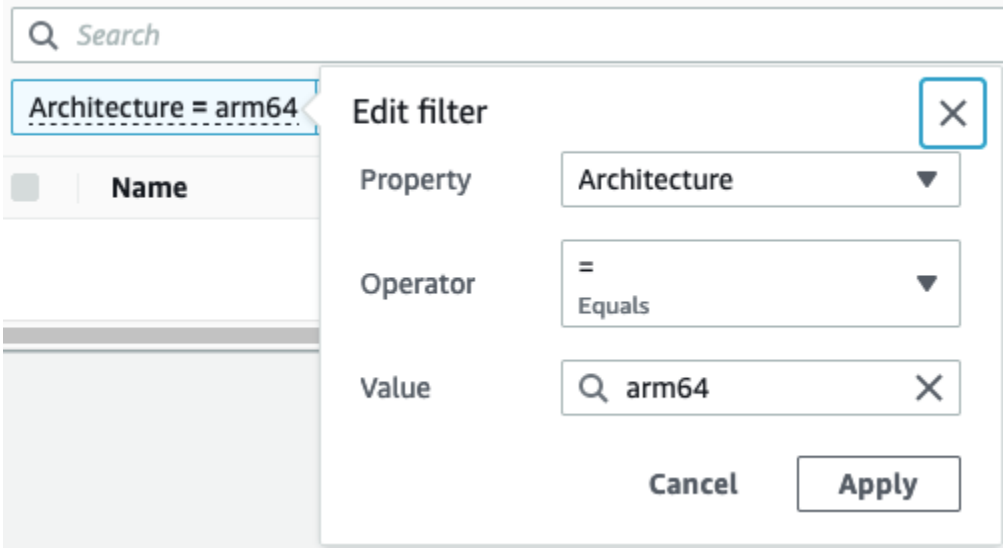
1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich die Option aus, die dem Ressourcentyp entspricht. Wenn Sie beispielsweise Ihre Instances auflisten möchten, wählen Sie Instances aus.

   Auf der Seite werden alle Ressourcen des ausgewählten Ressourcentyps angezeigt.

Filtern von Ressourcen mithilfe der Konsole

So filtern Sie eine Liste von Ressourcen

1. Wählen Sie im Navigationsbereich einen Ressourcentyp aus (z. B. Instances).
2. Wählen Sie das Suchfeld aus.
3. Wählen Sie den Filter aus der Liste aus.
4. Wählen Sie einen Operator aus, z. B.= (gleich). Einige Attribute haben mehr verfügbare Operatoren zur Auswahl. Beachten Sie, dass nicht alle Bildschirme die Auswahl eines Operators unterstützen.
5. Wählen Sie einen Filterwert aus.
6. Um einen ausgewählten Filter zu bearbeiten, wählen Sie das Filtertoken (blaues Feld) aus, nehmen Sie die erforderlichen Änderungen vor und wählen Sie dann Apply (Anwenden) aus. Beachten Sie, dass nicht alle Bildschirme ein Bearbeiten des ausgewählten Filters unterstützen.



7. Wenn Sie fertig sind, entfernen Sie den Filter.

Unterstützte Filter

Die Amazon EC2 EC2-Konsole unterstützt zwei Arten der Filterung.

- Die API-Filterung erfolgt auf der Serverseite. Die Filterung wird auf den API-Aufruf angewendet, was die Anzahl der Ressourcen reduziert, die vom Server zurückgegeben werden. Sie ermöglicht eine schnelle Filterung über große Mengen von Ressourcen und kann die Datenübertragungszeit und Kosten zwischen dem Server und dem Browser reduzieren. API-Filterung unterstützt die Operatoren = (gleich) und : (enthält) und berücksichtigt immer die Groß- und Kleinschreibung.
- Die Clientfilterung erfolgt auf der Clientseite. Sie ermöglicht Ihnen, nach Daten zu filtern, die bereits im Browser verfügbar sind (also Daten, die bereits von der API zurückgegeben wurden). Die Clientfilterung funktioniert gut in Verbindung mit einem API-Filter, um auf kleinere Datensätze im Browser zu filtern. Zusätzlich zu den Operatoren = (gleich) und : (enthält) kann die Client-Filterung auch Bereichsoperatoren unterstützen, wie >= (größer als oder gleich) und (inverse) Operatoren für die Negation, wie!= (ist nicht gleich).

Die Amazon EC2 EC2-Konsole unterstützt die folgenden Suchtypen:

Nach Schlüsselwort suchen

Die Suche nach Schlüsselwörtern ist eine Freitextsuche, mit der Sie nach einem Wert über alle Attribute oder Tags Ihrer Ressourcen hinweg suchen können, ohne ein zu suchendes Attribut oder Tag anzugeben.

> **Note**
>
> Bei allen Schlüsselwortsuchen wird die Clientfilterung verwendet.

Zur Suche nach Schlüsselwörtern geben oder fügen Sie in das Suchfeld ein, wonach Sie suchen, und drücken dann die Eingabetaste. Die Suche nach 123 findet als Übereinstimmung beispielsweise alle Instances mit 123 in einem ihrer Attribute, z. B. einer IP-Adresse, einer Instance-ID, einer VPC-ID oder einer AMI-ID oder in einem ihrer Tags, wie z. B. der Name. Wenn Ihre Freitextsuche unerwartete Übereinstimmungen zurückgibt, wenden Sie zusätzliche Filter an.

Suche nach Attribut

Wenn Sie nach einem Attribut suchen, können Sie ein bestimmtes Attribut über alle Ressourcen hinweg suchen.

> **Note**
>
> Attributsuchen verwenden je nach ausgewähltem Attribut entweder API-Filterung oder Clientfilterung. Bei einer Attributsuche werden die Attribute entsprechend gruppiert.

Sie können beispielsweise alle Instances nach dem Instance state (Instance-Status)-Attribut durchsuchen, um nur Instances mit dem Status `stopped` zurückzugeben. So gehen Sie vor:

1. Beginnen Sie im Suchfeld im Bildschirm Instances mit der Eingabe von `Instance state`. Wenn Sie die Zeichen eingeben, werden die beiden Filtertypen für den Instance-Status angezeigt: API-Filter und Client-Filter.
2. Um serverseitig zu suchen, wählen Sie unter API-Filter Instance-Status aus. Um clientseitig zu suchen, wählen Sie unter Client-Filter Instance-Status (Client) aus.

   Eine Liste möglicher Operatoren für das ausgewählte Attribut wird angezeigt.
3. Wählen Sie den Operator = (gleich) aus.

   Eine Liste möglicher Werte für das ausgewählte Attribut und den Operator wird angezeigt.
4. Wählen Sie in der Liste Gestoppt aus.

Suchen anhand eines Tags

Durch die Suche nach einem Tag können Sie die Ressourcen in der aktuell angezeigten Tabelle nach einem Tag-Schlüssel oder einem Tag-Wert filtern.

Tag-Suchen verwenden entweder die API-Filterung oder die Client-Filterung, abhängig von den Einstellungen im Fenster „Preferences“ (Voreinstellungen).

API-Filterung für Tags

1. Öffnen Sie die Registerkarte Preferences (Voreinstellungen).
2. Deaktivieren Sie das Kontrollkästchen Use regular expression matching (Übereinstimmung mit regulären Ausdrücken verwenden). Wenn dieses Kontrollkästchen aktiviert ist, wird die Client-Filterung durchgeführt.
3. Wählen Sie das Kontrollkästchen Use case sensitive matching (Groß-/Kleinschreibung bei Abgleich beachten). Wenn dieses Kontrollkästchen deaktiviert ist, wird die Client-Filterung durchgeführt.
4. Wählen Sie Bestätigen aus.

Wenn Sie nach Tag suchen, können Sie die folgenden Werte verwenden:

- (empty) (leer) – sucht alle Ressourcen mit dem angegebenen Tag-Schlüssel, aber es darf keinen Tag-Wert geben.
- All values (Alle Werte) – sucht alle Ressourcen mit dem angegebenen Tag-Schlüssel und einem beliebigen Tag-Wert.
- Not tagged (Nicht markiert) – sucht nach Ressourcen, denen der angegebene Tag-Schlüssel nicht zugewiesen wurde.
- „The displayed value“ (Der angezeigte Wert) – sucht alle Ressourcen mit dem angegebenen Tag-Schlüssel und dem angegebenen Tag-Wert.

Sie können Ihre Suche mit den folgenden Methoden verbessern oder verfeinern:

Inverse search (Umgekehrte Suche)

Mit umgekehrten Suchvorgängen können Sie nach Ressourcen suchen, die nicht mit einem angegebenen Wert übereinstimmen. Auf den Bildschirmen Instances und AMIs werden umgekehrte Suchen durch die Auswahl der Operatoren != (ist nicht gleich) oder !: (enthält nicht) und dann die Auswahl eines Werts durchgeführt. Auf anderen Bildschirmen wird die umgekehrte Suche durchgeführt, indem dem Suchbegriff das Ausrufezeichen (!) vorangestellt wird.

> **Note**
>
> Die umgekehrte Suche wird nur bei Schlüsselwortsuchen und Attributsuchen in Clientfiltern unterstützt. Sie wird bei Attributsuchen in API-Filtern nicht unterstützt.

Sie können beispielsweise alle Instances nach dem Instance state (Instance-Status)-Attribut durchsuchen, um alle Instances mit dem Status `terminated` auszuschließen. So gehen Sie vor:

1. Beginnen Sie im Suchfeld im Bildschirm Instances mit der Eingabe von `Instance state`. Wenn Sie die Zeichen eingeben, werden die beiden Filtertypen für den Instance-Status angezeigt: API-Filter und Client-Filter.
2. Wählen Sie unter Client filters (Client-Filter) die Option Instance state (client) (Instance-Status (Client)) aus. Die umgekehrte Suche wird nur für Client-Filter unterstützt.

   Eine Liste möglicher Operatoren für das ausgewählte Attribut wird angezeigt.
3. Klicken Sie auf != (ist nicht gleich), und wählen Sie dann terminated (beendet) aus.

Um Instances basierend auf einem Instance-Statusattribut zu filtern, können Sie auch die Suchsymbole (

) in der Spalte Instance-Status verwenden. Das Suchsymbol mit einem Pluszeichen (+) zeigt alle Instances an, die mit diesem Attribut übereinstimmen . Das Suchsymbol mit einem Minuszeichen (-) schließt alle Instances aus, die mit diesem Attribut übereinstimmen.

Hier ist ein weiteres Beispiel für die Verwendung der umgekehrten Suche: Wenn Sie alle Instances auflisten möchten, denen die Sicherheitsgruppe `launch-wizard-1` nicht zugewiesen ist, suchen Sie unter Client filters (Client-Filter) nach dem Attribut Security group name (Sicherheitsgruppenname), wählen Sie != aus und geben Sie in der Suchleiste `launch-wizard-1` ein.

Partial search (Partielle Suche)

Bei partiellen Suchvorgängen können Sie nach partiellen Zeichenfolgenwerten suchen. Um eine Teilsuche durchzuführen, geben Sie nur einen Teil des Schlüsselwortes ein, nach dem Sie suchen möchten. Auf den Bildschirmen Instances und AMIs können Teilsuchanfragen nur mit dem Operator : (enthält) durchgeführt werden. Auf anderen Bildschirmen können Sie das Client-Filterattribut auswählen und sofort nur den Teil des Suchbegriffs eingeben, nach dem Sie suchen möchten. Um beispielsweise auf dem Bildschirm Instance type (Instance-Typ) nach allen `t2.micro`-, `t2.small`- und `t2.medium`-Instances zu suchen, suchen Sie nach dem Attribut Instance type (Instance-Typ) und geben Sie als Schlüsselwort `t2` ein.

Suche nach regulären Ausdrücken

Um Suchen mit regulären Ausdrücken zu verwenden, müssen Sie in den Einstellungen das Kontrollkästchen Use regular expression matching (Übereinstimmung mit regulären Ausdrücken verwenden) aktivieren.

Reguläre Ausdrücke sind hilfreich, wenn Sie die Werte in einem Feld an ein spezifisches Muster angleichen müssen. Um beispielsweise nach einem Wert zu suchen, der mit `s` beginnt, suchen Sie nach `^s`. Um nach einem Wert zu suchen, der mit `xyz` endet, suchen Sie nach `xyz$`. Um nach einem Wert zu suchen, der mit einer Zahl beginnt, auf die ein oder mehrere Zeichen folgen, suchen Sie nach `[0-9]+.*`.

> **Note**
>
> Die Suche nach regulären Ausdrücken wird nur bei Schlüsselwortsuchen und Attributsuchen in Clientfiltern unterstützt. Sie wird bei Attributsuchen in API-Filtern nicht unterstützt.

Suche mit Unterscheidung von Groß-/Kleinschreibung

Um Suchvorgänge mit Beachtung der Groß-/Kleinschreibung zu verwenden, müssen Sie das Kontrollkästchen Use case sensitive matching (Abgleich mit Unterscheidung von Groß-/Kleinschreibung) im Fenster Preferences (Voreinstellungen) auswählen. Die Einstellung für die Groß-/Kleinschreibung gilt nur für Client- und Tag-Filter.

> **Note**
>
> Bei API-Filtern wird immer zwischen Groß-/Kleinschreibung unterschieden.

Suche nach Platzhaltern

Verwenden Sie den Platzhalter `*` als Entsprechung für null oder ein Zeichen. Verwenden Sie den Platzhalter `?` als Entsprechung für null oder ein Zeichen. Beispiel: Wenn Sie einen Datensatz mit den Werten `prod`, `prods` und `production` haben, gleicht eine Suche nach `prod*` alle Werte ab, während `prod?` nur `prod` und `prods` abgleicht. Um die Literalwerte zu verwenden, versehen Sie sie als Escape-Zeichen mit einem umgekehrten Schrägstrich (\). Beispielsweise würde „`prod \*`“ mit `prod*` übereinstimmen.

> **Note**
>
> Die Platzhaltersuche wird nur bei Attribut- und Tag-Suchen in API-Filtern unterstützt. Sie wird nicht bei Schlüsselwortsuchen und bei Attribut- und Tag-Suchen in Client-Filtern unterstützt.

Kombinieren von Suchen

Im Allgemeinen werden mehrere Filter mit demselben Attribut automatisch mit verbunde `OR`. Beispielsweise gibt die Suche nach `Instance State : Running` und `Instance State :`

`Stopped` alle Instances zurück, die entweder ausgeführt werden ODER gestoppt sind. Um die Suche mit `AND` zu verbinden, suchen Sie über verschiedene Attribute hinweg. Die Suche nach `Instance State : Running` und `Instance Type : c4.large` gibt z. B. nur Instances zurück, die vom Typ `c4.large` sind UND sich im Ausführungszustand befinden.

Auflisten und Filtern mit der CLI und API

Jeder Ressourcentyp weist einen entsprechenden CLI-Befehl oder eine API-Aktion auf, die Sie verwenden können, um die Ressourcen dieses Typs aufzulisten. Die resultierenden Listen von Ressourcen können lang sein, sodass es schneller und hilfreicher sein kann, die Ergebnisse so zu filtern, dass nur die Ressourcen berücksichtigt werden, die bestimmten Kriterien entsprechen.

Überlegungen zum Filtern

- Sie können bis zu 50 Filter und bis zu 200 Werte pro Filter in einer einzigen Anfrage angeben.
- Filterzeichenfolgen können bis zu 255 Zeichen lang sein.
- Sie können Platzhalter in den Filterwerten verwenden. Ein Sternchen (*) steht für kein Zeichen oder eine beliebige Kombination von mehreren Zeichen, und ein Fragezeichen (?) entspricht Null oder einem Zeichen.
- Bei Filterwerten muss die Groß- und Kleinschreibung beachtet werden.
- Ihre Suche kann die Literalwerte der Platzhalterzeichen enthalten. Sie müssen dafür nur einen Backslash vor dem Zeichen eingeben. Beispiel: Mit dem Wert `\*amazon\?\\` wird nach der Literalzeichenfolge `*amazon?\` gesucht.

Unterstützte Filter

Die unterstützten Filter für jede Amazon EC2-Ressource finden Sie in der folgenden Dokumentation:

- AWS CLI: Die `describe`-Befehle in der AWS CLI -Befehlsreferenz-Amazon EC2.
- Tools für Windows PowerShell: Die `Get` Befehle im AWS Tools for PowerShell Cmdlet Reference-Amazon EC2.
- Query API: Die `Describe`-API-Aktionen in der Amazon EC2-API-Referenz.

Example Beispiel: Angeben eines einzelnen Filters

Sie können Ihre Amazon-EC2-Instances mithilfe von describe-instances auflisten. Ohne Filter enthält die Antwort Informationen für alle Ihre Ressourcen. Sie können den folgenden Befehl verwenden, um nur die laufenden Instances in Ihre Ausgabe aufzunehmen.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running
```

Um nur die Instance-IDs für die laufenden Instances aufzulisten, fügen Sie den Parameter `--query` wie folgt hinzu.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=running --query
 "Reservations[*].Instances[*].InstanceId" --output text
```

Es folgt eine Beispielausgabe.

```
i-0ef1f57f78d4775a4
i-0626d4edd54f1286d
i-04a636d18e83cfacb
```

Example Beispiel: Angeben mehrerer Filter oder Filterwerte

Wenn Sie mehrere Filter oder mehrere Filterwerte angeben, muss die Ressource mit allen Filtern übereinstimmen, um in die Ergebnisse aufgenommen zu werden.

Mit dem folgenden Befehl können Sie alle Instances auflisten, deren Typ entweder `m5.large` oder `m5d.large` ist.

```
aws ec2 describe-instances --filters Name=instance-type,Values=m5.large,m5d.large
```

Sie können den folgenden Befehl verwenden, um alle gestoppten Instances aufzulisten, deren Typ is `t2.micro`.

```
aws ec2 describe-instances --filters Name=instance-state-name,Values=stopped
 Name=instance-type,Values=t2.micro
```

Example Beispiel: Verwenden von Platzhaltern in einem Filterwert

Wenn Sie als Filterwert für den Filter `database description` angeben, wenn Sie EBS-Snapshots mithilfe von describe-snapshots beschreiben, gibt der Befehl nur die Snapshots zurück, deren Beschreibung „database“ lautet.

```
aws ec2 describe-snapshots --filters Name=description,Values=database
```

Der Platzhalter „*“ entspricht null oder mehr Zeichen. Wenn Sie als Filterwert `*database*` angeben, gibt der Befehl nur Snapshots zurück, deren Beschreibung das Wort „database“ enthält.

```
aws ec2 describe-snapshots --filters Name=description,Values=*database*
```

Der Platzhalter „?“ entspricht genau 1 Zeichen. Wenn Sie `database?` als Filterwert angeben, gibt der Befehl nur Snapshots zurück, deren Beschreibung „database“ oder „database“ gefolgt von einem Zeichen ist.

```
aws ec2 describe-snapshots --filters Name=description,Values=database?
```

Wenn Sie `database????` angeben, gibt der Befehl nur Snapshots zurück, deren Beschreibung „Datenbank“ gefolgt von bis zu vier Zeichen ist. Beschreibungen mit „database“, gefolgt von fünf oder mehr Zeichen, werden ausgeschlossen.

```
aws ec2 describe-snapshots --filters Name=description,Values=database????
```

Example Beispiel: Filtern basierend auf Datum

Mit dem können Sie JMESPath verwenden AWS CLI, um Ergebnisse mithilfe von Ausdrücken zu filtern. *Mit dem folgenden describe-snapshotsBefehl werden beispielsweise die IDs aller Schnappschüsse angezeigt, die von Ihnen AWS-Konto (dargestellt durch 123456789012) vor dem angegebenen Datum (dargestellt durch 2020-03-31) erstellt wurden.* Wenn Sie den Eigentümer nicht angeben, enthalten die Ergebnisse alle öffentlichen Snapshots.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime<='2020-03-31')].[SnapshotId]" --output text
```

Der folgende Befehl zeigt die IDs aller Snapshots an, die im angegebenen Datumsbereich erstellt wurden.

```
aws ec2 describe-snapshots --filters Name=owner-id,Values=123456789012 --query
 "Snapshots[?(StartTime>='2019-01-01') && (StartTime<='2019-12-31')].[SnapshotId]" --
output text
```

Filtern basierend auf Tags (Markierungen)

Beispiele zum Filtern einer Liste von Ressourcen nach ihren Tags (Markierungen) finden Sie unter Arbeiten mit Tags (Markierungen) über die Befehlszeile.

Anzeigen von Ressourcen in verschiedenen Regionen mithilfe von Amazon EC2 Global View

Mit Amazon EC2 Global View können Sie Amazon EC2- und Amazon VPC-Ressourcen in einer einzelnen AWS Region oder in mehreren Regionen gleichzeitig in einer einzigen Konsole anzeigen und suchen. Weitere Informationen finden Sie unter Amazon EC2 Global View.

Amazon EC2 Global View

Amazon EC2 Global View ermöglicht es Ihnen, einige Ihrer Amazon-EC2- und Amazon-VPC-Ressourcen in einer einzigen AWS -Region oder über mehrere Regionen in einer einzigen Konsole anzuzeigen. Amazon EC2 Global View bietet auch eine globale Suchfunktion, mit der Sie nach bestimmten Ressourcen oder bestimmten Ressourcentypen in mehreren Regionen gleichzeitig suchen können.

Mit Amazon EC2 Global View können Sie Ressourcen in keiner Weise ändern.

Unterstützte Ressourcen

Mit Amazon EC2 Global View können Sie eine globale Zusammenfassung der folgenden Ressourcen in allen Regionen anzeigen, für die Ihre aktiviert AWS-Konto ist.

- Auto-Scaling-Gruppen
- DHCP-Optionsliste
- Internet-Gateways nur für ausgehenden Datenverkehr
- Elastische IP-Adressen
- Endpunkt-Services
- Instances

- Internet-Gateways
- Verwaltete Präfixlisten
- NAT gateways (NAT-Gateways)
- Netzwerk-ACLs
- Netzwerkschnittstellen
- Routing-Tabellen
- Sicherheitsgruppen
- Subnetze
- Datenträger
- VPCs
- VPC-Endpunkte
- VPC-Peering-Verbindungen

Erforderliche Berechtigungen

Ein Benutzer muss über die folgenden Berechtigungen verfügen, um Amazon EC2 Global View verwenden zu können.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
    "autoscaling:DescribeAutoScalingGroups",
    "ec2:DescribeRegions",
    "ec2:DescribeDhcpOptions",
    "ec2:DescribeEgressOnlyInternetGateways",
    "ec2:DescribeAddresses",
    "ec2:DescribeVpcEndpointServices",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribePrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribeRouteTables",
```

```
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections"
  ],
  "Resource": "*"
  }]
}
```

So verwenden Sie Amazon EC2 Global View

Öffnen Sie die Amazon EC2 Global View-Konsole unter https://console.aws.amazon.com/ec2globalview/home.

> **Important**
>
> Sie können kein privates Fenster in Firefox verwenden, um auf Amazon EC2 Global View zuzugreifen.

Die Konsole enthält die folgenden Elemente:

- Region-Explorer – Diese Registerkarte enthält die folgenden Abschnitte:
  - Zusammenfassung – Bietet einen allgemeinen Überblick über Ihre Ressourcen in allen Regionen.

    Aktivierte Regionen gibt die Anzahl der Regionen an, für die Ihre aktiviert AWS-Konto ist. Die verbleibenden Felder geben die Anzahl der Ressourcen an, die Sie derzeit in diesen Regionen haben. Wählen Sie einen der Links, um die Ressourcen dieses Typs in allen Regionen anzuzeigen. Wenn beispielsweise der Link unter dem Label Instances 29 in 10 Regionen ist, gibt es an, dass Sie derzeit 29 Instances über 10Regionen haben. Wählen Sie den Link, um eine Liste aller 29 Instances anzuzeigen.
  - Ressourcenanzahl pro Region – Listet alle AWS-Regionen auf (einschließlich derjenigen, für die Ihr Konto nicht aktiviert ist) und stellt Gesamtwerte für jeden Ressourcentyp für jede Region bereit.

    Wählen Sie eine Regionsbezeichnung, um alle Ressourcen aller Arten für diese bestimmte Region anzuzeigen. Wählen Sie z. B. Afrika (Kapstadt) af-south-1, um alle VPCs, Subnetze,

Instances, Sicherheitsgruppen, Volumes und Auto-Scaling-Gruppen in dieser Region anzuzeigen. Alternativ können Sie eine Region auswählen und Ressourcen für ausgewählte Region anzeigen auswählen.

Wählen Sie den Wert für einen bestimmten Ressourcentyp in einer bestimmten Region aus, um nur Ressourcen dieses Typs in dieser Region anzuzeigen. Wählen Sie z. B. den Wert für Instances für Afrika (Kapstadt) af-south-1, um nur die Instances in dieser Region anzuzeigen.

- Globale Suche: Auf dieser Registerkarte können Sie nach bestimmten Ressourcen oder bestimmten Ressourcentypen in einer einzelnen Region oder in mehreren Regionen suchen. Außerdem können Sie Details zu einer bestimmten Ressource anzeigen.

  Um nach Ressourcen zu suchen, geben Sie die Suchkriterien in das Feld vor dem Raster ein. Sie können nach Region, Ressourcentyp und nach den Tags suchen, die Ressourcen zugewiesen sind.

  Um die Details für eine bestimmte Ressource anzuzeigen, wählen Sie sie im Raster aus. Sie können auch die Ressourcen-ID einer Ressource auswählen, um sie in ihrer jeweiligen Konsole zu öffnen. Wählen Sie beispielsweise eine Instance-ID aus, um die Instance in der Amazon EC2 Konsole zu öffnen oder wählen Sie eine Subnetz-ID aus, um das Subnetz in der Amazon VPC Konsole zu öffnen.

> **Tip**
>
> Wenn Sie nur bestimmte Regionen oder Ressourcentypen verwenden, können Sie Amazon EC2 Global View so anpassen, dass nur diese Regionen und Ressourcentypen angezeigt werden. Um die angezeigten Regionen und Ressourcentypen anzupassen, wählen Sie im Navigationsbereich Einstellungen und dann auf den Registerkarten Ressourcen und Regionen die Regionen und Ressourcentypen aus, die nicht in Amazon EC2 Global View angezeigt werden sollen.

Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen)

Zur einfacheren Verwaltung von Instances, Images und anderen Amazon-EC2-Ressourcen können Sie den einzelnen Ressourcen bei Bedarf eigene Metadaten in Form von Tags (Markierungen) zuweisen. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie viele

Ressourcen desselben Typs haben — In diesem Fall können Sie schnell bestimmte Ressourcen basierend auf den zugewiesenen Tags (Markierungen) bestimmen. In diesem Thema werden Tags (Markierungen) und deren Erstellung beschrieben.

> **Warning**
>
> Tag (Markierung)-Schlüssel und ihre Werte werden von vielen verschiedenen API-Aufrufen zurückgegeben. Die Zugriffsverweigerung von `DescribeTags` verweigert nicht automtisch den Zugriff auf Tags (Markierungen), die von anderen APIs zurückgegeben wurden.
> Als bewährte Vorgehensweise empfehlen wir Ihnen, keine sensiblen Daten in Ihre Tags (Markierungen) aufzunehmen.

Inhalt

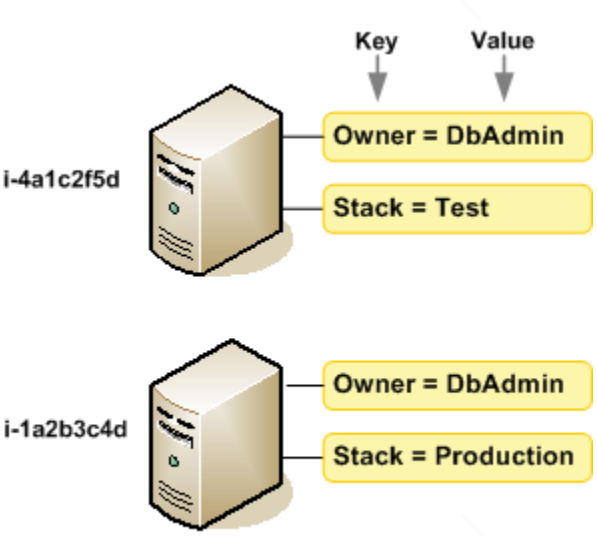
Grundlagen zu Tags (Markierungen)

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen.

Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Sie können zum Beispiel eine Reihe von Tags (Markierungen) für die Amazon-EC2-Instances in Ihrem Konto definieren, um die Eigentümer der einzelnen Instances und die Stack-Ebene nachzuverfolgen.

Das folgende Diagramm veranschaulicht, wie Markieren funktioniert. In diesem Beispiel wurden jeder Instance zwei Tags (Markierungen) zugewiesen: ein Tag (Markierung) mit dem Schlüssel `Owner`

und ein Tag (Markierung) mit dem Schlüssel `Stack`. Jeder Tag (Markierung) verfügt außerdem über einen zugewiesenen Wert.



Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Die Verwendung einheitlicher Tag-Schlüssel vereinfacht das Verwalten der -Ressourcen. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags (Markierungen) filtern und danach suchen. Weitere Informationen zur Implementierung einer effektiven Strategie zur Kennzeichnung von Ressourcen finden Sie im Whitepaper Best Practices für Tagging. AWS

Tags (Markierungen) haben keine semantische Bedeutung für Amazon EC2 und werden ausschließlich als Zeichenfolgen interpretiert. Außerdem werden Tags (Markierungen) nicht automatisch Ihren Ressourcen zugewiesen. Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

> **Note**
>
> Nachdem Sie eine Ressource gelöscht haben, bleiben ihre Tags möglicherweise für einen kurzen Zeitraum in der Konsolen-, API- und CLI-Ausgabe sichtbar. Diese Tags werden schrittweise von der Ressource getrennt und dauerhaft gelöscht.

Markieren Ihrer -Ressourcen mit Tags (Markierungen)

Sie können die meisten Amazon-EC2-Ressourcen markieren, die bereits in Ihrem Konto bestehen. In der folgenden Tabelle sind die Ressourcen aufgeführt, die das Markieren unterstützen.

Wenn Sie die Amazon EC2 EC2-Konsole verwenden, können Sie Tags auf Ressourcen anwenden, indem Sie die Registerkarte Tags auf dem entsprechenden Ressourcenbildschirm verwenden, oder Sie können den Tags-Editor in der AWS Resource Groups Konsole verwenden. Auf bestimmten Ressourcenbildschirmen können Sie Tags (Markierungen) beim Erstellen einer Ressource angeben, z. B. ein Tag (Markierung) mit einem Schlüssel von `Name` und einem benutzerdefinierten Wert. In den meisten Fällen wendet die Konsole Tags (Markierungen) direkt nach dem Erstellen der Ressource an und nicht während des Erstellens. Die Konsole strukturiert Ressourcen möglicherweise gemäß der `Name`-Markierung. Allerdings hat die Markierung keine semantische Bedeutung für den Amazon-EC2-Service.

Wenn Sie die Amazon EC2 EC2-API, das AWS CLI oder ein AWS SDK verwenden, können Sie die `CreateTags` EC2-API-Aktion verwenden, um Tags auf vorhandene Ressourcen anzuwenden. Zudem können Sie mit einigen Aktionen zur Ressourcenerstellung Tags beim Erstellen einer Ressource angeben. Wenn Tags (Markierungen) nicht während der Ressourcenerstellung angewendet werden können, wird die Ressourcenerstellung rückgängig gemacht. Auf diese Weise werden Ressourcen entweder mit Tags (Markierungen) oder überhaupt nicht erstellt und keine Ressourcen verbleiben ohne Tags (Markierungen). Indem Sie Ressourcen zum Erstellungszeitpunkt markieren, müssen Sie anschließend keine benutzerdefinierten Skripts ausführen. Weitere Informationen darüber, wie Sie Benutzern ermöglichen, Ressourcen bei der Erstellung zu markieren, finden Sie unter Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.

In der folgenden Tabelle werden die Amazon EC2 EC2-Ressourcen beschrieben, die markiert werden können, und die Ressourcen, die bei der Erstellung mit der Amazon EC2 EC2-API AWS CLI, dem oder einem AWS SDK markiert werden können.

Markierungsunterstützung für Amazon EC2-Ressourcen

Ressource	Unterstützt Tags (Markierungen)	Unterstützt Markierung bei der Erstellung
AFI	Ja	Ja
AMI	Ja	Ja

Ressource	Unterstützt Tags (Markierungen)	Unterstützt Markierung bei der Erstellung
Bundle Task	Nein	Nein
Capacity Reservation	Ja	Ja
Gateway des Netzbetreibers	Ja	Ja
Client-VPN-Endpunkt	Ja	Ja
Client-VPN-Route	Nein	Nein
Kunden-Gateway	Ja	Ja
Dedicated Host	Ja	Ja
Dedicated Host-Reservierung	Ja	Ja
DHCP-Optionen	Ja	Ja
EBS Snapshot	Ja	Ja
EBS-Volume	Ja	Ja
EC2 Fleet	Ja	Ja
Internet-Gateway nur für ausgehenden Verkehr	Ja	Ja
Elastic IP-Adresse	Ja	Ja
Elastic Graphics Accelerator	Ja	Nein
Instance	Ja	Ja
Instance-Ereignisfenster	Ja	Ja
Instance-Speicher-Volume	–	–
Internet-Gateway	Ja	Ja

Ressource	Unterstützt Tags (Markierungen)	Unterstützt Markierung bei der Erstellung
IP-Adresspool (BYOIP)	Ja	Ja
Schlüsselpaar	Ja	Ja
Startvorlage	Ja	Ja
Startvorlagenversion	Nein	Nein
Lokales Gateway	Ja	Nein
Routing-Tabelle für das lokale Gateway	Ja	Nein
Virtuelle Schnittstelle des lokalen Gateways	Ja	Nein
Virtuelle Schnittstellengruppe des lokalen Gateways	Ja	Nein
VPC-Zuordnung der Routing-Tabelle für das lokale Gateway	Ja	Ja
Zuordnung der virtuellen Schnittstellengruppe der Routing-Tabelle für das lokale Gateway	Ja	Nein
NAT-Gateway	Ja	Ja
Netzwerk-ACL	Ja	Ja
Netzwerkschnittstelle	Ja	Ja
Platzierungsgruppe	Ja	Ja
Liste der Präfixe	Ja	Ja
Reserved Instance	Ja	Nein

Ressource	Unterstützt Tags (Markierungen)	Unterstützt Markierung bei der Erstellung
Reserved Instance-Angebot	Nein	Nein
Routing-Tabelle	Ja	Ja
Spot-Flottenanforderung	Ja	Ja
Spot-Instance-Anforderung	Ja	Ja
Sicherheitsgruppe	Ja	Ja
Sicherheitsgruppenregel	Ja	Nein
Subnetz	Ja	Ja
Traffic Mirror-Filter	Ja	Ja
Traffic Mirror-Sitzung	Ja	Ja
Traffic Mirror-Ziel	Ja	Ja
Transit Gateway	Ja	Ja
Multicast-Domain des Transit Gateways	Ja	Ja
Routing-Tabelle für Transit Gateway	Ja	Ja
VPC-Verbindung für Transit Gateway	Ja	Ja
Virtual Private Gateway	Ja	Ja
VPC	Ja	Ja
VPC-Endpunkt	Ja	Ja
VPC-Endpunktservice	Ja	Ja

Ressource	Unterstützt Tags (Markierungen)	Unterstützt Markierung bei der Erstellung
VPC-Endpunktservice-Konfiguration	Ja	Ja
VPC-Flow-Protokoll	Ja	Ja
VPC-Peering-Verbindung	Ja	Ja
VPN-Verbindung	Ja	Ja

Sie können Instances, Volumes, elastische Grafiken, Netzwerkschnittstellen und Spot-Instance-Anforderungen bei der Erstellung mit dem Launch Instance Wizard von Amazon EC2 in der Amazon-EC2-Konsole markieren. Sie können Ihre EBS-Volumes bei der Erstellung über den Bildschirm Volumes oder EBS-Snapshots über den Bildschirm Snapshots mit Markierungen versehen. Verwenden Sie alternativ die Amazon EC2 EC2-APIs zur Ressourcenerstellung (z. B. RunInstances), um bei der Erstellung Ihrer Ressource Tags anzuwenden.

Sie können Tag (Markierung)-basierte Berechtigungen auf Ressourcenebene in Ihren IAM-Richtlinien auf die Amazon EC2 API-Aktionen anwenden, die die Markierung bei der Erstellung unterstützen, um eine granulare Kontrolle über die Benutzer und Gruppen zu implementieren, die Ressourcen bei der Erstellung mit Tags (Markierungen) versehen können. Ihre Ressourcen sind ab Erstellung ordnungsgemäß geschützt. Tags (Markierungen) werden direkt auf Ihre Ressourcen angewendet. Daher treten alle Tag (Markierung)-basierten Berechtigungen auf Ressourcenebene, die die Verwendung von Ressourcen steuern, direkt in Kraft. Ihre Ressourcen können nachverfolgt und genauer erfasst werden. Sie können das Markieren neuer Ressourcen gewährleisten und steuern, welche Tag (Markierung)-Schlüssel und Werte für Ihre Ressourcen festgelegt sind.

Sie können ebenfalls Berechtigungen auf Ressourcenebene auf die `CreateTags`- und `DeleteTags`-Amazon-EC2-API-Aktionen in den IAM-Richtlinien anwenden, um die Tag (Markierung)-Schlüssel und -Werte zu steuern, die für Ihre bestehenden Ressourcen festgelegt sind. Weitere Informationen finden Sie unter Beispiel: Markieren von Ressourcen.

Weitere Informationen zum Markieren von Ressourcen für die Fakturierung finden Sie unter Verwendung von Tags (Markierungen) zur Kostenzuordnung im Benutzerhandbuch für AWS Billing .

Tag (Markierung)-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags (Markierungen) pro Ressource: 50
- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Maximale Schlüssellänge: 128 Unicode-Zeichen in UTF-8
- Maximale Wertlänge: 256 Unicode-Zeichen in UTF-8
- Zulässige Zeichen
  - EC2 lässt zwar jedes beliebige Zeichen in seinen Tags zu, andere AWS Dienste sind jedoch restriktiver. Die zulässigen Zeichen in allen AWS Diensten sind: Buchstaben (`a-z,A-Z`), Zahlen (`0-9`) und Leerzeichen, die in UTF-8 dargestellt werden können, sowie die folgenden Zeichen:. `+ - = . _ : / @`
  - Wenn Sie Instance-Tags in Instance-Metadaten aktivieren, kann das Instance-Tag keys nur Buchstaben (`a-z,A-Z`), Zahlen (`0-9`) und die folgenden Zeichen verwenden: `+ - = . , _ : @`. Instance-Tag Schlüssel dürfen keine Leerzeichen oder `/` enthalten und dürfen nur `.` (ein Komma), `..` (zwei Kommas) oder `_index` enthalten. Weitere Informationen finden Sie unter Arbeiten mit Instance-Tags in Instance-Metadaten.
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Das `aws:` Präfix ist für die Verwendung reserviert. AWS Wenn der Tag (Markierung) über einen Tag (Markierung)-Schlüssel mit diesem Präfix verfügt, können Sie den Schlüssel oder Wert des Tags (Markierung) nicht bearbeiten oder löschen. Tags (Markierungen) mit dem Präfix `aws:` werden nicht als Ihre Tags (Markierungen) pro Ressourcenlimit angerechnet.

Sie können Ressourcen nicht allein auf Grundlage ihrer Tags (Markierungen) beenden, anhalten oder löschen. Sie müssen den Ressourcenbezeichner angeben. Um Snapshots zu löschen, die Sie mit dem Tag (Markierung)-Schlüssel `DeleteMe` markiert haben, müssen Sie die `DeleteSnapshots`-Aktion mit den Ressourcenbezeichnern der Snapshots verwenden, z. B. `snap-1234567890abcdef0`.

Wenn Sie öffentliche oder gemeinsam genutzte Ressourcen taggen, sind die von Ihnen zugewiesenen Tags nur für Ihr AWS Konto verfügbar. Kein anderes AWS Konto hat Zugriff auf diese Tags. Für die tagbasierte Zugriffskontrolle auf gemeinsam genutzte Ressourcen muss jedem AWS

Konto ein eigener Satz von Stichwörtern zugewiesen werden, um den Zugriff auf die Ressource zu kontrollieren.

Sie können nicht alle Ressourcen markieren. Weitere Informationen finden Sie unter Markierungsunterstützung für Amazon EC2-Ressourcen.

Tags (Markierungen) und Access Management

Wenn Sie AWS Identity and Access Management (IAM) verwenden, können Sie steuern, welche Benutzer in Ihrem AWS Konto berechtigt sind, Tags zu erstellen, zu bearbeiten oder zu löschen. Weitere Informationen finden Sie unter Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.

Sie können auch Resource-Tags (Markierungen) verwenden, um eine attributbasierte Steuerung (ABAC) zu implementieren. Sie können IAM-Richtlinien erstellen, die Vorgänge basierend auf den Tags (Markierungen) für die Ressource zulassen. Weitere Informationen finden Sie unter Steuerung des Zugriffs auf EC2-Ressourcen mithilfe von Ressourcen-Tags (Markierungen).

Markieren von Ressourcen für die Fakturierung

Sie können Tags verwenden, um Ihre AWS Rechnung so zu organisieren, dass sie Ihrer eigenen Kostenstruktur entspricht. Melden Sie sich dazu an, um Ihre AWS Kontorechnung mit den Tag-Schlüsselwerten zu erhalten. Weitere Informationen zum Einrichten eines Kostenzuordnungsberichts mit Markierungen finden Sie unter Monatlicher Kostenzuordnungsbericht im AWS Billing - Benutzerhandbuch. Um die Kosten kombinierter Ressourcen anzuzeigen, können Sie Ihre Fakturierungsinformationen nach Ressourcen mit gleichen Tag (Markierung)-Schlüsselwerten strukturieren. Beispielsweise können Sie mehrere Ressourcen mit einem bestimmten Anwendungsnamen markieren und dann Ihre Fakturierungsinformationen so organisieren, dass Sie die Gesamtkosten dieser Anwendung über mehrere Services hinweg sehen können. Weitere Informationen finden Sie unter Verwendung von Tags (Markierungen) zur Kostenzuordnung im Benutzerhandbuch für AWS Billing .

> **Note**
>
> Wenn Sie die Berichterstellung gerade erst aktiviert haben, werden die Daten für den aktuellen Monat nach 24 Stunden bereitgestellt.

Kostenzuordnungs-Tags (Markierungen) dienen der Anzeige, welche Ressourcen zu Ihrer Nutzung und Ihren Kosten beitragen. Das Löschen oder Deaktivieren der Ressourcen führt nicht zwangsläufig zur Kostensenkung. Beispiel: Snapshot-Daten, auf die von einem anderen Snapshot verwiesen wird, werden selbst dann beibehalten, wenn der Snapshot gelöscht wird, der die ursprünglichen Daten enthält. Weitere Informationen finden Sie unter Amazon Elastic Block Store-Volumes und -Snapshots im Benutzerhandbuch für AWS Billing .

> **Note**
>
> Elastic IP-Adressen, die mit Tags (Markierungen) versehen sind, erscheinen nicht in Ihrem Kostenzuordnungsbericht.

Arbeiten mit Tags (Markierungen) in der Konsole

Sie können die Amazon-EC2-Konsole verwenden, um die Markierungen einer einzelnen Ressource anzuzeigen und um Markierungen für jeweils eine Ressource anzuwenden oder zu entfernen.

Sie können den Tag-Editor in der AWS Resource Groups Konsole verwenden, um die Tags all Ihrer Amazon EC2 EC2-Ressourcen in allen Regionen anzuzeigen. Sie können Markierungen nach Ressource und nach Ressourcentyp anzeigen und sehen, welche Ressourcentypen mit einer bestimmten Markierung verbunden sind. Sie können Markierungen jeweils mehreren Ressourcen und mehreren Ressourcentypen gleichzeitig hinzufügen oder diese entfernen. Der Markierungs-Editor bietet eine zentrale, einheitliche Möglichkeit, Ihre Markierungen zu erstellen und zu verwalten. Weitere Informationen finden Sie im Tagging AWS Resources User Guide.

Aufgaben

- Anzeigen von Tags (Markierungen)
- Hinzufügen und Löschen von Tags (Markierungen) für einzelne Ressourcen
- Hinzufügen und Löschen von Markierungen für mehrere Ressourcen
- Hinzufügen eines Tags (Markierung) beim Starten einer Instance
- Filtern einer Ressourcenliste nach Tags (Markierungen)

Anzeigen von Tags (Markierungen)

Sie können die Markierungen einer einzelnen Ressource in der Amazon-EC2-Konsole anzeigen. Verwenden Sie den Markierungs-Editor in der AWS Resource Groups -Konsole, um die Markierungen all Ihrer Ressourcen anzuzeigen.

Markierungen einer einzelnen Ressource anzeigen

Wenn Sie eine ressourcenspezifische Seite in der Amazon EC2-Konsole auswählen, wird eine Liste der Ressourcen angezeigt. Beispiel: Wenn Sie im Navigationsbereich Instances auswählen, werden Ihre Amazon EC2-Instances in der Konsole angezeigt. Wenn Sie eine Ressource aus einer der Listen (beispielsweise eine Instance) auswählen und die Ressource Tags (Markierungen) unterstützt, können Sie deren Tags (Markierungen) anzeigen und verwalten. Auf den meisten Ressourcenseiten können Sie die Tags anzeigen, indem Sie die Registerkarte Tags auswählen.

Sie können der Ressourcenliste eine Spalte hinzufügen, um alle Werte für Markierungen mit demselben Schlüssel anzuzeigen. Sie können diese Spalte verwenden, um Ressourcenliste nach Tag zu sortieren und filtern.

New console

So fügen Sie der Ressourcenliste eine Spalte zur Anzeige Ihrer Markierungen hinzu

1. In der EC2-Konsole wählen Sie rechts oben in der Ecke das Symbol Einstellungen, das wie ein Zahnrad geformt ist.
2. Wählen Sie im Dialogfenster Einstellungen für die Markierungs-Spalten einen der mehrere Markierungs-Schlüssel aus, und wählen Sie dann Bestätigen.

Old console

Sie können der Ressourcenliste auf zwei Arten eine neue Spalte hinzufügen, um Ihre Tags (Markierungen) anzuzeigen:

- Wählen Sie auf der Registerkarte Tags Show Column aus. Der Konsole wird eine neue Spalte hinzugefügt.
- Klicken Sie auf das Zahnrädchensymbol Show/Hide Columns (Spalten ein-/ausblenden) und wählen Sie im Dialogfeld Show/Hide Columns (Spalten ein-/ausblenden) unter Your Tag Keys den Tag (Markierung)-Schlüssel aus.

Anzeigen von Markierungen für mehrere Ressourcen

Sie können Markierungen in mehreren Ressourcen anzeigen, indem Sie den Markierungs-Editor in der AWS Resource Groups -Konsole verwenden. Weitere Informationen finden Sie im Tagging AWS Resources User Guide.

Hinzufügen und Löschen von Tags (Markierungen) für einzelne Ressourcen

Sie können Tags (Markierungen) für einzelne Ressourcen direkt auf der Seite der Ressource verwalten.

Hinzufügen eines Tags (Markierung) zu einer einzelnen Ressource

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der sich die mit Tags zu versehende Ressource befindet. Weitere Informationen finden Sie unter Ressourcenstandorte.
3. Wählen Sie im Navigationsbereich einen Ressourcentyp aus (z. B. Instances).
4. Wählen Sie die Ressource aus der Ressourcenliste und die Registerkarte Tags aus.
5. Wählen Sie die Registerkarte Markierungen verwalten und dann Neue Markierung hinzufügen. Geben Sie den Schlüssel und den Wert für den Tags (Markierungen) ein. Wählen Sie für jede weitere Markierung Neue Markierung hinzufügen aus. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Speichern.

Löschen von Tags (Markierungen) von einer einzelnen Ressource

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie in der Navigationsleiste die Region aus, in der sich die Ressource befindet, dessen Tags sie entfernen möchten. Weitere Informationen finden Sie unter Ressourcenstandorte.
3. Wählen Sie im Navigationsbereich einen Ressourcentyp aus (z. B. Instances).
4. Wählen Sie die Ressource aus der Ressourcenliste und die Registerkarte Tags aus.
5. Wählen Sie Manage tags (Tags (Markierungen) verwalten) aus. Klicken Sie zum Entfernen bei jeder Markierung auf Entfernen. Wenn Sie mit dem Entfernen der Tags fertig sind, wählen Sie Speichern.

Hinzufügen und Löschen von Markierungen für mehrere Ressourcen

Hinzufügen von Markierungen zu mehreren Ressourcen

1. Öffnen Sie den Tag-Editor in der AWS Resource Groups Groups-Konsole unter https://console.aws.amazon.com/resource-groups/tag-editor.
2. Wählen Sie für Regionen eine oder mehrere Regionen aus, in denen sich die mit Markierungen zu versehenden Ressourcen befinden.
3. Wählen Sie unter Ressourcentypen den Ressourcentyp aus, den Sie taggen möchten (z. B. AWS::EC2::Instance).
4. Wählen Sie Ressourcen durchsuchen aus.
5. Aktivieren Sie unter den Ergebnissen der Ressourcensuche das Kontrollkästchen neben den einzelnen Ressourcen, die Sie mit Markierungen versehen möchten.
6. Wählen Sie Markierungen der ausgewählten Ressourcen verwalten aus.
7. Wählen Sie unter Markierungen aller ausgewählten Ressourcen bearbeiten die Option Markierung hinzufügen aus, und geben Sie dann den neuen Markierungs-Schlüssel und -Wert ein. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.

   > **Note**
   >
   > Wenn Sie einen neuen Tag (Markierung) mit demselben Tag (Markierung)-Schlüssel wie ein bestehender Tag (Markierung) hinzufügen, wird der bestehende Tag (Markierung) vom neuen überschrieben.

8. Wählen Sie Markierungsänderungen prüfen und anwenden aus.
9. Wählen Sie Apply changes to all selected (Änderungen auf gesamte Auswahl anwenden) aus.

Entfernen einer Markierung von mehreren Ressourcen

1. Öffnen Sie den Tag-Editor in der AWS Resource Groups Groups-Konsole unter https://console.aws.amazon.com/resource-groups/tag-editor.
2. Wählen Sie für Regionen die Regionen aus, in denen sich die Ressourcen befinden, deren Markierungen Sie entfernen möchten.
3. Wählen Sie unter Ressourcentypen den Ressourcentyp aus, für den die Markierung aufgehoben werden soll (z. B. AWS::EC2::Instance).

4. Wählen Sie Ressourcen durchsuchen aus.
5. Aktivieren Sie unter den Ergebnissen der Ressourcensuche das Kontrollkästchen neben den einzelnen Ressourcen, deren Markierungen Sie entfernen möchten.
6. Wählen Sie Markierungen der ausgewählten Ressourcen verwalten aus.
7. Wählen Sie unter Markierungen aller ausgewählten Ressourcen bearbeiten neben der zu entfernenden Markierung die Option Markierung entfernen aus.
8. Wählen Sie Markierungsänderungen prüfen und anwenden aus.
9. Wählen Sie Apply changes to all selected (Änderungen auf gesamte Auswahl anwenden) aus.

Hinzufügen eines Tags (Markierung) beim Starten einer Instance

New console

So fügen Sie ein Tag mithilfe des Launch Instance Wizard hinzu

1. Wählen Sie auf der Navigationsleiste die Region für die Instance aus. Die Auswahl ist wichtig, da nur bestimmte Amazon EC2-Ressourcen zwischen Regionen geteilt werden können. Wählen Sie die Region aus, die Ihren Anforderungen entspricht. Weitere Informationen finden Sie unter Ressourcenstandorte.
2. Wählen Sie Launch Instance (Instance starten) aus.
3. Unter Name and tags (Name und Tags) können Sie einen beschreibenden Namen für Ihre Instance eingeben und Tags angeben.

   Der Instance-Name ist ein Tag, wobei der Schlüssel Name ist und es sich bei dem Wert um den von Ihnen angegebenen Namen handelt. Sie können die Instance, Volumes, elastische Grafiken und Netzwerkschnittstellen markieren. Bei Spot-Instances können Sie nur die Spot-Instance-Anforderung mit Tags (Markierungen) versehen.

   Die Angabe eines Instance-Namens und zusätzlicher Tags ist optional.

   - Geben Sie unter Name einen beschreibenden Namen für die Instance ein. Wenn Sie keinen Namen angeben, kann die Instance anhand der ID identifiziert werden, die beim Starten der Instance automatisch generiert wird.
   - Wenn Sie zusätzliche Tags hinzufügen möchten, wählen Sie Add additional tags (Zusätzliche Tags hinzufügen) aus. Klicken Sie auf Tag hinzufügen, geben Sie dann einen Schlüssel und einen Wert ein und wählen Sie den Ressourcentyp aus, den Sie markieren

möchten. Wählen Sie für jedes weitere Tag Add another Tag (Weiteres Tag hinzufügen) aus.

4. Wählen Sie unter Application and OS Images (Amazon Machine Image) (Anwendungs- und Betriebssystem-Images (Amazon Machine Image)) das Betriebssystem (OS) für Ihre Instance und eine AMI aus. Weitere Informationen finden Sie unter Anwendungs- und Betriebssystem-Images (Amazon Machine Image).
5. Wählen Sie unter Schlüsselpaar (Anmeldung) für Schlüsselpaarname ein vorhandenes Schlüsselpaar aus oder erstellen Sie ein neues.
6. Behalten Sie entweder alle anderen Felder bei ihren Standardwerten oder wählen Sie bestimmte Werte für Ihre gewünschte Instance-Konfiguration aus. Informationen zu den einzelnen Feldern finden Sie unter Starten einer Instance mit definierten Parametern.
7. Überprüfen Sie im Bereich Summary (Zusammenfassung) die Konfiguration Ihrer Instance und wählen Sie dann Launch instance (Instance starten) aus.

Old console

So fügen Sie ein Tag mithilfe des Launch Instance Wizard hinzu

1. Wählen Sie auf der Navigationsleiste die Region für die Instance aus. Die Auswahl ist wichtig, da nur bestimmte Amazon EC2-Ressourcen zwischen Regionen geteilt werden können. Wählen Sie die Region aus, die Ihren Anforderungen entspricht. Weitere Informationen finden Sie unter Ressourcenstandorte.
2. Wählen Sie Launch Instance aus.
3. Auf der Seite Choose an Amazon Machine Image (AMI) (ein Amazon-Computer-Image (AMI) auswählen) wird eine Liste an Basiskonfigurationen anzeigt, die als Amazon Machine Images (AMIs) (Amazon-Computer-Images (AMIs)) bezeichnet werden. Wählen Sie das zu verwendende AMI und anschließend Select (Auswählen) aus. Weitere Informationen finden Sie unter Suchen eines AMI.
4. Konfigurieren Sie auf der Seite Configure Instance Details die erforderlichen Instance-Einstellungen und klicken Sie anschließend auf Next: Add Storage.
5. Auf der Seite Add Storage (Speicher hinzufügen) können Sie zusätzliche Speichervolumes für Ihre Instance angeben. Klicken Sie anschließend auf Next: Add Tags (Weiter: Tags (Markierungen) hinzufügen).
6. Auf der Seite Add Tags (Tags (Markierungen) hinzufügen) können Sie Tags (Markierungen) für die Instance, die Volumes oder beides angeben. Klicken Sie auf Add another tag

(Weiteren Tag (Markierung) hinzufügen), um der Instance mehrere Tags (Markierungen) hinzuzufügen. Wählen Sie Next: Configure Security Group, wenn Sie bereit sind.

7. Wählen Sie auf der Seite Configure Security Group eine Ihrer bestehenden Sicherheitsgruppen aus oder erstellen Sie eine neue Sicherheitsgruppe mithilfe des Assistenten. Klicken Sie abschließend auf Review and Launch.
8. Überprüfen Sie die Einstellungen. Wenn Sie mit Ihren Einstellungen zufrieden sind, klicken Sie auf Launch. Wählen Sie ein bestehendes Schlüsselpaar aus, aktivieren Sie das Kontrollkästchen zur Bestätigung und klicken Sie abschließend auf Launch Instances.

Filtern einer Ressourcenliste nach Tags (Markierungen)

Sie können Ihre Ressourcenliste auf Grundlage einer oder mehrerer Tag (Markierung)-Schlüssel und -Werte filtern.

Filtern von Ressourcen nach Markierung in der Amazon-EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich einen Ressourcentyp aus (z. B. Instances).
3. Wählen Sie das Suchfeld aus.
4. Wählen Sie in der Liste unter Markierungen den Markierungs-Schlüssel aus.
5. Wählen Sie den entsprechenden Tag (Markierung)-Wert aus der Liste.
6. Wenn Sie fertig sind, entfernen Sie den Filter.

Weitere Informationen zur Verwendung von Filtern in der Amazon-EC2-Konsole finden Sie unter Auflisten und Filtern Ihrer Ressourcen.

So filtern Sie mehrere Ressourcen über mehrere Regionen hinweg nach Markierungen mit dem Markierungs-Editor

Sie können den Tag-Editor in der AWS Ressourcengruppen-Konsole verwenden, um mehrere Ressourcen in mehreren Regionen nach Tag zu filtern. Weitere Informationen finden Sie unter Finden von zu markierenden Ressourcen im Benutzerhandbuch zum Markieren von AWS -Ressourcen.

Arbeiten mit Tags (Markierungen) über die Befehlszeile

Sie können vielen EC2-Ressourcen bei ihrer Erstellung Markierungen hinzufügen, indem Sie den Parameter „Tag Specifications“ beim Befehl „create“ verwenden. Sie können die Tags (Markierungen)

für eine Ressource mit dem describe-Befehl für die Ressource anzeigen. Sie können auch Tags (Markierungen) für vorhandene Ressourcen hinzufügen, aktualisieren oder löschen, indem Sie die folgenden Befehle verwenden.

Aufgabe	AWS CLI	AWS Tools for Windows PowerShell
Hinzufügen oder Überschreiben eines oder mehrerer Tags (Markierung)	create-tags	New-EC2Tag
Löschen eines oder mehrerer Tags (Markierung)	delete-tags	Remove-EC2Tag
Beschreiben eines oder mehrerer Tags (Markierung)	describe-tags	Get-EC2Tag

Aufgaben

- Hinzufügen von Tags (Markierungen) bei der Ressourcenerstellung
- Hinzufügen von Tags (Markierungen) zu einer vorhandenen Ressource
- Beschreiben markierter Ressourcen

Hinzufügen von Tags (Markierungen) bei der Ressourcenerstellung

In den folgenden Beispielen wird gezeigt, wie Sie Tags (Markierungen) beim Erstellen von Ressourcen anwenden.

> **Note**
>
> Wie Sie JSON-formatierte Parameter an der Befehlszeile eingeben, unterscheidet sich je nach Betriebssystem.
>
> - Linux, macOS oder Unix und Windows PowerShell — Verwenden Sie einfache Anführungszeichen (') , um die JSON-Datenstruktur einzuschließen.
> - Windows – Lassen Sie die einfachen Anführungszeichen weg, wenn Sie Befehle auf der Windows-Befehlszeile ausführen.

Weitere Informationen finden Sie unter Festlegen von Parameterwerten für AWS CLI.

Example Beispiel: Starten einer Instance und Anwenden von Tags (Markierungen) auf Instance und Volume

Der folgende run-instance-Befehl startet eine Instance und wendet ein Tag (Markierung) mit dem Schlüssel **webserver** und dem Wert **production** auf die Instance an. Der Befehl wendet auch ein Tag (Markierung) mit dem Schlüssel **cost-center** und dem Wert **cc123** auf ein erstelltes EBS-Volume an (in diesem Fall das Root-Volume).

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications
 'ResourceType=instance,Tags=[{Key=webserver,Value=production}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Sie können dieselben Tag (Markierung)-Schlüssel und -Werte auf beide Instances und Volumes beim Start anwenden. Der folgende Befehl startet eine Instance und wendet ein Tag (Markierung) mit einem Schlüssel von **cost-center** und einem Wert von **cc123** auf die Instance und alle erstellten EBS-Volumes an.

```
aws ec2 run-instances \
    --image-id ami-abc12345 \
    --count 1 \
    --instance-type t2.micro \
    --key-name MyKeyPair \
    --subnet-id subnet-6e7f829e \
    --tag-specifications 'ResourceType=instance,Tags=[{Key=cost-center,Value=cc123}]'
 'ResourceType=volume,Tags=[{Key=cost-center,Value=cc123}]'
```

Example Beispiel: Erstellen eines Volumes und Anwenden eines Tags (Markierung)

Der folgende create-volume-Befehl erstellt ein Volume und wendet zwei Tags an: **purpose=production** und **cost-center=cc123**.

```
aws ec2 create-volume \
    --availability-zone us-east-1a \
    --volume-type gp2 \
    --size 80 \
    --tag-specifications 'ResourceType=volume,Tags=[{Key=purpose,Value=production},
{Key=cost-center,Value=cc123}]'
```

Hinzufügen von Tags (Markierungen) zu einer vorhandenen Ressource

In den folgenden Beispielen wird veranschaulicht, wie Sie mithilfe des create-tags-Befehls Tags zu einer vorhandenen Ressource hinzufügen.

Example Beispiel: Hinzufügen eines Tags (Markierung) zu einer Ressource

Der folgende Befehl fügt das Tag **Stack=production** zu dem angegebenen Image hinzu oder überschreibt ein vorhandenes Tag für das AMI, wobei der Tag-Schlüssel **Stack** ist. Wird der Befehl erfolgreich ausgeführt, wird keine Ausgabe zurückgegeben.

```
aws ec2 create-tags \
    --resources ami-78a54011 \
    --tags Key=Stack,Value=production
```

Example Beispiel: Hinzufügen von Tags (Markierungen) zu mehreren Ressourcen

In diesem Beispiel werden zwei Tags (Markierungen) für ein AMI und eine Instance hinzugefügt (oder überschrieben). Eines der Tags enthält nur einen Schlüssel (**webserver**) ohne Wert (Wir legen den Wert auf eine leere Zeichenfolge fest). De andere Tag (Markierung) besteht aus einem Schlüssel (**stack**) und einem Wert (**Production**). Wird der Befehl erfolgreich ausgeführt, wird keine Ausgabe zurückgegeben.

```
aws ec2 create-tags \
    --resources ami-1a2b3c4d i-1234567890abcdef0 \
    --tags Key=webserver,Value=  Key=stack,Value=Production
```

Example Beispiel: Hinzufügen von Tags (Markierungen) mit Sonderzeichen

In diesem Beispiel wird der Tag (Markierung) **[Group]=test** zu einer Instance hinzugefügt. Die eckigen Klammern (**[** und **]**) sind Sonderzeichen, die mit Escape-Zeichen versehen werden müssen.

Wenn Sie Linux oder OS X verwenden, um die Sonderzeichen mit Escape-Zeichen zu versehen, schließen Sie das Element mit dem Sonderzeichen in doppelte Anführungszeichen (**"**) ein und schließen Sie dann die gesamte Schlüssel- und Wertstruktur in einfache Anführungszeichen (**'**) ein.

```
aws ec2 create-tags \
    --resources i-1234567890abcdef0 \
    --tags 'Key="[Group]",Value=test'
```

Wenn Sie Windows verwenden, um die Sonderzeichen mit Escape-Zeichen zu versehen, schließen Sie das Element, das Sonderzeichen enthält, in doppelte Anführungszeichen (") ein und stellen Sie jedem doppelten Anführungszeichen wie folgt einen umgekehrten Schrägstrich (****) voran:

```
aws ec2 create-tags ^
    --resources i-1234567890abcdef0 ^
    --tags Key=\"[Group]\",Value=test
```

Wenn Sie Windows verwenden PowerShell, schließen Sie den Wert, der Sonderzeichen enthält, mit doppelten Anführungszeichen (**"**) ein, stellen Sie jedem doppelten Anführungszeichen einen umgekehrten Schrägstrich (****) voran und schließen Sie dann die gesamte Schlüssel- und Wertstruktur wie folgt in einfache Anführungszeichen () ein: **'**

```
aws ec2 create-tags `
    --resources i-1234567890abcdef0 `
    --tags 'Key=\"[Group]\",Value=test'
```

Beschreiben markierter Ressourcen

Die folgenden Beispiele zeigen, wie Sie Filter mit describe-instances verwenden, um Instances mit bestimmten Tags anzuzeigen. Alle EC2-Beschreibungsbefehle verwenden diese Syntax, um nach Tags (Markierungen) über einen einzelnen Ressourcentyp hinweg zu filtern. Alternativ können Sie den Befehl describe-tags verwenden, um über EC2-Ressourcentypen hinweg nach Tag zu filtern.

Example Beispiel: Beschreiben von Instances mit dem angegebenen Tag (Markierung)-Schlüssel

Der folgende Befehl beschreibt die Instances mit einem **`Stack`**-Tag (Markierung), ungeachtet des Tag (Markierung)-Werts.

```
aws ec2 describe-instances \
    --filters Name=tag-key,Values=Stack
```

Example Beispiel: Beschreiben von Instances mit dem angegebenen Tag (Markierung)

Der folgende Befehl beschreibt die Instances mit dem Tag (Markierung) **`Stack=production`**.

```
aws ec2 describe-instances \
    --filters Name=tag:Stack,Values=production
```

Example Beispiel: Beschreiben von Instances mit dem angegebenen Tag (Markierung)-Wert

Der folgende Befehl beschreibt die Instances mit einem Tag (Markierung) mit dem Wert **`production`**, ungeachtet des Tag (Markierung)-Schlüssels.

```
aws ec2 describe-instances \
    --filters Name=tag-value,Values=production
```

Example Beispiel: Beschreiben aller EC2-Ressourcen mit dem angegebenen Tag (Markierung)

Der folgende Befehl beschreibt alle EC2-Ressourcen mit dem Tag (Markierung) **`Stack=Test`**.

```
aws ec2 describe-tags \
    --filters Name=key,Values=Stack Name=value,Values=Test
```

Arbeiten mit Instance-Tags in Instance-Metadaten

Sie können über die Instance-Metadaten auf die Tags einer Instance zugreifen. Wenn Sie über die Instance-Metadaten auf Tags zugreifen, werden die API-Aufrufe `DescribeInstances` und `DescribeTags` nicht mehr zum Abrufen von Tag-Informationen benötigt. Dadurch werden Ihre API-Transaktionen pro Sekunde reduziert und Ihre Tag-Abrufe können mit der Anzahl der Instances, die Sie steuern, skaliert werden. Darüber hinaus können lokale Prozesse, die auf einer Instance ausgeführt werden, die Tag-Informationen der Instance direkt in den Instance-Metadaten anzeigen.

Tags sind standardmäßig nicht in den Instance-Metadaten verfügbar; Sie müssen den Zugriff explizit zulassen. Sie können den Zugriff beim Start der Instance oder nach dem Start auf einer ausgeführten oder angehaltenen Instance zulassen. Sie können den Zugriff auf Tags auch zulassen, indem Sie dies in einer Startvorlage angeben. Instances, die mit der Vorlage gestartet werden, lassen den Zugriff auf Tags in den Instance-Metadaten zu.

Wenn Sie eine Instance-Markierung hinzufügen oder entfernen, werden die Instance-Metadaten aktualisiert, während die Instance läuft, ohne dass Sie die Instance anhalten und wieder starten müssen.

Themen

Zulassen des Zugriffs auf Tags in Instance-Metadaten

Standardmäßig gibt es keinen Zugriff auf Instance-Tags in den Instance-Metadaten. Sie müssen den Zugriff für jede Instance mit einer der folgenden Methoden explizit zulassen.

Zulassen des Zugriffs auf Tags in Instance-Metadaten mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie zuerst eine Instance aus und wählen Sie dann in den Instance settings (Instance-Einstellungen) unter Actions (Aktionen) die Option Allow tags in instance metadata (Zulassen von Tags in Instance-Metadaten).
4. Zum Zulassen des Zugriffs auf Tags in Instance-Metadaten aktivieren Sie das Kontrollkästchen Allow (Zulassen).
5. Wählen Sie Speichern.

Zulassen des Zugriffs auf Tags in Instance-Metadaten beim Start mithilfe der AWS CLI

Verwenden Sie den Befehl run-instances und legen Sie `InstanceMetadataTags` als `enabled` fest.

```
aws ec2 run-instances \
    --image-id ami-0abcdef1234567890 \
    --instance-type c3.large \
    ...
    --metadata-options "InstanceMetadataTags=enabled"
```

So lassen Sie den Zugriff auf Tags in Instance-Metadaten auf einer ausgeführten oder angehaltenen Instance mithilfe der AWS CLI zu

Verwenden Sie den Befehl modify-instance-metadata-options und legen Sie `--instance-metadata-tags` auf `enabled` fest.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags enabled
```

Deaktivieren des Zugriffs auf Tags in Instance-Metadaten

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf Instance-Tags in den Instance-Metadaten zu deaktivieren. Sie müssen den Zugriff auf Instance-Tags in Instance-Metadaten beim Start nicht deaktivieren, da dieser standardmäßig deaktiviert ist.

Deaktivieren des Zugriffs auf Tags in Instance-Metadaten mithilfe der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie zuerst eine Instance aus und wählen Sie dann in den Instance settings (Instance-Einstellungen) unter Actions (Aktionen) die Option Allow tags in instance metadata (Zulassen von Tags in Instance-Metadaten).
4. Zum Deaktivieren des Zugriffs auf Tags in Instance-Metadaten deaktivieren Sie das Kontrollkästchen Zulassen.
5. Wählen Sie Speichern.

Um den Zugriff auf Tags in Instanzmetadaten zu deaktivieren, verwenden Sie AWS CLI

Verwenden Sie den Befehl modify-instance-metadata-options und legen Sie `--instance-metadata-tags` auf `disabled` fest.

```
aws ec2 modify-instance-metadata-options \
    --instance-id i-123456789example \
    --instance-metadata-tags disabled
```

Anzeigen, ob der Zugriff auf Tags in den Metadaten der Instance erlaubt ist

Für jede Instance können Sie die Amazon EC2 EC2-Konsole verwenden oder überprüfen AWS CLI , ob der Zugriff auf Instance-Tags aus den Instance-Metadaten zulässig ist.

Wie Sie prüfen, ob der Zugriff auf Tags in den Metadaten der Instance über die Konsole erlaubt ist

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im Navigationsbereich Instances und dann eine Instance aus.
3. Aktivieren Sie auf der Registerkarte Details das Feld Allow tags in instance metadata (Tags in Instance-Metadaten zulassen). Wenn der Wert Enabled (Aktiviert) ist, sind Tags in Instance-Metadaten zulässig. Wenn der Wert Disabled (Deaktiviert) ist, sind Tags in Instance-Metadaten nicht zulässig.

Um zu sehen, ob der Zugriff auf Tags in Instance-Metadaten erlaubt ist, verwenden Sie den AWS CLI

Führen Sie den Befehl describe-instances aus und geben Sie die Instance-ID an.

```
aws ec2 describe-instances \
    --instance-ids i-1234567890abcdef0
```

In dem folgenden Beispiel ist die Ausgabe aus Platzgründen gekürzt. Der `"InstanceMetadataTags"`-Parameter gibt an, ob Tags in Instance-Metadaten zulässig sind. Wenn der Wert `enabled` ist, sind Tags in Instance-Metadaten zulässig. Wenn der Wert `disabled` ist, sind Tags in Instance-Metadaten nicht zulässig.

```
{
    "Reservations": [
        {
            "Groups": [],
            "Instances": [
                {
                    "AmiLaunchIndex": 0,
                    "ImageId": "ami-0abcdef1234567890",
                    "InstanceId": "i-1234567890abcdef0",
   ...

   "MetadataOptions": {
   "State": "applied",
   "HttpTokens": "optional",
   "HttpPutResponseHopLimit": 1,
   "HttpEndpoint": "enabled",
   "HttpProtocolIpv6": "disabled",
   "InstanceMetadataTags": "enabled"
   },
   ...
```

Abrufen von Tags aus Instance-Metadaten

Wenn Instance-Tags in den Instance-Metadaten zulässig sind, ist die `tags/instance`-Kategorie über die Instance-Metadaten zugänglich. Beispiele zum Abrufen von Tags aus den Instance-Metadaten finden Sie unter Abrufen von Instance-Tags für eine Instance.

Fügen Sie einer Ressource Tags hinzu mit CloudFormation

Bei Amazon-EC2-Ressourcentypen geben Sie Tags (Markierungen) entweder mithilfe einer `Tags`- oder einer `TagSpecifications`-Eigenschaft an.

In den folgenden Beispielen wird das Tag **`Stack=Production`** AWS::EC2::Instancemithilfe seiner `Tags` Eigenschaft hinzugefügt.

Example Beispiel: Tags (Markierungen) in YAML

```
Tags:
  - Key: "Stack"
    Value: "Production"
```

Example Beispiel: Tags (Markierungen) in JSON

```
"Tags": [
    {
        "Key": "Stack",
        "Value": "Production"
    }
]
```

In den folgenden Beispielen wird das Tag mithilfe seiner `TagSpecifications` Eigenschaft **`Stack=Production`** zu AWS::EC2::LaunchTemplate LaunchTemplateData hinzugefügt.

Example Beispiel: TagSpecifications in YAML

```
TagSpecifications:
  - ResourceType: "instance"
    Tags:
    - Key: "Stack"
      Value: "Production"
```

Example Beispiel: TagSpecifications in JSON

```
"TagSpecifications": [
    {
        "ResourceType": "instance",
        "Tags": [
            {
                "Key": "Stack",
                "Value": "Production"
            }
        ]
    }
]
```

Amazon-EC2-Service Quotas

Amazon EC2 stellt mehrere Ressourcen bereit, die Sie verwenden können. Diese Ressourcen umfassen Images, Instances, Volumes und Snapshots. Wenn Sie Ihre erstellen AWS-Konto, legen wir Standardkontingente (auch als Limits bezeichnet) für diese Ressourcen auf regionaler Basis fest. So gibt es z. B. eine maximale Anzahl der Instances, die Sie in einer Region starten können. Wenn Sie eine Instance in der Region USA West (Oregon) starten, darf die Anfrage daher z. B. nicht dazu führen, dass durch Ihre Nutzung Ihre maximale Anzahl von Instances in dieser Region überschritten wird.

Die Servicekontingenten-Konsole ist ein zentraler Ort, an dem Sie Ihre Kontingente für AWS Dienste anzeigen und verwalten und eine Erhöhung des Kontingents für viele der von Ihnen verwendeten Ressourcen beantragen können. Verwenden Sie die von uns bereitgestellten Kontingent , um Ihre AWS Infrastruktur zu verwalten. Planen Sie Anfragen zur Erhöhung der Kontingente im Voraus vor dem Zeitpunkt, zu dem Sie sie benötigen.

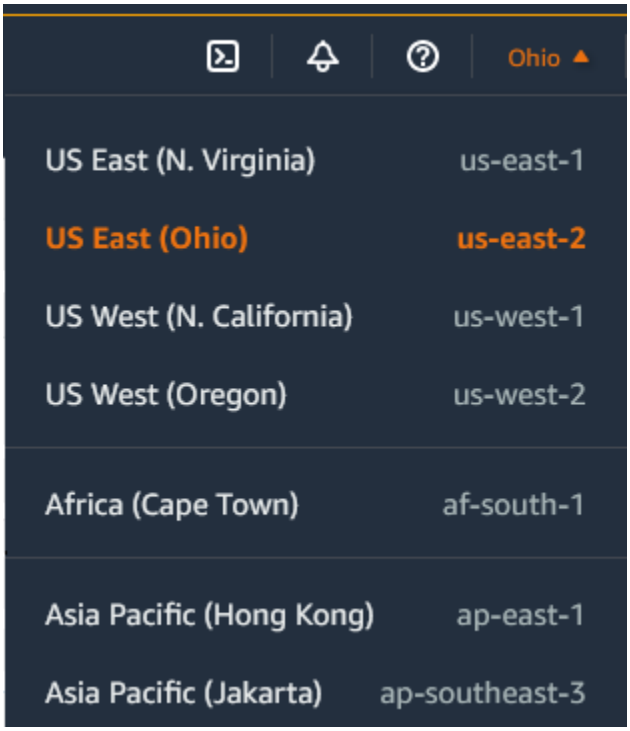
Weitere Informationen finden Sie unter Amazon EC2 EC2-Endpunkte und Kontingente und Amazon EBS-Endpunkte und Kontingente in der. Allgemeine Amazon Web Services-Referenz

Anzeigen Ihrer aktuellen Kontingente

Sie können Ihre Kontingente für jede Region mit der Service-Quotas-Konsole in anzeigen.

So zeigen Sie Ihre aktuellen Kontingente mit der Service-Quotas-Konsole an

1. Öffnen Sie die Service Quotas Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Wählen Sie auf der Navigationsleiste (oben auf dem Bildschirm) eine Region aus.



3. Verwenden Sie das Filterfeld, um die Liste nach Ressourcennamen zu filtern. Geben Sie beispielsweise **`On-Demand`** ein, um die Kontingente für On-Demand-Instances zu ermitteln.
4. Wählen Sie zum Anzeigen weiterer Informationen den Kontingentnamen aus, um die Detailseite für das Kontingent zu öffnen.

Beantragen einer Erhöhung

Sie können eine Kontingenterhöhung für jede Region beantragen.

So fordern Sie eine Erhöhung über die Service-Quotas-Konsole an

1. Öffnen Sie die Service Quotas Quotas-Konsole unter https://console.aws.amazon.com/servicequotas/home/services/ec2/quotas/.
2. Wählen Sie auf der Navigationsleiste (oben auf dem Bildschirm) eine Region aus.
3. Verwenden Sie das Filterfeld, um die Liste nach Ressourcennamen zu filtern. Geben Sie beispielsweise **`On-Demand`** ein, um die Kontingente für On-Demand-Instances zu ermitteln.

4. Wenn das Kontingent anpassbar ist, wählen Sie das Kontingent aus und wählen Sie dann Kontingenterhöhung anfordern.
5. Geben Sie unter Kontingentwert ändern den neuen Kontingentwert ein.
6. Wählen Sie Request (Anfrage).
7. Um ausstehende oder kürzlich genehmigte Anfragen in der Konsole anzuzeigen, wählen Sie im Navigationsbereich die Option Dashboard . Wählen Sie für ausstehende Anfragen den Status der Anfrage, um die Anfrage zu öffnen. Der Anfangsstatus einer Anfrage ist Pending (Ausstehend). Nachdem sich der Status in „Kontingent angefordert“ geändert hat, wird die Fallnummer mit angezeigt AWS Support. Wählen Sie die Fallnummer, um das Ticket für Ihre Anfrage zu öffnen.

Weitere Informationen, einschließlich der Verwendung der AWS CLI oder SDKs, um eine Kontingenterhöhung anzufordern, finden Sie unter Eine Kontingenterhöhung beantragen im Servicekontingents-Benutzerhandbuch.

Einschränkung für E-Mails, die über Port 25 gesendet werden

Amazon EC2 beschränkt bei allen Instances den ausgehenden Datenverkehr standardmäßig auf öffentliche IP-Adressen über Port 25. Sie können beantragen, dass diese Einschränkung entfernt wird. Weitere Informationen finden Sie unter Wie entferne ich die Beschränkung für Port 25 aus meiner Amazon EC2 EC2-Instance oder Lambda-Funktion?

> **Note**
>
> Diese Einschränkung gilt nicht für ausgehenden Datenverkehr, der über Port 25 gesendet wird an:
>
> - IP-Adressen im primären CIDR-Block der VPC, in der die ursprüngliche Netzwerkschnittstelle vorhanden ist.
> - IP-Adressen in den in RFC 1918, RFC 6598 und RFC 4193 definierten CIDRs.

Fehlerbehebung bei EC2-Instances

Die folgenden Verfahren und Tipps können Ihnen bei der Behebung von Problemen mit Ihren Amazon EC2 EC2-Instances helfen.

Inhalt

Häufige Probleme mit Windows-Instances

Mithilfe der folgenden Tipps können Sie Probleme beheben, die bei der Verwendung von EC2-Windows-Server-Instances häufiger auftreten können.

Problembereiche

- Die Instance verliert die Netzwerkverbindung oder geplante Aufgaben werden nicht zu dem erwarteten Zeitpunkt ausgeführt
- Abrufen der Konsoleausgabe nicht möglich
- Windows Server 2012 R2 nicht im Netzwerk verfügbar
- Kollision der Festplattensignatur

EBS-Volumes unter Windows Server 2016 und 2019 werden nicht initialisiert

Instances, die über Amazon Machine Images (AMIs) für Windows Server 2016 und 2019 erstellt werden, nutzen für verschiedene Aufgaben beim Systemstart den Agent EC2Launch v1, darunter die Initialisierung von EBS-Volumes. Standardmäßig initialisiert EC2Launch v1 keine sekundären Volumes. Auf folgende Weise können Sie EC2Launch v1 jedoch zum automatischen Initialisieren dieser Datenträger konfigurieren.

Zuordnen von Laufwerkbuchstaben zu Volumes

1. Stellen Sie eine Verbindung zu der Instance her, um die Datei `C:\ProgramData\Amazon\EC2-Windows\Launch\Config\DriveLetterMappingConfig.json` in einem Texteditor zu öffnen und zu konfigurieren.
2. Geben Sie die Volume-Einstellungen wie folgt an:

```
{
"driveLetterMapping": [
 {
   "volumeName": "sample volume",
   "driveLetter": "H"
 }]
}
```

3. Speichern Sie Ihre Änderungen und schließen Sie die Datei.
4. Öffnen Sie Windows PowerShell und führen Sie mit dem folgenden Befehl das EC2Launch v1-Skript aus, das die Festplatten initialisiert:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1
```

Fügen Sie die Flag `-Schedule` wie folgt hinzu, um die Datenträger bei jedem Start der Instance zu initialisieren:

```
PS C:\>  C:\ProgramData\Amazon\EC2-Windows\Launch\Scripts\InitializeDisks.ps1 -
Schedule
```

Der Agent EC2Launch v1 kann Skripts zur Instance-Initialisierung wie etwa `initializeDisks.ps1` parallel zum Skript `InitializeInstance.ps1` ausführen. Wenn das Skript `InitializeInstance.ps1` die Instance neu startet, können dadurch andere geplante Aufgaben, die beim Start der Instance ausgeführt werden, unterbrochen werden. Um mögliche Konflikte zu vermeiden, sollten Sie dem Skript `initializeDisks.ps1` Logik hinzufügen, damit die Initialisierung der Instance zuerst abgeschlossen wird.

> **Note**
>
> Wenn das EC2Launch-Skript die Volumes nicht initialisiert, stellen Sie sicher, dass die Volumes online sind. Wenn die Volumes offline sind, führen Sie den folgenden Befehl aus, um alle Festplatten online zu schalten.
>
> ```
> PS C:\> Get-Disk | Where-Object IsOffline -Eq $True | Set-Disk -IsOffline
>  $False
> ```

Starten einer EC2-Windows-Instance in die Verzeichnisdienstwiederherstellung (DSRM)

Wenn eine Instance unter Microsoft Active Directory einen Systemausfall oder andere kritische Fehler hat, können Sie eine Fehlerbehebung für die Instance einleiten, indem Sie das System in einem besonderen, abgesicherten Modus starten, der als Verzeichnisdienstwiederherstellung (Directory Services Restore Mode, DSRM) bezeichnet wird. In DSRM können Sie Active Directory reparieren oder wiederherstellen.

Treiberunterstützung für DSRM

Die Verfahren zur Aktivierung von DSRM und zum Starten der Instance richten sich nach den Treibern, die auf der Instance ausgeführt werden. In der EC2-Konsole können Sie im Systemprotokoll

Detailinformationen zu den Treiberversionen für eine Instance anzeigen. In der folgenden Tabelle wird aufgeführt, welche Treiber für DSRM unterstützt werden.

Treiberversionen	DSRM-Unterstützung?	Nächste Schritte
Citrix PV 5.9	Nein	Stellen Sie die Instance anhand einer Sicherung wieder her. DSRM kann nicht aktiviert werden.
AWS PV 7.2.0	Nein	Zwar unterstützt dieser Treiber DSRM nicht, aber Sie können das Stamm-Volume von der Instance lösen, einen Snapshot des Volumes nehmen oder anhand des Volumes ein AMI erstellen und es dann einer anderen Instance in derselben Availability Zone als sekundäres Volume zuweisen. Anschließend können Sie DSRM (wie in diesem Abschnitt beschrieben) aktivieren.
AWS PV 7.2.2 und höher	Ja	Lösen Sie das Stamm-Volume, hängen Sie es an eine andere Instance an und aktivieren Sie DSRM (wie in diesem Abschnitt beschrieben).
Enhanced Networking	Ja	Lösen Sie das Stamm-Volume, hängen Sie es an eine andere Instance an und aktivieren Sie DSRM (wie in diesem Abschnitt beschrieben).

Informationen zur Aktivierung von Enhanced Networking finden Sie unterthe section called “Elastic Network Adapter (ENA)”. Informationen zur Aktualisierung von AWS PV-Treibern finden Sie unter Aktualisieren von PV-Treibern auf Windows-Instanzen.

Konfigurieren einer Instance zum Starten im Verzeichnisdienst-Wiederherstellungsmodus (DSRM)

EC2-Windows-Instances werden erst an das Netzwerk angebunden, wenn das Betriebssystem ausgeführt wird. Daher können Sie auch nicht die Taste F8 auf der Tastatur drücken, um eine Startoption auszuwählen. Sie müssen eine der folgenden Vorgehensweise verwenden, um eine EC2-Windows Server-Instance in DSRM zu starten.

Wenn Sie den Verdacht haben, dass Active Directory beschädigt ist, die Instance aber noch ausgeführt wird, können Sie die Instance über das Dialogfeld „Systemkonfiguration“ oder über die Eingabeaufforderung so konfigurieren, dass sie im Verzeichnisdienst-Wiederherstellungsmodus (DSRM) gestartet wird.

So starten Sie eine laufende Instance über das Dialogfeld „Systemkonfiguration“ im Verzeichnisdienst-Wiederherstellungsmodus (DSRM)

1. Geben Sie im Dialogfeld Ausführen den Befehl `msconfig` ein und drücken Sie die Eingabetaste.
2. Wählen Sie die Registerkarte Start aus.
3. Aktivieren Sie unter Startoptionen das Kontrollkästchen Abgesicherter Start.
4. Wählen Sie die Option Active Directory-Wiederherstellung und klicken Sie dann auf OK. Sie werden aufgefordert, den Server neu zu starten.

So starten Sie eine laufende Instance über die Eingabeaufforderung im Verzeichnisdienst-Wiederherstellungsmodus (DSRM)

Führen Sie in einem Eingabeaufforderungsfenster den folgenden Befehl aus:

```
bcdedit /set safeboot dsrepair
```

Wenn eine Instance offline und damit nicht erreichbar ist, müssen Sie das Stamm-Volume von der Instance lösen und es an eine andere Instance anbinden, um den Verzeichnisdienst-Wiederherstellungsmodus (DSRM) zu aktivieren.

So starten Sie eine Offline-Instance im Verzeichnisdienst-Wiederherstellungsmodus (DSRM)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Suchen Sie die betroffene Instance und wählen Sie sie aus. Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten).
4. Wählen Sie Launch Instance (Instance starten) aus und erstellen Sie eine temporäre Instance in derselben Availability Zone wie die betroffene Instance. Wählen Sie einen Instance-Typ, der eine andere Version von Windows verwendet. Wenn es sich bei Ihrer Instanz beispielsweise um Windows Server 2016 handelt, wählen Sie eine Windows Server 2019-Instanz aus.

> **Important**
>
> Wenn Sie die Instance nicht in der gleichen Availability Zone wie die betroffene Instance erstellen, können Sie das Stamm-Volume der betroffenen Instance nicht der neuen Instance anfügen.

5. Wählen Sie im Navigationsbereich Volumes aus.
6. Lokalisieren Sie das Stamm-Volume der betroffenen Instance. Trennen Sie das Volume und fügen Sie es der neu erstellten temporären Instance an. Fügen Sie es dem standardmäßigen Gerätenamen (xvdf) an.
7. Stellen Sie über Remote Desktop eine Verbindung mit der temporären Instance her und verwenden Sie anschließend das Dienstprogramm für die Datenträgerverwaltung, um das Volume verfügbar zu machen und es zu verwenden.
8. Öffnen Sie eine Eingabeaufforderung und führen Sie den folgenden Befehl aus. Ersetzen Sie dabei D durch den Laufwerkbuchstaben, den Sie dem gerade angefügten sekundären Volume zugewiesen haben:

```
bcdedit /store D:\Boot\BCD /set {default} safeboot dsrepair
```

9. Wählen Sie im Dienstprogramm für die Datenträgerverwaltung das Laufwerk aus, das Sie zugewiesen haben, öffnen Sie das Kontextmenü (rechte Maustaste) und wählen Sie die Option Offline aus.
10. Trennen Sie in der EC2-Konsole das betroffene Volume von der temporären Instance und ordnen Sie es wieder der ursprünglichen Instance mit den Gerätenamen z `/dev/sda1`. Sie müssen diesen Gerätenamen angeben, um das Volume als Stamm-Volume hinzufügen zu können.
11. Starten Sie die Instance.
12. Wenn die Instance die Zustandsprüfungen in der EC2-Konsole bestanden hat, stellen Sie eine Remotedesktopverbindung mit der Instance her und überprüfen Sie, ob die Instance im Verzeichnisdienst-Wiederherstellungsmodus (DSRM) startet.
13. (Optional) Halten Sie die in dieser Prozedur erstellte temporäre Instance an bzw. löschen Sie sie.

Die Instance verliert die Netzwerkverbindung oder geplante Aufgaben werden nicht zu dem erwarteten Zeitpunkt ausgeführt

Wenn Sie Ihre Instance neu starten, und die Netzwerkverbindung Ihrer Instance getrennt wird, besteht die Möglichkeit, dass die Instance eine falsche Uhrzeit hat.

Windows-Instances verwenden standardmäßig UTC (Universal Time Coordinated). wenn Sie die Zeit für Ihre Instance auf eine andere Zeitzone einstellen und sie neu starten, ergibt sich ein Zeitversatz, und die Instance verliert vorübergehend ihre IP-Adresse. Die Instance erhält zwar nach einiger Zeit ihre Netzwerkverbindung zurück, aber dies kann einige Stunden dauern. Die Dauer, bis die Instance wieder ihre Netzwerkverbindung erhält, hängt von der Zeitdifferenz zwischen der UTC und der eingestellten Zeitzone ab.

Dasselbe Problem mit der Uhrzeit kann dazu führen, dass geplante Aufgaben zu einem unerwarteten Zeitpunkt ausgeführt werden. In diesem Fall werden die geplanten Aufgaben nicht zu dem erwarteten Zeitpunkt ausgeführt, weil die Instance eine andere Uhrzeit vorgeben.

Um dauerhaft eine andere Zeitzone als UTC zu verwenden, müssen Sie den RealTimeIsUniversalRegistrierungsschlüssel festlegen. Ohne diesen Schlüssel verwendet die Instance nach jedem Neustart wieder UTC.

So beheben Sie Probleme bei der Zeiteinstellung, die zu einem Verlust der Netzwerkverbindung führen

1. Stellen Sie sicher, dass Sie die empfohlenen PV-Treiber verwenden. Weitere Informationen finden Sie unter the section called “Upgrade für PV-Treiber”.
2. Stellen Sie sicher, dass der folgende Registrierungsschlüssel existiert und auf 1 HKEY_LOCAL_MACHINE\ SYSTEM\ Set\ Control\ Information\ gesetzt ist CurrentControl TimeZone RealTime IsUniversal

Abrufen der Konsoleausgabe nicht möglich

Bei Windows-Instances zeigt die Konsole der Instance die Ausgabe von Aufgaben, die während des Windows-Startprozesses durchgeführt werden. Wenn Windows erfolgreich gestartet wurde, wird als letzte Meldung `Windows is Ready to use` protokolliert. Sie können auch Ereignisprotokollmeldungen in der Konsole anzeigen, aber diese Funktion ist je nach Ihrer Windows-Version möglicherweise nicht standardmäßig aktiviert. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie Windows-Startagenten”.

Um die Ausgabe der Konsole für Ihre Instance mit der Amazon EC2-Konsole abzurufen, wählen Sie die Instance aus, wählen Sie dann Actions (Aktionen), Monitor and troubleshoot (Überwachung und Fehlerbehebung), Get System Log (Systemprotokoll abrufen). Verwenden Sie einen der folgenden Befehle, um die Konsolenausgabe über die Befehlszeile abzurufen: get-console-output (AWS CLI) oder Get-EC2ConsoleOutput().AWS Tools for Windows PowerShell

Für Instances, auf denen Windows Server 2012 R2 und früher ausgeführt werden: Wenn die Ausgabe der Konsole leer ist, kann dies auf ein Problem mit dem EC2Config-Service hinweisen, beispielsweise auf Fehler in einer Konfigurationsdatei oder einen fehlerhaften Windows-Start. Um dieses Problem zu beheben, laden Sie die neueste Version von EC2Config herunter und installieren Sie sie. Weitere Informationen finden Sie unter the section called “Installieren von EC2Config”.

Windows Server 2012 R2 nicht im Netzwerk verfügbar

Informationen zur Problembehandlung bei einer Windows Server 2012 R2-Instanz, die im Netzwerk nicht verfügbar ist, finden Sie unter Windows Server 2012 R2 verliert nach einem Instanzneustart die Netzwerk- und Speicherkonnektivität.

Kollision der Festplattensignatur

Sie können mithilfe von EC2Rescue for Windows Server nach Kollisionen der Festplattensignatur suchen und diese beheben. Oder Sie können Probleme mit der Festplattensignatur manuell beheben, indem Sie die folgenden Schritte ausführen:

> **Warning**
>
> Im folgenden Verfahren wird beschrieben, wie Sie mit dem Registrierungs-Editor die Windows-Registrierung bearbeiten. Wenn Sie nicht mit der Windows-Registrierung vertraut sind oder nicht wissen, wie man Änderungen mit dem Registrierungs-Editor vornimmt, finden Sie weitere Informationen unter Konfigurieren der Registrierung.

1. Öffnen Sie eine Eingabeaufforderung, geben Sie regedit.exe ein und drücken Sie die Eingabetaste.
2. Wählen Sie im Registrierungs-Editor im Kontextmenü (rechte Maustaste) HKEY_LOCAL_MACHINE aus und dann Suchen.
3. Geben Sie Windows Boot Manager ein und klicken Sie dann auf Weiteresuchen.

4. Wählen Sie den Schlüssel `11000001` aus. Dieser Schlüssel ist ein gleichgeordnetes Element des Schlüssels, den Sie im vorherigen Schritt gefunden haben.
5. Klicken Sie im rechten Bereich auf `Element` und wählen Sie dann im Kontextmenü (rechte Maustaste) die Option Ändern aus.
6. Suchen Sie die 4-Byte-Datenträgersignatur bei Versatz 0x38 in den Daten. Dies ist die Boot Configuration Database-Signatur (BCD). Kehren Sie die Bytes um, um die Datenträgersignatur zu erstellen, und notieren Sie diese. Die Datenträgersignatur der folgenden Daten lautet zum Beispiel `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

7. Führen Sie in einem Befehlszeilenfenster den folgenden Befehl aus, um Microsoft zu starten DiskPart.

```
diskpart
```

8. Führen Sie den `select disk` DiskPart Befehl aus und geben Sie die Festplattennummer für das Volume an, bei dem die Festplattensignatur kollidiert.

> **Tip**
>
> Verwenden Sie das Dienstprogramm Datenträgerverwaltung, um die Datenträgernummer des Datenträgers zu überprüfen, bei dem eine Kollision mit der Signatur aufgetreten ist. Öffnen Sie eine Eingabeaufforderung, geben Sie `compmgmt.msc` ein und drücken Sie die Eingabetaste. Doppelklicken Sie im linken Navigationsbereich auf Datenträgerverwaltung. Verwenden Sie das Dienstprogramm Datenträgerverwaltung, um die Datenträgernummer des Datenträgers zu überprüfen, bei dem eine Kollision mit der Signatur aufgetreten ist.

```
DISKPART> select disk 1
Disk 1 is now the selected disk.
```

9. Führen Sie den folgenden DiskPart Befehl aus, um die Festplattensignatur abzurufen.

```
DISKPART>  uniqueid disk
Disk ID: 0C764FA8
```

10. Wenn die im vorherigen Schritt angezeigte Festplattensignatur nicht mit der Festplattensignatur übereinstimmt, die Sie zuvor notiert haben, verwenden Sie den folgenden DiskPart Befehl, um die Festplattensignatur so zu ändern, dass sie übereinstimmt:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

Allgemeine Meldungen mit Windows-Instanzen

In diesem Abschnitt finden Sie Tipps zur Problembehandlung bei häufig angezeigten Fehlermeldungen.

Nachrichten

- Passwort nicht verfügbar
- Passwort noch nicht verfügbar
- Windows-Passwort kann nicht abgerufen werden
- Warten auf Metadaten-Service
- Windows kann nicht aktiviert werden
- Keine Original-Windows-Version (0x80070005)
- Kein Terminal Server License-Server verfügbar, um eine Lizenz bereitzustellen
- „Einige Einstellungen werden von Ihrer Organisation verwaltet.“ (Windows 2019)

Passwort nicht verfügbar

Um eine Verbindung zu der Windows-Instance unter Verwendung der Remotedesktopdienste herzustellen, müssen Sie einen Benutzernamen und ein Passwort angeben. Die bereitgestellten Benutzerkonten und Passwörter richten sich nach dem AMI, mit dem die Instance gestartet wurde. Sie können entweder das automatisch erzeugte Passwort für das Administrator-Konto abrufen oder das Benutzerkonto und das Passwort verwenden, das in der ursprünglichen Instance bei der Erstellung des AMI verwendet wurden.

Sie können ein Passwort für das Administratorkonto für Instances generieren, die unter Verwendung eines benutzerdefinierten Windows-AMIs gestartet wurden. Um das Passwort zu generieren, müssen Sie einige Einstellungen im Betriebssystem konfigurieren, bevor das AMI erstellt wird. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.

Wenn Ihre Windows-Instance nicht für die Generierung eines zufällig gewählten Passworts konfiguriert sind, wird bei dem Versuch, das automatisch generierte Passwort über die Konsole abzurufen, die folgende Meldung angezeigt:

```
Password is not available.
The instance was launched from a custom AMI, or the default password has changed. A
password cannot be retrieved for this instance. If you have forgotten your password,
 you can
reset it using the Amazon EC2 configuration service. For more information, see
 Passwords for a
Windows Server instance.
```

Überprüfen Sie die Ausgabe der Konsole für die Instance daraufhin, ob auf dem zum Starten der Instance verwendeten AMI die automatische Generierung des Passworts deaktiviert ist. Wenn die Generierung des Passworts deaktiviert ist, sieht die Ausgabe der Konsole wie folgt aus:

```
Ec2SetPassword: Disabled
```

Wenn die automatische Passwortgenerierung deaktiviert ist und Sie sich nicht an das Passwort der ursprünglichen Instance erinnern, können Sie das Passwort für diese Instance zurücksetzen. Weitere Informationen finden Sie unter Zurücksetzen eines Windows-Administratorpassworts, das verloren oder abgelaufen ist.

Passwort noch nicht verfügbar

Um eine Verbindung zu der Windows-Instance unter Verwendung der Remotedesktopdienste herzustellen, müssen Sie einen Benutzernamen und ein Passwort angeben. Die bereitgestellten Benutzerkonten und Passwörter richten sich nach dem AMI, mit dem die Instance gestartet wurde. Sie können entweder das automatisch erzeugte Passwort für das Administrator-Konto abrufen oder das Benutzerkonto und das Passwort verwenden, das in der ursprünglichen Instance bei der Erstellung des AMI verwendet wurden.

Ihr Passwort sollte innerhalb von einigen Minuten verfügbar sein. Wenn das Passwort noch nicht verfügbar ist, wird bei dem Versuch, das automatisch generierte Passwort über die Konsole abzurufen, die folgende Meldung angezeigt:

```
Password not available yet.
Please wait at least 4 minutes after launching an instance before trying to retrieve
 the
auto-generated password.
```

Wenn Sie das Passwort auch nach etwa vier Minuten nicht abrufen können, ist möglicherweise der Launch-Agent für Ihre Instance nicht für die Generierung eines Passworts konfiguriert. Sie können dies daran erkennen, dass die Ausgabe der Konsole leer ist. Weitere Informationen finden Sie unter Abrufen der Konsoleausgabe nicht möglich.

Stellen Sie außerdem sicher, dass für das AWS Identity and Access Management (IAM-) Konto, das für den Zugriff auf das Management Portal verwendet wird, die `ec2:GetPasswordData` Aktion zulässig ist. Weitere Informationen zum Verwalten von IAM-Berechtigungen finden Sie unter Was ist IAM?.

Windows-Passwort kann nicht abgerufen werden

Um das automatisch generierte Passwort für das Administrator-Konto abzurufen, müssen Sie das Schlüsselpaar verwenden, das Sie beim Starten der Instance festgelegt haben. Wenn Sie beim Starten Ihrer Instance kein Schlüsselpaar angegeben haben, wird die folgende Meldung angezeigt.

```
Cannot retrieve Windows password
```

Sie können diese Instance beenden und eine neue Instance mit demselben AMI starten. Stellen Sie dabei sicher, dass Sie ein Schlüsselpaar angeben.

Warten auf Metadaten-Service

Windows-Instances müssen Informationen aus den Instance-Metadaten abrufen, damit sie sich aktivieren können. Standardmäßig wird mit der Einstellung `WaitForMetaDataAvailable` sichergestellt, dass der EC2Config-Service darauf wartet, dass die Instance-Metadaten zugänglich sind, bevor der Startvorgang fortgesetzt wird. Weitere Informationen finden Sie unter Arbeiten mit Instance-Metadaten.

Wenn die Instance die Erreichbarkeitsprüfung nicht besteht, gehen Sie wie folgt vor, um dieses Problem zu beheben.

- Überprüfen Sie bei EC2-VPC den CIDR-Block Ihrer VPC. Windows-Instances können nicht ordnungsgemäß gestartet werden, wenn sie in einer VPC in einem IP-Adressbereich von

`224.0.0.0` bis `255.255.255.255` gestartet werden (IP-Adressbereiche Klasse D und Klasse E). Diese IP-Adressbereiche sind reserviert und sollten keinen Hostgeräten zugewiesen werden. Wir empfehlen, eine VPC mit einem CIDR-Block aus dem privaten (nicht öffentlich routingfähigen) IP-Adressbereich zu erstellen, wie in RFC 1918 spezifiziert.

- Möglicherweise wurde das System mit einer statischen IP-Adresse konfiguriert. Probieren Sie, eine Netzwerkschnittstelle zu erstellen und sie der Instance anzufügen.
- So aktivieren Sie DHCP auf einer Windows-Instance, zu der Sie keine Verbindung herstellen können

  1. Beenden Sie die betroffene Instance und trennen Sie das Stamm-Volume von der Instance.
  2. Starten Sie eine temporäre Instance in derselben Availability Zone wie die betroffene Instance.

     > **Warning**
     >
     > (Optional) Wenn ihre temporäre Instance auf demselben AMI basiert wie die ursprüngliche Instance, müssen Sie zusätzliche Schritte ausführen. Anderenfalls werden Sie die ursprüngliche Instance nach der Wiederherstellung des Stamm-Volumes wegen einer Festplatten-Signaturkollision nicht booten können. Alternativ können Sie ein anderes AMI für die temporäre Instance verwenden. Wenn die ursprüngliche Instance beispielsweise das AWS Windows AMI für Windows Server 2016 verwendet, starten Sie die temporäre Instance mit dem AWS Windows AMI für Windows Server 2019.

  3. Hängen Sie das Stamm-Volume aus der betroffenen Instance an diese temporäre Instance an. Stellen Sie eine Verbindung mit der temporären Instance her, öffnen Sie das Datenträgerverwaltung-Dienstprogramm und bringen Sie das Laufwerk online.
  4. Öffnen Sie von der temporären Instance aus Regedit und wählen Sie HKEY_LOCAL_MACHINE. Wählen Sie im Menü File die Option Load Hive aus. Wählen Sie das Laufwerk aus, öffnen Sie die Datei `Windows\System32\config\SYSTEM` und geben Sie einen (frei wählbaren) Schlüsselnamen ein, wenn Sie dazu aufgefordert werden.
  5. Wählen Sie den gerade geladenen Schlüssel aus und navigieren Sie zu `ControlSet001\Services\Tcpip\Parameters\Interfaces`. Dort sind alle Netzwerkschnittstellen nach ihrer GUID sortiert aufgelistet. Wählen Sie die richtige Netzwerkschnittstelle aus. Wenn DHCP deaktiviert und eine statische IP-Adresse zugewiesen ist, ist `EnableDHCP` auf 0 gesetzt. Um DHCP zu aktivieren, setzen Sie `EnableDHCP` auf 1 und löschen Sie die folgenden Schlüssel (falls vorhanden): `NameServer`, `SubnetMask`,

`IPAddress` und `DefaultGateway`. Wählen Sie den Schlüssel erneut aus und wählen Sie dann aus dem Menü File den Befehl Unload Hive.

> **Note**
>
> Wenn Sie mehrere Netzwerkschnittstellen konfiguriert haben, müssen Sie DHCP für die richtige Schnittstelle aktivieren. Um die richtige Netzwerkschnittstelle zu identifizieren, überprüfen Sie die folgenden Schlüsselwerte: `NameServer`, `SubnetMask`, `IPAddress` und `DefaultGateway`. Diese Werte enthalten die statische Konfiguration der vorangehenden Instance.

6. (Optional) Wenn DHCP bereits aktiviert ist, besteht die Möglichkeit, dass keine Route zu dem Metadaten-Service vorhanden ist. Sie können dieses Problem beheben, indem Sie EC2Config aktualisieren.

   a. Laden Sie die aktuelle Version des EC2Config-Service herunter und installieren Sie sie. Weitere Informationen zum Installieren dieses Service erhalten Sie unter the section called “Installieren von EC2Config”.

   b. Extrahieren Sie die Dateien aus der `.zip`-Datei in das `Temp`-Verzeichnis auf dem von Ihnen angefügten Laufwerk.

   c. Öffnen Sie Regedit und wählen Sie HKEY_LOCAL_MACHINE. Wählen Sie im Menü File die Option Load Hive aus. Wählen Sie das Laufwerk aus, öffnen Sie die Datei `Windows\System32\config\SOFTWARE` und geben Sie einen (frei wählbaren) Schlüsselnamen ein, wenn Sie dazu aufgefordert werden.

   d. Wählen Sie den gerade geladenen Schlüssel aus und navigieren Sie zu `Microsoft\Windows\CurrentVersion`. Wählen Sie den Schlüssel `RunOnce` aus. (Wenn dieser Schlüssel nicht vorhanden ist, klicken Sie mit der rechten Maustaste auf `CurrentVersion`, zeigen Sie auf New, wählen Sie die Option Schlüssel und benennen Sie den Schlüssel `RunOnce`.) Klicken Sie mit der rechten Maustaste auf den Schlüssel, zeigen Sie auf New und wählen Sie String Value. Geben Sie `Ec2Install` als den Namen und `C:\Temp\Ec2Install.exe -q` als die Daten ein.

   e. Wählen Sie den Schlüssel erneut aus und wählen Sie dann aus dem Menü File den Befehl Unload Hive.

7. (Optional) Wenn ihre temporäre Instance auf demselben AMI basiert wie die ursprüngliche Instance, müssen Sie die folgenden Schritte ausführen. Andernfalls werden Sie die

ursprüngliche Instance nach der Wiederherstellung des Stamm-Volumes wegen einer Festplatten-Signaturkollision nicht booten können.

> **Warning**
>
> Im folgenden Verfahren wird beschrieben, wie Sie mit dem Registrierungs-Editor die Windows-Registrierung bearbeiten. Wenn Sie nicht mit der Windows-Registrierung vertraut sind oder nicht wissen, wie man Änderungen mit dem Registrierungs-Editor vornimmt, finden Sie weitere Informationen unter Konfigurieren der Registrierung.

a. Öffnen Sie eine Eingabeaufforderung, geben Sie regedit.exe ein und drücken Sie die Eingabetaste.

b. Wählen Sie im Registrierungs-Editor im Kontextmenü (rechte Maustaste) HKEY_LOCAL_MACHINE aus und dann Suchen.

c. Geben Sie Windows Boot Manager ein und klicken Sie dann auf Weiteresuchen.

d. Wählen Sie den Schlüssel `11000001` aus. Dieser Schlüssel ist ein gleichgeordnetes Element des Schlüssels, den Sie im vorherigen Schritt gefunden haben.

e. Klicken Sie im rechten Bereich auf `Element` und wählen Sie dann im Kontextmenü (rechte Maustaste) die Option Ändern aus.

f. Suchen Sie die 4-Byte-Datenträgersignatur bei Versatz 0x38 in den Daten. Kehren Sie die Bytes um, um die Datenträgersignatur zu erstellen, und notieren Sie diese. Die Datenträgersignatur der folgenden Daten lautet zum Beispiel `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. Führen Sie in einem Befehlszeilenfenster den folgenden Befehl aus, um Microsoft zu starten DiskPart.

```
diskpart
```

h. Führen Sie den folgenden DiskPart Befehl aus, um das Volume auszuwählen. (Sie können mit dem Hilfsprogramm Datenträgerverwaltung überprüfen, ob die Datenträgernummer "1" ist.)

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Führen Sie den folgenden DiskPart Befehl aus, um die Festplattensignatur abzurufen.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Wenn die im vorherigen Schritt angezeigte Festplattensignatur nicht mit der Festplattensignatur von BCD übereinstimmt, die Sie zuvor notiert haben, verwenden Sie den folgenden DiskPart Befehl, um die Festplattensignatur so zu ändern, dass sie übereinstimmt:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

8. Bringen Sie das Laufwerk mit dem Datenträgerveraltung-Dienstprogramm offline.

> **Note**
>
> Das Laufwerk ist automatisch offline, wenn die temporäre Instance dasselbe Betriebssystem wie die betroffene Instance ausführt. Sie müssen es daher nicht manuell offline schalten.

9. Trennen Sie das Volume von der temporären Instance. Sie können die temporäre Instance beenden, falls Sie keine weitere Verwendung mehr dafür haben.
10. Stellen Sie das Stamm-Volume aus der betroffenen Instance wieder her, indem Sie es als anhänge `/dev/sda1`.
11. Starten Sie die betroffene Instance.

Wenn Sie mit der Instance verbunden sind, öffnen Sie auf der Instance einen Webbrowser und geben Sie den folgenden URL für den Metadaten-Server ein:

```
http://169.254.169.254/latest/meta-data/
```

Wenn Sie keine Verbindung zu dem Metadaten-Server herstellen können, versuchen Sie das Problem mit den folgenden Maßnahmen zu beheben.

- Laden Sie die aktuelle Version des EC2Config-Service herunter und installieren Sie sie. Weitere Informationen zum Installieren dieses Service erhalten Sie unter the section called “Installieren von EC2Config”.
- Überprüfen Sie, ob auf der Windows-Instance RedHat PV-Treiber ausgeführt werden. Wenn dies der Fall ist, führen Sie eine Treiberaktualisierung aus Citrix PV-Treiber durch. Weitere Informationen finden Sie unter the section called “Upgrade für PV-Treiber”.
- Überprüfen Sie, dass die Firewall-, IPSec- und Proxyeinstellungen nicht den ausgehenden Datenverkehr des Metadaten-Service (`169.254.169.254`) oder des AWS KMS -Servers (die Adressen sind in `TargetKMSServer`-Elementen in `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` angegeben) blockiert.
- Überprüfen Sie, ob Sie eine Route zu dem Metadaten-Server (`169.254.169.254`) haben, indem Sie den folgenden Befehl ausführen.

  ```
  route print
  ```

- Überprüfen Sie, ob (allgemeine) Netzwerkprobleme vorliegen, die die Availability Zone für Ihre Instance betreffen. Gehen Sie zu http://status.aws.amazon.com/.

Windows kann nicht aktiviert werden

Windows-Instanzen verwenden die AWS KMS Windows-Aktivierung. Sie können diese Meldung erhalten:`A problem occurred when Windows tried to activate. Error Code 0xC004F074`, wenn Ihre Instance den AWS KMS Server nicht erreichen kann. Windows muss alle 180 Tage aktiviert werden. EC2Config versucht, den AWS KMS Server vor Ablauf des Aktivierungszeitraums zu kontaktieren, um sicherzustellen, dass Windows aktiviert bleibt.

Wenn Sie ein Problem bei der Windows-Aktivierung haben, gehen Sie wie folgt vor, um das Problem zu beheben.

Für EC2Config (Windows Server 2012 R2-AMIs und früher)

1. Laden Sie die aktuelle Version des EC2Config-Service herunter und installieren Sie sie. Weitere Informationen zum Installieren dieses Service erhalten Sie unter the section called “Installieren von EC2Config”.
2. Melden Sie sich an der Instance an und öffnen Sie die folgende Datei: `C:\Program Files\Amazon\Ec2ConfigService\Settings\config.xml`.
3. Suchen Sie das WindowsActivateEc2-Plugin in der Datei. `config.xml` Ändern Sie den Status in Enabled und speichern Sie die Änderungen.
4. Starten Sie in dem Windows-Dienste-Snap-In den EC2Config-Service neu oder starten Sie die Instance neu.

Wenn dies das Aktivierungsproblem nicht behebt, führen Sie zusätzlich die folgenden Schritte aus.

1. Legen Sie das AWS KMS Ziel fest: C:\> slmgr.vbs /skms 169.254.169.250:1688
2. Aktivieren Sie Windows: C:\> slmgr.vbs /ato

Für EC2Launch (Windows Server 2016-AMIs und höher)

1. Importieren Sie das EC2Launch-Modul von einer PowerShell Eingabeaufforderung mit Administratorrechten aus:

```
PS C:\> Import-Module "C:\ProgramData\Amazon\EC2-Windows\Launch\Module
\Ec2Launch.psd1"
```

2. Rufen Sie die Funktion Add-Routes auf, um die Liste der neuen Routen anzuzeigen:

```
PS C:\> Add-Routes
```

3. Rufen Sie die Set-Funktion auf: ActivationSettings

```
PS C:\> Set-Activationsettings
```

4. Führen Sie das folgende Skript aus, um Windows zu aktivieren:

```
PS C:\> cscript "${env:SYSTEMROOT}\system32\slmgr.vbs" /ato
```

Sowohl für EC2Config als auch für EC2Launch: Wenn dann immer noch ein Aktivierungsfehler angezeigt wird, überprüfen Sie die folgenden Informationen.

- Stellen Sie sicher, dass Sie Routen zu den AWS KMS Servern haben. Öffnen Sie die Datei `C:\Program Files\Amazon\Ec2ConfigService\Settings\ActivationSettings.xml` und suchen Sie die `TargetKMSServer`-Elemente. Führen Sie den folgenden Befehl aus und überprüfen Sie, ob die Adressen für diese AWS KMS Server aufgeführt sind.

  ```
  route print
  ```

- Stellen Sie sicher, dass der AWS KMS Client-Schlüssel gesetzt ist. Führen Sie dazu den folgenden Befehl aus und überprüfen Sie die Ausgabe.

  ```
  C:\Windows\System32\slmgr.vbs /dlv
  ```

  Wenn die Ausgabe Fehler: Produktschlüssel nicht gefunden enthält, ist der AWS KMS Client-Schlüssel nicht festgelegt. Wenn der AWS KMS Client-Schlüssel nicht festgelegt ist, suchen Sie den Client-Schlüssel, wie in diesem Microsoft-Artikel beschrieben: AWS KMS Client-Setupschlüssel, und führen Sie dann den folgenden Befehl aus, um den AWS KMS Client-Schlüssel festzulegen.

  ```
  C:\Windows\System32\slmgr.vbs /ipk client_key
  ```

- Überprüfen Sie, ob für das System die Uhrzeit und die Zeitzone richtig eingestellt sind. Wenn Sie eine andere Zeitzone als UTC verwenden, fügen Sie den folgenden Registrierungsschlüssel hinzu und stellen Sie ihn auf ein, 1 um sicherzustellen, dass die Uhrzeit korrekt ist:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation\RealTimeIsUniversal`.
- Wenn die Windows-Firewall aktiviert ist, deaktivieren Sie sie vorübergehend mit dem folgenden Befehl.

  ```
  netsh advfirewall set allprofiles state off
  ```

Keine Original-Windows-Version (0x80070005)

Windows-Instanzen verwenden die AWS KMS Windows-Aktivierung. Wenn eine Instance den Aktivierungsprozess nicht abschließen kann, wird gemeldet, dass diese Kopie von Windows keine Original-Windows-Version ist.

Versuchen Sie die Empfehlungen unter Windows kann nicht aktiviert werden.

Kein Terminal Server License-Server verfügbar, um eine Lizenz bereitzustellen

Standardmäßig ist Windows Server über Remotedesktopdienste für zwei gleichzeitige Benutzersitzungen lizenziert. Wenn Sie einen gleichzeitigen Zugriff auf Ihre Windows-Instance über Remotedesktopdienste für mehr als zwei Benutzer bereitstellen möchten, können Sie eine zusätzliche Remotedesktopdienst-CAL (Client Access License) erwerben und die Serverrollen Remotedesktop-Sitzungshost und Remotedesktop-Lizenzierungsserver installieren.

Überprüfen Sie, ob folgende Probleme auftreten:

- Sie haben die maximal zulässige Anzahl an gleichzeitigen RDP-Sitzungen überschritten.
- Sie haben die Windows-Remotedesktopdienste-Rolle installiert.
- Die Lizenz ist abgelaufen. Wenn die Lizenz abgelaufen ist, können Sie keine Verbindung mehr zu der Windows-Instance als Benutzer herstellen. Sie können die folgenden Gegenmaßnahmen versuchen:
  - Stellen Sie über die Befehlszeile unter Verwendung eines `/admin`-Parameters eine Verbindung zu der Instance her. Beispiel:

    ```
    mstsc /v:instance /admin
    ```

    Weitere Informationen finden Sie in dem folgenden Microsoft-Artikel: Access Remote Desktop Via Command Line.
  - Halten Sie die Instance an, lösen Sie die Amazon EBS-Volumes und hängen Sie sie an eine neue Instance in derselben Availability Zone an, um Ihre Daten wiederherzustellen.

„Einige Einstellungen werden von Ihrer Organisation verwaltet.“ (Windows 2019)

Bei Instances, die aus den neuesten Windows Server AMIs gestartet werden, wird möglicherweise die Windows Update-Dialogfeldmeldung „Einige Einstellungen werden von Ihrer Organisation verwaltet.“ angezeigt. Diese Meldung erscheint aufgrund von Änderungen in Windows Server und wirkt sich nicht auf das Verhalten von Windows Update oder Ihre Fähigkeit zur Verwendung von Einstellungen aus.

So entfernen Sie die Warnung

1. Öffnen Sie `gpedit.msc` und navigieren Sie zu Computerkonfiguration, Administrative Vorlagen, Windows-Komponenten, Windows-Updates. Bearbeiten Sie Automatisches Update konfigurieren und setzen Sie diese Option auf aktiviert.
2. Aktualisieren Sie in einer Eingabeaufforderung die Gruppenrichtlinie mit gpupdate /force.
3. Schließen Sie die Windows-Aktualisierungseinstellungen und öffnen Sie sie erneut. Ihnen wird in der obigen Nachricht mitgeteilt, das Ihre Einstellungen von Ihrer Organisation verwaltet werden, gefolgt von: „Wir laden Updates automatisch herunter, abgesehen von gemessenen Verbindungen (wofür Gebühren anfallen können). In diesem Fall laden wir die Updates, die für das reibungslose Ausführen von Windows erforderlich sind, automatisch herunter.“
4. Kehren Sie zu `gpedit.msc` zurück und setzen Sie die Gruppenrichtlinie zurück auf nicht konfiguriert. Führen Sie gpupdate /force erneut aus.
5. Schließen Sie die Befehlsaufforderung und warten Sie einige Minuten.
6. Öffnen Sie die Windows-Aktualisierungseinstellungen erneut. Sie sollten die Meldung „Einige Einstellungen werden von Ihrer Organisation verwaltet.“ nicht sehen.

Beheben von Problemen beim Starten von Instances

Bei folgenden Problemen kann eine Instance nicht gestartet werden.

Startprobleme

- Ungültiger Gerätename
- Instance-Limit überschritten
- Ungenügend Kapazität der Instance

- Die angefragte Konfiguration wird derzeit nicht unterstützt. Bitte überprüfen Sie die Dokumentation auf unterstützte Konfigurationen.
- Die Instance wird sofort beendet
- Unzureichende Berechtigungen
- Hohe CPU-Auslastung kurz nach dem Start von Windows (nur Windows-Instances)

Ungültiger Gerätename

Beschreibung

Sie erhalten den `Invalid device name` *`device_name`*-Fehler, wenn Sie versuchen, eine neue Instance zu starten.

Ursache

Wenn Sie diesen Fehler erhalten, wenn Sie versuchen, eine Instance zu starten, hat der in der Anfrage für ein oder mehrere Volumes angegebene Gerätename einen ungültigen Gerätenamen. Mögliche Gründe hierfür sind:

- Der Gerätename wird möglicherweise vom ausgewählten AMI verwendet.
- Der Gerätename ist möglicherweise für Root-Volumes reserviert.
- Der Gerätename wird in der Anforderung möglicherweise für ein anderes Volume verwendet.
- Der Gerätename ist möglicherweise für das Betriebssystem nicht gültig.

Lösung

So beheben Sie das Problem:

- Stellen Sie sicher, dass der Gerätename nicht in dem ausgewählten AMI verwendet wird. Führen Sie den folgenden Befehl aus, um die Gerätename anzuzeigen, die vom AMI verwendet werden.

```
aws ec2 describe-images --image-id ami_id --query
 'Images[*].BlockDeviceMappings[].DeviceName'
```

- Stellen Sie sicher, dass Sie keinen Gerätenamen verwenden, der für Root-Volumes reserviert ist. Weitere Informationen finden Sie unter Verfügbare Gerätenamen.

- Stellen Sie sicher, dass jedes in Ihrer Anfrage angegebene Volume einen eindeutigen Gerätenamen hat.
- Stellen Sie sicher, dass die von Ihnen angegebenen Gerätenamen das richtige Format haben. Weitere Informationen finden Sie unter Verfügbare Gerätenamen.

Instance-Limit überschritten

Beschreibung

Die Fehlermeldung `InstanceLimitExceeded` wird angezeigt, wenn Sie versuchen, eine neue Instance zu starten oder eine angehaltene Instance erneut zu starten.

Ursache

Wenn beim Versuch, eine neue Instance zu starten oder eine angehaltene Instance erneut zu starten, die Fehlermeldung `InstanceLimitExceeded` angezeigt wird, haben Sie die maximal zulässige Anzahl von Instances erreicht, die Sie in einer Region starten können. Wenn Sie Ihr AWS Konto erstellen, legen wir Standardlimits für die Anzahl der Instances fest, die Sie pro Region ausführen können.

Lösung

Sie können eine Erhöhung des Instance-Limits für die jeweilige Region anfordern. Weitere Informationen finden Sie unter Amazon-EC2-Service Quotas.

Ungenügend Kapazität der Instance

Beschreibung

Die Fehlermeldung `InsufficientInstanceCapacity` wird angezeigt, wenn Sie versuchen, eine neue Instance zu starten oder eine angehaltene Instance erneut zu starten.

Ursache

Wenn bei dem Versuch, eine Instance zu starten oder eine angehaltene Instance erneut zu starten, diese Fehlermeldung angezeigt wird, verfügt AWS aktuell nicht über genügend On-Demand-Kapazität, um Ihre Anforderung zu erfüllen.

Lösung

Versuchen Sie, das Problem wie folgt zu beheben:

- Warten Sie einige Minuten und senden Sie Ihre Anfrage erneut. Die Kapazität kann häufig schwanken.
- Senden Sie eine neue Anfrage mit einer geringeren Anzahl von Instances. Wenn Sie z. B. eine einzelne Anfrage zum Starten von 15 Instances senden möchten, versuchen Sie stattdessen, 3 Anfragen für 5 Instances oder 15 Anfragen für 1 Instance zu erstellen.
- Wenn Sie eine Instance starten, senden Sie eine neue Anfrage ohne Angabe einer Availability Zone.
- Wenn Sie eine Instance starten, senden Sie eine neue Anfrage unter Verwendung eines anderen Instance-Typs (die Größe können Sie später anpassen). Weitere Informationen finden Sie unter Ändern des Instance-Typs.
- Wenn Sie Instances in einer Cluster Placement-Gruppe starten, kann es zu einem Fehler wegen unzureichender Kapazität kommen. Weitere Informationen finden Sie unter Mit Platzierungsgruppe arbeiten.

Die angefragte Konfiguration wird derzeit nicht unterstützt. Bitte überprüfen Sie die Dokumentation auf unterstützte Konfigurationen.

Beschreibung

Die Fehlermeldung `Unsupported` wird angezeigt, wenn Sie versuchen, eine neue Instance zu starten, da die Instance-Konfiguration nicht unterstützt wird.

Ursache

Die Fehlermeldung enthält zusätzliche Details. Beispielsweise wird ein Instance-Typ oder eine Instance-Kaufoption in der angegebenen Region oder Availability Zone möglicherweise nicht unterstützt.

Lösung

Versuchen Sie es mit einer anderen Instance-Konfiguration. Informationen zum Suchen nach einem Instance-Typ, der Ihren Anforderungen entspricht, finden Sie unter Suchen eines Amazon EC2-Instance-Typs.

Die Instance wird sofort beendet

Beschreibung

Ihre Instance wechselt vom Status `pending` in den Status `terminated`.

Ursache

Nachfolgend sind einige Gründe genannt, warum eine Instance sofort beendet werden kann:

- Sie haben Ihre EBS-Volumenlimits überschritten. Weitere Informationen finden Sie unter Volume-Limits für Instances.
- Ein EBS-Snapshot ist beschädigt.
- Das EBS-Stamm-Volume ist verschlüsselt und Sie sind nicht berechtigt, auf den Verschlüsselung zur Entschlüsselung zuzugreifen.
- Ein Snapshot, der in der Blockgerätezuordnung für das AMI angegeben ist, ist verschlüsselt, und Sie haben keine Berechtigungen für den Zugriff auf den Verschlüsselung für die Entschlüsselung oder Sie haben keinen Zugriff auf den Verschlüsselung für die Verschlüsselung der wiederhergestellten Volumes.
- Dem Instance Store-Backed AMI, das Sie zum Starten der Instance verwendet haben, fehlt eine erforderliche Komponente (eine image.part.xx-Datei).

Um weitere Informationen zu erhalten, fordern Sie mit einer der folgenden Methoden den Beendigungsgrund an.

So verwenden Sie die Amazon EC2-Konsole, um den Grund für die Beendigung zu erfahren

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Instance aus.
3. Suchen Sie auf der ersten Registerkarte neben Grund für den Zustandsübergang nach dem Grund.

Um den Grund für die Kündigung zu ermitteln, verwenden Sie AWS Command Line Interface

1. Führen Sie den Befehl describe-instances aus und geben Sie die Instance-ID an.

```
aws ec2 describe-instances --instance-id instance_id
```

2. Sehen Sie sich die von dem Befehl zurückgegebene JSON-Antwort an und notieren Sie die Werte im `StateReason`-Antwortelement.

   Der folgende Codeblock zeigt ein Beispiel für ein `StateReason`-Antwortelement.

```
"StateReason": {
  "Message": "Client.VolumeLimitExceeded: Volume limit exceeded",
  "Code": "Server.InternalError"
},
```

Um den Kündigungsgrund zu ermitteln, verwenden Sie AWS CloudTrail

Weitere Informationen finden Sie im AWS CloudTrail Benutzerhandbuch unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Lösung

Führen Sie abhängig von dem notierten Beendigungsgrund eine der folgenden Aktionen aus:

- **`Client.VolumeLimitExceeded: Volume limit exceeded`** — Löschen Sie nicht verwendete Volumes. Sie können einen Antrag zum Erhöhen Ihres Volume-Limits absenden.
- **`Client.InternalError: Client error on launch`**— Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen für den Zugriff auf die zum Entschlüsseln und Verschlüsseln AWS KMS keys verwendeten Volumes verfügen. Weitere Informationen finden Sie unter Verwenden von Schlüsselrichtlinien in AWS KMS im Entwicklerhandbuch für AWS Key Management Service .

Unzureichende Berechtigungen

Beschreibung

Sie erhalten den `"errorMessage": "You are not authorized to perform this operation."`-Fehler, wenn Sie versuchen, eine neue Instance zu starten, und der Startvorgang ist nicht erfolgreich.

Ursache

Falls beim Versuch, eine Instance zu starten, dieser Fehler auftritt, verfügen Sie nicht über die erforderlichen IAM-Berechtigungen, um die Instance zu starten.

Mögliche fehlende Berechtigungen:

- `ec2:RunInstances`
- `iam:PassRole`

Unter Umständen sind auch noch weitere Berechtigungen erforderlich. Die Liste der Berechtigungen, die zum Starten einer Instance erforderlich sind, finden Sie in den exemplarischen IAM-Richtlinien unter Beispiel: Verwenden des EC2 Launch Instance Wizard und Instanzen starten (RunInstances).

Lösung

So beheben Sie das Problem:

- Wenn Sie Anforderungen als IAM-Benutzer erstellen, vergewissern Sie sich, dass Sie über die folgenden Berechtigungen verfügen:
  - `ec2:RunInstances` mit einer Platzhalterressource ("*")
  - `iam:PassRole` mit der Ressource entsprechend dem ARN der Rolle (z. B. `arn:aws:iam::999999999999:role/ExampleRoleName`)
- Sollten Sie nicht über die oben genannten Berechtigungen verfügen, bearbeiten Sie die IAM-Richtlinie, die der IAM-Rolle oder dem IAM-Benutzer zugeordnet ist, um die fehlenden erforderlichen Berechtigungen hinzuzufügen.

Falls Ihr Problem dadurch nicht behoben wird und Sie weiterhin einen Fehler beim Starten erhalten, können Sie die im Fehler enthaltene Autorisierungsfehlermeldung decodieren. Die decodierte Meldung enthält die Berechtigungen, die in der IAM-Richtlinie fehlen. Weitere Informationen finden Sie unter Wie dekodiere ich eine Meldung über einen Autorisierungsfehler, nachdem ich beim Start einer EC2-Instance einen Fehler UnauthorizedOperation "" erhalte?

Hohe CPU-Auslastung kurz nach dem Start von Windows (nur Windows-Instances)

> **Note**
>
> Dieser Tipp zur Fehlerbehebung gilt nur für Windows-Instanzen.

Wenn Sie für Windows Update die Option Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen (Standardeinstellung für Instances) auswählen, kann diese Überprüfung auf Updates zwischen 50 % und 99 % der CPU-Ressourcen in der Instance beanspruchen. Wenn diese CPU-Auslastung für Ihre Anwendungen problematisch ist, können Sie die Windows Update-Einstellungen in der Systemsteuerung ändern oder das folgende Script im Amazon EC2-Dialogfeld „View/Change User Data“ verwenden:

```
reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Auto Update" /v
 AUOptions /t REG_DWORD /d 3 /f net stop wuauserv net start wuauserv
```

Wenn Sie dieses Script ausführen, geben Sie einen Wert für die Option „/d“ an. Der Standardwert ist 3. Die folgenden Werte sind möglich:

1. Nie nach Updates suchen
2. Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren manuell festlegen
3. Updates herunterladen, aber Installation manuell durchführen
4. Updates automatisch installieren

Nachdem Sie die Benutzerdaten für Ihre Instance geändert haben, können Sie die Instance ausführen. Weitere Informationen finden Sie unter Befehle beim Start auf Ihrer Windows-Instance ausführen.

Problembehandlung beim Herstellen einer Verbindung zu Ihrer Linux-Instance

Die folgenden Informationen und häufigen Fehler können Ihnen bei der Fehlersuche für die Verbindung zu Ihrer Linux-Instance helfen.

Verbindungsprobleme

- Häufige Ursachen für Verbindungsprobleme
- Fehler beim Herstellen der Verbindung mit Ihrer Instance: „Connection timed out“
- Fehler: Schlüssel kann nicht geladen werden ... Erwartend: JEDER PRIVATE SCHLÜSSEL
- Fehler: Benutzerschlüssel wird vom Server nicht erkannt
- Fehler: Berechtigung verweigert oder Verbindung durch [instance] Port 22 geschlossen

- Fehler: Ungeschützte private Schlüsseldatei
- Fehler: Der private Schlüssel muss mit „-----BEGIN RSA PRIVATE KEY-----“ und mit „-----END RSA PRIVATE KEY-----“ enden
- Fehler: Der Server lehnte unseren Schlüssel ab oder es sind keine unterstützten Authentifizierungsmethoden verfügbar.
- Die Instance ist nicht per Ping erreichbar.
- Fehler: Der Server hat die Netzwerkverbindung unerwartet geschlossen
- Fehler: Hostschlüssel-Validierung fehlgeschlagen für EC2 Instance Connect
- Mit EC2 Instance Connect kann keine Verbindung zur Ubuntu-Instance hergestellt werden
- Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Linux-Instance verbinden?

Häufige Ursachen für Verbindungsprobleme

Wir empfehlen, dass Sie mit der Behebung von Instance-Verbindungsproblemen beginnen, indem Sie sicherstellen, dass Sie die folgenden Aufgaben korrekt ausgeführt haben.

Überprüfen des Benutzernamens für Ihre Instance

Sie können mit dem Benutzernamen für Ihr Benutzerkonto oder dem Standardbenutzernamen für das AMI, das Sie zum Starten Ihrer Instance verwendet haben, eine Verbindung zu Ihrer Instance herstellen.

- Abrufen des Benutzernamens für Ihr Benutzerkonto ab.

  Weitere Informationen zum Erstellen eines Benutzerkontos finden Sie unter Verwalten Sie Systembenutzer auf Ihrer Linux-Instance.
- Abrufen des Standardbenutzernamens für das AMI, das Sie zum Starten der Instance verwendet haben:

Zum Starten der Instance verwendetes AMI	Standardbenutzername
AL2023	`ec2-user`
Amazon Linux 2	
Amazon Linux	

Zum Starten der Instance verwendetes AMI	Standardbenutzername
CentOS	`centos` oder `ec2-user`
Debian	`admin`
Fedora	`fedora` oder `ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

Überprüfen Sie, ob Ihre Sicherheitsgruppenregeln Datenverkehr zulassen.

Stellen Sie sicher, dass die mit Ihrer Instance verknüpfte Sicherheitsgruppe eingehenden SSH-Datenverkehr von Ihrer IP-Adresse zulässt. Die standardmäßige Sicherheitsgruppe für die VPC lässt keinen eingehenden SSH-Datenverkehr zu. Die über den Start-Instance-Assistenten erstellte Sicherheitsgruppe lässt eingehenden SSH-Datenverkehr standardmäßig zu. Schritte zum Hinzufügen einer Regel für eingehenden SSH-Datenverkehr zu Ihrer Linux-Instance finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus. Schritte zur Überprüfung finden Sie unter Fehler beim Herstellen der Verbindung mit Ihrer Instance: „Connection timed out“.

Stellen Sie sicher, dass Ihre Instance bereit ist.

Wenn Sie die Instance starten, kann es einige Minuten dauern, bis die Instance zur Verbindung bereitsteht. Überprüfen Sie Ihre Instance, um sicherzustellen, dass sie ausgeführt wird und ihre Statusüberprüfungen bestanden hat.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.

3. Überprüfen Sie Folgendes:

    a. Stellen Sie in der Spalte Instance state (Instance-Status) sicher, dass sich Ihre Instance im `running`-Status befindet.

    b. Überprüfen Sie in der Spalte Status check (Statusprüfung), ob Ihre Instance die beiden Statusprüfungen bestanden hat.

Sicherstellen, dass alle Voraussetzungen zum Herstellen einer Verbindung erfüllt sind

Stellen Sie sicher, dass Sie über alle Informationen verfügen, die Sie für die Verbindung benötigen. Weitere Informationen finden Sie unter Herstellen einer Verbindung zur Linux-Instance.

Spezifische Voraussetzungen für Verbindungstypen wie SSH, EC2 Instance Connect, OpenSSH, PuTTY und mehr finden Sie in den folgenden Optionen.

Linux oder macOS X

Wenn es sich bei Ihrem lokalen Computer-Betriebssystem um Linux oder macOS X handelt, überprüfen Sie die spezifischen Voraussetzungen für die folgenden Verbindungsoptionen:

- SSH-Client
- EC2 Instance Connect
- AWS Systems Manager Sitzungsmanager

Windows

Wenn es sich bei Ihrem lokalen Computer-Betriebssystem um Windows handelt, überprüfen Sie die spezifischen Voraussetzungen für die folgenden Verbindungsoptionen:

- OpenSSH
- PuTTY
- AWS Systems Manager Sitzungsmanager
- Windows-Subsystem für Linux

Fehler beim Herstellen der Verbindung mit Ihrer Instance: „Connection timed out“

Wenn Sie versuchen, eine Verbindung zu Ihrer Instance herzustellen, und die Fehlermeldung `Network error: Connection timed out` oder `Error connecting to [instance], reason: -> Connection timed out: connect` erhalten, versuchen Sie Folgendes:

Prüfen Sie Ihre Sicherheitsgruppenregeln.

Sie benötigen eine Sicherheitsgruppenregel, die den eingehenden Datenverkehr von Ihrer öffentlichen IPv4-Adresse Ihres lokalen Computers auf dem entsprechenden Port zulässt.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Überprüfen Sie auf der Registerkarte Security (Sicherheit) am unteren Rand der Konsolenseite unter Inbound rules (Eingangsregeln), die Liste der Regeln, die für die ausgewählte Instance gültig sind.

   - Für Linux-Instances: Überprüfen Sie, dass eine Regel vorhanden ist, die den Datenverkehr von Ihrem lokalen Computer auf Port 22 (SSH) zulässt.
   - Für Windows-Instances: Überprüfen Sie, dass eine Regel vorhanden ist, die den Datenverkehr von Ihrem lokalen Computer auf Port 3389 (RDP) zulässt.

   Wenn Ihre Sicherheitsgruppe keine Regel enthält, die eingehenden Datenverkehr von Ihrem lokalen Computer zulässt, fügen Sie eine Regel zu Ihrer Sicherheitsgruppe hinzu. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.
4. Die Regel, die eingehenden Datenverkehr zulässt, finden Sie im Feld Quelle. Wenn der Wert eine einzelne IP-Adresse ist und die IP-Adresse nicht statisch ist, wird bei jedem Neustart des Computers eine neue IP-Adresse zugewiesen. Dies führt dazu, dass die Regel den IP-Adressverkehr Ihres Computers nicht berücksichtigt. Die IP-Adresse darf nicht statisch sein, wenn sich Ihr Computer in einem Unternehmensnetzwerk befindet oder Sie eine Verbindung über einen Internetdienstanbieter (ISP) herstellen oder Ihre Computer-IP-Adresse dynamisch ist und sich bei jedem Neustart des Computers ändert. Um sicherzustellen, dass Ihre Sicherheitsgruppenregel eingehenden Datenverkehr von Ihrem lokalen Computer zulässt, geben Sie den IP-Adressbereich an, der von Client-Computern verwendet wird, anstatt eine einzelne IP-Adresse für Quelle anzugeben.

Weitere Informationen zu den Regeln der Sicherheitsgruppe finden Sie unter Sicherheitsgruppenregeln im Amazon VPC-Benutzerhandbuch.

Überprüfen Sie die Routing-Tabelle für das Subnetz.

Sie benötigen eine Route, die den gesamten Datenverkehr außerhalb der VPC an das Internet-Gateway für die VPC sendet.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Notieren Sie sich auf der Registerkarte Networking (Netzwerk) die Werte für VPC ID (VPC-ID) und Subnet ID (Subnetz-ID).
4. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
5. Wählen Sie im Navigationsbereich Internet Gateways aus. Überprüfen Sie, ob Ihrer VPC ein Internet-Gateway angefügt ist. Andernfalls wählen Sie Create internet gateway (Internet-Gateway erstellen), geben Sie einen Namen für das Internet-Gateway ein und wählen Sie Create internet gateway (Internet-Gateway erstellen). Wählen Sie dann für das von Ihnen erstellte Internet-Gateway Actions (Aktionen), Attach to VPC (An VPC anhängen), wählen Sie Ihre VPC aus und wählen Sie dann Attach internet gateway (Internet-Gateway anhängen), um es an Ihre VPC anzuhängen.
6. Wählen Sie im Navigationsbereich die Option Subnets und dann Ihr Subnetz aus.
7. Überprüfen Sie, ob auf der Registerkarte Route Table (Routing-Tabelle) eine Route mit `0.0.0.0/0` unter "Destination" und das Internet-Gateway für Ihre VPC unter "Target" vorhanden ist. Wenn Sie eine Verbindung mit Ihrer Instance mithilfe der IPv6-Adresse herstellen, überprüfen Sie, dass eine Route für den gesamten IPv6-Datenverkehr (`::/0`) vorhanden ist, die zum Internet-Gateway führt. Andernfalls gehen Sie wie folgt vor:

   a. Wählen Sie die ID der Routing-Tabelle (rtb-xxxxxxxx) aus, um zur Routing-Tabelle zu gelangen.

   b. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten). Wählen Sie Add route (Route hinzufügen) aus, verwenden Sie `0.0.0.0/0` als Ziel und das Internet-Gateway als Ziel. Wählen Sie für IPv6 Add route (Route hinzufügen) aus, verwenden Sie `::/0` als Ziel und das Internet-Gateway als Ziel.

   c. Wählen Sie Save Rules (Routen speichern) aus.

Überprüfen Sie die Access Control List (ACL) für das Subnetz.

Die Netzwerk-ACLs müssen ein- und ausgehenden Datenverkehr von Ihrer lokalen IP-Adresse auf Port 22 (für Linux-Instances) bzw. Port 3389 (für Windows-Instances) zulassen. Sie müssen auch ausgehenden Datenverkehr zu den kurzlebigen Ports (1024-65535) zulassen.

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Subnetz auswählen
4. Stellen Sie auf der Registerkarte Netzwerk-ACL für Eingehende Regeln sicher, dass die Regeln eingehenden Datenverkehr von Ihrem Computer auf dem erforderlichen Port zulassen. Andernfalls löschen oder ändern Sie die Regel, die den Datenverkehr blockiert.
5. Überprüfen Sie für ausgehende Regeln, ob die Regeln ausgehenden Datenverkehr zu Ihrem Computer über die kurzlebigen Ports zulassen. Andernfalls löschen oder ändern Sie die Regel, die den Datenverkehr blockiert.

Wenn sich Ihr Computer in einem Unternehmensnetzwerk befindet

Fragen Sie Ihren Netzwerkadministrator, ob die interne Firewall ein- und ausgehenden Datenverkehr von Ihrem Computer auf Port 22 (für Linux-Instances) bzw. Port 3389 (für Windows-Instances) zulässt.

Wenn auf Ihrem Computer eine Firewall aktiviert ist, überprüfen Sie, dass diese den ein- und ausgehenden Datenverkehr von Ihrem Computer auf Port 22 (für Linux-Instances) bzw. Port 3389 (für Windows-Instances) zulässt.

Prüfen Sie, ob Ihre Instance über eine öffentliche IPv4-Adresse verfügt.

Falls nicht, verknüpfen Sie eine Elastic IP-Adresse mit der Instance. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

Überprüfen Sie die CPU-Auslastung auf Ihrer Instance. Möglicherweise ist der Server überlastet.

AWS stellt automatisch Daten wie CloudWatch Amazon-Metriken und Instance-Status bereit, anhand derer Sie sehen können, wie hoch die CPU-Last auf Ihrer Instance ist, und gegebenenfalls anpassen können, wie Ihre Lasten verarbeitet werden. Weitere Informationen finden Sie unter Überwachen Sie Ihre Instances mit CloudWatch.

- Wenn Ihre Last variabel ist, können Sie Ihre Instances automatisch mit Auto Scaling und Elastic Load Balancing nach oben und unten skalieren.
- Wenn Ihre Last kontinuierlich zunimmt, können Sie auf einen größeren Instance-Typ umsteigen. Weitere Informationen finden Sie unter Ändern des Instance-Typs.

Um eine Verbindung mit Ihrer Instance mit einer IPv6-Adresse herzustellen, prüfen Sie Folgendes:

- Ihr Subnetz muss einer Routing-Tabelle zugeordnet sein, die über eine Route für IPv6-Datenverkehr (`::/0`) zu einem Internet-Gateway verfügt.
- Ihre Sicherheitsgruppenregeln müssen den eingehenden Datenverkehr von Ihrer lokalen IPv6-Adresse auf dem entsprechenden Port zulassen (22 für Linux und 3389 für Windows).
- Ihre Netzwerk-ACL-Regeln müssen ein- und ausgehenden IPv6-Datenverkehr zulassen.
- Wenn Sie Ihre Instance aus einem älteren AMI gestartet haben, ist sie möglicherweise nicht für DHCPv6 konfiguriert (IPv6-Adressen werden nicht automatisch von der Netzwerkschnittstelle erkannt). Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Ihren Instances im Benutzerhandbuch von Amazon VPC.
- Ihr lokaler Computer muss über eine IPv6-Adresse verfügen und zur Verwendung von IPv6 konfiguriert sein.

Fehler: Schlüssel kann nicht geladen werden ... Erwartend: JEDER PRIVATE SCHLÜSSEL

Wenn Sie versuchen, eine Verbindung mit Ihrer Instance herzustellen und die Fehlermeldung `unable to load key ... Expecting: ANY PRIVATE KEY` erhalten, ist die Datei, in der der private Schlüssel gespeichert ist, nicht korrekt konfiguriert. Auch wenn die Datei mit dem privaten Schlüssel auf `.pem` endet, ist sie möglicherweise dennoch falsch konfiguriert. Eine mögliche Ursache für eine falsch konfigurierte Datei für den privaten Schlüssel ist ein fehlendes Zertifikat.

Wenn die Datei für den privaten Schlüssel falsch konfiguriert ist, führen Sie die folgenden Schritte aus, um den Fehler zu beheben.

1. Erstellen Sie ein neues Schlüsselpaar. Weitere Informationen finden Sie unter Erstellen eines Schlüsselpaars mit Amazon EC2.

> **Note**
>
> Alternativ können Sie auch mit einem Drittanbietertool ein neues Schlüsselpaar erstellen. Weitere Informationen finden Sie unter Erstellen Sie ein Schlüsselpaar mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel in Amazon EC2.

2. Fügen Sie das neue Schlüsselpaar Ihrer Instance hinzu. Weitere Informationen finden Sie unter Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Linux-Instance verbinden?.
3. Stellen Sie mittels des neuen Schlüsselpaars eine Verbindung mit Ihrer Instance her.

Fehler: Benutzerschlüssel wird vom Server nicht erkannt

Bei Verwendung von SSH zum Verbinden mit Ihrer Instance

- Verwenden Sie `ssh -vvv`, um beim Herstellen der Verbindung ausführliche Debugging-Informationen zu erhalten:

```
ssh -vvv -i path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Die folgende Beispielausgabe veranschaulicht, was Sie sehen, wenn Sie versuchen, eine Verbindung mit Ihrer Instance mithilfe eines Schlüssels herzustellen, der vom Server nicht erkannt wird:

```
open/ANT/myusername/.ssh/known_hosts).
debug2: bits set: 504/1024
debug1: ssh_rsa_verify: signature correct
debug2: kex_derive_keys
debug2: set_newkeys: mode 1
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug2: set_newkeys: mode 0
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
```

```
debug2: key: boguspem.pem ((nil))
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-
interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: boguspem.pem
debug1: read PEM private key done: type RSA
debug3: sign_and_send_pubkey: RSA 9c:4c:bc:0c:d0:5c:c7:92:6c:8e:9b:16:e4:43:d8:b2
debug2: we sent a publickey packet, wait for reply
debug1: Authentications that can continue: publickey
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

Bei Verwendung von PuTTY zum Verbinden mit Ihrer Instance

- Überprüfen Sie, dass Ihre private Schlüsseldatei (PEM) in das Format konvertiert wurde, das von PuTTY (PPK) erkannt wird. Weitere Informationen zum Konvertieren Ihres privaten Schlüssels finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance über Windows mit PuTTY.

  > **Note**
  >
  > Laden Sie Ihren privaten Schlüssel in PuTTYgen und wählen Sie Save Private Key (Privaten Schlüssel speichern) statt Generate (Generieren) aus.

- Überprüfen Sie, dass Sie eine Verbindung mit dem entsprechenden Benutzernamen für Ihr AMI herstellen. Geben Sie den Benutzernamen im Feld Host name (Hostname) des Fensters PuTTY Configuration (PuTTY-Konfiguration) ein.

Zum Starten der Instance verwendetes AMI	Standardbenutzername
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`

Zum Starten der Instance verwendetes AMI	Standardbenutzername
CentOS	`centos` oder `ec2-user`
Debian	`admin`
Fedora	`fedora` oder `ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

- Überprüfen Sie, dass eine eingehende Sicherheitsgruppenregel vorhanden ist, um den eingehenden Datenverkehr am entsprechenden Port zuzulassen. Weitere Informationen finden Sie unter Regeln für die Verbindung mit Instances von Ihrem Computer aus.

Fehler: Berechtigung verweigert oder Verbindung durch [instance] Port 22 geschlossen

Wenn Sie beim Herstellen einer Verbindung mit Ihrer Instance über SSH den Fehler `Host key not found in [directory]`, `Permission denied (publickey)`, `Authentication failed, permission denied` oder `Connection closed by [instance] port 22` erhalten, stellen Sie sicher, dass Sie die Verbindung mit dem entsprechenden Benutzernamen für Ihr AMI herstellen und dass Sie den richtigen privaten Schlüssel (`.pem`-Datei) für Ihre Instance angegeben haben.

Die entsprechenden Benutzernamen lauten wie folgt:

Zum Starten der Instance verwendetes AMI	Standardbenutzername
AL2023	`ec2-user`

Zum Starten der Instance verwendetes AMI	Standardbenutzername
Amazon Linux 2 Amazon Linux	
CentOS	`centos` oder `ec2-user`
Debian	`admin`
Fedora	`fedora` oder `ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

Um beispielsweise einen SSH-Client für die Verbindung mit einer Amazon Linux-Instance zu verwenden, verwenden Sie den folgenden Befehl:

```
ssh -i /path/key-pair-name.pem instance-user-
name@ec2-203-0-113-25.compute-1.amazonaws.com
```

Vergewissern Sie sich, dass Sie den privaten Schlüssel verwenden, der dem Schlüsselpaar entspricht, das Sie beim Starten der Instance angegeben haben.

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Überprüfen Sie auf der Registerkarte Details unter Instance details (Instance-Details) den Wert des Key pair name (Schlüsselpaarnamens).

4. Wenn Sie beim Starten der Instance kein Schlüsselpaar angegeben haben, können Sie die Instance beenden und eine neue unter Angabe eines Schlüsselpaars starten. Wenn Sie diese Instance zwar verwendet haben, aber die `.pem`-Datei für Ihr Schlüsselpaar nicht mehr vorliegt, können Sie das Schlüsselpaar durch ein neues ersetzen. Weitere Informationen finden Sie unter Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Linux-Instance verbinden?.

Wenn Sie ein eigenes Schlüsselpaar generiert haben, stellen Sie sicher, dass Ihr Schlüsselgenerator für das Erstellen von RSA-Schlüssel eingerichtet ist. DSA-Schlüssel werden nicht akzeptiert.

Wenn Sie einen `Permission denied (publickey)`-Fehler erhalten und keiner der oben angegebenen Fälle zutrifft (z. B. wenn Sie zuvor eine Verbindung herstellen konnten), wurden die Berechtigungen für das Stammverzeichnis Ihrer Instance möglicherweise geändert. Berechtigungen für /home/*instance-user-name*/.ssh/authorized_keys müssen auf den Eigentümer beschränkt sein.

So überprüfen Sie die Berechtigungen für Ihre Instance

1. Beenden Sie Ihre Instance und trennen Sie das Stamm-Volume von der Instance. Weitere Informationen finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.
2. Starten Sie eine temporäre Instance in derselben Availability Zone wie Ihre aktuelle Instance (verwenden Sie ein ähnliches oder dasselbe AMI wie für die aktuelle Instance) und fügen Sie der temporären Instance das Stamm-Volume an.
3. Stellen Sie eine Verbindung mit der temporären Instance her, erstellen Sie einen Mountingpunkt und mounten Sie das angefügte Volume.
4. Überprüfen Sie über die temporäre Instance die Berechtigungen des Verzeichnisses /home/*instance-user-name*/ des angefügten Volumes. Passen Sie die Berechtigungen bei Bedarf wie folgt an:

```
[ec2-user ~]$ chmod 600 mount_point/home/instance-user-name/.ssh/authorized_keys
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name/.ssh
```

```
[ec2-user ~]$ chmod 700 mount_point/home/instance-user-name
```

5. Heben Sie die Bereitstellung des Volumes auf, trennen Sie es von der temporären Instance und fügen Sie es der ursprünglichen Instance wieder an. Stellen Sie sicher, dass Sie den richtigen Gerätenamen für das Stamm-Volume verwenden; z. B, `/dev/xvda`.
6. Starten Sie Ihre Instance. Sie können die temporäre Instance beenden, wenn Sie sie nicht mehr benötigen.

Fehler: Ungeschützte private Schlüsseldatei

Ihre private Schlüsseldatei muss vor Lese- und Schreibvorgängen anderer Benutzer geschützt sein. Wenn Ihr privater Schlüssel nur von anderen, aber nicht von Ihnen gelesen oder geschrieben werden kann, ignoriert SSH Ihren Schlüssel und Sie erhalten die folgende Warnmeldung.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0777 for '.ssh/my_private_key.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: .ssh/my_private_key.pem
Permission denied (publickey).
```

Wenn Sie beim Anmelden bei Ihrer Instance eine ähnliche Meldung erhalten, sehen Sie sich die erste Zeile der Fehlermeldung an, um zu überprüfen, ob Sie den richtigen öffentlichen Schlüssel für Ihre Instance verwenden. Das obige Beispiel verwendet den privaten Schlüssel `.ssh/my_private_key.pem` mit Dateiberechtigungen `0777`, die zulassen, das jeder Benutzer diese Datei lesen oder beschreiben kann. Da diese Berechtigungsebene sehr unsicher ist, wird dieser Schlüssel von SSH ignoriert.

Wenn Sie eine Verbindung über macOS oder Linux herstellen, führen Sie den folgenden Befehl aus, um diesen Fehler zu beheben, und ersetzen Sie dabei den Pfad durch Ihre private Schlüsseldatei.

```
[ec2-user ~]$ chmod 0400 .ssh/my_private_key.pem
```

Wenn Sie die Verbindung unter Windows herstellen möchten, führen Sie die folgenden Schritte auf dem lokalen Computer aus.

1. Navigieren Sie zu Ihrer PEM-Datei.
2. Klicken Sie mit der rechten Maustaste auf die PEM-Datei und wählen Sie Eigenschaften aus.

3. Wählen Sie die Registerkarte Sicherheit aus.
4. Klicken Sie auf Erweitert.
5. Stellen Sie sicher, dass Sie der Besitzer der Datei sind. Wenn nicht, ändern Sie den Besitzer in Ihren Benutzernamen.
6. Wählen Sie Vererbung deaktivieren und Alle vererbten Berechtigungen aus diesem Objekt entfernen aus.
7. Wählen Sie Hinzufügen und Prinzipal auswählen aus, geben Sie Ihren Benutzernamen ein und klicken Sie auf OK.
8. Erteilen Sie im Fenster Berechtigungseintrag die Berechtigungen zum Lesen und klicken Sie auf OK.
9. Klicken auf Apply (Anwenden), damit alle Einstellungen gespeichert werden.
10. Klicken Sie auf OK, um das Fenster Erweiterte Sicherheitseinstellungen zu schließen.
11. Klicken Sie auf OK, um das Fenster Eigenschaften zu schließen.
12. Sie sollten in der Lage sein, per SSH eine Verbindung aus Windows mit Ihrer Linux-Instance herzustellen.

Führen Sie in einer Windows-Eingabeaufforderung die folgenden Befehle aus:

1. Navigieren Sie von der Eingabeaufforderung zum Dateipfad Ihrer PEM-Datei.
2. Führen Sie den folgenden Befehl aus, um explizite Berechtigungen zurückzusetzen und zu entfernen:

   ```
   icacls.exe $path /reset
   ```

3. Führen Sie den folgenden Befehl aus, um dem aktuellen Benutzer Leseberechtigungen zu erteilen:

   ```
   icacls.exe $path /GRANT:R "$($env:USERNAME):(R)"
   ```

4. Führen Sie den folgenden Befehl aus, um die Vererbung zu deaktivieren und geerbte Berechtigungen zu entfernen.

   ```
   icacls.exe $path /inheritance:r
   ```

5. Sie sollten in der Lage sein, per SSH eine Verbindung aus Windows mit Ihrer Linux-Instance herzustellen.

Fehler: Der private Schlüssel muss mit „-----BEGIN RSA PRIVATE KEY-----“ und mit „-----END RSA PRIVATE KEY-----“ enden

Wenn Sie ein Tools von Drittanbietern, wie ssh-keygen, zum Erstellen eines RSA-Schlüsselpaars verwenden, generiert es den privaten Schlüssel im Format für OpenSSH-Schlüssel. Wenn Sie eine Verbindung zu Ihrer Instance herstellen und den privaten Schlüssel im OpenSSH-Format verwenden, um das Passwort zu entschlüsseln, erhalten Sie folgenden Fehler: `Private key must begin with "-----BEGIN RSA PRIVATE KEY-----" and end with "-----END RSA PRIVATE KEY-----"`.

Der private Schlüssel muss im PEM-Format vorliegen, damit dieser Fehler nicht auftritt. Verwenden Sie folgenden Befehl, um den privaten Schlüssel im PEM-Format zu erstellen:

```
ssh-keygen -m PEM
```

Fehler: Der Server lehnte unseren Schlüssel ab oder es sind keine unterstützten Authentifizierungsmethoden verfügbar.

Wenn Sie die Verbindung mit Ihrer Instance über PuTTY herstellen und einen der folgenden Fehler, Error: Server refused our key (Fehler: Server hat unseren Schlüssel abgelehnt) oder Error: No supported authentification methods available (Fehler: Keine unterstützten Authentifizierungsservices verfügbar), erhalten, überprüfen Sie, ob Sie die Verbindung mit dem korrekten Benutzernamen für Ihr AMI herstellen. Geben Sie den Benutzernamen im Feld User name (Benutzername) des Fensters PuTTY Configuration (PuTTY-Konfiguration) ein.

Die entsprechenden Benutzernamen lauten wie folgt:

Zum Starten der Instance verwendetes AMI	Standardbenutzername
AL2023 Amazon Linux 2 Amazon Linux	`ec2-user`
CentOS	`centos` oder `ec2-user`
Debian	`admin`

Zum Starten der Instance verwendetes AMI	Standardbenutzername
Fedora	`fedora` oder `ec2-user`
RHEL	`ec2-user` oder `root`
SUSE	`ec2-user` oder `root`
Ubuntu	`ubuntu`
Oracle	`ec2-user`
Bitnami	`bitnami`
Rocky Linux	`rocky`
Sonstige	Wenden Sie sich an den AMI-Anbieter

Sie sollten auch Folgendes überprüfen:

- Verwenden Sie die neueste Version von PuTTY? Weitere Informationen finden Sie auf der PuTTY-Webseite.
- Ihre private Schlüsseldatei (PEM) wurde korrekt in das Format konvertiert, das von PuTTY (.ppk) erkannt wird. Weitere Informationen zum Konvertieren Ihres privaten Schlüssels finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance über Windows mit PuTTY.

Die Instance ist nicht per Ping erreichbar.

Der `ping`-Befehl ist eine Art ICMP—Datenverkehr. Wenn Sie Ihre Instance per Ping nicht erreichen können, stellen Sie sicher, dass Ihre eingehenden Sicherheitsgruppenregeln ICMP-Datenverkehr für die `Echo Request`-Meldung von allen Quellen oder vom Computer bzw. von der Instance zulassen, auf dem bzw. der Sie den Befehl ausgeben.

Wenn Sie keinen `ping`-Befehl auf Ihrer Instance ausgeben können, stellen Sie sicher, dass Ihre ausgehenden Sicherheitsgruppenregeln ICMP-Datenverkehr für die `Echo Request`-Meldung an alle Ziele oder an den Host, den Sie per Ping zu erreichen versuchen, zulassen.

`Ping`-Befehle können aufgrund von Netzwerklatenz oder Hardwareproblemen auch von einer Firewall blockiert werden oder es kann zu einer Zeitüberschreitung kommen. Wenden Sie sich an

Ihren lokalen Netzwerk- oder Systemadministrator, um Hilfe bei der weiteren Fehlerbehebung zu erhalten.

Fehler: Der Server hat die Netzwerkverbindung unerwartet geschlossen

Wenn Sie mit Ihrer Instance mit PuTTY verbunden sind und den Fehler "Server unexpectedly closed network connection (Der Server hat die Netzwerkverbindung unerwartet geschlossen)" erhalten, vergewissern Sie sich, dass Sie Keepalives auf der Verbindungsseite der PuTTY-Konfiguration aktiviert haben, um eine Trennung der Verbindung zu vermeiden. Einige Server trennen die Verbindung von Clients, wenn sie innerhalb des angegebenen Zeitraums keine Daten empfangen. Legen Sie als Anzahl der Sekunden zwischen Keepalives 59 Sekunden fest.

Wenn nach dem Aktivieren von Keepalives weiterhin Probleme auftreten, versuchen Sie, den Nagle-Algorithmus auf der Verbindungsseite der PuTTY-Konfiguration zu deaktivieren.

Fehler: Hostschlüssel-Validierung fehlgeschlagen für EC2 Instance Connect

Wenn Sie Ihre Instance-Hostschlüssel rotieren, werden die neuen Hostschlüssel nicht automatisch in die Datenbank mit AWS vertrauenswürdigen Hostschlüsseln hochgeladen. Dies führt dazu, dass die Hostschlüssel-Validierung fehlschlägt, wenn Sie versuchen, eine Verbindung zu Ihrer Instance über den browserbasierten Client EC2 Instance Connect herzustellen, und Sie keine Verbindung mit Ihrer Instance herstellen können.

Um den Fehler zu beheben, müssen Sie das `eic_harvest_hostkeys`-Skript auf Ihrer Instance ausführen, das Ihren neuen Hostschlüssel in EC2 Instance Connect hochlädt. Das Skript befindet sich bei `/opt/aws/bin/` auf Amazon Linux 2-Instances und bei `/usr/share/ec2-instance-connect/` auf Ubuntu-Instances.

Amazon Linux 2

Beheben des Fehlers der Hostschlüssel-Validierung auf einer Amazon Linux 2-Instance

1. Stellen Sie per SSH eine Verbindung mit Ihrer Instance her.

   Sie können eine Verbindung herstellen, indem Sie die EC2 Instance Connect-CLI verwenden oder das SSH-Schlüsselpaar verwenden, das beim Start Ihrer Instance dieser zugewiesen wurde, und den Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Bei Amazon Linux 2 ist der Standardbenutzername `ec2-user`.

Beispiel: Wenn Ihre Instance mit Amazon Linux 2 gestartet wurde und der öffentliche DNS-Name Ihrer Instance ist `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` und das Schlüsselpaar `my_ec2_private_key.pem`, nutzen Sie den folgenden Befehl, um eine SSH-Sitzung auf Ihrer Instance zu starten:

```
$ ssh -i my_ec2_private_key.pem ec2-user@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH.

2. Navigieren Sie zum folgenden Ordner.

```
[ec2-user ~]$ cd /opt/aws/bin/
```

3. Führen Sie den folgenden Befehl auf Ihrer Instance aus.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Beachten Sie, dass ein erfolgreicher Anruf zu keiner Ausgabe führt.

Sie können jetzt den browserbasierten Clienten EC2 Instance Connect benutzen, um mit Ihrer Instance eine Verbindung herzustellen

Ubuntu

Beheben des Fehlers der Hostschlüssel-Validierung auf einer Ubuntu-Instance

1. Stellen Sie per SSH eine Verbindung mit Ihrer Instance her.

Sie können eine Verbindung herstellen, indem Sie die EC2 Instance Connect-CLI verwenden oder das SSH-Schlüsselpaar verwenden, das beim Start Ihrer Instance dieser zugewiesen wurde, und den Standardbenutzernamen des AMI, mit dem Sie Ihre Instance gestartet haben. Für Ubuntu lautet der Standardbenutzername `ubuntu`.

Beispiel: Wenn Ihre Instance mit Ubuntu gestartet wurde und der öffentliche DNS-Name Ihrer Instance ist `ec2-a-b-c-d.us-west-2.compute.amazonaws.com` und das

Schlüsselpaar `my_ec2_private_key.pem`, nutzen Sie den folgenden Befehl, um eine SSH-Sitzung auf Ihrer Instance zu starten:

```
$ ssh -i my_ec2_private_key.pem ubuntu@ec2-a-b-c-d.us-
west-2.compute.amazonaws.com
```

Weitere Informationen zum Herstellen einer Verbindung mit Ihrer Instance finden Sie unter Herstellen einer Verbindung zu Ihrer Linux-Instance von Linux oder macOS aus mithilfe von SSH.

2. Navigieren Sie zum folgenden Ordner.

```
[ec2-user ~]$ cd /usr/share/ec2-instance-connect/
```

3. Führen Sie den folgenden Befehl auf Ihrer Instance aus.

```
[ec2-user ~]$ ./eic_harvest_hostkeys
```

Beachten Sie, dass ein erfolgreicher Anruf zu keiner Ausgabe führt.

Sie können jetzt den browserbasierten Clienten EC2 Instance Connect benutzen, um mit Ihrer Instance eine Verbindung herzustellen

Mit EC2 Instance Connect kann keine Verbindung zur Ubuntu-Instance hergestellt werden

Wenn Sie EC2 Instance Connect verwenden, um eine Verbindung zu Ihrer Ubuntu-Instance herzustellen und beim Verbindungsversuch eine Fehlermeldung angezeigt wird, können Sie die folgenden Informationen verwenden, um das Problem zu beheben.

Mögliche Ursache

Das `ec2-instance-connect`-Paket auf der Instance ist nicht die neueste Version.

Lösung

Aktualisieren Sie das `ec2-instance-connect`-Paket auf der Instance wie folgt auf die neueste Version:

1. Stellen Sie eine Verbindung mit einer anderen Methode als EC2 Instance Connect mit Ihrer Instance her.
2. Führen Sie den folgenden Befehl auf Ihrer Instance aus, um das `ec2-instance-connect`-Paket auf die neueste Version zu aktualisieren.

```
apt update && apt upgrade
```

Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Linux-Instance verbinden?

Falls Sie den privaten Schlüssel für eine per EBS abgesicherte Instance verlieren, können Sie den Zugriff auf Ihre Instance zurückerlangen. Sie müssen die Instance anhalten, das Stamm-Volume trennen, es einer anderen Instance als Daten-Volume anfügen, die Datei `authorized_keys` mit einem neuen öffentlichen Schlüssel modifizieren, das Volume zurück zur ursprünglichen Instance verschieben und die Instance neu starten. Weitere Informationen zum Starten, Herstellen von Verbindungen und Anhalten von Instances finden Sie im Abschnitt Instance-Lebenszyklus.

Dieses Verfahren wird nur für Instance mit EBS-Stamm-Volumes unterstützt. Wenn es sich beim Stammgerät um ein Instance-Speicher-Volume handelt, können Sie dieses Verfahren nicht verwenden, um den Zugriff auf Ihre Instance wiederherzustellen. Sie benötigen den privaten Schlüssel, um eine Verbindung mit der Instance herzustellen. Zur Feststellung des Root-Gerätetyps Ihrer Instance öffnen Sie die Amazon-EC2-Konsole, wählen Sie Instances, wählen Sie die Instance aus, wählen Sie die Registerkarte Speicher und überprüfen Sie im Abschnitt Root-Gerätedetails den Wert des Root-Gerätetyps.

Der Wert ist entweder `EBS` oder `INSTANCE-STORE`.

Wenn Sie Ihren privaten Schlüssel verlieren, gibt es weitere Möglichkeiten, eine Verbindung mit Ihrer Linux-Instance herzustellen. Weitere Informationen finden Sie unter Wie kann ich eine Verbindung zu meiner Amazon EC2 Instance herstellen, wenn ich mein SSH-Schlüsselpaar nach dem ersten Start verloren habe?

Schritte für die Herstellung einer Verbindung zu einer EBS-gestützten Instance mittels eines anderen Schlüsselpaars

- Schritt 1: Erstellen eines neuen Schlüsselpaars
- Schritt 2: Abrufen von Informationen über die ursprüngliche Instance und ihr Stamm-Volume
- Schritt 3: Anhalten der ursprünglichen Instance

- Schritt 4: Starten einer temporären Instance
- Schritt 5: Trennen des Stamm-Volumes von der ursprünglichen Instance und Anfügen an die temporäre Instance
- Schritt 6: Hinzufügen des neuen öffentlichen Schlüssels zu authorized_keys auf dem ursprünglichen Volume, das auf der temporären Instance gemountet wird
- Schritt 7: Aufheben der Bereitstellung und Trennen des ursprünglichen Volumes von der temporären Instance und erneutes Anfügen an die ursprüngliche Instance
- Schritt 8: Verbinden Sie sich mit der ursprünglichen Instance mit dem neuen Schlüsselpaar
- Schritt 9: Bereinigen

Schritt 1: Erstellen eines neuen Schlüsselpaars

Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole oder einem Tool eines Drittanbieters. Falls der Name des neuen Schlüsselpaares dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen. Weitere Informationen zum Erstellen eines neuen Schlüsselpaars finden Sie unter Erstellen eines Schlüsselpaars mit Amazon EC2 oder Erstellen Sie ein Schlüsselpaar mit einem Drittanbieter-Tool und importieren Sie den öffentlichen Schlüssel in Amazon EC2.

Schritt 2: Abrufen von Informationen über die ursprüngliche Instance und ihr Stamm-Volume

Notieren Sie sich die folgenden Informationen, da Sie sie benötigen werden, um dieses Verfahren abzuschließen.

So erhalten Sie Informationen zu Ihrer ursprünglichen Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und dann die Instance aus, zu der Sie eine Verbindung herstellen möchten. (Wir bezeichnen diese als ursprüngliche Instance.)
3. Notieren Sie sich auf der Registerkarte Details die Instance-ID und die AMI-ID.
4. Notieren Sie sich auf der Registerkarte Network (Netzwerk) die Availability Zone.
5. Notieren Sie sich auf der Registerkarte Storage (Speicher) den Gerätenamen für das Root-Volume unter Root device name (Root-Gerätename) (z. B. `/dev/xvda`). Suchen Sie diesen Gerätenamen unter Block devices (Geräte blockieren) und notieren Sie sich die Volume-ID (z. B. vol-0a1234b5678c910de).

Schritt 3: Anhalten der ursprünglichen Instance

Wählen Sie Instance state (Instance-Status), Stop instance (Instance anhalten). Wenn diese Option deaktiviert ist, wurde die Instance entweder bereits angehalten oder das Root-Gerät ist ein Instance-Speicher-Volume.

> **Warning**
>
> Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Schritt 4: Starten einer temporären Instance

New console

So starten Sie eine temporäre Instance

1. Wählen Sie im Navigationsbereich Instances und Launch instances (Instances starten) aus.
2. Im Abschnitt Name and tags (Name und Tags) geben Sie beiName Temporary (Temporär) ein.
3. Im Abschnitt Application and OS Images (Anwendungs- und Betriebssystem-Images) wählen Sie dasselbe AMI aus, das Sie beim Start der ursprünglichen Instance verwendet haben. Falls diese AMI nicht verfügbar ist, können Sie eine AMI erstellen, die Sie von der angehaltenen Instance verwenden können. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.
4. Behalten Sie im Abschnitt Instance type (Instance-Typ) den standardmäßigen Instance-Typ bei.
5. Im Abschnitt Key pair (Schlüsselpaar) unter Key pair name (Schlüsselpaarname) wählen Sie das vorhandene Schlüsselpaar aus, das Sie verwenden oder erstellen Sie ein neues.
6. Im Abschnitt Network settings (Netzwerkeinstellungen) wählen Sie Edit (Bearbeiten), aus. Wählen Sie dann unter Subnet (Subnetz) ein Subnetz in derselben Availability Zone wie die ursprüngliche Instance aus.
7. Wählen Sie im Bereich Summary (Übersicht) Launch (Starten) aus.

Old console

Wählen Sie Launch Instances (Instances starten), und verwenden Sie dann den Start-Assistenten, um eine temporäre Instance mit den folgenden Optionen zu starten:

- Wählen Sie auf der Seite Choose an AMI (AMI wählen) dieselbe AMI aus, die Sie beim Start der ursprünglichen Instance verwendet haben. Falls diese AMI nicht verfügbar ist, können Sie eine AMI erstellen, die Sie von der angehaltenen Instance verwenden können. Weitere Informationen finden Sie unter Erstellen Sie ein Amazon EBS-backed AMI.
- Lassen Sie auf der Seite Choose an Instance Type (Instance-Typ wählen) den Standard-Instance-Typ, den der Assistent für Sie auswählt, unverändert.
- Geben Sie auf der Seite Configure Instance Details (Instance-Details konfigurieren) dieselbe Availability Zone wie für die ursprüngliche Instance an. Falls Sie eine Instance in einem VPC starten, wählen Sie ein Subnetz in dieser Availability Zone.
- Fügen Sie auf der Seite Add Tags (Tags (Markierungen) hinzufügen) das Tags (Markierungen) `Name=Temporary` zur Instance hinzu, um anzugeben, dass es sich um eine temporäre Instance handelt.
- Klicken Sie auf der Seite Review auf Launch. Wählen Sie das Schlüsselpaar aus, das Sie in Schritt 1 erstellt haben, und wählen Sie dann Launch Instances (Instances starten) aus.

Schritt 5: Trennen des Stamm-Volumes von der ursprünglichen Instance und Anfügen an die temporäre Instance

1. Wählen Sie im Navigationsbereich Volumes und wählen Sie das Root-Geräte-Volume für die ursprüngliche Instance aus (Sie haben die Volume-ID in einem früheren Schritt notiert). Wählen Sie Actions (Aktionen) und danach Detach volume (Volume trennen) aus, gefolgt von Detach (Trennen). Warten Sie, bis der Status des Volumes `available` wird. (Sie müssen möglicherweise das Symbol Refresh (Aktualisieren) wählen.)
2. Wählen Sie bei ausgewähltem Volume Actions (Aktionen) und wählen Sie dann Attach Volume (Volume anfügen) aus. Wählen Sie die Instance-ID der vorübergehenden Instance aus, notieren Sie den Gerätenamen unter Device name (Gerätenamen) (zum Beispiel `/dev/sdf`) und wählen Sie dann Attach volume (Volume anhängen) aus.

> **Note**
>
> Wenn Sie Ihre ursprüngliche Instance von einem AWS Marketplace AMI aus gestartet haben und Ihr Volume AWS Marketplace Codes enthält, müssen Sie zuerst die temporäre Instance beenden, bevor Sie das Volume anhängen können.

Schritt 6: Hinzufügen des neuen öffentlichen Schlüssels zu **`authorized_keys`** auf dem ursprünglichen Volume, das auf der temporären Instance gemountet wird

1. Stellen Sie eine Verbindung mit der temporären Instance her.
2. Mounten Sie in der temporären Instance das Volume, das Sie an die Instance angefügt haben, damit Sie auf ihr Dateisystem zugreifen können. Beispiel: Falls der Gerätename `/dev/sdf` lautet, verwenden Sie die folgenden Befehle zum Mounten des Volume als `/mnt/tempvol`.

   > **Note**
   >
   > Der Gerätename wird auf Ihrer Instance möglicherweise anders angezeigt. Beispiel: Geräte, die als `/dev/sdf` gemountet wurden, werden auf der Instance möglicherweise als `/dev/xvdf` angezeigt. Einige Versionen von Red Hat (oder Varianten wie CentOS) können den letzten Buchstaben möglicherweise noch um 4 Zeichen erhöhen, wobei `/dev/sd`*`f`* zu `/dev/xvd`*`k`* wird.

   a. Verwenden Sie den Befehl lsblk, um zu ermitteln, ob das Volume partitioniert ist.

   ```
   [ec2-user ~]$ lsblk
   NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
   xvda    202:0    0    8G  0 disk
   ##xvda1 202:1    0    8G  0 part /
   xvdf    202:80   0  101G  0 disk
   ##xvdf1 202:81   0  101G  0 part
   xvdg    202:96   0   30G  0 disk
   ```

   Im Beispiel oben sind `/dev/xvda` und `/dev/xvdf` partitionierte Volumes und `/dev/xvdg` nicht. Falls Ihr Volume partitioniert ist, mounten Sie die Partition (`/dev/xvdf1`) anstelle des Rohdatenträgers (`/dev/xvdf`) in den nächsten Schritten.

b. Erstellen Sie ein temporäres Verzeichnis zum Mounten des Volumes.

```
[ec2-user ~]$ sudo mkdir /mnt/tempvol
```

c. Mounten Sie das Volume (oder die Partitionierung) am temporären Mount-Punkt mithilfe des Volume-Namens oder des Gerätenamens, den Sie vorher in Erfahrung gebracht haben. Der erforderliche Befehl hängt vom Dateisystem Ihres Betriebssystems ab. Beachten Sie, dass der Gerätename auf Ihrer Instance möglicherweise anders angezeigt wird. Weitere Informationen finden Sie in note in Schritt 6.

- Amazon Linux, Ubuntu und Debian

```
[ec2-user ~]$ sudo mount /dev/xvdf1 /mnt/tempvol
```

- Amazon Linux 2, CentOS, SUSE Linux 12 und RHEL 7.x

```
[ec2-user ~]$ sudo mount -o nouuid /dev/xvdf1 /mnt/tempvol
```

> **Note**
>
> Wenn Sie einen Fehler erhalten, der besagt, dass das Dateisystem beschädigt ist, führen Sie den folgenden Befehl aus, um mit dem Dienstprogramm fsck das Dateisystem zu prüfen und mögliche Probleme zu beheben:
>
> ```
> [ec2-user ~]$ sudo fsck /dev/xvdf1
> ```

3. Verwenden Sie in der temporären Instance den folgenden Befehl, um `authorized_keys` mit dem neuen öffentlichen Schlüssel über `authorized_keys` für die temporäre Instance am gemounteten Volume zu aktualisieren.

> **Important**
>
> Die folgenden Beispiele verwenden den Amazon Linux-Benutzernamen `ec2-user`. Sie können ihn durch einen anderen Benutzernamen ersetzen, wie etwa `ubuntu` für Ubuntu-Instances.

```
[ec2-user ~]$ cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Falls diese Kopie erfolgreich verlief, können Sie mit dem nächsten Schritt fortfahren.

(Optional) Falls Sie keine Berechtigung zum Bearbeiten von Dateien in `/mnt/tempvol` besitzen, müssen Sie die Datei mithilfe von sudo aktualisieren und dann die Berechtigungen für die Datei überprüfen, um zu gewährleisten, dass Sie sich an der ursprünglichen Instance anmelden können. Führen Sie den folgenden Befehl aus, um die Berechtigungen für die Datei zu prüfen.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
total 4
-rw------- 1 222 500 398 Sep 13 22:54 authorized_keys
```

In dieser Beispielausgabe lautet die Benutzer-ID *222* und die Gruppen-ID *500*. Verwenden Sie als Nächstes sudo, um den fehlgeschlagenen Kopierbefehl erneut auszuführen.

```
[ec2-user ~]$ sudo cp .ssh/authorized_keys /mnt/tempvol/home/ec2-user/.ssh/
authorized_keys
```

Führen Sie den folgenden Befehl noch einmal aus, um zu ermitteln, ob sich die Berechtigungen geändert haben.

```
[ec2-user ~]$ sudo ls -l /mnt/tempvol/home/ec2-user/.ssh
```

Falls sich die Benutzer-ID und die Gruppen-ID geändert haben, verwenden Sie den folgenden Befehl, um sie wiederherzustellen.

```
[ec2-user ~]$ sudo chown 222:500 /mnt/tempvol/home/ec2-user/.ssh/authorized_keys
```

Schritt 7: Aufheben der Bereitstellung und Trennen des ursprünglichen Volumes von der temporären Instance und erneutes Anfügen an die ursprüngliche Instance

1. Entfernen Sie in der temporären Instance das Volume, das Sie angefügt haben, damit Sie es wieder an der ursprünglichen Instance anhängen können. Verwenden Sie beispielsweise den folgenden Befehl, um die Bereitstellung des Volumes unter aufzuhebe `/mnt/tempvol`.

   ```
   [ec2-user ~]$ sudo umount /mnt/tempvol
   ```

2. Trennen Sie das Volume von der temporären Instance (Sie haben das Mounting der Bereitstellung im vorherigen Schritt aufgehoben): Wählen Sie in der Amazon EC2-Konsole im NavigationsbereichVolumes wählen sie das Stamm-Gerät-Volume für die ursprüngliche Instance (Sie haben die Volume-ID in einem vorherigen Schritt notiert) wählen Sie Actions (Aktionen), Detach volume (Volumen trennen) und dann Detach (Trennen) aus. Warten Sie, bis der Status des Volumes `available` wird. (Sie müssen möglicherweise das Symbol Refresh (Aktualisieren) wählen.)

3. Erneutes Anfügen des Volume an die ursprüngliche Instance: Wählen Sie bei weiter ausgewähltem Volume Actions (Aktionen) die Option Attach Volume (Volume anfügen) aus. Wählen Sie die Instance-ID der ursprünglichen Instance aus, geben Sie den Gerätenamen an, den Sie zuvor in Schritt 2 für die ursprüngliche Stammgeräte-Anlage (`/dev/sda1` oder `/dev/xvda`) notiert haben, und wählen Sie dann Attach volume (Volume anhängen) aus.

   > **Important**
   >
   > Falls Sie nicht denselben Gerätenamen als ursprünglichen Anhang angeben, können Sie die ursprüngliche Instance nicht starten. Amazon EC2 erwartet den Root-Gerät-Datenträger unter `sda1` oder `/dev/xvda`.

Schritt 8: Verbinden Sie sich mit der ursprünglichen Instance mit dem neuen Schlüsselpaar

Wählen Sie die ursprüngliche Instance und dann Instance state (Instance-Status), Start instance (Instance starten). Wenn die Instance den Status `running` erhält, können Sie mit der Datei mit dem privaten Schlüssel für Ihr neues Schlüsselpaar eine Verbindung zu ihr herstellen.

> **Note**
>
> Falls sich der Name Ihres neuen Schlüsselpaars und der entsprechenden Datei mit dem privaten Schlüssel vom Namen des ursprünglichen Schlüsselpaars unterscheidet, müssen Sie den Namen der Datei mit dem neuen privaten Schlüssel angeben, wenn Sie eine Verbindung mit Ihrer Instance herstellen.

Schritt 9: Bereinigen

(Optional) Sie können die temporäre Instance beenden, falls Sie keine weitere Verwendung mehr dafür haben. Wählen Sie die temporäre Instance und dann Instance state (Instance-Status), Terminate instance (Instance beenden) aus.

Beheben von Verbindungsproblemen mit Ihrer Windows-Instance

Die folgenden Informationen und häufig auftretenden Fehler können Ihnen bei der Problembehandlung beim Herstellen einer Verbindung mit Ihrer Windows-Instanz helfen.

Verbindungsprobleme

- Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen
- Fehler beim Verwenden des macOS RDP-Clients
- RDP zeigt anstelle des Desktops einen schwarzen Bildschirm an
- Die Remote-Anmeldung bei einer Instance mit einem Benutzer, der kein Administrator ist, ist nicht möglich
- Behebung von Remotedesktop-Problemen mit AWS Systems Manager
- Aktivieren von Remotedesktop für eine EC2-Instance mit Remote-Registrierung
- Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Windows-Instance verbinden?

Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen

Versuchen Sie, Verbindungsprobleme mit Ihre Instance mit den folgenden Maßnahmen zu beheben:

- Vergewissern Sie sich, dass Sie den richtigen öffentlichen DNS-Hostnamen verwenden. (Wählen Sie in der Amazon EC2-Konsole die Instance aus und überprüfen Sie im Detailbereich den Wert für Public DNS (IPv4).) Wenn sich Ihre Instance in einer VPC befindet, aber kein öffentlicher DNS-Name angezeigt wird, müssen Sie die DNS-Hostnamen aktivieren. Weitere Infomationen finden Sie unter DNS-Attribute für Ihre VPC im Amazon VPC-Benutzerhandbuch.
- Überprüfen Sie, ob Ihre Instance über eine öffentliche IPv4-Adresse verfügt. Falls nicht, verknüpfen Sie eine Elastic IP-Adresse mit der Instance. Weitere Informationen finden Sie unter Elastic-IP-Adressen.
- Um eine Verbindung zu Ihrer Instance mit einer IPv6-Adresse herzustellen, überprüfen Sie, dass Ihr lokaler Computer muss über eine IPv6-Adresse verfügt und zur Verwendung von IPv6 konfiguriert ist. Weitere Informationen finden Sie unter Konfigurieren von IPv6 auf Ihren Instances im Benutzerhandbuch von Amazon VPC.
- Überprüfen Sie, ob für Ihre Sicherheitsgruppe eine Regel eingerichtet ist, die den RDP-Zugriff zulässt.
- Wenn Sie das Passwort kopiert und eingefügt haben, und die Fehlermeldung `Your credentials did not work` angezeigt wird, geben Sie das Passwort manuell ein. Möglicherweise ist beim Kopieren des Passworts ein Buchstabe zu wenig oder ein Leerzeichen zu viel markiert gewesen.
- Überprüfen Sie, ob Ihre Instance ihre Statusprüfungen bestanden hat. Weitere Informationen finden Sie unter Statusprüfungen für Ihre Instances und the section called “Fehlgeschlagene Statusprüfungen unter Linux”.
- Überprüfen Sie, dass die Routing-Tabelle für das Subnetz eine Route hat, die den gesamten Datenverkehr mit Zielen außerhalb der VPC an das Internet-Gateway für die VPC sendet. Weitere Informationen finden Sie unter Erstellen einer benutzerdefinierten Routing-Tabelle (Internet-Gateways) im Amazon VPC Benutzerhandbuch.
- Überprüfen Sie, ob die Windows-Firewall – oder eine andere Firewall-Software – den RDP-Datenverkehr zu Ihrer Instance blockiert. Wir empfehlen, die Windows-Firewall zu deaktivieren und den Zugriff auf Ihre Instance mithilfe von Sicherheitsgruppenregeln zu steuern. Sie können AWSSupport-TroubleshootRDP für disable the Windows Firewall profiles using SSM Agent verwenden. Gehen Sie wie folgt vor, um die Windows-Firewall auf einer Windows-Instanz zu deaktivieren AWSSupport-ExecuteEC2Rescue, die nicht dafür AWS Systems Manager konfiguriert ist:

Manuelle Schritte

1. Beenden Sie die betroffene Instance und trennen Sie das Stamm-Volume von der Instance.

2. Starten Sie eine temporäre Instance in derselben Availability Zone wie die betroffene Instance.

> **Warning**
>
> (Optional) Wenn ihre temporäre Instance auf demselben AMI basiert wie die ursprüngliche Instance, müssen Sie zusätzliche Schritte ausführen. Anderenfalls werden Sie die ursprüngliche Instance nach der Wiederherstellung des Stamm-Volumes wegen einer Festplatten-Signaturkollision nicht booten können. Alternativ können Sie ein anderes AMI für die temporäre Instance verwenden. Wenn die ursprüngliche Instance beispielsweise das AWS Windows AMI für Windows Server 2016 verwendet, starten Sie die temporäre Instance mit dem AWS Windows AMI für Windows Server 2019.

3. Hängen Sie das Stamm-Volume aus der betroffenen Instance an diese temporäre Instance an. Stellen Sie eine Verbindung mit der temporären Instance her, öffnen Sie das Datenträgerverwaltung-Dienstprogramm und bringen Sie das Laufwerk online.
4. Öffnen Sie Regedit und wählen Sie HKEY_LOCAL_MACHINE. Wählen Sie im Menü File die Option Load Hive aus. Wählen Sie das Laufwerk aus, öffnen Sie die Datei `Windows\System32\config\SYSTEM` und geben Sie einen (frei wählbaren) Schlüsselnamen ein, wenn Sie dazu aufgefordert werden.
5. Wählen Sie den gerade geladenen Schlüssel aus und navigieren Sie zu `ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy`. Wählen Sie nacheinander alle Schlüssel mit Namen „xxxxProfile“ aus und ändern Sie den Wert für `EnableFirewall` von 1 in 0. Wählen Sie den Schlüssel erneut aus und wählen Sie dann aus dem Menü File den Befehl Unload Hive.
6. (Optional) Wenn ihre temporäre Instance auf demselben AMI basiert wie die ursprüngliche Instance, müssen Sie die folgenden Schritte ausführen. Andernfalls werden Sie die ursprüngliche Instance nach der Wiederherstellung des Stamm-Volumes wegen einer Festplatten-Signaturkollision nicht booten können.

> **Warning**
>
> Im folgenden Verfahren wird beschrieben, wie Sie mit dem Registrierungs-Editor die Windows-Registrierung bearbeiten. Wenn Sie nicht mit der Windows-Registrierung vertraut sind oder nicht wissen, wie man Änderungen mit dem Registrierungs-Editor vornimmt, finden Sie weitere Informationen unter Konfigurieren der Registrierung.

a. Öffnen Sie eine Eingabeaufforderung, geben Sie regedit.exe ein und drücken Sie die Eingabetaste.

b. Wählen Sie im Registrierungs-Editor im Kontextmenü (rechte Maustaste) HKEY_LOCAL_MACHINE aus und dann Suchen.

c. Geben Sie Windows Boot Manager ein und klicken Sie dann auf Weiteresuchen.

d. Wählen Sie den Schlüssel `11000001` aus. Dieser Schlüssel ist ein gleichgeordnetes Element des Schlüssels, den Sie im vorherigen Schritt gefunden haben.

e. Klicken Sie im rechten Bereich auf `Element` und wählen Sie dann im Kontextmenü (rechte Maustaste) die Option Ändern aus.

f. Suchen Sie die 4-Byte-Datenträgersignatur bei Versatz 0x38 in den Daten. Kehren Sie die Bytes um, um die Datenträgersignatur zu erstellen, und notieren Sie diese. Die Datenträgersignatur der folgenden Daten lautet zum Beispiel `E9EB3AA5`:

```
...
0030  00 00 00 00 01 00 00 00
0038  A5 3A EB E9 00 00 00 00
0040  00 00 00 00 00 00 00 00
...
```

g. Führen Sie in einem Befehlszeilenfenster den folgenden Befehl aus, um Microsoft zu starten DiskPart.

```
diskpart
```

h. Führen Sie den folgenden DiskPart Befehl aus, um das Volume auszuwählen. (Sie können mit dem Hilfsprogramm Datenträgerverwaltung überprüfen, ob die Datenträgernummer "1" ist.)

```
DISKPART> select disk 1

Disk 1 is now the selected disk.
```

i. Führen Sie den folgenden DiskPart Befehl aus, um die Festplattensignatur abzurufen.

```
DISKPART>  uniqueid disk

Disk ID: 0C764FA8
```

j. Wenn die im vorherigen Schritt angezeigte Festplattensignatur nicht mit der Festplattensignatur von BCD übereinstimmt, die Sie zuvor notiert haben, verwenden Sie den folgenden DiskPart Befehl, um die Festplattensignatur so zu ändern, dass sie übereinstimmt:

```
DISKPART> uniqueid disk id=E9EB3AA5
```

7. Bringen Sie das Laufwerk mit dem Datenträgerveraltung-Dienstprogramm offline.

> **Note**
>
> Das Laufwerk ist automatisch offline, wenn die temporäre Instance dasselbe Betriebssystem wie die betroffene Instance ausführt. Sie müssen es daher nicht manuell offline schalten.

8. Trennen Sie das Volume von der temporären Instance. Sie können die temporäre Instance beenden, falls Sie keine weitere Verwendung mehr dafür haben.
9. Stellen Sie das Stamm-Volume aus der betroffenen Instance wieder her, indem Sie es als anhänge `/dev/sda1`.
10. Starten Sie die Instance.

- Stellen Sie sicher, dass die Authentifizierung auf Netzwerkebene für Instances, die nicht Teil einer Active-Directory-Domain sind, deaktiviert ist (verwenden Sie AWSSupport-TroubleshootRDP um disable NLA auszuführen).
- Stellen Sie sicher, dass der Starttyp des Remotedesktopdienstes (TermService) auf Automatisch eingestellt ist und der Dienst gestartet ist (verwenden AWSSupport-TroubleshootRDPSieenable and start the RDP service).
- Stellen Sie sicher, dass Sie die Verbindung mit dem richtigen Port des Remotedesktop-Protokolls herstellen, der standardmäßig 3389 lautet (verwenden Sie AWSSupport-TroubleshootRDP um read the current RDP port und change it back to 3389 auszuführen).
- Stellen Sie sicher, dass Remote-Desktop-Verbindungen auf Ihrer Instance hergestellt werden können (verwenden Sie AWSSupport-TroubleshootRDP um enable Remote Desktop connections auszuführen).
- Überprüfen Sie, dass das Passwort nicht abgelaufen ist. Wenn das Passwort abgelaufen ist, können Sie es zurücksetzen. Weitere Informationen finden Sie unter Zurücksetzen eines Windows-Administratorpassworts, das verloren oder abgelaufen ist.

- Wenn Sie versuchen, eine Verbindung mit einem Benutzer herzustellen, den Sie auf der Instance erstellt haben, und den Fehler `The user cannot connect to the server due to insufficient access privileges` erhalten, überprüfen Sie, ob Sie dem Benutzer das Recht zur lokalen Anmeldung gewährt haben. Weitere Informationen finden Sie unter Einem Mitglied das Recht zur lokalen Anmeldung gewähren.
- Wenn Sie versuchen, eine Sitzung zu starten, und es ist bereits die Höchstgrenze gleichzeitiger RDP-Sitzungen erreicht, wird Ihre Sitzung mit der folgenden Meldung beendet: `Your Remote Desktop Services session has ended. Another user connected to the remote computer, so your connection was lost.` Standardmäßig sind pro Instance zwei gleichzeitige RDP-Sitzungen pro Instance erlaubt.

Fehler beim Verwenden des macOS RDP-Clients

Wenn Sie mit dem Remote Desktop Connection-Client von der Microsoft-Website aus eine Verbindung zu einer Windows Server-Instanz herstellen, wird möglicherweise die folgende Fehlermeldung angezeigt:

```
Remote Desktop Connection cannot verify the identity of the computer that you want to
 connect to.
```

Laden Sie die Microsoft Remote Desktop App vom Mac App Store herunter und stellen Sie die Verbindung mit Ihrer Instance über die App her.

RDP zeigt anstelle des Desktops einen schwarzen Bildschirm an

Versuchen Sie, das Problem wie folgt zu beheben:

- Überprüfen Sie die Ausgabe der Konsole, ob weitere Informationen gegeben werden. Um die Ausgabe der Konsole für Ihre Instance mit der Amazon EC2-Konsole abzurufen, wählen Sie die Instance aus, wählen Sie dann Actions (Aktionen), Monitor and troubleshoot (Überwachung und Fehlerbehebung), Get System Log (Systemprotokoll abrufen).
- Überprüfen Sie, ob Sie die neueste Version Ihres RDP-Clients verwenden.
- Verwenden Sie versuchsweise die Standardeinstellungen für den RDP-Client. Weitere Informationen finden Sie unter Remote Session Environment (Remote-Sitzungsumgebung).
- Wenn Sie eine Remotedesktopverbindung verwenden, versuchen Sie, diese wie folgt mit der Option `/admin` zu starten.

```
mstsc /v:instance /admin
```

- Wenn der Server eine Anwendung im Vollbildschirmmodus ausführt, besteht die Möglichkeit, dass diese Anwendung nicht mehr reagiert. Starten Sie mit Strg+Umschalt+Esc den Windows-Task-Manager und beenden Sie die betreffende Anwendung.
- Wenn der Server überlastet ist, besteht die Möglichkeit, dass der Server nicht mehr reagiert. Um die Instance mit der Amazon EC2-Konsole zu überwachen, wählen Sie die Instance aus und wählen Sie dann die Registerkarte Monitoring. Wenn Sie den Typ der Instance in einen größeren Typ ändern müssen, siehe Ändern des Instance-Typs.

Die Remote-Anmeldung bei einer Instance mit einem Benutzer, der kein Administrator ist, ist nicht möglich

Wenn Sie sich mit einem Benutzer, bei dem es sich nicht um ein Administratorkonto handelt, nicht remote an einer Windows-Instance anmelden können, stellen Sie sicher, dass Sie dem Benutzer das Recht zur lokalen Anmeldung gewährt haben. Siehe Einem Benutzer oder einer Gruppe das Recht zur lokalen Anmeldung bei den Domain-Controllern in der Domain gewähren.

Behebung von Remotedesktop-Problemen mit AWS Systems Manager

Sie können AWS Systems Manager es verwenden, um Probleme beim Herstellen einer Verbindung zu Ihrer Windows-Instanz mithilfe von RDP zu beheben.

AWSSupport-Problembehandlung bei RDP

Das Automatisierungsdokument AWSSupport -TroubleshooTRDP ermöglicht es dem Benutzer, allgemeine Einstellungen auf der Zielinstanz zu überprüfen oder zu ändern, die sich auf RDP-Verbindungen (Remote Desktop Protocol) auswirken können, z. B. den RDP-Port, die Network Layer Authentication (NLA) und Windows-Firewallprofile. Standardmäßig liest das Dokument die Werte dieser Einstellungen und gibt sie aus.

Das Automatisierungsdokument AWSSupport -TroubleshooTRDP kann mit EC2-Instances, lokalen Instanzen und virtuellen Maschinen (VMs) verwendet werden, die für die Verwendung mit (verwalteten Instanzen) aktiviert sind. AWS Systems Manager Darüber hinaus kann es auch mit EC2-Instances für Windows Server verwendet werden, die nicht für die Verwendung mit Systems Manager aktiviert sind. Informationen zur Aktivierung von Instanzen für die Verwendung mit finden Sie unter Verwaltete Knoten im AWS Systems Manager Benutzerhandbuch.AWS Systems Manager

Zur Fehlerbehebung verwenden Sie das Dokument AWSSupport -TroubleshootRDP

1. Melden Sie sich bei der Systems Manager-Konsole an.
2. Vergewissern Sie sich, dass Sie sich in der gleichen Region wie die beeinträchtigte -Instance befinden.
3. Wählen Sie im linken Navigationsbereich Documents (Dokumente) aus.
4. Auf der Registerkarte Owned by Amazon (Im Besitz von Amazon) geben Sie `AWSSupport-TroubleshootRDP` im Suchfeld ein. Wenn das Dokument `AWSSupport-TroubleshootRDP` angezeigt wird, wählen Sie es aus.
5. Wählen Sie Execute automation (Automatisierung ausführen).
6. Wählen Sie für Execution mode (Ausführungsmodus) die Option Simple execution (Einfache Ausführung) aus.
7. Aktivieren Sie für Eingabeparameter die Option Interaktiven InstanceIdInstanzwähler anzeigen.
8. Wählen Sie Ihre Amazon EC2-Instance aus.
9. Überprüfen Sie die Beispiele und wählen Sie dann Execute (Ausführen) aus.
10. Um den Fortschritt der Ausführung zu überwachen, warten Sie bei Execution status (Ausführungsstatus), bis sich der Status von Pending (Ausstehend) in Success (Erfolg) ändert. Erweitern Sie Outputs, um die Ergebnisse anzuzeigen. Zum Anzeigen der Ausgabe der einzelnen Schritte wählen Sie unter Executed Steps (Ausgeführte Schritte) ein Element aus Step ID (Schritt-ID) aus.

AWSSupport-TroubleshootRDP-Beispiele

Die folgenden Beispiele zeigen Ihnen, wie Sie allgemeine Problembehandlungsaufgaben mit -TroubleshootRDP ausführen können. AWSSupport Sie können entweder den AWS CLI start-automation-executionBeispielbefehl oder den bereitgestellten Link zum verwenden. AWS Management Console

Example Beispiel: Überprüfen des aktuellen RDP-Status

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP" --
parameters "InstanceId=instance_id, Action=Custom" --region region_code
```

AWS Systems Manager Konsole:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region#documentVersion=$LATEST
```

Example Beispiel: Deaktivieren der Windows-Firewall

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, Firewall=Disable" --
region region_code
```

AWS Systems Manager Konsole:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&Firewall=Disable
```

Example Beispiel: Deaktivieren der Authentifizierung auf Netzwerkebene

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, NLASettingAction=Disable" --
region region_code
```

AWS Systems Manager Konsole:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion
```

Example Beispiel: Stellen Sie den Startup-Typ des RDP-Services auf „Automatic“ (Automatisch) ein und starten Sie den RDP-Service

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPServiceStartupType=Auto,
 RDPServiceAction=Start" --region region_code
```

AWS Systems Manager Konsole:

```
https://console.aws.amazon.com/systems-manager/automation/execute/
AWSSupport-TroubleshootRDP?region=region_code#documentVersion=
$LATEST&RDPServiceStartupType=Auto&RDPServiceAction=Start
```

Example Beispiel: Wiederherstellen des Standard-RDP-Ports (3389)

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RDPPortAction=Modify" --
region region_code
```

AWS Systems Manager Konsole:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RDPPortAction=Modify
```

Example Beispiel: Zulassen von Remote-Verbindungen

AWS CLI:

```
aws ssm start-automation-execution --document-name "AWSSupport-TroubleshootRDP"
 --parameters "InstanceId=instance_id, Action=Custom, RemoteConnections=Enable" --
region region_code
```

AWS Systems Manager Konsole:

```
https://console.aws.amazon.com/systems-manager/automation/execute/AWSSupport-
TroubleshootRDP?region=region_code#documentVersion=$LATEST&RemoteConnections=Enable
```

AWSSupport- Führen Sie EC2 Rescue aus

Das Automatisierungsdokument AWSSupport -executeEC2Rescue verwendet EC2Rescue für Windows Server, um EC2-Instance-Konnektivitäts- und RDP-Probleme automatisch zu beheben und wiederherzustellen. Weitere Informationen finden Sie unter Ausführen des EC2Rescue-Tools auf nicht erreichbaren Instances.

Das Automatisierungsdokument AWSSupport -executeEC2Rescue erfordert einen Stopp und einen Neustart der Instanz. Die Systems Manager-Automatisierung hält die Instance an und erstellt ein

Amazon Machine Image (AMI). Alle in den Instance-Speichervolumes gespeicherten Daten gehen verloren. Die öffentliche IP-Adresse ändert sich, wenn Sie keine Elastic IP-Adresse verwenden. Weitere Informationen finden Sie unter Ausführen des EC2Rescue-Tools auf nicht erreichbaren Instances im Benutzerhandbuch von AWS Systems Manager .

Zur Fehlerbehebung verwenden Sie das Dokument -executeEC2Rescue AWSSupport

1. Öffnen Sie die Systems Manager-Konsole.
2. Vergewissern Sie sich, dass Sie sich in der gleichen Region wie die beeinträchtigte Amazon EC2-Instance befinden.
3. Wählen Sie im Navigationsbereich die Option Dokumente.
4. Suchen Sie nach dem Dokument `AWSSupport-ExecuteEC2Rescue`, wählen Sie es aus und wählen Sie dann Automatisierung ausführen.
5. Wählen Sie unter Execution mode (Ausführungsmodus) die Option Simple execution (Einfache Ausführung) aus.
6. Geben Sie im Abschnitt Eingabeparameter für UnreachableInstanceID die Amazon EC2 EC2-Instance-ID der nicht erreichbaren Instance ein.
7. (Optional) Geben Sie den Bucket-Namen für LogDestinationAmazon Simple Storage Service (Amazon S3) ein, wenn Sie Betriebssystemprotokolle für die Fehlerbehebung Ihrer Amazon EC2 EC2-Instance sammeln möchten. Protokolle werden automatisch in den angegebenen Bucket hochgeladen.
8. Wählen Sie Execute (Ausführen).
9. Um den Fortschritt der Ausführung zu überwachen, warten Sie unter Execution status (Ausführungsstatus), bis sich der Status von Pending (Ausstehend) in Success (Erfolg) ändert. Erweitern Sie Outputs, um die Ergebnisse anzuzeigen. Zum Anzeigen der Ausgabe der einzelnen Schritte klicken Sie unter Executed Steps (Ausgeführte Schritte) auf Step ID (Schritt-ID).

Aktivieren von Remotedesktop für eine EC2-Instance mit Remote-Registrierung

Wenn Ihre nicht erreichbare Instanz nicht vom AWS Systems Manager Session Manager verwaltet wird, können Sie Remote Desktop mithilfe der Remote-Registrierung aktivieren.

1. Beenden Sie die nicht erreichbare Instance über die EC2-Konsole.

2. Trennen Sie das Stamm-Volume der nicht erreichbaren Instance und fügen Sie es an eine erreichbare Instance in der gleichen Availability Zone an, in der sich auch ein Speicher-Volume befindet. Sollten Sie über keine erreichbare Instance in der gleichen Availability Zone verfügen, starten Sie eine. Notieren Sie sich den Gerätenamen des Stamm-Volumes in der nicht erreichbaren Instance.
3. Öffnen Sie in der erreichbaren Instance die Datenträgerverwaltung. Hierzu können Sie den folgenden Befehl in einem Eingabeaufforderungsfenster ausführen.

   ```
   diskmgmt.msc
   ```

4. Klicken Sie mit der rechten Maustaste auf das neu angefügte Volume, das von der nicht erreichbaren Instance stammt, und wählen Sie anschließend Online aus.
5. Öffnen Sie den Windows Registrierungs-Editor. Hierzu können Sie den folgenden Befehl in einem Eingabeaufforderungsfenster ausführen.

   ```
   regedit
   ```

6. Wählen Sie im Registrierungs-Editor die Option HKEY_LOCAL_MACHINE und anschließend Datei > Hive laden aus.
7. Wählen Sie das Laufwerk des angeschlossenen Volumes aus, navigieren Sie zu `\Windows\System32\config\`, wählen Sie `SYSTEM` aus und wählen Sie dann Open (Öffnen) aus.
8. Geben Sie unter Key Name (Schlüsselname) einen eindeutigen Namen für die Struktur ein, und wählen Sie OK.
9. Sichern Sie die Registrierungsstruktur, bevor Sie Änderungen an der Registrierung vornehmen.

   a. Wählen Sie in der Baumstruktur der Konsole des Registrierungs-Editors die von Ihnen geladene Struktur aus: HKEY_LOCAL_MACHINE*Name Ihres Schlüssels*.

   b. Wählen Sie Datei >Exportieren aus.

   c. Wählen Sie im Dialogfeld „Registrierungsdatei exportieren“ den Speicherort aus, an dem die Sicherungskopie gespeichert werden soll, und geben Sie dann im Feld Dateiname einen Namen für die Sicherungsdatei ein.

   d. Wählen Sie Save (Speichern) aus.

10. Navigieren Sie im Registrierungs-Editor zu `HKEY_LOCAL_MACHINE\`*`your key name`*`\ControlSet001\Control\Terminal Server` und doppelklicken Sie anschließend im Detailbereich auf fDenyTSConnections.

11. Geben Sie im Fenster Edit DWORD (DWORD bearbeiten) in das Feld Value data (Wertedaten) `0` ein.
12. Klicken Sie auf OK.

> **Note**
>
> Wenn der Wert im Wert-Datenfeld 1 lautet, verweigert die Instance Remotedesktopverbindungen. Der Wert `0` erlaubt Remotedesktopverbindungen.

13. Wählen Sie im Registrierungs-Editor die Option HKEY_LOCAL_MACHINE*Name Ihres Schlüssels* und anschließend Datei > Hive entladen aus.
14. Schließen Sie den Registrierungs-Editor und die Datenträgerverwaltung.
15. Trennen Sie über die EC2-Konsole das Volume von der erreichbaren Instance und fügen Sie es wieder an die nicht erreichbare Instance an. Geben Sie beim Anfügen des Volumes an die nicht erreichbare Instance den zuvor gespeicherten Gerätenamen in das Feld Gerät ein.
16. Starten Sie die unerreichbare Instance neu.

Ich habe meinen privaten Schlüssel verloren. Wie kann ich mich mit meiner Windows-Instance verbinden?

Wenn Sie eine Verbindung zu einer neu gestarteten Windows-Instance herstellen, entschlüsseln Sie das Passwort für das Administrator-Konto mithilfe des privaten Schlüssels des Schlüsselpaars, das Sie beim Starten der Instance festgelegt haben.

Wenn Sie das Administratorpasswort und den privaten Schlüssel nicht mehr haben, müssen Sie das Passwort zurücksetzen oder eine neue Instance erstellen. Weitere Informationen finden Sie unter Zurücksetzen eines Windows-Administratorpassworts, das verloren oder abgelaufen ist. Schritte zum Zurücksetzen des Kennworts mithilfe eines Systems-Manager-Dokuments finden Sie unter Zurücksetzen von Kennwörtern und SSH-Schlüsseln auf EC2-Instances im AWS Systems Manager - Benutzerhandbuch.

Zurücksetzen eines Windows-Administratorpassworts, das verloren oder abgelaufen ist

> **Note**
>
> Dieser Abschnitt bezieht sich nur auf Windows-Instanzen.

Wenn Sie nicht länger Zugriff auf die Windows-Amazon EC2-Instance haben, da Sie das Windows-Administratorpasswort verloren haben oder das Passwort abgelaufen ist, können Sie das Passwort zurücksetzen.

> **Note**
>
> Es gibt ein AWS Systems Manager Automatisierungsdokument, das automatisch die manuellen Schritte anwendet, die zum Zurücksetzen des lokalen Administratorkennworts erforderlich sind. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Passwörter und SSH-Schlüssel auf EC2-Instances zurücksetzen.

Für die manuellen Methoden zum Zurücksetzen des Administratorpassworts wird EC2Launch v2, EC2Config oder EC2Launch verwendet.

- Verwenden Sie für alle unterstützten Windows-AMIs, die den EC2Launch-v2-Agenten enthalten, EC2Launch v2.
- Verwenden Sie für Windows-AMIs vor Windows Server 2016 den EC2Config-Service.
- Für AMIs ab Windows Server 2016 und höher verwenden Sie den EC2Launch-Service.

In diesen Verfahren wird auch beschrieben, wie Sie eine Verbindung zu einer Instance herstellen können, wenn Sie das Schlüsselpaar verloren haben, das zum Erstellen der Instance verwendet wurde. Amazon EC2 verwendet öffentliche Schlüssel, um Daten (z. B. ein Passwort) zu verschlüsseln. Mithilfe eines privaten Schlüssels werden die Daten entschlüsselt. Der öffentliche und der private Schlüssel werden als Schlüsselpaar bezeichnet. Bei Windows-Instances verwenden Sie ein Schlüsselpaar, um das Administratorpasswort zu erhalten und sich dann mit RDP anzumelden.

> **Note**
>
> Wenn Sie das lokale Administratorkonto für die Instance deaktiviert haben und Ihre Instance für Systems Manager konfiguriert ist, können Sie auch EC2Rescue und Run Command verwenden, um das lokale Administratorpasswort wieder zu aktivieren und zurückzusetzen. Weitere Informationen finden Sie unter Verwenden von EC2Rescue für Windows Server mit dem Systems Manager Run-Befehl.

Inhalt

Zurücksetzen des Windows-Administratorpassworts mithilfe von EC2Launch v2

Wenn Sie Ihr Windows-Administratorpasswort verloren haben und ein unterstütztes Windows-AMI verwenden, das EC2Launch v2 Agent enthält, können Sie EC2Launch v2 verwenden, um ein neues Passwort zu generieren.

Wenn Sie ein AMI für Windows Server 2016 oder höher verwenden, das EC2Launch v2 Agent nicht enthält, siehe Zurücksetzen des Windows-Administratorpassworts mithilfe von EC2Launch.

Wenn Sie eine ältere Version des Windows Server AMI als Windows Server 2016 verwenden, die EC2Launch v2-Agent nicht enthält, siehe Zurücksetzen des Windows-Administratorpassworts mithilfe von EC2Config.

> **Note**
>
> Wenn Sie das lokale Administratorkonto für die Instance deaktiviert haben und Ihre Instance für Systems Manager konfiguriert ist, können Sie auch EC2Rescue und Run Command verwenden, um das lokale Administratorpasswort wieder zu aktivieren und zurückzusetzen. Weitere Informationen finden Sie unter Verwenden von EC2Rescue für Windows Server mit dem Systems Manager Run-Befehl.

> **Note**
>
> Es gibt ein AWS Systems Manager Automatisierungsdokument, das automatisch die manuellen Schritte anwendet, die zum Zurücksetzen des lokalen Administratorkennworts erforderlich sind. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Passwörter und SSH-Schlüssel auf EC2-Instances zurücksetzen.

So setzen Sie Ihr Windows-Administratorpasswort mithilfe von EC2Launch v2 zurück:

- Schritt 1: Stellen Sie sicher, dass der EC2Launch-v2-Agent ausgeführt wird
- Schritt 2: Trennen des Stamm-Volumes von der Instance
- Schritt 3: Anfügen des Volumes an eine temporäre Instance
- Schritt 4: Löschen der .run-once-Datei
- Schritt 5: Starten Sie die Original-Instance neu

Schritt 1: Stellen Sie sicher, dass der EC2Launch-v2-Agent ausgeführt wird

Bevor Sie versuchen, das Administratorpasswort zurückzusetzen, überprüfen Sie, ob der EC2Launch-v2-Agent installiert ist und ausgeführt wird. Sie werden den EC2Launch-v2-Agent weiter unten in diesem Abschnitt zum Zurücksetzen des Administratorpassworts verwenden.

Sicherstellen, dass der EC2Launch-v2-Agent ausgeführt wird

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und anschließend die Instance aus, für die das Passwort zurückgesetzt werden muss. Diese Instance wird in diesem Verfahren als Original-Instance bezeichnet.
3. Wählen Sie Actions (Aktionen), Monitor and Troubleshoot (Überwachung und Fehlerbehebung), Get system log (Systemprotokoll abrufen).
4. Suchen Sie den Eintrag „EC2 Launch“, z. B. Launch: EC2Launch v2 service v2.0.124. Wenn dieser Eintrag angezeigt wird, wird der EC2Launch v2-Service ausgeführt.

   Wenn die System-Protokoll-Ausgabe leer ist oder wenn der EC2Launch-v2-Agent nicht ausgeführt wird, führen Sie auf der Instance eine Problembehebung mithilfe des Instance-Console-Screenshot-Services durch. Weitere Informationen finden Sie unter Aufnehmen eines Screenshots einer nicht erreichbaren Instance.

Schritt 2: Trennen des Stamm-Volumes von der Instance

Sie können ein Administratorpasswort mit EC2Launch v2 nicht zurücksetzen, wenn das Volume, auf dem das Passwort gespeichert ist, als Stamm-Volume an einer Instance angefügt ist. Sie müssen das Volume von der ursprünglichen Instance trennen, bevor Sie es als sekundäres Volume an eine temporäre Instance anfügen können.

Trennen des Stamm-Volumes von der Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, für die ein Passwort zurückgesetzt werden muss, und wählen Sie Instanzstatus, Instanz beenden aus. Nachdem sich der Status der Instance in Angehalten geändert hat, können Sie mit dem nächsten Schritt fortfahren.
4. (Optional) Wenn Sie über den privaten Schlüssel verfügen, den Sie beim Start dieser Instance angegeben haben, fahren Sie mit dem nächsten Schritt fort. Führen Sie andernfalls die folgenden Schritte aus, um die Instance durch eine neue Instance mit einem neuen Schlüsselpaar zu ersetzen.

    a. Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole. Wenn der Name des neuen Schlüsselpaars dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen.

    b. Wählen Sie die zu ersetzende Instance aus. Notieren Sie sich den Instance-Typ, die VPC, das Subnetz, die Sicherheitsgruppe und die IAM-Rolle der Instance.

    c. Wählen Sie Actions (Aktionen), Image and templates (Image und Vorlagen), Create image (Image erstellen). Geben Sie einen Namen und eine Beschreibung für das Image ein und wählen Sie anschließend Create image (Image erstellen) aus. Wählen Sie im Navigationsbereich die Option AMIs. Nachdem sich der Image-Status in available (verfügbar) geändert hat, fahren Sie mit dem nächsten Schritt fort.

    d. Wählen Sie das Image aus, klicken Sie auf Actions (Aktionen) und dann auf Launch (Starten).

    e. Schließen Sie den Assistenten ab, wählen Sie dieselben Werte (Instance-Typ, VPC, Subnetz, Sicherheitsgruppe und IAM-Rolle) wie bei der zu ersetzenden Instance aus, und klicken Sie dann auf Launch (Starten).

f. Wenn Sie dazu aufgefordert werden, wählen Sie das Schlüsselpaar aus, das Sie für die neue Instance erstellt haben, wählen Sie das Kästchen zur Bestätigung aus und klicken Sie dann auf Launch Instances (Instances starten).

g. (Optional) Wenn die ursprüngliche Instance über eine zugeordnete elastische IP-Adresse verfügt, sollten Sie sie auf die neue Instance übertragen. Wenn die ursprüngliche Instance zusätzlich zum Stamm-Volume EBS-Volumes enthält, übertragen Sie diese auf die neue Instance.

5. Trennen Sie das Stamm-Volume wie folgt von der ursprünglichen Instance:

   a. Wählen Sie die ursprüngliche Instanz aus und wählen Sie den Tab Speicher. Notieren Sie sich den Namen des Root-Geräts unter Root-Gerätename. Suchen Sie unter Geräte sperren nach dem Volume mit diesem Gerätenamen und notieren Sie sich die Volume-ID.

   b. Wählen Sie im Navigationsbereich Volumes aus.

   c. Wählen Sie in der Liste der Volumes das Volume aus, das Sie als Root-Gerät notiert haben, und klicken Sie dann auf Aktionen, Volume trennen. Nachdem der Status des Volumes in available (verfügbar) geändert wurde, fahren Sie mit dem nächsten Schritt fort.

6. Wenn Sie eine neue Instanz erstellt haben, um Ihre ursprüngliche Instanz zu ersetzen, können Sie die ursprüngliche Instanz jetzt beenden. Sie wird nicht mehr benötigt. Für den Rest dieses Verfahrens gelten alle Verweise auf die ursprüngliche Instanz für die neue Instanz, die Sie erstellt haben.

Schritt 3: Anfügen des Volumes an eine temporäre Instance

Starten Sie als Nächstes eine temporäre Instance, um das Volume als sekundäres Volume an sie anzufügen. Dies ist die Instance, die Sie zum Bearbeiten der Konfigurationsdatei verwenden.

So starten Sie eine temporäre Instance und fügen das Volume an

1. Starten Sie die temporäre Instance wie folgt:

   a. Wählen Sie im Navigationsbereich die Option Instances und dann Launch Instances (Instances starten) aus. Wählen Sie dann ein AMI aus.

> **Important**
>
> Um Datenträger-Signaturkollisionen zu vermeiden, müssen Sie ein AMI für eine andere Version von Windows auswählen. Wenn die ursprüngliche Instance

beispielsweise Windows Server 2019 verwendet, starten Sie die temporäre Instance mit dem Basis-AMI für Windows Server 2016.

b. Übernehmen Sie den standardmäßigen Instance-Typen und wählen Next: Configure Instance Details (Weiter: Konfigurieren von Instance-Details) aus.

c. Wählen Sie auf der Seite Configure Instance Details (Konfigurieren von Instance-Details) für Subnet (Subnetz) dieselbe Availability Zone aus wie für die ursprüngliche Instance und klicken Sie auf Review and Launch (Überprüfen und starten).

> **Important**
>
> Die temporäre Instance muss sich in derselben Availability Zone befinden wie die ursprüngliche Instance. Wenn sich Ihre temporäre Instance in einer anderen Availability Zone befindet, können Sie ihr nicht das Stamm-Volume der ursprünglichen Instance anfügen.

d. Klicken Sie auf der Seite Review Instance Launch auf Launch.

e. Wenn Sie dazu aufgefordert werden, erstellen Sie ein neues Schlüsselpaar, laden Sie es an einen sicheren Speicherort auf Ihrem Computer herunter und wählen Sie dann Launch Instances (Instances starten) aus.

2. Fügen Sie das Volume der temporären Instance wie folgt als sekundäres Volume an:

a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der ursprünglichen Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der temporären Instance ein und wählen Sie die Instance aus der Liste aus.

c. Geben Sie für Device (Gerät) **`xvdf`** ein (wenn es noch nicht vorhanden ist) und wählen Sie Attach (Anfügen) aus.

Schritt 4: Löschen der .run-once-Datei

Sie müssen nun die Datei `.run-once` von dem mit der Instance verbundenen Offline-Volume löschen. Hierdurch wird EC2Launch v2 angewiesen, alle Aufgaben mit einer Häufigkeit von `once` auszuführen, wozu auch das Festlegen des Administratorpassworts gehört. Der Dateipfad auf dem

sekundären Volume, das Sie angehängt haben, wird ähnlich sein wie `D:\ProgramData\Amazon\EC2Launch\state\.run-once`.

So löschen Sie die .run-once-Datei

1. Öffnen Sie das Festplattenverwaltungsprogramm und schalten Sie das Laufwerk mithilfe der folgenden Anweisungen online: Machen Sie ein Amazon EBS-Volume für die Verwendung verfügbar.
2. Suchen Sie die Datei `.run-once` auf dem Datenträger, den Sie online gestellt haben.
3. Löschen Sie die Datei „.run-once“.

> **Important**
>
> Alle Skripte, die einmal ausgeführt werden, werden durch diese Aktion ausgelöst.

Schritt 5: Starten Sie die Original-Instance neu

Nachdem Sie die `.run-once`-Datei gelöscht haben, fügen Sie das Volume wieder als Stamm-Volume an die ursprüngliche Instance an. Stellen Sie dann mithilfe ihres Schlüsselpaars eine Verbindung zur Instance her, um das Administratorpasswort abzurufen.

1. Fügen Sie das Volume wie folgt wieder der ursprünglichen Instance an:
   a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der temporären Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).
   b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der ursprünglichen Instance ein und wählen Sie die Instance aus.
   c. Geben Sie für Device (Gerät) **`/dev/sda1`** ein.
   d. Wählen Sie Attach (Anfügen) aus. Nachdem sich der Status des Volumes in `in-use` (In Verwendung) geändert hat, fahren Sie mit dem nächsten Schritt fort.
2. Wählen Sie im Navigationsbereich Instances aus. Wählen Sie die ursprüngliche Instance aus und klicken Sie auf Instance state (Instance-Zustand), Start instance (Instance starten). Nachdem sich der Status der Instance in `Running` (Wird ausgeführt) geändert hat, fahren Sie mit dem nächsten Schritt fort.

3. Rufen Sie Ihr neues Windows-Administratorpasswort mit dem privaten Schlüssel für das neue Schlüsselpaar ab und stellen Sie eine Verbindung mit der Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer -Windows-Instance.

   Important

   Die Instance erhält eine neue öffentliche IP-Adresse, nachdem Sie sie stoppen und starten. Stellen Sie sicher, dass Sie sich mit der Instance unter deren aktuellem öffentlichen DNS-Namen verbinden. Weitere Informationen finden Sie unter Instance-Lebenszyklus.

4. (Optional) Sie können die temporäre Instance beenden, wenn Sie sie nicht mehr benötigen. Wählen Sie die temporäre Instance aus und klicken Sie auf Instance state (Instance-Zustand), Terminate instance (Instance beenden).

Zurücksetzen des Windows-Administratorpassworts mithilfe von EC2Config

Wenn Sie das Windows-Administratorpasswort verloren haben und ein Windows-AMI für Windows Server 2016 verwenden, können Sie EC2Config-Agent verwenden, um ein neues Passwort zu generieren.

Wenn Sie ein AMI für Windows Server 2016 oder höher verwenden, siehe Zurücksetzen des Windows-Administratorpassworts mithilfe von EC2Launch. Andernfalls können Sie das EC2Rescue-Tool verwenden, das den EC2Launch-Service nutzt, um ein neues Kennwort zu generieren.

Note

Wenn Sie das lokale Administratorkonto für die Instance deaktiviert haben und Ihre Instance für Systems Manager konfiguriert ist, können Sie auch EC2Rescue und Run Command verwenden, um das lokale Administratorpasswort wieder zu aktivieren und zurückzusetzen. Weitere Informationen finden Sie unter Verwenden von EC2Rescue für Windows Server mit dem Systems Manager Run-Befehl.

Note

Es gibt ein AWS Systems Manager Automatisierungsdokument, das automatisch die manuellen Schritte anwendet, die zum Zurücksetzen des lokalen Administratorkennworts

erforderlich sind. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Passwörter und SSH-Schlüssel auf EC2-Instances zurücksetzen.

So setzen Sie Ihr Windows-Administratorpasswort mithilfe von EC2Config zurück:

- Schritt 1: Überprüfen, ob der EC2Config-Service ausgeführt wird
- Schritt 2: Trennen des Stamm-Volumes von der Instance
- Schritt 3: Anfügen des Volumes an eine temporäre Instance
- Schritt 4: Bearbeiten der Konfigurationsdatei
- Schritt 5: Starten Sie die Original-Instance neu

Schritt 1: Überprüfen, ob der EC2Config-Service ausgeführt wird

Bevor Sie versuchen, das Administratorpasswort zurückzusetzen, überprüfen Sie, ob der EC2Config-Service installiert ist und ausgeführt wird. Sie werden den EC2Config-Service weiter unten in diesem Abschnitt zum Zurücksetzen des Administratorpassworts verwenden.

So überprüfen Sie, ob der EC2Config-Service ausgeführt wird

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances und anschließend die Instance aus, für die das Passwort zurückgesetzt werden muss. Diese Instance wird in diesem Verfahren als Original-Instance bezeichnet.
3. (Neue Konsole) Wählen Sie Actions (Aktionen), Monitor and troubleshoot (Überwachung und Fehlerbehebung), Get system log (Systemprotokoll abrufen).

   (Alte Konsole) Wählen Sie Actions (Aktionen), System Settings (Systemeinstellungen),Get System Log (Systemprotokoll abrufen).
4. Suchen Sie den EC2 Agent-Eintrag, z. B. EC2 Agent: Ec2Config Service v3.18.1118. Wenn Sie diesen Eintrag sehen, läuft der EC2Config-Service.

   Wenn die System-Log-Ausgabe leer ist oder wenn der EC2Config-Service nicht läuft, führen Sie auf der Instance eine Problembehebung mithilfe des Instance Console Screenshot-Service durch. Weitere Informationen finden Sie unter Aufnehmen eines Screenshots einer nicht erreichbaren Instance.

Schritt 2: Trennen des Stamm-Volumes von der Instance

Sie können ein Administratorpasswort mit EC2Config nicht zurücksetzen, wenn das Volume, auf dem das Passwort gespeichert ist, als Stamm-Volume an einer Instance angefügt ist. Sie müssen das Volume von der ursprünglichen Instance trennen, bevor Sie es als sekundäres Volume an eine temporäre Instance anfügen können.

Trennen des Stamm-Volumes von der Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, für die ein Passwort zurückgesetzt werden muss, und wählen Sie Instanzstatus, Instanz beenden aus. Nachdem sich der Status der Instance in Angehalten geändert hat, können Sie mit dem nächsten Schritt fortfahren.
4. (Optional) Wenn Sie über den privaten Schlüssel verfügen, den Sie beim Start dieser Instance angegeben haben, fahren Sie mit dem nächsten Schritt fort. Führen Sie andernfalls die folgenden Schritte aus, um die Instance durch eine neue Instance mit einem neuen Schlüsselpaar zu ersetzen.
   a. Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole. Wenn der Name des neuen Schlüsselpaars dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen.
   b. Wählen Sie die zu ersetzende Instance aus. Notieren Sie sich den Instance-Typ, die VPC, das Subnetz, die Sicherheitsgruppe und die IAM-Rolle der Instance.
   c. Wählen Sie Actions (Aktionen), Image and templates (Image und Vorlagen), Create image (Image erstellen). Geben Sie einen Namen und eine Beschreibung für das Image ein und wählen Sie anschließend Create image (Image erstellen) aus. Wählen Sie im Navigationsbereich die Option AMIs. Nachdem sich der Image-Status in available (verfügbar) geändert hat, fahren Sie mit dem nächsten Schritt fort.
   d. Wählen Sie das Image aus, klicken Sie auf Actions (Aktionen) und dann auf Launch (Starten).
   e. Schließen Sie den Assistenten ab, wählen Sie dieselben Werte (Instance-Typ, VPC, Subnetz, Sicherheitsgruppe und IAM-Rolle) wie bei der zu ersetzenden Instance aus, und klicken Sie dann auf Launch (Starten).

f. Wenn Sie dazu aufgefordert werden, wählen Sie das Schlüsselpaar aus, das Sie für die neue Instance erstellt haben, wählen Sie das Kästchen zur Bestätigung aus und klicken Sie dann auf Launch Instances (Instances starten).

g. (Optional) Wenn die ursprüngliche Instance über eine zugeordnete elastische IP-Adresse verfügt, sollten Sie sie auf die neue Instance übertragen. Wenn die ursprüngliche Instance zusätzlich zum Stamm-Volume EBS-Volumes enthält, übertragen Sie diese auf die neue Instance.

5. Trennen Sie das Stamm-Volume wie folgt von der ursprünglichen Instance:

   a. Wählen Sie die ursprüngliche Instanz aus und wählen Sie den Tab Speicher. Notieren Sie sich den Namen des Root-Geräts unter Root-Gerätename. Suchen Sie unter Geräte sperren nach dem Volume mit diesem Gerätenamen und notieren Sie sich die Volume-ID.

   b. Wählen Sie im Navigationsbereich Volumes aus.

   c. Wählen Sie in der Liste der Volumes das Volume aus, das Sie als Root-Gerät notiert haben, und klicken Sie dann auf Aktionen, Volume trennen. Nachdem der Status des Volumes in available (verfügbar) geändert wurde, fahren Sie mit dem nächsten Schritt fort.

6. Wenn Sie eine neue Instanz erstellt haben, um Ihre ursprüngliche Instanz zu ersetzen, können Sie die ursprüngliche Instanz jetzt beenden. Sie wird nicht mehr benötigt. Für den Rest dieses Verfahrens gelten alle Verweise auf die ursprüngliche Instanz für die neue Instanz, die Sie erstellt haben.

Schritt 3: Anfügen des Volumes an eine temporäre Instance

Starten Sie als Nächstes eine temporäre Instance, um das Volume als sekundäres Volume an sie anzufügen. Dies ist die Instance, die Sie zum Bearbeiten der Konfigurationsdatei verwenden.

So starten Sie eine temporäre Instance und fügen das Volume an

1. Starten Sie die temporäre Instance wie folgt:

   a. Wählen Sie im Navigationsbereich die Option Instances und dann Launch Instances (Instances starten) aus. Wählen Sie dann ein AMI aus.

> **Important**
>
> Um Datenträger-Signaturkollisionen zu vermeiden, müssen Sie ein AMI für eine andere Version von Windows auswählen. Wenn die ursprüngliche Instance

beispielsweise Windows Server 2019 verwendet, starten Sie die temporäre Instance mit dem Basis-AMI für Windows Server 2016.

b. Übernehmen Sie den standardmäßigen Instance-Typen und wählen Next: Configure Instance Details (Weiter: Konfigurieren von Instance-Details) aus.

c. Wählen Sie auf der Seite Configure Instance Details (Konfigurieren von Instance-Details) für Subnet (Subnetz) dieselbe Availability Zone aus wie für die ursprüngliche Instance und klicken Sie auf Review and Launch (Überprüfen und starten).

> **Important**
>
> Die temporäre Instance muss sich in derselben Availability Zone befinden wie die ursprüngliche Instance. Wenn sich Ihre temporäre Instance in einer anderen Availability Zone befindet, können Sie ihr nicht das Stamm-Volume der ursprünglichen Instance anfügen.

d. Klicken Sie auf der Seite Review Instance Launch auf Launch.

e. Wenn Sie dazu aufgefordert werden, erstellen Sie ein neues Schlüsselpaar, laden Sie es an einen sicheren Speicherort auf Ihrem Computer herunter und wählen Sie dann Launch Instances (Instances starten) aus.

2. Fügen Sie das Volume der temporären Instance wie folgt als sekundäres Volume an:

a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der ursprünglichen Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der temporären Instance ein und wählen Sie die Instance aus der Liste aus.

c. Geben Sie für Device (Gerät) **`xvdf`** ein (wenn es noch nicht vorhanden ist) und wählen Sie Attach (Anfügen) aus.

Schritt 4: Bearbeiten der Konfigurationsdatei

Nachdem Sie das Volume der temporären Instance als sekundäres Volume angefügt haben, ändern Sie das `Ec2SetPassword`-Plugin in der Konfigurationsdatei.

So bearbeiten Sie die Konfigurationsdatei

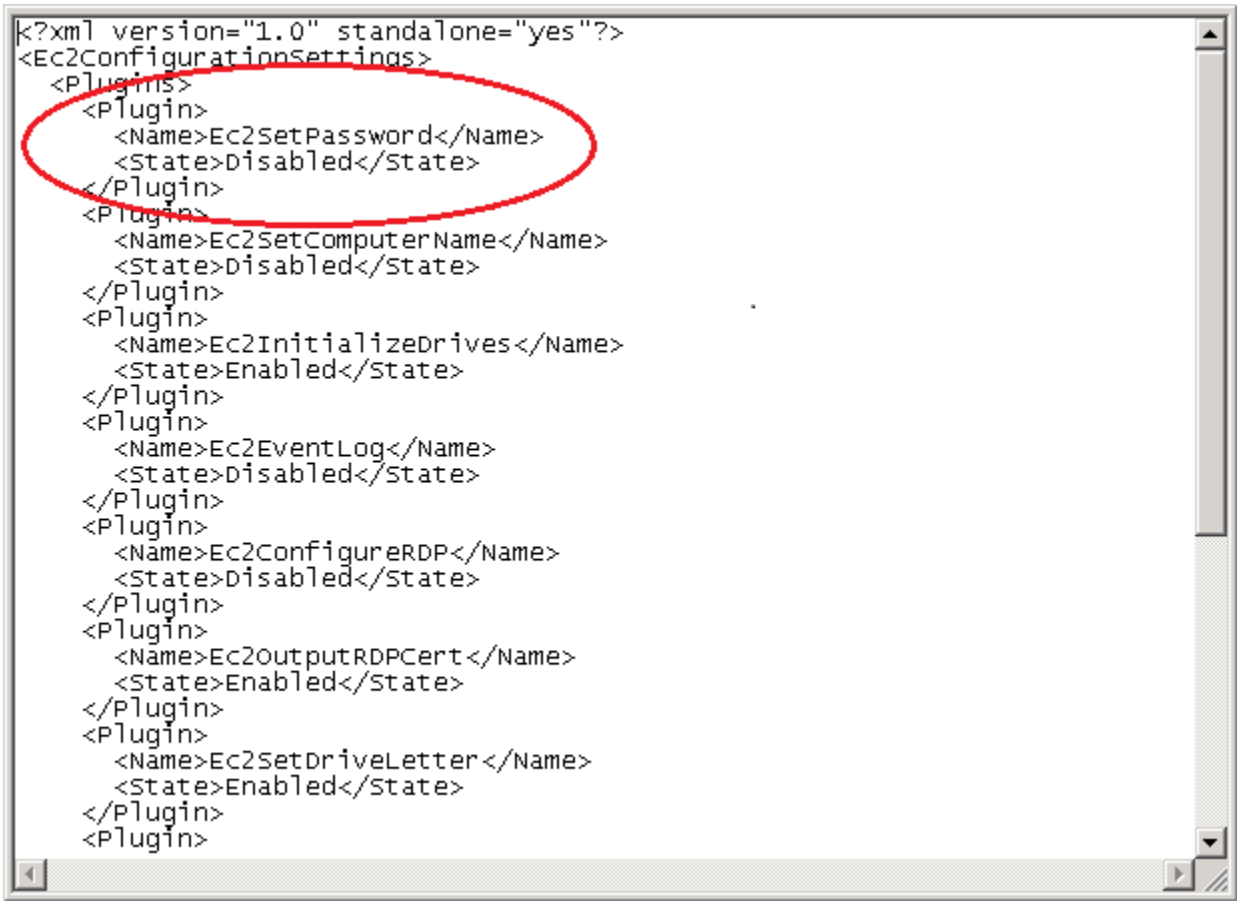
1. Bearbeiten Sie die Konfigurationsdatei auf dem sekundären Volume wie folgt über die temporäre Instance:

   a. Starten Sie die temporäre Instance und stellen Sie eine Verbindung mit ihr her.

   b. Gehen Sie wie folgt vor, um das Laufwerk online zu schalten: Machen Sie ein Amazon EBS-Volume für die Verwendung verfügbar.

   c. Navigieren Sie zum sekundären Volume und öffnen Sie `\Program Files\Amazon \Ec2ConfigService\Settings\config.xml` mithilfe eines Texteditors, wie Notepad.

   d. Suchen Sie am Anfang der Datei das Plugin mit dem Namen `Ec2SetPassword`, wie im Screenshot dargestellt. Ändern Sie den Status von `Disabled` in `Enabled` und speichern Sie die Datei.



2. Nachdem Sie die Konfigurationsdatei bearbeitet haben, trennen Sie das sekundäre Volume wie folgt von der temporären Instance:

   a. Mit dem Disk Management (Datenträgerverwaltung)-Tool bringen Sie das Volume offline.

b. Trennen Sie es von der temporären Instance und kehren Sie zur Amazon EC2-Konsole zurück.

c. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus. Klicken Sie dann auf Actions (Aktionen) und Detach Volume (Volume trennen). Nachdem der Status der Volume zu available (verfügbar) geändert wurde, fahren Sie fort mit dem nächsten Schritt.

Schritt 5: Starten Sie die Original-Instance neu

Nachdem Sie die Konfigurationsdatei bearbeitet haben, fügen Sie das Volume wieder als Stamm-Volume an die ursprüngliche Instance an. Stellen Sie dann mithilfe ihres Schlüsselpaars eine Verbindung zur Instance her, um das Administratorpasswort abzurufen.

1. Fügen Sie das Volume wie folgt wieder der ursprünglichen Instance an:

   a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der temporären Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

   b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der ursprünglichen Instance ein und wählen Sie die Instance aus.

   c. Geben Sie für Device (Gerät) **`/dev/sda1`** ein.

   d. Wählen Sie Attach (Anfügen) aus. Nachdem sich der Status des Volumes in `in-use` (In Verwendung) geändert hat, fahren Sie mit dem nächsten Schritt fort.

2. Wählen Sie im Navigationsbereich Instances aus. Wählen Sie die ursprüngliche Instance aus und klicken Sie auf Instance state (Instance-Zustand), Start instance (Instance starten). Nachdem sich der Status der Instance in `Running` (Wird ausgeführt) geändert hat, fahren Sie mit dem nächsten Schritt fort.

3. Rufen Sie Ihr neues Windows-Administratorpasswort mit dem privaten Schlüssel für das neue Schlüsselpaar ab und stellen Sie eine Verbindung mit der Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer -Windows-Instance.

> **Important**
>
> Die Instance erhält eine neue öffentliche IP-Adresse, nachdem Sie sie stoppen und starten. Stellen Sie sicher, dass Sie sich mit der Instance unter deren aktuellem

öffentlichen DNS-Namen verbinden. Weitere Informationen finden Sie unter Instance-Lebenszyklus.

4. (Optional) Sie können die temporäre Instance beenden, wenn Sie sie nicht mehr benötigen. Wählen Sie die temporäre Instance aus und klicken Sie auf Instance state (Instance-Zustand), Terminate instance (Instance beenden).

Zurücksetzen des Windows-Administratorpassworts mithilfe von EC2Launch

Wenn Sie das Windows-Administratorpasswort verloren haben und ein AMI für Windows Server 2016 oder höher verwenden, können Sie das EC2Rescue-Tool verwenden, das den EC2Launch-Service nutzt, um ein neues Passwort zu generieren.

Wenn Sie ein AMI mit Windows Server 2016 oder höher verwenden, das nicht den EC2Launch-v2-Agenten enthält, können Sie EC2Launch v2 verwenden, um ein neues Passwort zu generieren.

Wenn Sie ein Windows Server-AMI vor Windows Server 2016 verwenden, finden Sie weitere Informationen unter Zurücksetzen des Windows-Administratorpassworts mithilfe von EC2Config.

Warning

Wenn Sie eine Instance anhalten, werden sämtliche Daten auf allen Instance-Speicher-Volumes gelöscht. Wenn Sie Daten von Instance-Speicher-Volumes behalten möchten, sichern Sie diese auf einem persistenten Speicher.

Note

Wenn Sie das lokale Administratorkonto für die Instance deaktiviert haben und Ihre Instance für Systems Manager konfiguriert ist, können Sie auch EC2Rescue und Run Command verwenden, um das lokale Administratorpasswort wieder zu aktivieren und zurückzusetzen. Weitere Informationen finden Sie unter Verwenden von EC2Rescue für Windows Server mit dem Systems Manager Run-Befehl.

> **Note**
>
> Es gibt ein AWS Systems Manager Automatisierungsdokument, das automatisch die manuellen Schritte anwendet, die zum Zurücksetzen des lokalen Administratorkennworts erforderlich sind. Weitere Informationen finden Sie im AWS Systems Manager Benutzerhandbuch unter Passwörter und SSH-Schlüssel auf EC2-Instances zurücksetzen.

So setzen Sie Ihr Windows-Administratorpasswort mithilfe von EC2Launch zurück:

- Schritt 1: Trennen des Stamm-Volumes von der Instance
- Schritt 2: Anfügen des Volumes an eine temporäre Instance
- Schritt 3: Zurücksetzen des Administratorpassworts
- Schritt 4: Starten Sie die ursprüngliche Instance neu

Schritt 1: Trennen des Stamm-Volumes von der Instance

Sie können ein Administratorpasswort mit EC2Launch nicht zurücksetzen, wenn das Volume, auf dem das Passwort gespeichert ist, als Stamm-Volume an einer Instance angefügt ist. Sie müssen das Volume von der ursprünglichen Instance trennen, bevor Sie es als sekundäres Volume an eine temporäre Instance anfügen können.

Trennen des Stamm-Volumes von der Instance

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance aus, für die ein Passwort zurückgesetzt werden muss, und wählen Sie Instanzstatus, Instanz beenden aus. Nachdem sich der Status der Instance in Angehalten geändert hat, können Sie mit dem nächsten Schritt fortfahren.
4. (Optional) Wenn Sie über den privaten Schlüssel verfügen, den Sie beim Start dieser Instance angegeben haben, fahren Sie mit dem nächsten Schritt fort. Führen Sie andernfalls die folgenden Schritte aus, um die Instance durch eine neue Instance mit einem neuen Schlüsselpaar zu ersetzen.

    a. Erstellen Sie ein neues Schlüsselpaar mit der Amazon EC2-Konsole. Wenn der Name des neuen Schlüsselpaars dem des verlorenen privaten Schlüssels genau entsprechen soll, müssen Sie das vorhandene Schlüsselpaar erst löschen.

b. Wählen Sie die zu ersetzende Instance aus. Notieren Sie sich den Instance-Typ, die VPC, das Subnetz, die Sicherheitsgruppe und die IAM-Rolle der Instance.

c. Wählen Sie Actions (Aktionen), Image and templates (Image und Vorlagen), Create image (Image erstellen). Geben Sie einen Namen und eine Beschreibung für das Image ein und wählen Sie anschließend Create image (Image erstellen) aus. Wählen Sie im Navigationsbereich die Option AMIs. Nachdem sich der Image-Status in available (verfügbar) geändert hat, fahren Sie mit dem nächsten Schritt fort.

d. Wählen Sie das Image aus, klicken Sie auf Actions (Aktionen) und dann auf Launch (Starten).

e. Schließen Sie den Assistenten ab, wählen Sie dieselben Werte (Instance-Typ, VPC, Subnetz, Sicherheitsgruppe und IAM-Rolle) wie bei der zu ersetzenden Instance aus, und klicken Sie dann auf Launch (Starten).

f. Wenn Sie dazu aufgefordert werden, wählen Sie das Schlüsselpaar aus, das Sie für die neue Instance erstellt haben, wählen Sie das Kästchen zur Bestätigung aus und klicken Sie dann auf Launch Instances (Instances starten).

g. (Optional) Wenn die ursprüngliche Instance über eine zugeordnete elastische IP-Adresse verfügt, sollten Sie sie auf die neue Instance übertragen. Wenn die ursprüngliche Instance zusätzlich zum Stamm-Volume EBS-Volumes enthält, übertragen Sie diese auf die neue Instance.

5. Trennen Sie das Stamm-Volume wie folgt von der ursprünglichen Instance:

   a. Wählen Sie die ursprüngliche Instanz aus und wählen Sie den Tab Speicher. Notieren Sie sich den Namen des Root-Geräts unter Root-Gerätename. Suchen Sie unter Geräte sperren nach dem Volume mit diesem Gerätenamen und notieren Sie sich die Volume-ID.

   b. Wählen Sie im Navigationsbereich Volumes aus.

   c. Wählen Sie in der Liste der Volumes das Volume aus, das Sie als Root-Gerät notiert haben, und klicken Sie dann auf Aktionen, Volume trennen. Nachdem der Status des Volumes in available (verfügbar) geändert wurde, fahren Sie mit dem nächsten Schritt fort.

6. Wenn Sie eine neue Instanz erstellt haben, um Ihre ursprüngliche Instanz zu ersetzen, können Sie die ursprüngliche Instanz jetzt beenden. Sie wird nicht mehr benötigt. Für den Rest dieses Verfahrens gelten alle Verweise auf die ursprüngliche Instanz für die neue Instanz, die Sie erstellt haben.

Schritt 2: Anfügen des Volumes an eine temporäre Instance

Starten Sie als Nächstes eine temporäre Instance, um das Volume als sekundäres Volume an sie anzufügen. Dies ist die Instance, mit der Sie EC2Launch ausführen.

So starten Sie eine temporäre Instance und fügen das Volume an

1. Starten Sie die temporäre Instance wie folgt:

   a. Wählen Sie im Navigationsbereich die Option Instances und dann Launch Instances (Instances starten) aus. Wählen Sie dann ein AMI aus.

   > **Important**
   >
   > Um Datenträger-Signaturkollisionen zu vermeiden, müssen Sie ein AMI für eine andere Version von Windows auswählen. Wenn die ursprüngliche Instance beispielsweise Windows Server 2019 verwendet, starten Sie die temporäre Instance mit dem Basis-AMI für Windows Server 2016.

   b. Übernehmen Sie den standardmäßigen Instance-Typen und wählen Next: Configure Instance Details (Weiter: Konfigurieren von Instance-Details) aus.

   c. Wählen Sie auf der Seite Configure Instance Details (Konfigurieren von Instance-Details) für Subnet (Subnetz) dieselbe Availability Zone aus wie für die ursprüngliche Instance und klicken Sie auf Review and Launch (Überprüfen und starten).

   > **Important**
   >
   > Die temporäre Instance muss sich in derselben Availability Zone befinden wie die ursprüngliche Instance. Wenn sich Ihre temporäre Instance in einer anderen Availability Zone befindet, können Sie ihr nicht das Stamm-Volume der ursprünglichen Instance anfügen.

   d. Klicken Sie auf der Seite Review Instance Launch auf Launch.

   e. Wenn Sie dazu aufgefordert werden, erstellen Sie ein neues Schlüsselpaar, laden Sie es an einen sicheren Speicherort auf Ihrem Computer herunter und wählen Sie dann Launch Instances (Instances starten) aus.

2. Fügen Sie das Volume der temporären Instance wie folgt als sekundäres Volume an:

a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der ursprünglichen Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der temporären Instance ein und wählen Sie die Instance aus der Liste aus.

c. Geben Sie für Device (Gerät) **`xvdf`** ein (wenn es noch nicht vorhanden ist) und wählen Sie Attach (Anfügen) aus.

Schritt 3: Zurücksetzen des Administratorpassworts

Verbinden Sie sich als Nächstes mit der temporären Instance und setzen Sie mit EC2Launch das Administratorpasswort zurück.

Zum Zurücksetzen des Administratorpassworts

1. Stellen Sie eine Verbindung mit der temporären Instance her und verwenden Sie das EC2Rescue for Windows Server-Tool auf der Instance, um das Administratorpasswort wie folgt zurückzusetzen:

   a. Laden Sie die Zip-Datei EC2Rescue for Windows Server herunter, extrahieren Sie den Inhalt und führen Sie EC2Rescue.exe aus.

   b. Lesen Sie die Lizenzvereinbarung im Bildschirm License Agreement (Lizenzvereinbarung). Wenn Sie den Bedingungen zustimmen, wählen Sie I Agree (Ich stimme zu).

   c. Klicken Sie im Bildschirm Welcome to EC2Rescue for Windows Server (Willkommen bei EC2Rescue for Windows Server) auf Next (Weiter).

   d. Wählen Sie im Bildschirm Select mode (Modus auswählen) die Option Offline instance (Offline-Instance).

   e. Wählen Sie im Bildschirm Select a disk (Datenträger auswählen) das Gerät xvdf aus und klicken Sie auf Next (Weiter).

   f. Bestätigen Sie die Festplattenauswahl und wählen Sie Yes aus.

   g. Nachdem das Volume geladen wurde, klicken Sie auf OK.

   h. Wählen Sie im Bildschirm Select Offline Instance Option (Offline-Instance-Option auswählen) die Option Diagnose and Rescue (Diagnose und Datenrettung).

   i. Überprüfen Sie die Informationen im Bildschirm Summary (Übersicht) und klicken Sie auf Next (Weiter).

j. Wählen Sie im Bildschirm Detected possible issues (Mögliche Probleme erkennen) die Option Reset Administrator Password (Administratorpasswort zurücksetzen) und klicken Sie auf Next (Weiter).

k. Klicken Sie im Bildschirm Confirm (Bestätigen) auf Rescue (Datenrettung) und danach auf OK.

l. Klicken Sie im Bildschirm Done (Fertig) auf Finish (Beenden).

m. Schließen Sie das Tool EC2Rescue for Windows Server, trennen Sie die Verbindung mit der temporären Instance und kehren Sie zur Amazon EC2-Konsole zurück.

2. Trennen Sie das sekundäre Volume (`xvdf`) wie folgt von der temporären Instance:

a. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die temporäre Instance aus.

b. Notieren Sie sich auf der Registerkarte Storage (Speicher) der temporären Instance die ID des EBS-Volumes, die als xvdf aufgelistet wird.

c. Wählen Sie im Navigationsbereich Volumes aus.

d. Wählen Sie in der Liste der Volumes das im vorigen Schritt notierte Volume aus und wählen Sie anschließend Actions (Aktionen), Detach Volume (Volume trennen). Nachdem der Status des Volumes in available (verfügbar) geändert wurde, fahren Sie mit dem nächsten Schritt fort.

Schritt 4: Starten Sie die ursprüngliche Instance neu

Nachdem Sie das Administratorpasswort mit EC2Launch zurückgesetzt haben, fügen Sie das Volume wieder als Stamm-Volume an die ursprüngliche Instance an. Stellen Sie dann mithilfe ihres Schlüsselpaars eine Verbindung zur Instance her, um das Administratorpasswort abzurufen.

So starten Sie die ursprüngliche Instance neu

1. Fügen Sie das Volume wie folgt wieder der ursprünglichen Instance an:

a. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume aus, das Sie von der temporären Instance getrennt haben. Klicken Sie dann auf Actions (Aktionen) und Attach Volume (Volume anfügen).

b. Geben Sie im Dialogfeld Attach Volume (Volume anfügen) für Instances den Namen oder die ID der ursprünglichen Instance ein und wählen Sie die Instance aus.

c. Geben Sie für Device (Gerät) **`/dev/sda1`** ein.

   d. Wählen Sie Attach (Anfügen) aus. Nachdem sich der Status des Volumes in `in-use` (In Verwendung) geändert hat, fahren Sie mit dem nächsten Schritt fort.

2. Wählen Sie im Navigationsbereich Instances aus. Wählen Sie die ursprüngliche Instance aus und klicken Sie auf Instance state (Instance-Zustand), Start instance (Instance starten). Nachdem sich der Status der Instance in `Running` (Wird ausgeführt) geändert hat, fahren Sie mit dem nächsten Schritt fort.
3. Rufen Sie Ihr neues Windows-Administratorpasswort mit dem privaten Schlüssel für das neue Schlüsselpaar ab und stellen Sie eine Verbindung mit der Instance her. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer -Windows-Instance.
4. (Optional) Sie können die temporäre Instance beenden, wenn Sie sie nicht mehr benötigen. Wählen Sie die temporäre Instance aus und klicken Sie auf Instance state (Instance-Zustand), Terminate instance (Instance beenden).

Problembehandlung bei unerreichbaren Instances

Sie können die folgenden Methoden verwenden, um Fehler bei einer Amazon EC2 EC2-Instance zu beheben, die nicht erreichbar ist.

Inhalt

Instance-Neustart

Die Möglichkeit, Instances, die sonst unerreichbar sind, neu zu starten, ist sowohl für die Problembehebung als auch für die allgemeine Instance-Verwaltung nützlich.

So wie Sie einen Computer über die Reset-Taste zurücksetzen können, so können Sie EC2 Instances mit der Amazon EC2-Konsole, der CLI oder der API zurücksetzen. Weitere Informationen finden Sie unter Durchführen eines Neustarts Ihrer Instance.

Instance-Konsolenausgabe

Die Konsolenausgabe ist ein nützliches Tool für die Problemdiagnose. Es ist besonders hilfreich zur Behebung von Problemen mit dem Kernel und der Servicekonfiguration, die dazu führen können, dass eine Instance beendet wird oder nicht mehr erreichbar ist, bevor ihr SSH-Daemon gestartet werden kann.

- Linux-Instances — Die Ausgabe der Instance-Konsole zeigt genau die Konsolenausgabe an, die normalerweise auf einem physischen Monitor angezeigt würde, der an einen Computer angeschlossen ist. Die Konsolenausgabe gibt gepufferte Informationen zurück, die kurz nach einem Instance-Übergangsstatus (Start, Stopp, Neustart und Abbruch) gepostet wurden. Die bereitgestellte Ausgabe wird nicht kontinuierlich aktualisiert, sondern nur wenn es besonders sinnvoll ist.
- Windows-Instanzen — Die Ausgabe der Instanzkonsole enthält die letzten drei Fehler im Systemereignisprotokoll.

Sie können optional die neueste Ausgabe der seriellen Konsole zu einem beliebigen Zeitpunkt während des Instance-Lebenszyklus abrufen. Diese Option wird nur für Instanzen unterstützt, die auf dem AWS Nitro-System basieren. Sie wird nicht über die Amazon EC2-Konsole unterstützt.

> **Note**
>
> Es werden nur die aktuellen 64 KB der bereitgestellten Ausgabe gespeichert. Diese bleiben mindestens 1 Stunde nach der letzten Bereitstellung verfügbar.

Auf die Konsolenausgabe kann nur der Instance-Eigentümer zugreifen.

Verwenden Sie eine der folgenden Methoden, um die Konsolenausgabe zu erhalten.

Console

Abrufen der Konsoleausgabe

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus und wählen Sie dann Aktionen, Überwachung und Fehlerbehebung, Systemprotokoll abrufen.

Command line

Abrufen der Konsoleausgabe

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- get-console-output (AWS CLI)
- Get-EC2ConsoleOutput (AWS Tools for Windows PowerShell)

Aufnehmen eines Screenshots einer nicht erreichbaren Instance

Wenn Sie keine Verbindung zu Ihrer Instance herstellen können, können Sie einen Screenshot Ihrer Instanz aufnehmen und ihn als Bild anzeigen. Das Image kann den Status der Instance sichtbar machen, und die Problembehebung kann schneller durchgeführt werden.

Sie können während der Ausführung oder nach dem Absturz einer Instance Screenshots erstellen. Das Image wird im JPG-Format erstellt und umfasst maximal 100 KB. Für den Screenshot fallen keine Datenübertragungskosten an.

Einschränkungen

Dieses Feature wird in folgenden Fällen nicht unterstützt:

- Bare-Metal-Instances (Instances des Typs `*.metal`)
- Die Instance verwendet einen NVIDIA-GRID-Treiber
- Instances, die mit ARM-basierten Graviton-Prozessoren betrieben werden
- Windows-Instanzen auf AWS Outposts

Unterstützte Regionen

Dieses Feature ist in den folgenden Regionen verfügbar:

- US East (N. Virginia) Region
- Region USA Ost (Ohio)
- Region US West (N. California)
- Region USA West (Oregon)
- Region Afrika (Kapstadt)

- Region Asien-Pazifik (Hongkong)
- Region Asien-Pazifik (Hyderabad)
- Region Asien-Pazifik (Jakarta)
- Region Asien-Pazifik (Melbourne)
- Region Asien-Pazifik (Mumbai)
- Region Asien-Pazifik (Osaka)
- Asia Pacific (Seoul) Region
- Region Asien-Pazifik (Singapur)
- Region Asien-Pazifik (Sydney)
- Region Asien-Pazifik (Tokio)
- Region Kanada (Zentral)
- Region Kanada West (Calgary)
- Region China (Peking)
- Region China (Ningxia)
- Region Europa (Frankfurt)
- Region Europa (Irland)
- Region Europa (London)
- Region Europa (Mailand)
- Region Europa (Paris)
- Region Europa (Spanien)
- Region Europa (Stockholm)
- Region Europa (Zürich)
- Region Israel (Tel Aviv)
- Region Südamerika (São Paulo)
- Region Naher Osten (Bahrain)
- Region Naher Osten (UAE)

Console

So rufen Sie einen Screenshot einer Instance ab

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.

2. Wählen Sie im linken Navigationsbereich die Option Instances aus.
3. Wählen Sie die Instance aus, für die Sie einen Screenshot aufnehmen möchten.
4. Wählen Sie Actions (Aktionen), Monitor and Troubleshoot (Überwachung und Fehlerbehebung), Get instance screenshot (Instance-Screenshot abrufen).
5. Wählen Sie Download (Herunterladen) oder klicken Sie mit der rechten Maustaste auf das Image, um es herunterzuladen und zu speichern.

Command line

So erstellen Sie einen Screenshot einer Instance

Verwenden Sie einen der folgenden Befehle. Der entsprechende Inhalt ist base64-kodiert. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Zugriff auf Amazon EC2.

- get-console-screenshot (AWS CLI)
- GetConsoleBildschirmfoto (Amazon EC2 EC2-Abfrage-API)

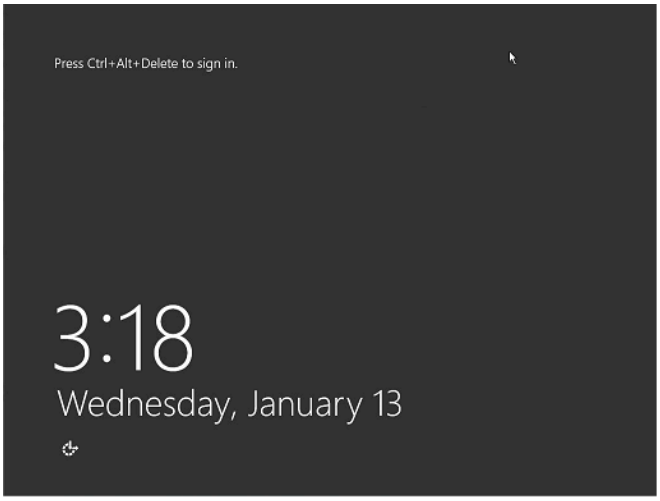
Allgemeine Screenshots für Windows-Instances

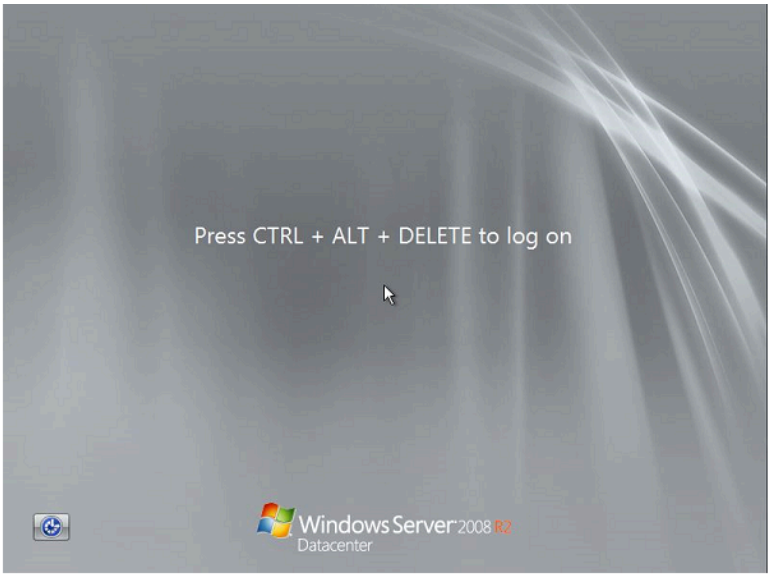
Die folgenden Informationen können Ihnen dabei helfen, Probleme in Zusammenhang mit unerreichbaren Windows-Instances zu beheben, indem Sie die Screenshots analysieren, die von dem Service zurückgegeben werden.

- Anmeldebildschirm (Strg+Alt+Entf)
- Wiederherstellungskonsolen-Bildschirm
- Windows-Start-Manager-Bildschirm
- Sysprep-Bildschirm
- Vorbereitungsbildschirm
- Windows Update-Bildschirm
- Chkdsk

Anmeldebildschirm (Strg+Alt+Entf)

Der Console Screenshot Service hat Folgendes zurückgegeben.





Wenn eine Instance bei der Anmeldung nicht mehr erreichbar ist, ist möglicherweise Ihre Netzwerkanbindung falsch konfiguriert oder es liegt ein Problem mit dem Windows-Remotedesktopdienst vor. Außerdem kann es vorkommen, dass eine Instance nicht mehr reagiert, wenn ein Prozess die CPU extrem stark auslastet.

Netzwerkkonfiguration

Verwenden Sie die folgenden Informationen, um sicherzustellen AWS, dass Ihre Netzwerkkonfigurationen, Microsoft Windows und lokale (oder lokale) Netzwerkkonfigurationen den Zugriff auf die Instanz nicht blockieren.

AWS Netzwerkkonfiguration

Konfiguration	Überprüfen
Sicherheitsgruppenkonfiguration	Überprüfen Sie, ob Port 3389 für Ihre Sicherheitsgruppe offen ist. Stellen Sie sicher, dass die Verbindung zu der richtigen öffentlichen IP-Adresse hergestellt wird. Wenn die Instance mit keiner Elastic IP-Adresse verknüpft war, ändert sich die öffentliche IP-Adresse nach einem erneuten Start der Instance. Weitere Informationen finden Sie unter Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen.

Konfiguration	Überprüfen
VPC-Konfiguration (Netzwerk-ACLs)	Stellen Sie sicher, dass die Access Control List (ACL) für Ihre Amazon VPC den Zugriff nicht blockiert. Weitere Informationen finden Sie unter Netzwerk-ACLs im Amazon VPC Benutzerhandbuch.
VPN-Konfiguration	Wenn Sie die Verbindung zu Ihrer VPC unter Verwendung einer Virtual Private Network (VPN) herstellen, überprüfen Sie die Anbindung des VPN-Tunnels. Weitere Informationen finden Sie unter How do I troubleshoot VPN tunnel connectivity to an Amazon VPC.

Windows-Netzwerkkonfiguration

Konfiguration	Überprüfen
Windows-Firewall	Überprüfen Sie, ob die Windows-Firewall die Verbindung zu Ihrer Instance blockiert. Deaktivieren Sie die Windows-Firewall wie in Punkt 7 im Abschnitt zur Problembehandlung für Remotedesktopverbindungen unter Der Remotedesktopdienst kann keine Verbindung zu dem Remotecomputer herstellen beschrieb en.
Erweiterte TCP/IP-Konfiguration (statische IP-Adresse)	Möglicherweise reagiert die Instance nicht, weil Sie eine statische IP-Adresse konfiguriert haben. Wenn Sie eine VPC haben, erstellen Sie eine Netzwerkschnittstelle und fügen diese der Instance an.

On-Premises- bzw. über die private Cloud eingerichtete Netzwerkkonfiguration

Überprüfen Sie, ob nicht die lokale Netzwerkkonfiguration den Zugriff blockiert. Versuchen Sie, eine Verbindung zu einer anderen Instance herzustellen, die sich in derselben VPC befindet wie die nicht erreichbare Instance. Wenn Sie auch nicht auf diese andere Instance zugreifen können, überprüfen Sie zusammen mit Ihrem Netzwerkadministrator, ob der Zugriff durch lokale Richtlinien beschränkt wird.

Probleme mit Remotedesktopdiensten

Wenn die Instance bei der Anmeldung nicht erreichbar ist, liegt möglicherweise dem Remotedesktopdienst (Remote Desktop Service, RDS) auf der Instance vor.

> **Tip**
>
> Sie können das `AWSSupport-TroubleshootRDP` Runbook verwenden, um verschiedene Einstellungen zu überprüfen und zu ändern, die sich auf RDP-Verbindungen (Remote Desktop Protocol) auswirken können. Weitere Informationen finden Sie unter `AWSSupport-TroubleshootRDP` in der Referenz zum AWS Systems Manager -Automation-Runbook.

Remotedesktopdienst-Konfiguration

Konfiguration	Überprüfen
RDS wird ausgeführt.	Überprüfen Sie, ob RDS auf der Instance ausgeführt wird. Stellen Sie unter Verwendung der Microsoft Management Console (MMC) mit dem Dienste-Snap-In (`services.msc`) eine Verbindung zu der Instance her. Überprüfen Sie in der Liste der Dienste, dass der Dienst Remotedesktopdienste den Status Wird ausgeführt trägt. wenn dies nicht der Fall ist, starten Sie den Dienst und legen Sie als Startup-Typ Automatisch fest. Wenn Sie auch über das Dienste-Snap-In keine Verbindung zu der Instance herstellen können, lösen Sie das Stamm-Volume von der Instance, nehmen Sie einen Snapshot des Volumes oder erstellen Sie anhand des Volumes ein AMI, weisen Sie dann das gelöste Stamm-Volume einer anderen Instance in derselben Availability Zone als sekundäres Volume zu und modifizieren Sie den Start-Registrierungsschlüssel. Wenn

Konfiguration	Überprüfen
	Sie fertig sind, binden Sie das Stamm-Volume wieder an die ursprüngliche Instance an.
RDS ist aktiviert.	Selbst wenn der Dienst gestartet wird, kann er deaktiviert sein. Trennen Sie das Stammvolume von der Instance, erstellen Sie einen Snapshot des Volumes oder erstellen Sie ein AMI daraus, fügen Sie das ursprüngliche Volume an eine andere Instance in derselben Availability Zone wie ein sekundäres Volume an und aktivieren Sie den Service, indem Sie den Terminals erver-Registrierungsschlüssel ändern, wie in Aktivieren von Remotedesktop für eine EC2-Instance mit Remote-Registrierung beschrieben. Wenn Sie fertig sind, binden Sie das Stamm-Volume wieder an die ursprüngliche Instance an.

Hohe CPU-Auslastung

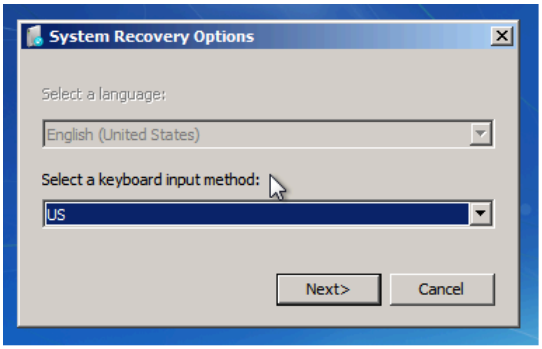
Überprüfen Sie die Metrik CPUUtilization (Maximum) auf Ihrer Instance mithilfe von Amazon. CloudWatch Wenn CPUUtilization (Maximum) sehr hoch ist, warten Sie, bis die CPU weniger stark ausgelastet ist, und wiederholen Sie dann den Verbindungsversuch. Eine hohe CPU-Auslastung kann die folgenden Ursachen haben:

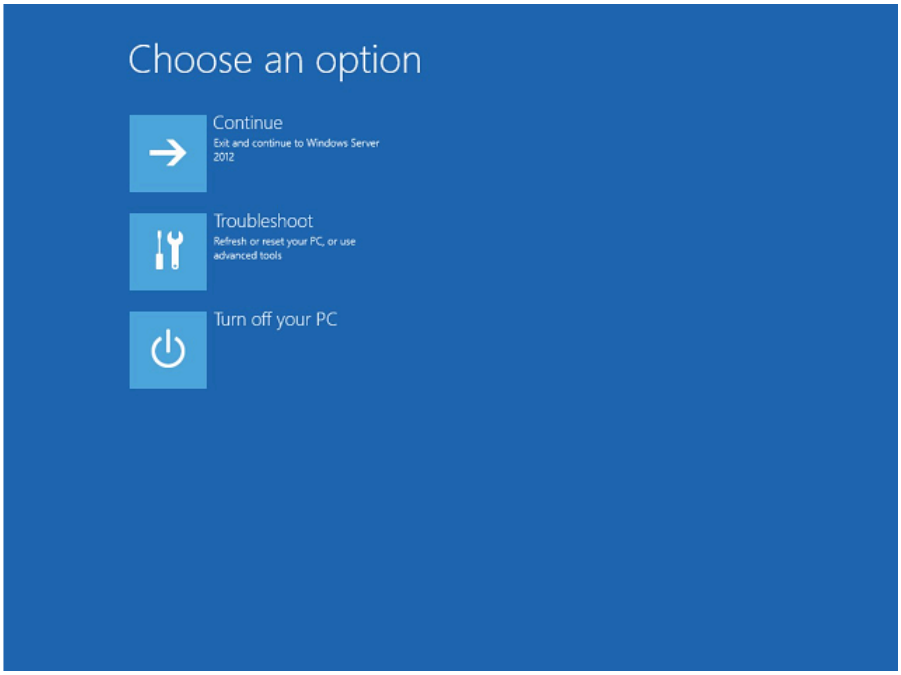
- Windows Update
- Scan-Aktivität von Sicherheitssoftware
- Benutzerdefiniertes Startup-Script
- Aufgaben-Scheduler

Weitere Informationen finden Sie unter Get Statistics for a Specific Resource im CloudWatch Amazon-Benutzerhandbuch. Weitere Tipps zur Fehlerbehebung finden Sie unter Hohe CPU-Auslastung kurz nach dem Start von Windows (nur Windows-Instances).

Wiederherstellungskonsolen-Bildschirm

Der Console Screenshot Service hat Folgendes zurückgegeben.





Wenn für `bootstatuspolicy` ein anderer Wert als `ignoreallfailures` festgelegt ist, besteht die Möglichkeit, dass das Betriebssystem beim Starten die Wiederherstellungskonsole startet und in diesem Zustand verbleibt. Führen Sie folgende Schritte durch, um die Konfiguration für `bootstatuspolicy` in `ignoreallfailures` zu ändern.

Standardmäßig AWS ist die von bereitgestellte Richtlinienkonfiguration für öffentliche Windows-AMIs auf eingestellt`ignoreallfailures`.

1. Halten Sie die unerreichbare Instance an.
2. Erstellen Sie einen Snapshot des Stamm-Volumes. Das Stamm-Volume ist als an die Instance angefüg `/dev/sda1`.

   Lösen Sie das Stamm-Volume von der nicht erreichbaren Instance, nehmen Sie einen Snapshot des Volumes oder erstellen Sie anhand des Volumes ein AMI und verbinden Sie es dann mit einer anderen Instance in derselben Availability Zone als sekundäres Volume.

   > **Warning**
   >
   > Wenn Ihre temporäre Instance und die ursprüngliche Instance mit demselben AMI gestartet wurden, müssen Sie zusätzliche Schritte durchführen, da Sie sonst die ursprüngliche Instance nach der Wiederherstellung ihres Root-Volumes aufgrund einer Kollision der Festplattensignaturen nicht mehr booten können. Wenn Sie eine temporäre Instance mit demselben AMI erstellen müssen, um eine Kollision

der Festplattensignaturen zu vermeiden, führen Sie die Schritte in Kollision der Festplattensignatur aus.
Alternativ können Sie ein anderes AMI für die temporäre Instance verwenden. Wenn die ursprüngliche Instance beispielsweise ein AMI für Windows Server 2016 verwendet, starten Sie die temporäre Instance mit einem AMI für Windows Server 2019.

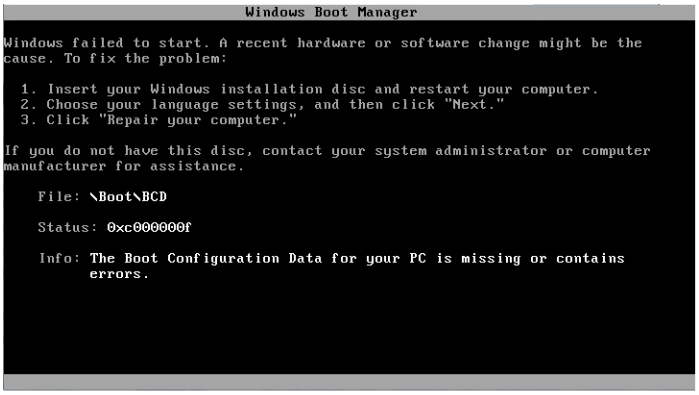
3. Melden Sie sich an der Instance an und führen Sie an der Eingabeaufforderung den folgenden Befehl aus, um die `bootstatuspolicy`-Konfiguration in `ignoreallfailures` zu ändern:

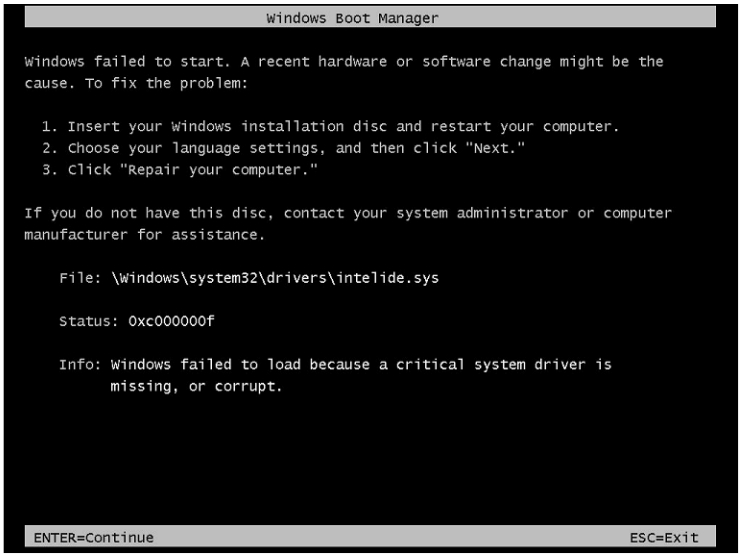
```
bcdedit /store Drive Letter:\boot\bcd /set {default} bootstatuspolicy
 ignoreallfailures
```

4. Hängen Sie das Volume wieder an die unerreichbare Instance an und starten Sie die Instance wieder.

Windows-Start-Manager-Bildschirm

Der Console Screenshot Service hat Folgendes zurückgegeben.

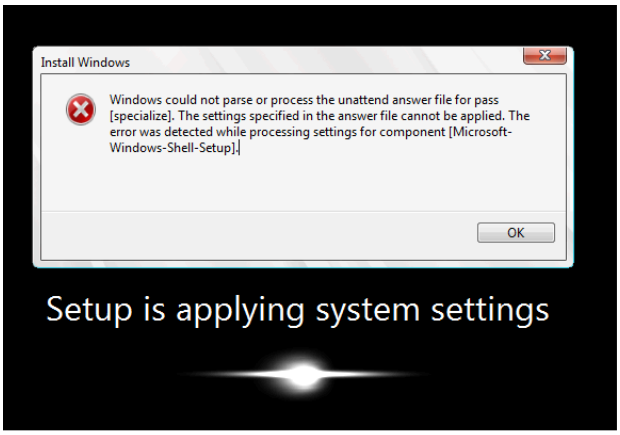


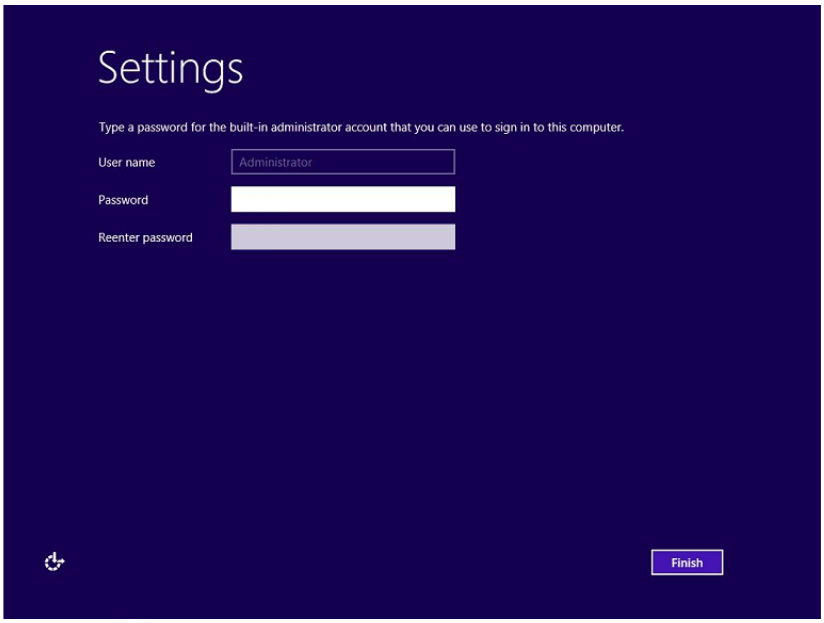


Das Betriebssystem wurde aufgrund eines fatalen Fehlers im Dateisystem oder in der Registrierung angehalten. Wenn eine Instance auf diese Weise „einfriert“, sollten Sie sie aus einem möglichst neuen Sicherungs-AMI wiederherstellen oder eine Austausch-Instance starten. Wenn Sie noch auf Daten auf der Instance zugreifen müssen, lösen Sie alle Stamm-Volumes von der nicht erreichbaren Instance, nehmen Sie einen Snapshot dieser Volumes oder erstellen Sie anhand der Volumes AMIs und verbinden Sie sie dann mit einer anderen Instance in derselben Availability Zone als sekundäres Volume.

Sysprep-Bildschirm

Der Console Screenshot Service hat Folgendes zurückgegeben.

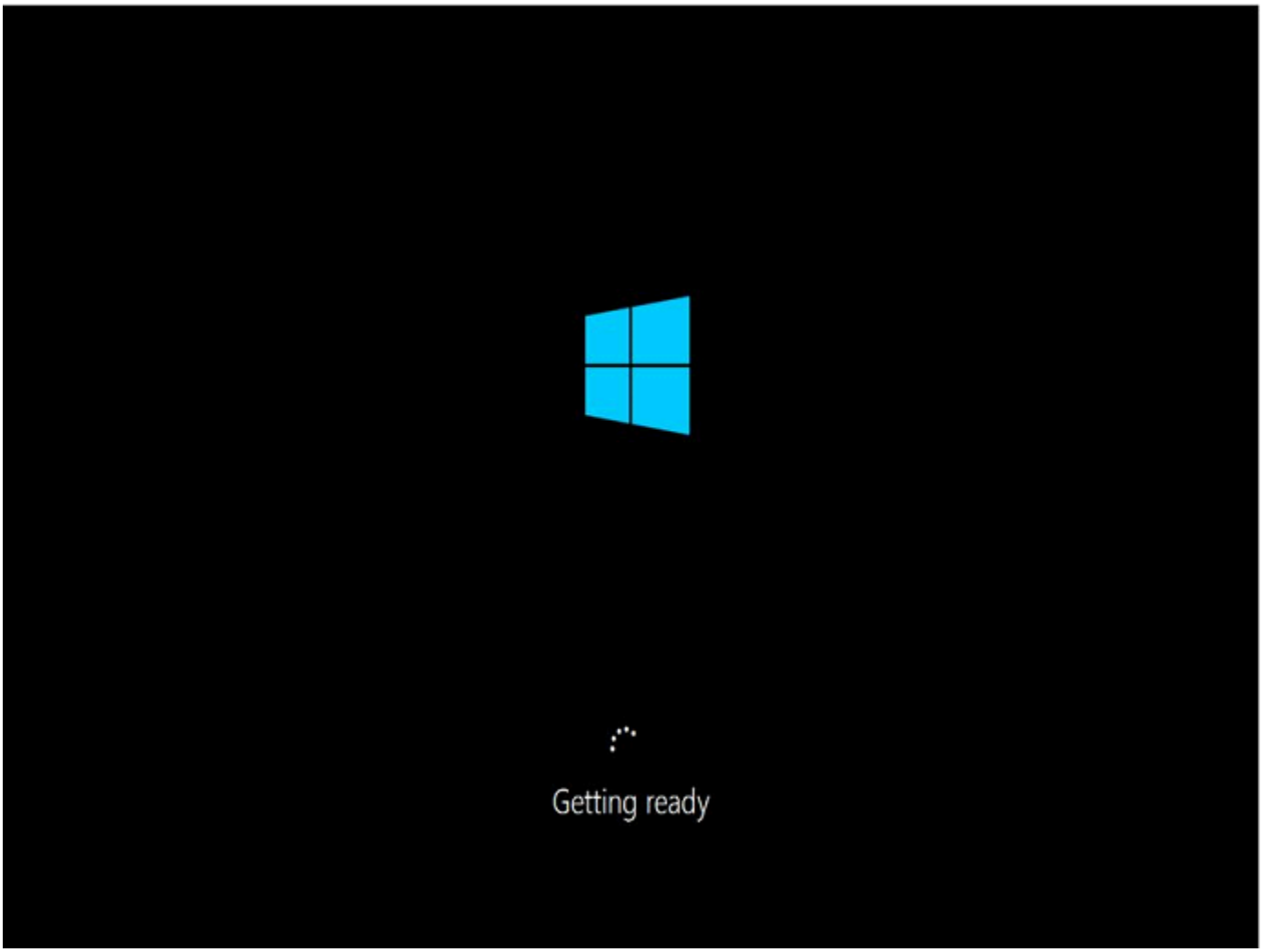




Dieser Bildschirm wird möglicherweise angezeigt, wenn Sie den EC2Config-Service nicht zum Aufrufen von Sysprep verwendet haben oder wenn das Betriebssystem während der Ausführung von Sysprep fehlgeschlagen ist. Sie können das Passwort mit EC2Rescue zurücksetzen. Andernfalls lesen Sie unter Erstellen Sie ein AMI mit Windows Sysprep weiter.

Vorbereitungsbildschirm

Der Console Screenshot Service hat Folgendes zurückgegeben.



Aktualisieren Sie den Instance Console Screenshot Service einige Male, um sicherzustellen, dass sich das Ringsymbol für die Fortschrittsanzeige dreht. Wenn sich das Ringsymbol dreht, warten Sie, bis das Betriebssystem gestartet ist. Sie können auch die Metrik CPUUtilization (Maximum) auf Ihrer Instance überprüfen, indem Sie Amazon verwenden CloudWatch , um festzustellen, ob das Betriebssystem aktiv ist. Wenn sich das Ringsymbol nicht dreht, ist die Instance möglicherweise während des Startvorgangs eingefroren. Starten Sie die Instance neu. Wenn sich das Problem nicht durch einen Neustart beheben lässt, sollten Sie die Instance aus einem möglichst neuen Sicherungs-AMI wiederherstellen oder eine Austausch-Instance starten. Wenn Sie noch auf Daten in der Instance zugreifen müssen, lösen Sie das Stamm-Volume aus der nicht erreichbaren Instance und erstellen Sie einen Snapshot des Volumes oder erstellen Sie ein AMI aus dem Volume. Hängen Sie das Volume an eine andere Instance in derselben Availability Zone als sekundäres Volume an.

Windows Update-Bildschirm

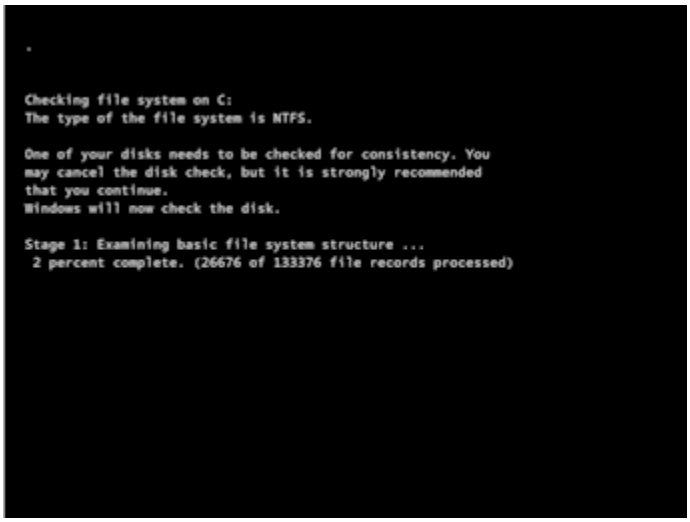
Der Console Screenshot Service hat Folgendes zurückgegeben.

Der Windows Update-Prozess aktualisiert die Registrierung. Warten Sie bis die Aktualisierung abgeschlossen ist. Halten Sie die Instance nicht an und starten Sie sie nicht neu, da dies während einer Aktualisierung zu einer Datenbeschädigung führen kann.

> **Note**
>
> Der Windows Update-Prozess kann während der Aktualisierung Serverressourcen beanspruchen. Falls dieses Problem bei Ihnen häufiger auftritt, sollten Sie möglicherweise schnellere Instance-Typen bzw. schnellere EBS-Volumes verwenden.

Chkdsk

Der Console Screenshot Service hat Folgendes zurückgegeben.



Windows führt das System-Tool chkdsk über dem Laufwerk aus, um die Integrität des Dateisystems zu überprüfen und logische Fehler in dem Dateisystem zu beheben. Warten Sie, bis der Vorgang abgeschlossen ist.

Wiederherstellung einer Instance beim Ausfall eines Host-Computers

Wenn ein nicht wiederherstellbarer Fehler mit der Hardware eines zugrunde liegenden Host-Computers vorliegt, kann AWS ein "Stop"-Ereignis für die Instance planen. Sie werden im Vorfeld per E-Mail über ein solches Ereignis informiert.

So stellen Sie eine Amazon EBS-gestützte Instance, die auf einem ausgefallen Host-Computer ausgeführt wird, wieder her

1. Sichern Sie alle wichtigen Daten auf Ihren Instance-Speicher-Volumes in Amazon EBS oder Amazon S3.
2. Halten Sie die Instance an.
3. Starten Sie die Instance.
4. Stellen Sie alle wichtigen Daten wieder her.

Weitere Informationen finden Sie unter Beenden und starten Sie Amazon EC2 EC2-Instances.

So stellen Sie eine Instance Store-Backupe Instance, die auf einem ausgefallen Host-Computer ausgeführt wird, wieder her

1. Erstellen Sie aus der Instance ein AMI.
2. Laden Sie das Image in Amazon S3 hoch.
3. Sichern Sie wichtige Daten in Amazon EBS oder Amazon S3.
4. Beenden Sie die Instance.
5. Starten Sie eine neue Instance aus dem AMI.
6. Stellen Sie alle wichtigen Daten auf der neuen Instance wieder her.

Beheben von Problemen beim Anhalten Ihrer Instance

Wenn Sie Ihre Amazon EBS-gestützte Instance angehalten haben und sie im Status `stopping` hängen bleibt, liegt möglicherweise ein Problem mit dem zugrunde liegenden Host-Computer vor.

Während sich eine Instance im Status `stopping` oder einem anderen Status außer `running` befindet, entstehen keine Kosten für die Instance-Nutzung. Ihnen wird die Instance-Nutzung nur in Rechnung gestellt, wenn sich eine Instance im `running`-Status befindet.

Erzwungenes Anhalten der Instance

Erzwingen Sie über die Konsole oder die , dass die Instance angehalten wir AWS CLI.

> **Note**
>
> Sie können nur dann erzwingen, dass eine Instance die Konsole nicht mehr verwendet, wenn sich die Instance im Zustand `stopping` befindet. Sie können erzwingen, dass eine Instance die AWS CLI nicht mehr verwendet, wenn sich die Instance in jedem Zustand außer `shutting-down` und `terminated` befindet.

Console

Erzwungenes Anhalten der Instance mit der Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die hängen gebliebene Instance aus.
3. Wählen Sie Instance state (Instance-Status), Force stop instance (Anhalten der Instance erzwingen), Stop (Anhalten).

   Beachten Sie, dass Force stop instance (Anhalten der Instance erzwingen) nur dann in der Konsole verfügbar ist, wenn sich Ihre Instance im Zustand `stopping` befindet. Wenn sich Ihre Instance in einem anderen Status befindet (außer `shutting-down` und`terminated`), können Sie den verwenden, AWS CLI um das Stoppen Ihrer Instance zu erzwingen.

AWS CLI

Um das Stoppen der Instanz zu erzwingen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl stop-instances und geben Sie die Option `--force` wie folgt an:

```
aws ec2 stop-instances --instance-ids i-0123ab456c789d01e --force
```

Wenn die Instance nach 10 Minuten nicht gestoppt wurde, posten Sie eine Hilfeanforderung im AWS re:Post. Um schneller eine Lösung zu erhalten, geben Sie die Instance-ID dabei an und beschreiben

Sie die Schritte, die Sie unternommen haben. Wenn Sie einen Supportplan haben, können Sie auch einen technischen Support-Fall im Support Center erstellen.

Erstellen einer Ersatz-Instance

Um zu versuchen, das Problem zu lösen, während Sie auf Hilfe vom AWS re:Post oder vom Support-Center warten, erstellen Sie eine Ersatz-Instance. Erstellen Sie eine AMI der hängen gebliebenen Instance und starten Sie mit dem neuen AMI eine neue Instance.

> **Important**
>
> Das Erstellen einer Ersatz-Instance wird empfohlen, wenn nur Systemstatusprüfungen registriert werden, da Instance-Statusprüfungen dazu führen, dass das AMI eine exakte Kopie des defekten Betriebssystems kopiert. Nachdem Sie die Statusmeldung bestätigt haben, erstellen Sie das AMI und starten Sie eine neue Instance mit dem neuen AMI.

Console

Eine Ersatz-Instance mithilfe der Konsole erstellen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die hängen gebliebene Instance aus.
3. Wählen Sie Actions (Aktionen), Image and templates (Image und Vorlagen), Create image (Image erstellen).
4. Gehen Sie auf der Seite Create image (Image erstellen) wie folgt vor:

   a. Geben Sie einen Namen und eine Beschreibung für das AMI ein.

   b. Wählen Sie No reboot aus.

   c. Wählen Sie Create Image (Abbild erstellen) aus.

   Weitere Informationen finden Sie unter the section called “Erstellen Sie ein AMI aus einer Instance”.
5. Starten Sie eine neue Instance über das AMI und überprüfen Sie, ob die neue Instance funktioniert.

6. Wählen Sie die hängen gebliebene Instance und anschließend Actions (Aktionen) aus. Wählen Sie dann die Optionen Instance State (Instance-Status) und Terminate instance (Instance beenden) aus. Wenn die Instance beim Beenden auch hängen bleibt, erzwingt Amazon EC2 das Beenden automatisch innerhalb weniger Stunden.

AWS CLI

Eine Ersatz-Instance mithilfe der CLI erstellen

1. Erstellen Sie ein AMI aus der hängen gebliebenen Instance unter Verwendung des create-image (AWS CLI)-Befehls und der Option `--no-reboot`, wie folgt:

```
aws ec2 create-image --instance-id i-0123ab456c789d01e --name "AMI" --
description "AMI for replacement instance" --no-reboot
```

2. Starten Sie aus dem AMI eine neue Instance unter Verwendung des run-instances (AWS CLI)-Befehls, wie folgt:

```
aws ec2 run-instances --image-id ami-1a2b3c4d --count 1 --instance-type c3.large
 --key-name MyKeyPair --security-groups MySecurityGroup
```

3. Überprüfen Sie, ob die neue Instance ausgeführt wird.
4. Beenden Sie die hängen gebliebene Instance mit dem terminate-instances (AWS CLI)-Befehl wie folgt:

```
aws ec2 terminate-instances --instance-ids i-1234567890abcdef0
```

Wenn Sie kein AMI auf der Instance wie in den vorherigen Schritten beschrieben erstellen können, richten Sie eine Ersatz-Instance wie folgt ein:

(Alternativ) Eine Ersatz-Instance mithilfe der Konsole erstellen

1. Wählen Sie die Instance und dann Description (Beschreibung), Block devices (Blockgeräte). Wählen Sie jedes Volume aus und notieren Sie sich seine Volume-ID. Machen Sie sich auch eine Notiz, welches Volume das Stamm-Volume ist.
2. Wählen Sie im Navigationsbereich Volumes aus. Wählen Sie jedes einzelne Volume für die Instance aus und klicken Sie dann auf Actions und Create Snapshot.

3. Wählen Sie im Navigationsbereich die Option Snapshots. Wählen Sie den Snapshot aus, den Sie gerade erstellt haben, und klicken Sie dann auf Actions und Create Volume.
4. Starten Sie eine Instance mit demselben Betriebssystem wie die hängen gebliebene Instance. Notieren Sie sich die Volume-ID und den Gerätenamen des Stamm-Volumes.
5. Wählen Sie im Navigationsbereich Instances aus, wählen Sie die Instance, die Sie soeben gestartet haben, aus und klicken Sie auf Instance State (Instance-Status), Stop instance (Instance anhalten).
6. Wählen Sie im Navigationsbereich Volumes und dann das Stamm-Volume der angehaltenen Instance aus. Klicken Sie auf Actions und Detach Volume.
7. Wählen Sie das Stamm-Volume aus, dass Sie von der hängen gebliebenen Instance erstellt haben. Klicken Sie auf Actions (Aktionen) und Attach Volume (Volume anhängen) und hängen Sie es der neuen Instance als Stamm-Volume an (mit dem Gerätenamen, den Sie sich notiert haben). Fügen Sie der Instance ggf. weitere nicht Stamm-Volumes an.
8. Klicken Sie im Navigationsbereich auf Instances und wählen Sie die Ersatz-Instance aus. Wählen Sie Instance state (Instance-Status), Start instance (Instance starten). Überprüfen Sie, ob die Instance ausgeführt wird.
9. Wählen Sie die hängen gebliebene Instance und anschließend Instance State (Instance-Status) und Terminate instance (Instance beenden) aus. Wenn die Instance beim Beenden auch hängen bleibt, erzwingt Amazon EC2 das Beenden automatisch innerhalb weniger Stunden.

Beheben von Problemen bei der Beendigung von Instances (Herunterfahren)

Während sich die Instance nicht im Status `running` befindet, wird Ihnen keine zusätzlichen Instance-Nutzung berechnet. Mit anderen Worten, wenn Sie eine Instance beenden, fallen für diese Instance keine Gebühren mehr an, sobald sich ihr Status in `shutting-down` ändert.

Die Instance wird sofort beendet

Mehrere Probleme können dazu führen, dass Ihre Instance beim Start sofort beendet wird. Weitere Informationen finden Sie unter Die Instance wird sofort beendet.

Verzögertes Beenden einer Instance

Wenn Ihre Instance länger als einige Minuten im Status `shutting-down` bleibt, kann sie aufgrund von Skripts zum Herunterfahren, die von der Instance ausgeführt werden, verzögert sein.

Eine andere mögliche Ursache ist, dass ein Problem mit dem zugrunde liegenden Host-Computer besteht. Wenn Ihre Instance mehrere Stunden im Status `shutting-down` bleibt, wird sie von Amazon EC2 als hängen geblieben behandelt und das Beenden wird erzwungen.

Wenn Ihre Instance anscheinend beim Beenden hängen geblieben ist und dieser Zustand bereits mehrere Stunden andauert, stellen Sie eine Anfrage an AWS re:Post. Um schneller eine Lösung zu erhalten, geben Sie die Instance-ID dabei an und beschreiben Sie die Schritte, die Sie unternommen haben. Wenn Sie einen Supportplan haben, können Sie auch einen technischen Support-Fall im Support Center erstellen.

Fortdauernde Anzeige einer beendeten Instance

Nachdem Sie eine Instance beendet haben, bleibt sie kurze Zeit sichtbar, bevor sie gelöscht wird. Der Status wird als angezeig `terminated`. Wenn der Eintrag nach einigen Stunden nicht gelöscht wird, wenden Sie sich an den Support.

Fehler: Die Instance ist möglicherweise nicht beendet worden. Ändern Sie das Instanzattribut „DeaktivierenApiTermination“

Wenn Sie versuchen, eine Instance zu beenden, und die Fehlermeldung `The instance` *`instance_id`* `may not be terminated. Modify its 'disableApiTermination' instance attribute` angezeigt wird, bedeutet dies, dass für die Instance der Beendigungsschutz aktiviert wurde. Der Beendigungsschutz verhindert, dass die Instance versehentlich beenden wird. Weitere Informationen finden Sie unter Aktivieren des Beendigungsschutzes.

Bevor Sie die Instance beenden können, müssen Sie den Beendigungsschutz deaktivieren.

Um den Beendigungsschutz mithilfe der Amazon-EC2-Konsole zu deaktivieren, wählen Sie die Instance aus und klicken Sie dann auf Aktionen, Instance-Einstellungen, Beendigungsschutz ändern.

Verwenden Sie den folgenden Befehl AWS CLI, um den Kündigungsschutz mit dem zu deaktivieren.

```
aws ec2 modify-instance-attribute --instance-id instance_id --no-disable-api-
termination
```

Instances automatisch gestartet oder beendet

Im Allgemeinen bedeuten die folgenden Verhaltensweisen, dass Sie Ihre Datenverarbeitungsressourcen mit Amazon EC2 Auto Scaling, mit einer EC2-Flotte oder mit einer Spot-Flotte basierend auf von Ihnen festgelegten Kriterien automatisch skaliert haben.

- Sie beenden eine Instance, und eine neue Instance wird automatisch gestartet.
- Sie starten eine Instance, und eine Ihrer Instances wird automatisch beendet.
- Sie halten eine Instance an, und sie wird beendet, worauf eine neue Instance automatisch gestartet wird.

Wie Sie die automatische Skalierung deaktivieren können, erfahren Sie im Benutzerhandbuch für Amazon EC2 Auto Scaling, EC2-Flotte oder Erstellen eine Spot-Flotten-Anforderung.

Beheben Sie Linux-Instances mit fehlgeschlagenen Statusprüfungen

> **Note**
>
> Dieses Thema gilt nur für Linux-Instances.

Die folgenden Informationen können Ihnen bei der Behebung von Problemen helfen, wenn Ihre Linux-Instance eine Statusprüfung nicht besteht. Stellen Sie zunächst fest, ob in Ihren Anwendungen Probleme bestehen. Wenn Sie feststellen, dass die Instance Ihre Anwendung nicht erwartungsgemäß ausführt, gehen Sie die Informationen der Statusprüfung und die Systemprotokolle durch.

Beispiele für Probleme, die dazu führen können, dass Statusprüfungen fehlschlagen, finden Sie unter Statusprüfungen für Ihre Instances.

Inhalt

- "FATAL: kernel too old" und "fsck: No such file or directory while trying to open /dev" (fehlende Übereinstimmung zwischen Kernel und AMI)
- „SCHWERWIEGEND: /lib/modules" oder "BusyBox" (Fehlende Kernelmodule) konnten nicht geladen werden
- ERROR Invalid kernel (mit EC2 nicht kompatibler Kernel)
- fsck: No such file or directory while trying to open... (Dateisystem nicht gefunden)
- Allgemeiner Fehler beim Mounten von Dateisystemen (Mountfehler)
- VFS: Unable to mount root fs on unknown-block (fehlende Übereinstimmung des Stammdateisystems)
- Error: Unable to determine major/minor number of root device... (fehlende Übereinstimmung des Stammdateisystems/Geräts)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (Dateisystemprüfung erforderlich)
- fsck died with exit status... (fehlendes Gerät)
- GRUB prompt (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (hartcodierte MAC-Adresse)
- Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (falsche SELinux-Konfiguration)
- XENBUS: Timeout connecting to devices (Xenbus-Timeout)

Informationen der Statusprüfung durchgehen

So untersuchen Sie nicht funktionsfähige Instances mit der Amazon EC2-Konsole

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie anschließend Ihre Instance aus.
3. Wählen Sie im Detailbereich Status und Alarme aus, um die einzelnen Ergebnisse für alle Systemstatusprüfungen und Zustandsprüfungen der Instance zu sehen.

Wenn eine Systemstatusprüfung fehlgeschlagen ist, verwenden Sie eine der folgenden Optionen:

- Erstellen Sie einen Wiederherstellungsalarm für die Instance. Weitere Informationen finden Sie unter Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird.
- Wenn Sie den Instanztyp auf eine auf dem AWS Nitro-System basierende Instanz geändert haben, schlagen die Statusprüfungen fehl, wenn Sie von einer Instanz migriert haben, die nicht über die erforderlichen ENA- und NVMe-Treiber verfügt. Weitere Informationen finden Sie unter Kompatibilität zum Ändern des Instance-Typs.
- Bei einer Instance, die ein Amazon EBS-gestütztes AMI verwendet, halten Sie die Instance an und starten Sie sie erneut.
- Bei einer Instance, die ein Instance Store-Backed AMI verwendet, beenden Sie die Instance und starten Sie eine Ersatz-Instance.
- Warten Sie, bis Amazon EC2 das Problem behoben hat.
- Poste dein Problem auf AWS re:POST.
- Wenn Ihre Instance eine Auto Scaling-Gruppe ist, startet der Amazon EC2 Auto Scaling-Service automatisch eine Ersatz-Instance. Weitere Informationen finden Sie unter Zustandsprüfungen für Auto Scaling-Instances im Amazon EC2 Auto Scaling-Benutzerhandbuch.
- Rufen Sie das Systemprotokoll ab und prüfen Sie es auf Fehler.

Systemprotokolle abrufen

Wenn eine Instance-Statusprüfung fehlschlägt, können Sie die Instance neu starten und die Systemprotokolle abrufen. Die Protokolle geben Aufschluss, ob ein Fehler vorliegt, was Ihnen bei der Problembehebung helfen kann. Durch den Neustart werden nicht benötigte Informationen in den Protokollen gelöscht.

So starten Sie eine Instance neu und rufen das Systemprotokoll ab

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances und wählen Sie Ihre Instance aus.
3. Wählen Sie Instance state (Instance-Status), Reboot instance (Instance neu starten). Es kann einige Minuten dauern, bis Ihre Instance neu gestartet wird.
4. Überprüfen Sie, ob das Problem nach wie vor besteht. In einigen Fällen lässt sich das Problem durch den Neustart lösen.
5. Wenn die Instance im `running`-Status ist, wählen Sie Actions (Aktionen), Monitor and Troubleshoot (Überwachung und Fehlerbehebung), Get system log (Systemprotokoll abrufen).

6. Sehen Sie sich das Protokoll an, das auf dem Bildschirm angezeigt wird, und greifen Sie zur Problembehebung auf die Liste der bekannten Systemprotokoll-Fehlermeldungen zurück.
7. Wenn Ihr Problem nicht behoben ist, posten Sie es auf AWS re:Post.

Beheben Sie Systemprotokollfehler für Linux-Instances

Vergewissern Sie sich bei Linux-Instances, die eine Instanzstatusprüfung nicht bestanden haben, z. B. die Erreichbarkeitsprüfung der Instanz, dass Sie die oben genannten Schritte zum Abrufen des Systemprotokolls befolgt haben. Die folgende Liste enthält einige allgemeine Systemprotokollfehler und Vorschläge für Aktionen, die Sie ausführen können, um den jeweiligen Fehler zu beheben.

Memory Errors

- Out of memory: kill process
- ERROR: mmu_update failed (Fehler beim Aktualisieren der Speicherverwaltung)

Device Errors

- I/O-Fehler (Blockgerätfehler)
- I/O ERROR: neither local nor remote disk (defektes verteiltes Blockgerät)

Kernel Errors

- request_module: runaway loop modprobe (Endlosschleife des modprobe-Programms auf Legacy-Kerneln älterer Linux-Versionen)
- "FATAL: kernel too old" und "fsck: No such file or directory while trying to open /dev" (fehlende Übereinstimmung zwischen Kernel und AMI)
- „SCHWERWIEGEND: /lib/modules" oder "BusyBox" (Fehlende Kernelmodule) konnten nicht geladen werden
- ERROR Invalid kernel (mit EC2 nicht kompatibler Kernel)

File System Errors

- fsck: No such file or directory while trying to open... (Dateisystem nicht gefunden)
- Allgemeiner Fehler beim Mounten von Dateisystemen (Mountfehler)

- VFS: Unable to mount root fs on unknown-block (fehlende Übereinstimmung des Stammdateisystems)
- Error: Unable to determine major/minor number of root device... (fehlende Übereinstimmung des Stammdateisystems/Geräts)
- XENBUS: Device with no driver...
- ... days without being checked, check forced (Dateisystemprüfung erforderlich)
- fsck died with exit status... (fehlendes Gerät)

Operating System Errors

- GRUB prompt (grubdom>)
- Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (hartcodierte MAC-Adresse)
- Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (falsche SELinux-Konfiguration)
- XENBUS: Timeout connecting to devices (Xenbus-Timeout)

Out of memory: kill process

Ein out-of-memory Fehler wird durch einen Systemprotokolleintrag angezeigt, der dem unten abgebildeten ähnelt.

```
[115879.769795] Out of memory: kill process 20273 (httpd) score 1285879
or a child
[115879.769795] Killed process 1917 (php-cgi) vsz:467184kB, anon-
rss:101196kB, file-rss:204kB
```

Mögliche Ursache

Unzureichender Speicher

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie eine der folgenden Aufgaben aus:

Für diesen Instance-Typ	Vorgehensweise
	• Halten Sie die Instance an und ändern Sie sie in einen anderen Instance-Typ. Starten Sie die Instance dann erneut. Verwenden Sie z. B. einen größeren oder speicheroptimierten Instance-Typ. • Starten Sie die Instance neu, um sie in einen nicht eingeschränkten Status zu versetzen. Das Problem tritt wahrscheinlich erneut auf, wenn Sie den Instance-Typ nicht ändern.
Instance Store-Backup	Führen Sie eine der folgenden Aufgaben aus: • Beenden Sie die Instance und starten Sie eine neue Instance unter Angabe eines anderen Instance-Typs. Verwenden Sie z. B. einen größeren oder speicheroptimierten Instance-Typ. • Starten Sie die Instance neu, um sie in einen nicht eingeschränkten Status zu versetzen. Das Problem tritt wahrscheinlich erneut auf, wenn Sie den Instance-Typ nicht ändern.

ERROR: mmu_update failed (Fehler beim Aktualisieren der Speicherverwaltung)

Update-Fehler bei der Speicherverwaltung werden von einem Systemprotokolleintrag ähnlich wie unten dargestellt angegeben:

```
...
Press `ESC' to enter the menu... 0   [H[J  Booting 'Amazon Linux 2011.09
 (2.6.35.14-95.38.amzn1.i686)'


root (hd0)

 Filesystem type is ext2fs, using whole disk
```

```
kernel /boot/vmlinuz-2.6.35.14-95.38.amzn1.i686 root=LABEL=/ console=hvc0 LANG=

en_US.UTF-8 KEYTABLE=us

initrd /boot/initramfs-2.6.35.14-95.38.amzn1.i686.img

ERROR: mmu_update failed with rc=-22
```

Mögliche Ursache

Problem mit Amazon Linux

Vorgeschlagene Aktion

Posten Sie Ihr Problem im Developer Forum oder wenden Sie sich an den AWS Support.

I/O-Fehler (Blockgerätfehler)

Ein Ein-/Ausgabefehler wird von einem Systemprotokolleintrag ähnlich wie im folgenden Beispiel dargestellt angegeben:

```
[9943662.053217] end_request: I/O error, dev sde, sector 52428288
[9943664.191262] end_request: I/O error, dev sde, sector 52428168
[9943664.191285] Buffer I/O error on device md0, logical block 209713024
[9943664.191297] Buffer I/O error on device md0, logical block 209713025
[9943664.191304] Buffer I/O error on device md0, logical block 209713026
[9943664.191310] Buffer I/O error on device md0, logical block 209713027
[9943664.191317] Buffer I/O error on device md0, logical block 209713028
[9943664.191324] Buffer I/O error on device md0, logical block 209713029
[9943664.191332] Buffer I/O error on device md0, logical block 209713030
[9943664.191339] Buffer I/O error on device md0, logical block 209713031
[9943664.191581] end_request: I/O error, dev sde, sector 52428280
[9943664.191590] Buffer I/O error on device md0, logical block 209713136
[9943664.191597] Buffer I/O error on device md0, logical block 209713137
[9943664.191767] end_request: I/O error, dev sde, sector 52428288
[9943664.191970] end_request: I/O error, dev sde, sector 52428288
[9943664.192143] end_request: I/O error, dev sde, sector 52428288
[9943664.192949] end_request: I/O error, dev sde, sector 52428288
[9943664.193112] end_request: I/O error, dev sde, sector 52428288
[9943664.193266] end_request: I/O error, dev sde, sector 52428288
...
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursache
Amazon EBS-gestützt	Ein ausgefallenes Amazon EBS-Volume
Instance Store-Backup	Ein ausgefallenes physisches Laufwerk

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Volume ab. 3. Versuchen Sie, das Volume wiederher zustellen. **Note** Es hat sich bewährt, häufig Snapshots von Amazon EBS-Volum es zu erstellen. Dadurch wird das Risiko von Datenverlusten aufgrund eines Ausfalls erheblich gesenkt. 4. Fügen Sie das Volume der Instance wieder an. 5. Starten Sie die Instance.
Instance Store-Backup	Beenden Sie die Instance und starten Sie eine neue Instance.

Für diesen Instance-Typ	Vorgehensweise
	Note Die Daten können nicht wiederher gestellt werden. Führen Sie eine Wiederherstellung anhand von Datensicherungen durch. **Note** Es hat sich bewährt, entweder Amazon S3 oder Amazon EBS für Datensich erungen zu verwenden. Ausfälle von einzelnen Hosts und Datenträg ern wirken sich direkt auf Instance-Speicher-Volumes aus.

I/O ERROR: neither local nor remote disk (defektes verteiltes Blockgerät)

Ein Ein-/Ausgabefehler auf dem Gerät, der von einem Systemprotokolleintrag ähnlich wie im folgenden Beispiel dargestellt angegeben wird:

```
...
block drbd1: Local IO failed in request_timer_fn. Detaching...

Aborting journal on device drbd1-8.

block drbd1: IO ERROR: neither local nor remote disk

Buffer I/O error on device drbd1, logical block 557056

lost page write due to I/O error on drbd1

JBD2: I/O error detected when updating journal superblock for drbd1-8.
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursache
Amazon EBS-gestützt	Ein ausgefallenes Amazon EBS-Volume
Instance Store-Backup	Ein ausgefallenes physisches Laufwerk

Vorgeschlagene Aktion

Beenden Sie die Instance und starten Sie eine neue Instance.

Bei einer Amazon EBS-gestützten Instance können Sie Daten anhand eines aktuellen Snapshots wiederherstellen, indem Sie ein Image davon erstellen. Alle Daten, die nach dem Snapshot hinzugefügt wurden, können nicht wiederhergestellt werden.

request_module: runaway loop modprobe (Endlosschleife des modprobe-Programms auf Legacy-Kerneln älterer Linux-Versionen)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben. Die Verwendung eines instabilen oder alten Linux-Kernels (z. B. 2.6.16-xenU) kann beim Startup eine Endlosschleife verursachen.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007

BIOS-provided physical RAM map:

 Xen: 0000000000000000 - 0000000026700000 (usable)

0MB HIGHMEM available.
...

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c

request_module: runaway loop modprobe binfmt-464c
```

```
request_module: runaway loop modprobe binfmt-464c
```

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Verwenden Sie einen neueren Kernel, entweder GRUB-basiert oder statisch, indem Sie eine der folgenden Optionen auswählen: Option 1: Beenden Sie die Instance und starten Sie eine neue Instance unter Angabe der Parameter `-kernel` und `-ramdisk`. Option 2: 1. Halten Sie die Instance an. 2. Ändern Sie die Attribute "kernel" und "ramdisk" und legen Sie sie auf einen neueren Kernel fest. 3. Starten Sie die Instance.
Instance Store-Backup	Beenden Sie die Instance und starten Sie eine neue Instance unter Angabe der Parameter `-kernel` und `-ramdisk`.

"FATAL: kernel too old" und "fsck: No such file or directory while trying to open /dev" (fehlende Übereinstimmung zwischen Kernel und AMI)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Linux version 2.6.16.33-xenU (root@dom0-0-50-45-1-a4-ee.z-2.aes0.internal)
(gcc version 4.1.1 20070105 (Red Hat 4.1.1-52)) #2 SMP Wed Aug 15 17:27:36 SAST 2007
...
FATAL: kernel too old
Kernel panic - not syncing: Attempted to kill init!
```

Mögliche Ursachen

Kernel und Land des Benutzers sind nicht kompatibel.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Ändern Sie die Konfiguration zur Verwendung eines neueren Kernels. 3. Starten Sie die Instance.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Erstellen Sie ein AMI, das einen neueren Kernel verwendet. 2. Beenden Sie die Instance. 3. Starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben.

„SCHWERWIEGEND: /lib/modules" oder "BusyBox" (Fehlende Kernelmodule) konnten nicht geladen werden

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
[    0.370415] Freeing unused kernel memory: 1716k freed
Loading, please wait...
WARNING: Couldn't open directory /lib/modules/2.6.34-4-virtual: No such file or
 directory
FATAL: Could not open /lib/modules/2.6.34-4-virtual/modules.dep.temp for writing: No
 such file or directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Couldn't get a file descriptor referring to the console
Begin: Loading essential drivers... ...
```

```
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
Done.
Begin: Running /scripts/init-premount ...
Done.
Begin: Mounting root file system... ...
Begin: Running /scripts/local-top ...
Done.
Begin: Waiting for root file system... ...
Done.
Gave up waiting for root device.  Common problems:
 - Boot args (cat /proc/cmdline)
   - Check rootdelay= (did the system wait long enough?)
   - Check root= (did the system wait for the right device?)
 - Missing modules (cat /proc/modules; ls /dev)
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
FATAL: Could not load /lib/modules/2.6.34-4-virtual/modules.dep: No such file or
 directory
ALERT! /dev/sda1 does not exist. Dropping to a shell!


BusyBox v1.13.3 (Ubuntu 1:1.13.3-1ubuntu5) built-in shell (ash)
Enter 'help' for a list of built-in commands.

(initramfs)
```

Mögliche Ursachen

Dieses Problem kann durch einen oder mehrere der folgenden Zustände verursacht werden:

- Fehlende Ramdisk
- Fehlende korrekte Module von der Ramdisk
- Amazon EBS-Stamm-Volume nicht korrekt als angefüg `/dev/sda1`

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Wählen Sie die korrigierte Ramdisk für das Amazon EBS-Volume aus. 2. Halten Sie die Instance an. 3. Trennen Sie das Volume und reparieren Sie es. 4. Fügen Sie das Volume der Instance an. 5. Starten Sie die Instance. 6. Ändern Sie das AMI so, dass die korrigierte Ramdisk verwendet wird.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Beenden Sie die Instance und starten Sie eine neue Instance mit der korrekten Ramdisk. 2. Erstellen Sie ein neues AMI mit der korrekten Ramdisk.

ERROR Invalid kernel (mit EC2 nicht kompatibler Kernel)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
...
root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz root=/dev/sda1 ro

initrd /initrd.img
```

```
ERROR Invalid kernel: elf_xen_note_check: ERROR: Will only load images
built for the generic loader or Linux images
xc_dom_parse_image returned -1

Error 9: Unknown boot failure

  Booting 'Fallback'

root (hd0)

 Filesystem type is ext2fs, using whole disk

kernel /vmlinuz.old root=/dev/sda1 ro

Error 15: File not found
```

Mögliche Ursachen

Dieses Problem kann durch einen oder beide der folgenden Zustände verursacht werden:

- Der bereitgestellte Kernel wird von GRUB nicht unterstützt.
- Der Fallback-Kernel ist nicht vorhanden.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Tauschen Sie sie durch einen funktioni erenden Kernel aus. 3. Installieren Sie einen Fallback-Kernel. 4. Ändern Sie das AMI, indem Sie den Kernel korrigieren.
Instance Store-Backup	Führen Sie die folgenden Schritte aus:

Für diesen Instance-Typ	Vorgehensweise
	1. Beenden Sie die Instance und starten Sie eine neue Instance mit dem korrekten Kernel. 2. Erstellen Sie ein AMI mit dem korrekten Kernel. 3. (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwied erherstellung zu erhalten AWS Support.

fsck: No such file or directory while trying to open... (Dateisystem nicht gefunden)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
  Welcome to Fedora
  Press 'I' to enter interactive startup.
Setting clock : Wed Oct 26 05:52:05 EDT 2011 [  OK  ]

Starting udev: [  OK  ]

Setting hostname localhost:  [  OK  ]

No devices found
Setting up Logical Volume Management: File descriptor 7 left open
  No volume groups found
[  OK  ]

Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1: clean, 82081/1310720 files, 2141116/2621440 blocks
[/sbin/fsck.ext3 (1) -- /mnt/dbbackups] fsck.ext3 -a /dev/sdh
fsck.ext3: No such file or directory while trying to open /dev/sdh

/dev/sdh:
The superblock could not be read or does not describe a correct ext2
filesystem.  If the device is valid and it really contains an ext2
filesystem (and not swap or ufs or something else), then the superblock
```

```
is corrupt, and you might try running e2fsck with an alternate superblock:
    e2fsck -b 8193 <device>

[FAILED]


*** An error occurred during the file system check.
*** Dropping you to a shell; the system will reboot
*** when you leave the shell.
Give root password for maintenance
(or type Control-D to continue):
```

Mögliche Ursachen

- In den Ramdisk-Dateisystemdefinitionen "/etc/fstab" liegt ein Fehler vor.
- Die Dateisystemdefinitionen in "/etc/fstab" sind falsch konfiguriert.
- Das Laufwerk fehlt/ist fehlerhaft.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an, trennen Sie das Stamm-Volume, reparieren/ändern Sie das Volume bzw. ändern Sie etc/fstab für das Volume, fügen Sie der Instance das Volume an und starten Sie die Instance. 2. Korrigieren Sie die Ramdisk, sodass die geänderte Datei "/etc/fstab" enthalten ist (falls zutreffend). 3. Ändern Sie das AMI zur Verwendung einer neueren Ramdisk. Das sechste Feld in der fstab-Datei definiert die Verfügbarkeitsanforderungen für das

Für diesen Instance-Typ	Vorgehensweise
	Mounting. Ein Wert ungleich null implizier t, dass ein fsck-Befehl für dieses Volume ausgeführt wird und erfolgreich beendet werden muss. Die Verwendung dieses Felds kann in Amazon EC2 problematisch sein, da ein Ausfall in der Regel zu einer interaktiven Konsoleneingabeaufforderung führt, die derzeit in Amazon EC2 nicht verfügbar ist. Verwenden Sie dieses Feature mit Bedacht und lesen Sie den Abschnitt über die fstab-Datei im Linux-Handbuch.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Beenden Sie die Instance und starten Sie eine neue Instance. 2. Trennen Sie fehlerhafte Amazon EBS-Volum es und die Neustart-Instance. 3. (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwied erherstellung zu erhalten AWS Support.

Allgemeiner Fehler beim Mounten von Dateisystemen (Mountfehler)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Loading xenblk.ko module
xen-vbd: registered block device major 8

Loading ehci-hcd.ko module
Loading ohci-hcd.ko module
Loading uhci-hcd.ko module
USB Universal Host Controller Interface driver v3.0

Loading mbcache.ko module
Loading jbd.ko module
```

```
Loading ext3.ko module
Creating root device.
Mounting root filesystem.
kjournald starting.  Commit interval 5 seconds

EXT3-fs: mounted filesystem with ordered data mode.

Setting up other filesystems.
Setting up new root fs
no fstab.sys, mounting internal defaults
Switching to new root and running init.
unmounting old /dev
unmounting old /proc
unmounting old /sys
mountall:/proc: unable to mount: Device or resource busy
mountall:/proc/self/mountinfo: No such file or directory
mountall: root filesystem isn't mounted
init: mountall main process (221) terminated with status 1

General error mounting filesystems.
A maintenance shell will now be started.
CONTROL-D will terminate this shell and re-try.
Press enter for maintenance
(or type Control-D to continue):
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursache
Amazon EBS-gestützt	• Das Amazon EBS-Volume wurde getrennt oder ist ausgefallen. • Das Dateisystem ist beschädigt. • Die Ramdisk- und AMI-Kombination stimmt nicht überein (z. B. Debian-Ramdisk mit einem SUSE-AMI).
Instance Store-Backup	• Das Laufwerk ist ausgefallen. • Ein Dateisystem ist beschädigt.

Instance-Typ	Mögliche Ursache
	• Die Ramdisk- und AMI-Kombination stimmt nicht überein (z. B. Debian-Ramdisk mit einem SUSE-AMI).

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Stamm-Volume. 3. Fügen Sie das Stamm-Volume einer funktionierenden Instance an. 4. Führen Sie eine Dateisystemprüfung aus (fsck -a /dev/...). 5. Beheben Sie vorhandene Fehler. 6. Trennen Sie das Volume von der funktioni erenden Instance. 7. Fügen Sie das Volume der angehaltenen Instance an. 8. Starten Sie die Instance. 9. Prüfen Sie den Status der Instance erneut.
Instance Store-Backup	Führen Sie einen der folgenden Schritte aus: • Starten Sie eine neue Instance. • (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwied erherstellung zu erhalten AWS Support.

VFS: Unable to mount root fs on unknown-block (fehlende Übereinstimmung des Stammdateisystems)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
 20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
Kernel command line:  root=/dev/sda1 ro 4
...
Registering block device major 8
...
Kernel panic - not syncing: VFS: Unable to mount root fs on unknown-block(8,1)
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursache
Amazon EBS-gestützt	• Das Gerät ist nicht ordnungsgemäß angefügt. • Das Stammgerät wurde nicht am korrekten Gerätepunkt angefügt. • Das Dateisystem hat nicht das erwartete Format. • Es wurde ein Legacy-Kernel (z. B. 2.6.16-XenU) verwendet. • Ein aktuelles Kernel-Update Ihrer Instance wurde fehlerhaft ausgeführt oder enthält einen Fehler.
Instance Store-Backup	Das Hardware-Gerät ist ausgefallen.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie eine der folgenden Aufgaben aus:

Für diesen Instance-Typ	Vorgehensweise
	• Halten Sie die Instance an und starten Sie sie neu. • Ändern Sie das Stamm-Volume und fügen Sie es am richtigen Gerätepunkt an, möglicherweise "/dev/sda1" statt "/dev/sda". • Halten Sie das Gerät an und ändern Sie es auf einen aktuellen Kernel. • Bekannte Fehler beim Update finden Sie in der Dokumentation Ihrer Linux-Verteilung. Ändern Sie den Kernel oder installieren Sie ihn neu.
Instance Store-Backup	Beenden Sie die Instance und starten Sie eine neue Instance mit einem aktuellen Kernel.

Error: Unable to determine major/minor number of root device... (fehlende Übereinstimmung des Stammdateisystems/Geräts)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
...
XENBUS: Device with no driver: device/vif/0
XENBUS: Device with no driver: device/vbd/2048
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
```

```
[ramfs /]#
```

Mögliche Ursachen

- Der virtuelle Blockgerättreiber fehlt oder ist falsch konfiguriert.
- Es liegt eine Gerätenummerierungskollision vor (sda statt xvda oder sda statt sda1).
- Der falsche Instance-Kernel wurde ausgewählt.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Volume ab. 3. Beheben Sie das Gerätezuweisungspr oblem. 4. Starten Sie die Instance. 5. Ändern Sie das AMI, um die Gerätezuw eisungsprobleme zu beheben.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Erstellen Sie ein neues AMI mit der entsprechenden Fehlerbehebung (weisen Sie das Blockgerät korrekt zu). 2. Beenden Sie die Instance und starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben.

XENBUS: Device with no driver...

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
XENBUS: Device with no driver: device/vbd/2048
```

```
drivers/rtc/hctosys.c: unable to open rtc device (rtc0)
Initializing network drop monitor service
Freeing unused kernel memory: 508k freed
:: Starting udevd...
done.
:: Running Hook [udev]
:: Triggering uevents...<30>udevd[65]: starting version 173
done.
Waiting 10 seconds for device /dev/xvda1 ...
Root device '/dev/xvda1' doesn't exist. Attempting to create it.
ERROR: Unable to determine major/minor number of root device '/dev/xvda1'.
You are being dropped to a recovery shell
    Type 'exit' to try and continue booting
sh: can't access tty; job control turned off
[ramfs /]#
```

Mögliche Ursachen

- Der virtuelle Blockgerättreiber fehlt oder ist falsch konfiguriert.
- Es liegt eine Gerätenummerierungskollision vor (sda statt xvda).
- Der falsche Instance-Kernel wurde ausgewählt.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Volume ab. 3. Beheben Sie das Gerätezuweisungsproblem. 4. Starten Sie die Instance. 5. Ändern Sie das AMI, um die Gerätezuweisungsprobleme zu beheben.
Instance Store-Backup	Führen Sie die folgenden Schritte aus:

Für diesen Instance-Typ	Vorgehensweise
	1. Erstellen Sie ein AMI mit der entsprechenden Fehlerbehebung (weisen Sie das Blockgerät korrekt zu). 2. Beenden Sie die Instance und starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben.

... days without being checked, check forced (Dateisystemprüfung erforderlich)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
...
Checking filesystems
Checking all file systems.
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a /dev/sda1
/dev/sda1 has gone 361 days without being checked, check forced
```

Mögliche Ursachen

Der Zeitpunkt der Dateisystemprüfung ist überschritten; eine Dateisystemprüfung wird erzwungen.

Vorgeschlagene Aktionen

- Warten Sie, bis die Dateisystemprüfung abgeschlossen ist. Eine solche Prüfung kann je nach Größe des Stammdateisystems einige Zeit in Anspruch nehmen.
- Ändern Sie Ihre Dateisysteme, um die Erzwingung der Dateisystemprüfung (fsck) mit tune2fs oder mit für Ihr Dateisystem geeigneten Tools zu entfernen.

fsck died with exit status... (fehlendes Gerät)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Cleaning up ifupdown....
Loading kernel modules...done.
```

```
...
Activating lvm and md swap...done.
Checking file systems...fsck from util-linux-ng 2.16.2
/sbin/fsck.xfs: /dev/sdh does not exist
fsck died with exit status 8
[31mfailed (code 8).[39;49m
```

Mögliche Ursachen

- Die Ramdisk sucht nach einem fehlenden Laufwerk.
- Die Konsistenzprüfung des Dateisystems wurde erzwungen.
- Das Laufwerk ist ausgefallen oder wurde getrennt.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie einen oder mehrere der folgenden Schritte aus, um das Problem zu lösen: • Halten Sie die Instance an und fügen Sie das Volume einer vorhandenen, aktuell ausgeführten Instance an. • Führen Sie Konsistenzprüfungen manuell aus. • Korrigieren Sie die Ramdisk, sodass sie relevante Dienstprogramme umfasst. • Ändern Sie Parameter zur Optimierung des Dateisystems, um Konsistenzanforderungen zu entfernen (nicht empfohlen).
Instance Store-Backup	Führen Sie einen oder mehrere der folgenden Schritte aus, um das Problem zu lösen: • Bündeln Sie die Ramdisk mit den richtigen Tools neu.

Für diesen Instance-Typ	Vorgehensweise
	• Ändern Sie Parameter zur Optimierung des Dateisystems, um Konsistenzanforderungen zu entfernen (nicht empfohlen). • Beenden Sie die Instance und starten Sie eine neue Instance. • (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwied erherstellung zu erhalten AWS Support.

GRUB prompt (grubdom>)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
    GNU GRUB  version 0.97  (629760K lower / 0K upper memory)

       [ Minimal BASH-like line editing is supported.   For

         the   first   word,  TAB  lists  possible  command

         completions.  Anywhere else TAB lists the possible

         completions of a device/filename. ]

grubdom>
```

Mögliche Ursachen

Instance-Typ	Mögliche Ursachen
Amazon EBS-gestützt	• Die GRUB-Konfigurationsdatei fehlt. • Es wird ein falsches GRUB-Image verwendet , sodass die GRUB-Konfigurationsdatei an einem anderen Speicherort erwartet wird. • Es wird ein nicht unterstütztes Dateisystem zum Speichern Ihrer GRUB-Konfiguration

Instance-Typ	Mögliche Ursachen
	sdatei verwendet (Ihr Stammdateisystem wird z. B. in einen Typ konvertiert, der von einer früheren GRUB-Version nicht unterstüt zt wird).
Instance Store-Backup	• Die GRUB-Konfigurationsdatei fehlt. • Es wird ein falsches GRUB-Image verwendet , sodass die GRUB-Konfigurationsdatei an einem anderen Speicherort erwartet wird. • Es wird ein nicht unterstütztes Dateisystem zum Speichern Ihrer GRUB-Konfiguration sdatei verwendet (Ihr Stammdateisystem wird z. B. in einen Typ konvertiert, der von einer früheren GRUB-Version nicht unterstüt zt wird).

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Option 1: Ändern Sie das AMI und starten Sie die Instance neu: 1. Ändern Sie das Quell-AMI, um eine GRUB-Konfigurationsdatei am Standardspeicherort zu erstellen (/boot/grub/menu.lst). 2. Überprüfen Sie, dass Ihre GRUB-Version den zugrunde liegenden Dateisystemtyp unterstützt, und upgraden Sie GRUB, falls erforderlich. 3. Wählen Sie das geeignete GRUB-Image aus ("hd0-1st drive" oder "hd00 – 1st drive, 1st partition").

Für diesen Instance-Typ	Vorgehensweise
	4. Beenden Sie die Instance, und starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben. Option 2: Reparieren Sie die vorhandene Instance: 1. Halten Sie die Instance an. 2. Trennen Sie das Stammdateisystem. 3. Fügen Sie das Stammdateisystem einer funktionierenden Instance an. 4. Mounten Sie das Dateisystem. 5. Erstellen Sie eine GRUB-Konfiguration sdatei. 6. Überprüfen Sie, dass Ihre GRUB-Version den zugrunde liegenden Dateisystemtyp unterstützt, und upgraden Sie GRUB, falls erforderlich. 7. Trennen Sie das Dateisystem. 8. Fügen Sie es der ursprünglichen Instance an. 9. Ändern Sie das Kernel-Attribut zur Verwendung des entsprechenden GRUB-Images ("hd0-1st drive" oder "hd00 – 1st drive, 1st partition"). 10. Starten Sie die Instance.

Für diesen Instance-Typ	Vorgehensweise
Instance Store-Backup	Option 1: Ändern Sie das AMI und starten Sie die Instance neu: 1. Erstellen Sie das neue AMI mit einer GRUB-Konfigurationsdatei am Standardspeicherort (/boot/grub/menu.lst). 2. Wählen Sie das geeignete GRUB-Image aus ("hd0-1st drive" oder "hd00 – 1st drive, 1st partition"). 3. Überprüfen Sie, dass Ihre GRUB-Version den zugrunde liegenden Dateisystemtyp unterstützt, und upgraden Sie GRUB, falls erforderlich. 4. Beenden Sie die Instance und starten Sie eine neue Instance mit dem AMI, das Sie erstellt haben. Option 2: Beenden Sie die Instance und starten Sie eine neue Instance unter Angabe des korrekten Kernels. **Note** Wenden Sie sich an den AWS Support, um Daten von der vorhandenen Instance wiederherzustellen.

Bringing up interface eth0: Device eth0 has different MAC address than expected, ignoring. (hartcodierte MAC-Adresse)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
. . .
```

```
Bringing up loopback interface:  [  OK  ]

Bringing up interface eth0:  Device eth0 has different MAC address than expected,
 ignoring.
[FAILED]

Starting auditd: [  OK  ]
```

Mögliche Ursachen

In der AMI-Konfiguration ist eine hartcodierte MAC-Schnittstelle enthalten.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie eine der folgenden Aufgaben aus: • Ändern Sie das AMI, um die Hartcodierung zu entfernen, und starten Sie die Instance neu. • Ändern Sie die Instance, um die hartcodierte MAC-Adresse zu entfernen. ODER Führen Sie die folgenden Schritte aus: 1. Halten Sie die Instance an. 2. Trennen Sie das Stamm-Volume. 3. Fügen Sie das Volume einer anderen Instance an und ändern Sie das Volume, um die hartcodierte MAC-Adresse zu entfernen. 4. Fügen Sie das Volume der ursprünglichen Instance an. 5. Starten Sie die Instance.
Instance Store-Backup	Führen Sie eine der folgenden Aufgaben aus:

Für diesen Instance-Typ	Vorgehensweise
	• Ändern Sie die Instance, um die hartcodierte MAC-Adresse zu entfernen. • Beenden Sie die Instance und starten Sie eine neue Instance.

Unable to load SELinux Policy. Machine is in enforcing mode. Halting now. (falsche SELinux-Konfiguration)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
audit(1313445102.626:2): enforcing=1 old_enforcing=0 auid=4294967295
Unable to load SELinux Policy. Machine is in enforcing mode. Halting now.
Kernel panic - not syncing: Attempted to kill init!
```

Mögliche Ursachen

SELinux wurde versehentlich aktiviert:

- Der bereitgestellte Kernel wird von GRUB nicht unterstützt.
- Der Fallback-Kernel ist nicht vorhanden.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie die folgenden Schritte aus: 1. Halten Sie die ausgefallene Instance an. 2. Trennen Sie die ausgefallene Instance vom Stamme-Volume. 3. Fügen Sie das Stamm-Volume einer anderen, aktuell ausgeführten Linux-Instance an (diese wird nachfolgend als Wiederher stellungs-Instance bezeichnet).

Für diesen Instance-Typ	Vorgehensweise
	4. Stellen Sie eine Verbindung mit der Wiederherstellungs-Instance her und mounten Sie das Stamm-Volume der ausgefallenen Instance. 5. Deaktivieren Sie SELinux auf dem gemounteten Stamm-Volume. Dieser Prozess ist je nach Linux-Verteilung unterschiedlich. Weitere Informationen finden Sie in der betriebssystemspezifischen Dokumentation. **Note** In einigen Systemen deaktivieren Sie SELinux, indem Sie `SELINUX=disabled` in der `/mount_point/etc/sysconfig/selinux` -Datei festlegen, wobei *mount_point* der Punkt ist, an dem Sie das Volume auf Ihrer Wiederherstellungs-Instance gemountet haben. 6. Heben Sie die Bereitstellung des Stamm-Volumes auf, trennen Sie es von der Wiederherstellungs-Instance und fügen Sie es der ursprünglichen Instance wieder an. 7. Starten Sie die Instance.
Instance Store-Backup	Führen Sie die folgenden Schritte aus: 1. Beenden Sie die Instance und starten Sie eine neue Instance. 2. (Optional) Wenden Sie sich an den , um technische Unterstützung zur Datenwiederherstellung zu erhalten AWS Support.

XENBUS: Timeout connecting to devices (Xenbus-Timeout)

Dieser Zustand wird von einem Systemprotokoll ähnlich wie unten dargestellt angegeben.

```
Linux version 2.6.16-xenU (builder@xenbat.amazonsa) (gcc version 4.0.1
20050727 (Red Hat 4.0.1-5)) #1 SMP Mon May 28 03:41:49 SAST 2007
...
XENBUS: Timeout connecting to devices!
...
Kernel panic - not syncing: No init found.  Try passing init= option to kernel.
```

Mögliche Ursachen

- Das Blockgerät ist nicht mit der Instance verbunden.
- Die Instance verwendet einen alten Instance-Kernel.

Vorgeschlagene Aktionen

Für diesen Instance-Typ	Vorgehensweise
Amazon EBS-gestützt	Führen Sie eine der folgenden Aufgaben aus: • Ändern Sie das AMI und die Instance, um einen aktuellen Kernel zu verwenden, und starten Sie die Instance neu. • Starten Sie die Instance neu.
Instance Store-Backup	Führen Sie eine der folgenden Aufgaben aus: • Beenden Sie die Instance. • Ändern Sie das AMI, um einen aktuellen Kernel zu verwenden, und starten Sie eine neue Instance mit dem geänderten AMI.

Beheben Sie Fehler beim Booten der Linux-Instance vom falschen Volume

> **Note**
>
> Dieses Thema zur Fehlerbehebung gilt nur für Linux-Instances.

In einigen Situationen stellen Sie möglicherweise fest, dass ein anderes Volume als das der Datei `/dev/xvda` oder `/dev/sda` angefügte als Stamm-Volume Ihrer Instance verwendet wird. Dies kann der Fall sein, wenn Sie das Stamm-Volume einer anderen Instance – oder ein aus dem Snapshot eines Stamm-Volumes erstelltes Volume – einer Instance mit einem vorhandenen Stamm-Volume angefügt haben.

Die Ursache ist in der Funktionsweise der anfänglichen Ramdisk in Linux zu suchen. Sie wählt das Volume, das als `/` in `/etc/fstab` definiert ist, aus und in einigen Verteilungen wird dies durch die Bezeichnung bestimmt, die der Volume-Partition angefügt ist. Ihre `/etc/fstab`-Datei sieht ähnlich aus wie im folgenden Beispiel dargestellt:

```
LABEL=/ / ext4 defaults,noatime 1 1
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
```

Wenn Sie die Bezeichnung beider Volumes überprüfen, stellen Sie fest, dass beide die `/`-Bezeichnung enthalten:

```
[ec2-user ~]$ sudo e2label /dev/xvda1
/
[ec2-user ~]$ sudo e2label /dev/xvdf1
/
```

In diesem Beispiel wird `/dev/xvdf1` möglicherweise zum Stammgerät, von dem aus Ihre Instance startet, nachdem die anfängliche Ramdisk ausgeführt wird, statt dass der Start wie beabsichtigt über das `/dev/xvda1`-Volume erfolgt. Um dies zu beheben, verwenden Sie denselben e2label-Befehl, um die Bezeichnung des angefügten Volumes zu ändern, von dem aus der Start nicht erfolgen soll.

In manchen Fällen kann dies durch die Angabe einer UUID in `/etc/fstab` gelöst werden. Wenn jedoch beide Volumes aus demselben Snapshot kommen oder das sekundäre Volume aus einem Snapshot des primären Volumes erstellt wird, haben sie eine gemeinsame UUID.

```
[ec2-user ~]$ sudo blkid
/dev/xvda1: LABEL="/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
/dev/xvdf1: LABEL="old/" UUID=73947a77-ddbe-4dc7-bd8f-3fe0bc840778 TYPE="ext4"
 PARTLABEL="Linux" PARTUUID=d55925ee-72c8-41e7-b514-7084e28f7334
```

So ändern Sie die Bezeichnung eines angefügten ext4- Volumes

1. Ändern Sie mit dem e2label-Befehl die Bezeichnung des Volumes, sodass sie nicht / lautet.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1 old/
   ```

2. Überprüfen Sie, dass das Volume über die neue Bezeichnung verfügt.

   ```
   [ec2-user ~]$ sudo e2label /dev/xvdf1
   old/
   ```

So ändern Sie die Bezeichnung eines angefügten xfs-Volumes

- Ändern Sie mit dem xfs_admin-Befehl die Bezeichnung des Volumes, sodass sie nicht / lautet.

  ```
  [ec2-user ~]$ sudo xfs_admin -L old/ /dev/xvdf1
  writing all SBs
  new label = "old/"
  ```

Nachdem Sie die Bezeichnung des Volumes wie gezeigt geändert haben, sollten Sie die Instance neu starten können und das richtige Volume sollte von der anfänglichen Ramdisk beim Start der Instance ausgewählt werden.

> **Important**
>
> Wenn Sie das Volume mit dem neuen Etikett trennen und an eine andere Instance zur Verwendung als Root-Volume zurückgeben möchten, müssen Sie das obige Verfahren erneut durchführen und das Volumeetikett wieder auf seinen ursprünglichen Wert setzen.

Andernfalls wird die andere Instance nicht gestartet, da die Ramdisk das Volume mit dem Etikett nicht finden kan `/`.

Beheben Sie Sysprep-Probleme mit Windows-Instanzen

> **Note**
>
> Dieses Thema zur Problembehandlung gilt nur für Windows-Instanzen.

Wenn Sie Probleme bei der Vorbereitung von Images haben oder Fehlermeldungen ausgegeben werden, prüfen Sie folgende Protokolle. Der Protokollspeicherort variiert, je nachdem, ob Sie EC2Config, EC2Launch v1 oder EC2Launch v2 mit Sysprep ausführen.

- `%WINDIR%\Panther\Unattendgc` (EC2Config, EC2Launch v1 und EC2Launch v2)
- `%WINDIR%\System32\Sysprep\Panther` (EC2Config, EC2Launch v1 und EC2Launch v2)
- `C:\Program Files\Amazon\Ec2ConfigService\Logs\Ec2ConfigLog.txt` (nur EC2Config)
- `C:\ProgramData\Amazon\Ec2Config\Logs` (nur EC2Config)
- `C:\ProgramData\Amazon\EC2-Windows\Launch\Log\EC2Launch.log` (nur EC2Launch v1)
- `%ProgramData%\Amazon\EC2Launch\log\agent.log` (nur EC2Launch v2)

Wenn bei der Vorbereitung von Images mit Sysprep eine Fehlermeldung ausgegeben wird, ist das Betriebssystem möglicherweise nicht erreichbar. Um die Protokolldateien zu überprüfen, halten Sie die Instance an, fügen Sie das Root-Volume einer anderen fehlerfreien Instance als sekundäres Volume an und prüfen Sie anschließend die zuvor erwähnten Protokolle für das sekundäre Volume. Weitere Informationen zum Zweck der Protokolldateien nach Namen finden Sie unter Windows Setup-bezogene Protokolldateien in der Microsoft-Dokumentation.

Wenn in der Unattendgc-Protokolldatei Fehler aufgeführt sind, verwenden Sie das Fehlersuchtool von Microsoft, um weitere Details zum Fehler zu erfahren. Das folgende in der Unattendgc-Protokolldatei aufgeführte Problem ergibt sich normalerweise aus einem oder mehreren fehlerhaften Benutzerprofilen in der Instance:

```
Error [Shell Unattend] _FindLatestProfile failed (0x80070003) [gle=0x00000003]
Error [Shell Unattend] CopyProfile failed (0x80070003) [gle=0x00000003]
```

Dieses Problem lässt sich auf zwei Arten lösen:

Option 1

Suchen Sie mit Regedit in der Instance nach folgendem Schlüssel. Überprüfen Sie, ob Profilregistrierungsschlüssel für gelöschte Benutzer vorhanden sind.

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
\ProfileList\
```

Option 2

1. Aktualisieren Sie die relevante Datei wie folgt:
   - Windows Server 2012 R2 und früher – bearbeiten Sie die EC2Config-Antwortdatei (`C:\Program Files\Amazon\Ec2ConfigService\sysprep2008.xml`).
   - Windows Server 2016 und 2019 – bearbeiten Sie die Antwortdatei „unattend.xml“ (`C:\ProgramData\Amazon\EC2-Windows\Launch\Sysprep\Unattend.xml`).
   - Windows Server 2022 – bearbeiten Sie die Antwortdatei „unattend.xml“ (`C:\ProgramData\Amazon\EC2Launch\sysprep\unattend.xml`).
2. Ändern Sie `<CopyProfile>true</CopyProfile>` zu `<CopyProfile>false</CopyProfile>`.
3. Führen Sie Sysprep erneut aus. Hinweis: Mit dieser Konfigurationsänderung wird das integrierte Administratorbenutzerprofil nach Abschluss von Sysprep gelöscht.

Verwenden von EC2Rescue für Linux

EC2Rescue für Linux ist ein Open-Source-Tool easy-to-use, das auf einer Amazon EC2 EC2-Linux-Instance ausgeführt werden kann, um mithilfe seiner Bibliothek mit über 100 Modulen häufig auftretende Probleme zu diagnostizieren und zu beheben. Ein paar verallgemeinerte Anwendungsfälle für EC2Rescue für Linux sind unter anderem das Erfassen von Syslog- und Paket-Manager-Protokollen, das Erfassen von Ressourcenauslastungsdaten und die Diagnose/das Beheben bekannter problematischer Kernelparameter und häufiger OpenSSH-Probleme.

Die `AWSSupport-TroubleshootSSH`-Runbook installiert EC2Rescue für Linux und verwendet dann das Tool, um häufig auftretende Probleme zu beheben, die eine Remote-Verbindung zu einem Linux-Computer über SSH verhindern. Weitere Informationen und zum Ausführen dieser Automatisierung finden Sie unter AWS Support-Support-TroubleshootSSH .

Wenn Sie eine Windows-Instance verwenden, finden Sie weitere Informationen unter. the section called “EC2Rescue for Windows Server”

Inhalt

Installieren EC2Rescue für Linux

Das Tool EC2Rescue für Linux kann in einer Amazon EC2-Linux-Instance installiert werden, die die folgenden Voraussetzungen erfüllt.

Voraussetzungen

- Unterstützte Betriebssysteme:
  - Amazon Linux 2
  - Amazon Linux 2016.09+
  - SUSE Linux Enterprise Server 12+
  - RHEL 7+
  - Ubuntu 16.04+
- Software-Anforderungen:
  - Python 2.7.9+ oder 3.2+

Die `AWSSupport-TroubleshootSSH`-Runbook installiert EC2Rescue für Linux und verwendet dann das Tool, um häufig auftretende Probleme zu beheben, die eine Remote-Verbindung zu einem Linux-Computer über SSH verhindern. Weitere Informationen und zum Ausführen dieser Automatisierung finden Sie unter AWS Support-Support-TroubleshootSSH .

Falls Ihr System die erforderliche Python-Version besitzt, können Sie den Standard-Build installieren. Andernfalls können Sie den Bundle-Build installieren, der eine minimale Kopie von Python enthält.

Installieren des Standard-Builds

1. Laden Sie in einer funktionierenden Linux-Instance das Tool EC2Rescue für Linux herunter:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz
```

2. (Optional) Vor dem Fortfahren können Sie optional die Signatur der EC2Rescue für Linux-Installationsdatei überprüfen. Weitere Informationen finden Sie unter (Optional) Überprüfen der Signatur von EC2Rescue für Linux.
3. Laden Sie die sha256-Hash-Datei herunter:

```
curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sha256
```

4. Überprüfen Sie die Integrität des Tarballs:

```
sha256sum -c ec2rl.tgz.sha256
```

5. Extrahieren Sie den Tarball:

```
tar -xzvf ec2rl.tgz
```

6. Überprüfen Sie die Installation, indem Sie die Hilfedatei aufrufen:

```
cd ec2rl-<version_number>
./ec2rl help
```

Installieren des Bundle-Builds

Einen Link zum Download und eine Liste der Einschränkungen finden Sie unter EC2Rescue für Linux auf Github.

(Optional) Überprüfen der Signatur von EC2Rescue für Linux

Der empfohlene Prozess zur Überprüfung der Gültigkeit des EC2Rescue für Linux-Pakets für Linux-basierte Betriebssysteme:

Wenn Sie eine Anwendung aus dem Internet herunterladen, empfehlen wir Ihnen, die Identität des Software-Publishers zu authentifizieren und sicherzustellen, dass die Anwendung nach ihrer Veröffentlichung nicht verändert oder beschädigt wurde. Dies schützt Sie davor, eine Version der Anwendung zu installieren, die einen Virus oder einen anderen bösartigen Code enthält.

Wenn Sie nach dem Ausführen der Schritte in diesem Thema feststellen, dass die Software für EC2Rescue für Linux verändert oder beschädigt wurde, führen Sie die Installationsdatei nicht aus. Wenden Sie sich stattdessen an Amazon Web Services.

EC2Rescue für Linux-Dateien für Linux-basierte Betriebssysteme werden unter Verwendung von GnuPG, einer Open-Source-Implementierung des Pretty Good Privacy (OpenPGP)-Standards für sichere digitale Signaturen, signiert. GnuPG (auch bekannt als GPG) ermöglicht Authentifizierung und Integritätsprüfung durch eine digitale Signatur. AWS veröffentlicht einen öffentlichen Schlüssel und Signaturen, die Sie verwenden können, um das heruntergeladene EC2Rescue-Paket für Linux zu überprüfen. Weitere Informationen zu PGP und GnuPG (GPG) finden Sie unter http://www.gnupg.org.

Der erste Schritt besteht darin, eine Vertrauensstellung mit dem Software-Publisher zu schaffen. Laden Sie den öffentlichen Schlüssel des Software-Publisher herunter, überprüfen Sie, ob der Besitzer des öffentlichen Schlüssels derjenige ist, der er behauptet zu sein, und fügen Sie dann den öffentlichen Schlüssel zu Ihrem Schlüsselbund hinzu. Ihr Schlüsselbund ist eine Sammlung von bekannten öffentlichen Schlüsseln. Nachdem Sie die Echtheit des öffentlichen Schlüssels überprüft haben, können Sie ihn verwenden, um die Signatur der Anwendung zu überprüfen.

Aufgaben

- Installieren der GPG-Tools
- Authentifizieren und Importieren des öffentlichen Schlüssels
- Verifizieren der Signatur des Pakets

Installieren der GPG-Tools

Wenn Sie das Betriebssystem Linux oder Unix verwenden, sind die GPG-Tools möglicherweise bereits installiert. Um zu testen, ob die Tools auf Ihrem System installiert sind, geben Sie an einer Eingabeaufforderung gpg2 ein. Wenn die GPG-Tools installiert sind, sehen Sie eine Eingabeaufforderung. Wenn die GPG-Tools nicht installiert sind, sehen Sie eine Fehlermeldung, die anzeigt, dass der Befehl nicht gefunden werden kann. Sie können das GnuPG-Paket von einem Repository aus installieren.

So installieren Sie GPG-Tools auf Debian-basiertem Linux

- Führen Sie von einem Terminal folgenden Befehl aus:

```
apt-get install gnupg2
```

So installieren Sie GPG-Tools unter Red-Hat-basiertem Linux

- Führen Sie von einem Terminal folgenden Befehl aus:

```
yum install gnupg2
```

Authentifizieren und Importieren des öffentlichen Schlüssels

Der nächste Schritt des Vorgangs besteht darin, den öffentlichen Schlüssel von EC2Rescue für Linux zu authentifizieren und ihn als vertrauenswürdigen Schlüssel Ihrem GPG-Schlüsselbund hinzuzufügen.

So authentifizieren und importieren Sie den öffentlichen Schlüssel von EC2Rescue für Linux

1. Verwenden Sie in einer Eingabeaufforderung den folgenden Befehl, um eine Kopie Ihres öffentlichen GPG-Schlüssels zu erhalten:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.key
   ```

2. Verwenden Sie bei einer Eingabeaufforderung in dem Verzeichnis, in dem Sie `ec2rl.key` gespeichert haben, den folgenden Befehl zum Importieren des öffentlichen Schlüssels EC2Rescue für Linux in den Schlüsselbund:

   ```
   gpg2 --import ec2rl.key
   ```

   Der Befehl gibt Ergebnisse wie die folgenden zurück:

   ```
   gpg: /home/ec2-user/.gnupg/trustdb.gpg: trustdb created
   gpg: key 2FAE2A1C: public key "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
    imported
   gpg: Total number processed: 1
   gpg:               imported: 1  (RSA: 1)
   ```

Verifizieren der Signatur des Pakets

Nachdem Sie die GPG-Tools installiert, den öffentlichen Schlüssel von EC2Rescue für Linux authentifiziert, importiert und überprüft haben, ob der öffentliche Schlüssel von EC2Rescue für Linux

vertrauenswürdig ist, sind Sie bereit, die Signatur des EC2Rescue für Linux-Installationsskripts zu überprüfen.

So überprüfen Sie die Signatur des EC2Rescue für Linux-Installationsskripts

1. Führen Sie bei einer Eingabeaufforderung den folgenden Befehl aus, um die Signaturdatei für das Installationsskript herunterzuladen:

   ```
   curl -O https://s3.amazonaws.com/ec2rescuelinux/ec2rl.tgz.sig
   ```

2. Überprüfen Sie die Signatur, indem Sie den folgenden Befehl an einer Eingabeaufforderung in dem Verzeichnis ausführen, in dem Sie `ec2rl.tgz.sig` und die EC2Rescue für Linux-Installationsdatei gespeichert haben. Beide Dateien müssen vorhanden sein.

   ```
   gpg2 --verify ./ec2rl.tgz.sig
   ```

   Die Ausgabe sollte wie folgt aussehen:

   ```
   gpg: Signature made Thu 12 Jul 2018 01:57:51 AM UTC using RSA key ID 6991ED45
   gpg: Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"
   gpg: WARNING: This key is not certified with a trusted signature!
   gpg:          There is no indication that the signature belongs to the owner.
   Primary key fingerprint: E528 BCC9 0DBF 5AFA 0F6C  C36A F780 4843 2FAE 2A1C
        Subkey fingerprint: 966B 0D27 85E9 AEEC 1146  7A9D 8851 1153 6991 ED45
   ```

   Wenn die Ausgabe den Begriff `Good signature from "ec2autodiag@amazon.com <EC2 Rescue for Linux>"` enthält, bedeutet dies, dass die Signatur erfolgreich überprüft wurde und Sie mit der Ausführung des EC2Rescue für Linux-Installationsskripts fortfahren können.

   Wenn die Ausgabe die Bezeichnung `BAD signature`enthält, überprüfen Sie, ob Sie das Verfahren korrekt durchgeführt haben. Wenn Sie diese Antwort weiterhin erhalten, kontaktieren Sie Amazon Web Services und führen Sie die Installationsdatei, die Sie zuvor heruntergeladen haben, nicht aus.

Im Folgenden finden Sie Details zu den Warnungen, die möglicherweise angezeigt werden:

- WARNING: This key is not certified with a trusted signature! There is no indication that the signature belongs to the owner. Dies bezieht sich auf Ihr persönliches Vertrauen im Glauben, dass Sie einen authentischen öffentlichen Schlüssel für EC2Rescue für Linux besitzen. In einer

idealen Welt würden Sie ein Amazon Web Services-Büro aufsuchen und den Schlüssel persönlich erhalten. Doch häufiger laden Sie ihn von einer Website herunter. In diesem Fall handelt es sich bei der Website um eine Amazon Web Services-Website.

- gpg2: no ultimately trusted keys found. Dies bedeutet, dass der bestimmte Schlüssel nicht "endgültig vertrauenswürdig" für Sie oder für andere Personen ist, denen Sie vertrauen.

Weitere Informationen finden Sie unter http://www.gnupg.org.

Arbeiten mit EC2Rescue für Linux

Die folgenden Aufgaben können Sie als erste Schritte mit diesem Tool durchführen.

Aufgaben

- Führen Sie Folgendes aus:EC2Rescue für Linux
- Hochladen der Ergebnisse
- Erstellen von Backups
- Hilfe anfordern

Führen Sie Folgendes aus:EC2Rescue für Linux

Sie können EC2Rescue für Linux wie in den folgenden Beispielen ausführen.

Example Beispiel: alle Module ausführen

Um alle Module auszuführen, führen Sie EC2Rescue für Linux ohne Optionen aus:

```
./ec2rl run
```

Einige Module erfordern Root-Zugriff. Falls Sie kein Root-Benutzer sind, verwenden Sie sudo, um diese Module folgendermaßen auszuführen:

```
sudo ./ec2rl run
```

Example Beispiel: Ein spezifisches Modul ausführen

Um nur bestimmte Module auszuführen, verwenden Sie den Parameter --only-modules:

```
./ec2rl run --only-modules=module_name --arguments
```

Beispiel: Bei diesem Befehl wird das dig-Modul ausgeführt, um die `amazon.com`-Domäne abzufragen:

```
./ec2rl run --only-modules=dig --domain=amazon.com
```

Example Beispiel: Ergebnisse anzeigen

Sie können die Ergebnisse in anzeige `/var/tmp/ec2rl`:

```
cat /var/tmp/ec2rl/logfile_location
```

Beispiel: Zeigen Sie die Protokolldatei für das dig-Modul an.

```
cat /var/tmp/ec2rl/2017-05-11T15_39_21.893145/mod_out/run/dig.log
```

Hochladen der Ergebnisse

Wenn Sie AWS Support die Ergebnisse angefordert haben oder die Ergebnisse aus einem S3-Bucket teilen möchten, laden Sie sie mit dem CLI Tool EC2Rescue for Linux hoch. In der Ausgabe des EC2Rescue für Linux-Befehls sollten die Befehle aufgeführt sein, die Sie verwenden müssen.

Example Beispiel: Ergebnisse hochladen AWS Support

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --support-url="URLProvidedByAWSSupport"
```

Example Beispiel: Ergebnisse in einen S3-Bucket hochladen

```
./ec2rl upload --upload-directory=/var/tmp/ec2rl/2017-05-11T15_39_21.893145 --presigned-url="YourPresignedS3URL"
```

Weitere Informationen zum Generieren vorsignierter URLs für Amazon S3 finden Sie unter Hochladen von Objekten mithilfe vorsignierter URLs.

Erstellen von Backups

Erstellen Sie eine Sicherung für Ihre Instance, für ein oder mehrere Volumes oder für eine bestimmte Geräte-ID, indem Sie die folgenden Befehle verwenden.

Example Beispiel: Eine Instance mit einem Amazon Machine Image (AMI) sichern

```
./ec2rl run --backup=ami
```

Example Beispiel: Alle Volumes, die der Instance zugeordnet sind, sichern

```
./ec2rl run --backup=allvolumes
```

Example Beispiel: Ein spezifisches Volume sichern

```
./ec2rl run --backup=volumeID
```

Hilfe anfordern

In EC2Rescue für Linux ist eine Hilfedatei enthalten, in der Sie Informationen zu jedem verfügbaren Befehl und zur jeweiligen Syntax finden können.

Example Beispiel: Die allgemeine Hilfe anzeigen

```
./ec2rl help
```

Example Beispiel: Die verfügbaren Module auflisten

```
./ec2rl list
```

Example Beispiel: Die Hilfe für ein spezifisches Modul anzeigen

```
./ec2rl help module_name
```

Verwenden Sie z. B. den folgenden Befehl, um die Hilfedatei für das dig-Modul anzuzeigen:

```
./ec2rl help dig
```

Entwickeln von EC2Rescue-Modulen

Module werden in YAML geschrieben, einem Datenserialisierungsstandard. Die YAML-Datei für ein Modul besteht aus einem einzigen Dokument für die Beschreibung des Moduls und seiner Attribute.

Hinzufüge von Modulattributen

In der folgenden Tabelle werden die verfügbaren Modulattribute aufgeführt.

Attribut	Beschreibung
name	Der Name des Moduls. Die Länge des Namens sollte höchstens 18 Zeichen betragen.
Version	Die Versionsnummer des Moduls
Titel	Eine kurze, aussagekräftige Beschreibung des Moduls. Die Länge dieses Werts sollte höchstens 50 Zeichen betragen.

helptext	Die ausführliche Beschreibung des Moduls. Die Länge jeder Zeile sollte höchstens 75 Zeichen betragen. Wenn das Modul mit (obligatorischen oder optionalen) Argumenten aufgerufen wird, sollten sie in dem helptext-Wert einhalten sein.
	
	Beispiel:
	
	`helptext: !!str |`
	`  Collect output from ps for system analysis`
	`  Consumes --times= for number of times to repeat`
	`  Consumes --period= for time period between repetition`

placement	Die Stufe, in der das Modul ausgeführt werden sollte. Unterstützte Werte: • prediagnostic • run • postdiagnostic

Attribut	Beschreibung
language	Die Sprache, in der das Modul geschrieben wurde. Unterstützte Werte: • bash • python **Note** Python-Code muss sowohl mit Python 2.7.9+ als auch mit Python 3.2+ kompatibel sein.
remediation	Zeit an, ob das Modul eine Problembehebung unterstützt. Unterstützte Werte sind `True` oder `False`. Das Modul ist standardmäßig `False`, wenn diese Angabe fehlt, womit sie zu einem optionalen Attribut für Module wird, die keine Problembehebung unterstützen.
content	Der gesamte Code für das Skript.
constraint	Der Name des Objekts, das Werte für die Beschränkung enthält.
Domain	Eine Beschreibung, wie das Modul gruppiert oder klassifiziert wird. Die enthaltenen Module verwenden die folgenden Bereiche: • Anwendung • net • os • Leistung

Attribut	Beschreibung
class	Eine Beschreibung der Aufgabe, die von dem Modul durchgeführt wird. Die enthaltenen Module verwenden die folgenden Klassen: • collect (erfasste die Ausgabe von Programmen) • diagnose (bestanden/durchgefallen auf Basis einer Reihe von Kriterien) • gather (kopiert Dateien und schriebt in bestimmte Dateien)
distro	Die Liste der Linux-Distributionen, die dieses Modul unterstützt. Die enthaltenen Module verwenden die folgenden Distributionen: • alami (Amazon Linux) • rhel • ubuntu • suse
Erforderlich	Die obligatorischen Argumente für den Aufruf des Moduls mit dem CLI.
optional	Die optionalen Argumente für den Aufruf des Moduls.
software	Die ausführbare Software, die in dem Modul verwendet wird. Dieses Attribut dient der Spezifikation von Software, die nicht standardm äßig installiert ist. Die Logik von EC2Rescue für Linux stellt vor der Ausführung des Moduls sicher, dass diese Programme vorhanden sind und ausgeführt werden können.

Attribut	Beschreibung
package	Das Quellcode-Paket für eine ausführbare Software. Dieses Attribut dient der Spezifikation ausführlicher Details zu dem Softwarepaket, einschließlich einer URL, unter der weitere Informationen heruntergeladen oder abgerufen werden können.
sudo	Zeigt an, ob für die Ausführung des Moduls Root-Berechtigungen erforderlich sind. Sie müssen keine sudo-Checks in dem Skript für das Modul implementieren. Wenn dieser Wert auf „true” gesetzt wird, führt die EC2Rescue für Linux-Logik das Modul nur aus, wenn der ausführende Benutzer über Root-Berechtigungen verfügt.
perfimpact	Zeigt an, ob das Modul signifikante Auswirkungen auf die Leistung in der Umgebung haben kann, in der es ausgeführt wird. Wenn dieser Wert auf „true” gesetzt und das `--perfimpact=true` -Argument nicht aufgerufen wird, dann wird das Modul übersprungen.
parallelexclusive	Spezifiziert ein Programm, dass gegenseitige Exklusivität erfordert. So können z. B. alle Module, für die hier „bpf” angegeben wird, nur nacheinander ausgeführt werden.

Hinzufügen von Umgebungsvariablen

In der folgenden Tabelle werden die verfügbaren Umgebungsvariablen aufgeführt.

Umgebungsvariable	Beschreibung
EC2RL_CALLPATH	Der Pfad zu `ec2rl.py`. Anhand dieses Pfades können Sie das Lib-Verzeichnis finden und von Anbietern bereitgestellte Python-Module benutzen.
EC2RL_WORKDIR	Das primäre temporäre Verzeichnis für das Diagnosetool Standardwer: `/var/tmp/ec2rl` .
EC2RL_RUNDIR	Das Verzeichnis, in dem alle Ausgaben gespeichert werden Standardwer: `/var/tmp/ec2rl/<date&timestamp>` .
EC2RL_GATHEREDDIR	Das Stammverzeichnis für die erfassten Moduldaten Standardwer:`/var/tmp/ec2rl/<date&timestamp>/mod_out/gathered/` .
EC2RL_NET_DRIVER	Der Treiber für die erste, alphabetisch sortierte , nicht virtuelle Netzwerkschnittstelle in der Instance Beispiele: • xen_netfront • ixgbevf • ena
EC2RL_SUDO	„true”, wenn EC2Rescue für Linux mit Root-Berechtigungen ausgeführt wird; andernfalls „false”

Umgebungsvariable	Beschreibung
`EC2RL_VIRT_TYPE`	Der Virtualisierungstyp gemäß der bereitgestellten Instance-Metadaten Beispiele: • default-hvm • default-paravirtual
`EC2RL_INTERFACES`	Eine nummerierte List der Schnittstellen in dem System. Der Wert besteht aus einer Zeichenfolge, die Namen wie `eth0`, `eth1` usw. enthält. Er wird über `functions.bash` generiert und ist nur für Module verfügbar, die diese aufgerufen haben.

Verwenden des YAML-Syntax

Beachten Sie unbedingt die folgenden Punkte, wenn Sie die YAML-Dateien für ein Modul erstellen:

- Drei Bindestriche hintereinander (`---`) zeigen den Beginn eines Dokuments explizit an.
- Der Tag `!ec2rlcore.module.Module` zeigt dem YAML-Parser an, welcher Konstruktor aufgerufen werden soll, um das Objekt aus dem Datenstrom zu erstellen. Sie finden den Konstruktor in der Datei `module.py`.
- Der Tag `!!str` weist den YAML-Parser an, keinen Versuch zur Bestimmung des Datentyps zu unternehmen, sondern den Inhalt als Zeichenfolgeliteral zu interpretieren.
- Das Pipe-Zeichen (`|`) zeigt dem YAML-Parser an, dass es sich um einen skalaren Wert handelt – ähnlich einem Literal. In diesem Fall übernimmt der Parser alle Leerraumzeichen. Dies ist im Zusammenhang mit Modulen sehr wichtig, da Einrückungen und Zeilenumbrüche erhalten bleiben.
- Die Standardeinrückung in YAML besteht aus zwei Leerzeichen, wie in den folgenden Beispielen gezeigt. Stellen Sie sicher, dass Sie in Ihrem Skript mit den jeweiligen Standard-Einrückungen arbeiten (z. B. vier Leerzeichen in Python) und den gesamten Inhalt anschließend in der Moduldatei um zwei Leerzeichen einrücken.

Beispielmodule

Beispiel 1 (`mod.d/ps.yaml`):

```
--- !ec2rlcore.module.Module
# Module document. Translates directly into an almost-complete Module object
name: !!str ps
path: !!str
version: !!str 1.0
title: !!str Collect output from ps for system analysis
helptext: !!str |
  Collect output from ps for system analysis
  Requires --times= for number of times to repeat
  Requires --period= for time period between repetition
placement: !!str run
package:
  - !!str
language: !!str bash
content: !!str |
  #!/bin/bash
  error_trap()
  {
      printf "%0.s=" {1..80}
      echo -e "\nERROR: "$BASH_COMMAND" exited with an error on line ${BASH_LINENO[0]}"
      exit 0
  }
  trap error_trap ERR

  # read-in shared function
  source functions.bash
  echo "I will collect ps output from this $EC2RL_DISTRO box for $times times every
 $period seconds."
  for i in $(seq 1 $times); do
      ps auxww
      sleep $period
  done
constraint:
  requires_ec2: !!str False
  domain: !!str performance
  class: !!str collect
  distro: !!str alami ubuntu rhel suse
  required: !!str period times
  optional: !!str
  software: !!str
```

```
  sudo: !!str False
  perfimpact: !!str False
  parallelexclusive: !!str
```

Verwenden von EC2Rescue for Windows Server

EC2Rescue for Windows Server ist ein easy-to-use Tool, das Sie auf einer Amazon EC2 Windows Server-Instance ausführen, um mögliche Probleme zu diagnostizieren und zu beheben. Das Tool ist nützlich zum Sammeln von Protokolldateien, zur Behebung von Problemen und zur proaktiven Suche nach möglichen Problembereichen. Es kann sogar Amazon EBS-Stamm-Volumes von anderen Instances untersuchen und relevante Protokolle zur Fehlerbehebung bei Windows-Server-Instances mithilfe des entsprechenden Volumes erfassen.

EC2Rescue for Windows Server hat zwei verschiedene Module: ein Datensammlungsmodul, das Daten aus vielen verschiedenen Quellen sammelt, und ein Analysemodul, das die gesammelten Daten nach einer Reihe vordefinierter Regeln analysiert, um Probleme zu erfassen und Vorschläge zu unterbreiten.

Das Tool EC2Rescue for Windows Server läuft nur auf Amazon EC2 EC2-Instances, auf denen Windows Server 2012 und höher ausgeführt wird. Wenn das Tool startet, überprüft es, ob es auf einer Amazon EC2 Instance ausgeführt wird.

Das `AWSSupport-ExecuteEC2Rescue`-Runbook verwendet das Tool EC2Rescue, um Probleme zu beheben und, sofern möglich, allgemeine Verbindungsprobleme mit der angegebenen EC2-Instance zu beheben. Weitere Informationen und Informationen zum Ausführen dieser Automatisierung finden Sie unter -executeEC2Rescue. AWSSupport

Wenn Sie eine Linux-Instanz verwenden, finden Sie weitere Informationen unter. the section called “EC2Rescue for Linux”

Inhalt

Benutzen von EC2Rescue for Windows Server-GUI

EC2Rescue for Windows Server kann die folgende Analyse bei Offline-Instances durchführen:

Option	Beschreibung

Diagnose und Datenrettung	EC2Rescue for Windows Server kann Probleme mit den folgenden Service-Einstellungen erkennen und beheben:
	• Systemzeit
	  • RealTimeisUniversal - Erkennt, ob der `RealTimeisUniversal` Registrierungsschlüssel aktiviert ist. Andernfalls weicht die Windows-Systemzeit ab, wenn die Zeitzone auf einen anderen Wert als UTC eingestellt ist.
	• Windows-Firewall
	  • Domain networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist.
	  • Private networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist.
	  • Guest or public networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist.
	• Remotedesktop
	  • Service Start – Erkennt, ob der Remote Desktop Service aktiviert ist.
	  • Remote Desktop Connections – Erkennt, ob diese Funktion aktiviert ist.
	  • TCP Port – Erkennt, welchen Port der Remote Desktop Service überwacht.

Option	Beschreibung

	• EC2Config (Windows Server 2012 R2 und früher)
	  • Installation – Erkennt, welche EC2Config-Version installiert ist.
	  • Service Start – Erkennt, ob der EC2Config-Service aktiviert ist.
	  • Ec2 SetPassword - Generiert ein neues Administratorkennwort.
	  • Ec2 HandleUser Data - Ermöglicht es Ihnen, beim nächsten Start der Instance ein Benutzerdatenskript auszuführen.
	• EC2Launch (Windows Server 2016 und höher)
	  • Installation – Erkennt, welche EC2Launch-Version installiert ist.
	  • Ec2 SetPassword - Generiert ein neues Administratorkennwort.
	• Netzwerkschnittstelle
	  • DHCP Service Startup – Erkennt, ob der DHCP-Service aktiviert ist.
	  • Ethernet detail – Zeigt Informationen zur Netzwerktreiber-Version an, falls diese erkannt wird.
	  • DHCP on Ethernet – Erkennt, ob DHCP aktiviert ist.
	• Festplattensignaturstatus
	  • Signature on disk und Signature on Boot Configuration Database (BCD) – erkennt, ob die Festplattensignatur und die BCD-Signatur identisch sind. Wenn die Werte

Option	Beschreibung
	unterschiedlich sind, versucht EC2Rescue, die Festplattensignatur mit der Signatur auf BCD zu überschreiben.
Wiederherstellung	Durchführen einer der folgenden Aktionen: • Last Known Good Configuration – Versucht, die Instance im letzten bekannten bootfähig en Zustand zu starten. • Restore registry from backup – Stellt die Registrierung aus `\Windows\System32\config\RegBack` wieder her.
Erfassen von Protokollen	Erlaubt das Erfassen von Protokollen in der Instance zur Analyse.

EC2Rescue for Windows Server kann die folgenden Daten aus aktiven und Offline-Instances erfassen:

Item	Beschreibung
Ereignisprotokoll	Sammelt Anwendungs-, System- und EC2Config-Ereignisprotokolle.
Registrierung	Sammelt `SYSTEM`- und `SOFTWARE`-Hives.
Windows-Aktualisierungsprotokoll	Sammelt vom Windows Update generierte Protokolldateien. **Note** In Windows Server 2016 und höher wird das Protokoll im Format Ereignisa blaufverfolgung für Windows (ETW) gesammelt.

Item	Beschreibung
Sysprep-Protokoll	Sammelt vom Windows-Systemvorbereitungs-Tool generierte Protokolldateien.
Driver-Setup-Protokoll	Sammelt Windows-SetupAPI-Protokolle (`setupapi.dev.log` und `setupapi.setup.log`).
Boot-Konfiguration	Sammelt `HKEY_LOCAL_MACHINE\BCD00000000` -Hive.
Speicherabbild	Sammelt alle existierenden Speicherabbilddateien in der Instance.
EC2Config-Datei	Sammelt vom EC2Config-Service generierte Protokolldateien.
EC2Launch-Datei	Sammelt von den EC2Launch-Skripts generierte Protokolldateien.
SSM-Agent-Datei	Sammelt vom SSM-Agenten generierte Protokolldateien und Patch-Manager-Protokolle.
EC2-ElasticGPUs-Datei	Erfasst Ereignisprotokolle mit Bezug auf Elastic GPUs.
ECS	Sammelt Protokolle im Zusammenhang mit Amazon ECS.
CloudEndure	Sammelt Protokolldateien, die sich auf den CloudEndure Agenten beziehen.

EC2Rescue for Windows Server kann folgende zusätzliche Daten aus aktiven Instances sammeln:

Item	Beschreibung
Systeminformationen	Sammelt MSInfo32.
Ergebnis der Gruppenrichtlinie	Erfasst einen Bericht zu einer Gruppenrichtlinie.

Analysieren einer Offline-Instance

Die Offline Instance-Option ist nützlich zur Fehlerbehebung von Startproblemen bei Windows-Instances.

So führen Sie eine Aktion bei einer Offline-Instance aus

1. Laden Sie von einer funktionierenden Windows Server-Instance das Tool EC2Rescue for Windows Server herunter und extrahieren Sie die Dateien.

   Sie können den folgenden PowerShell Befehl ausführen, um EC2Rescue herunterzuladen, ohne Ihre verstärkte Sicherheitskonfiguration (ESC) für Internet Explorer zu ändern:

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Durch diesen Befehl wird die EC2Rescue-.zip-Datei auf das Desktop des aktuell angemeldeten Benutzers heruntergeladen.

   > **Note**
   >
   > Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:
   >
   > ```
   > [Net.ServicePointManager]::SecurityProtocol =
   >  [Net.SecurityProtocolType]::Tls12
   > ```

2. Halten Sie die fehlerhafte Instance an, falls Sie das noch nicht getan haben.

3. Trennen Sie das EBS-Stamm-Volume von der fehlerhaften Instance, und fügen Sie das Volume an eine funktionierende Windows-Instance an, auf der EC2Rescue for Windows Server installiert ist.
4. Führen Sie das Tool EC2Rescue for Windows Server bei der funktionierenden Instance aus, und wählen Sie Offline Instance aus.
5. Wählen Sie die Festplatte mit dem neu gemounteten Volume und anschließend Next aus.
6. Bestätigen Sie die Festplattenauswahl und wählen Sie Yes aus.
7. Wählen Sie die Offline-Instance-Option zur Durchführung und anschließend Next aus.

Das Tool EC2Rescue for Windows Server scannt das Volume und sammelt basierend auf den ausgewählten Protokolldateien Informationen zur Fehlerbehebung.

Sammeln von Daten aus einer aktiven Instance

Sie können Protokolle und andere Daten aus einer aktiven Instance sammeln.

So sammeln Sie Daten aus einer aktiven Instance

1. Herstellen einer Verbindung mit Ihrer Windows-Instance.
2. Laden Sie das Tool EC2Rescue for Windows Server in Ihre Windows-Instance herunter und extrahieren Sie die Dateien.

   Sie können den folgenden PowerShell Befehl ausführen, um EC2Rescue herunterzuladen, ohne Ihre Internet Explorer Enhanced Security Configuration (ESC) zu ändern:

   ```
   Invoke-WebRequest https://s3.amazonaws.com/ec2rescue/windows/EC2Rescue_latest.zip -
   OutFile $env:USERPROFILE\Desktop\EC2Rescue_latest.zip
   ```

   Durch diesen Befehl wird die EC2Rescue-.zip-Datei auf das Desktop des aktuell angemeldeten Benutzers heruntergeladen.

   > **Note**
   >
   > Wenn beim Herunterladen der Datei eine Fehlermeldung angezeigt wird und Sie Windows Server 2016 oder eine frühere Version verwenden, muss TLS 1.2 möglicherweise für Ihr PowerShell Terminal aktiviert werden. Sie können TLS 1.2 für die

aktuelle PowerShell Sitzung mit dem folgenden Befehl aktivieren und es dann erneut versuchen:

```
[Net.ServicePointManager]::SecurityProtocol =
 [Net.SecurityProtocolType]::Tls12
```

3. Öffnen Sie die Anwendung EC2Rescue for Windows Server, und akzeptieren Sie die Lizenzvereinbarung.
4. Wählen Sie Next, Current instance, Capture logs.
5. Wählen Sie die Datenelemente, die gesammelt werden sollen, und anschließend Collect... aus. Lesen Sie den Warnhinweis, und wählen Sie zum Fortfahren Yes aus.
6. Wählen Sie einen Dateinamen und einen Speicherort für die ZIP-Datei und anschließend Save aus.
7. Wenn der Vorgang von EC2Rescue for Windows Server abgeschlossen ist, wählen Sie Open Containing Folder aus, um die ZIP-Datei anzuzeigen.
8. Klicken Sie auf Finish.

Verwenden von EC2Rescue for Windows Server mit der Befehlszeile

Mit der EC2Rescue for Windows Server-Befehlszeilenschnittstelle (command line interface, CLI) können Sie ein EC2Rescue for Windows Server-Plug-in (wird auch als Aktion bezeichnet) programmgesteuert ausführen.

Das Tool EC2Rescue for Windows Server weist zwei Ausführungsmodi auf:

- /online — Damit können Sie Aktionen in der Instance ausführen, in der EC2Rescue for Windows Server installiert wurde, z. B. Protokolldateien erfassen.
- /offline:<device_id> — Damit können Sie Aktionen auf dem Offline-Stamm-Volumen ausführen, das der separaten Amazon EC2-Windows-Instance zugeordnet ist, in der EC2Rescue for Windows Server installiert wurde.

Laden Sie das Tool EC2Rescue for Windows Server in Ihre Windows-Instance herunter und extrahieren Sie die Dateien. Sie können die Hilfedatei mit dem folgenden Befehl anzeigen:

```
EC2RescueCmd.exe /help
```

EC2Rescue for Windows Server kann die folgenden Aktionen in einer Amazon EC2-Windows-Instance ausführen:

- Erfassen-Aktion
- Rettungsaktion
- Wiederherstellen-Aktion

Erfassen-Aktion

> **Note**
>
> Sie können alle Protokolle, eine ganze Protokollgruppe oder ein einzelnes Protokoll in einer Gruppe erfassen.

EC2Rescue for Windows Server kann die folgenden Daten aus aktiven und Offline-Instances erfassen.

Protokollgruppe	Verfügbare Protokolle	Beschreibung
`all`		Erfasst alle verfügbaren Protokolle.
`eventlog`	• `'Application'` • `'System'` • `'EC2ConfigService'`	Sammelt Anwendungs-, System- und EC2Config-Ereignisprotokolle.
`memory-dump`	• `'Memory Dump File'` • `'Mini Dump Files'`	Sammelt alle existierenden Speicherabbilddateien in der Instance.
`ec2config`	• `'Log Files'` • `'Configuration Files'`	Sammelt vom EC2Config-Service generierte Protokoll dateien.

Protokollgruppe	Verfügbare Protokolle	Beschreibung
`ec2launch`	• `'Logs'` • `'Config'`	Sammelt von den EC2Launch -Skripts generierte Protokoll dateien.
`ssm-agent`	• `'Log Files'` • `'Patch Baseline Logs'` • `'InstanceData'`	Sammelt vom SSM-Agenten generierte Protokolldateien und Patch-Manager-Prot okolle.
`sysprep`	`'Log Files'`	Sammelt vom Windows-S ystemvorbereitungs-Tool generierte Protokolldateien.
`driver-setup`	• `'SetupAPI Log Files'` • `'DPInst Log File'` • `'AWS PV Setup Log File'`	Sammelt Windows-SetupAPI-Protokolle (`setupapi.dev.log` und `setupapi.setup.log`).
`registry`	• `'SYSTEM'` • `'SOFTWARE'` • `'BCD'`	Sammelt `SYSTEM`- und `SOFTWARE`-Hives.
`egpu`	• `'Event Log'` • `'System Files'`	Erfasst Ereignisprotokolle mit Bezug auf Elastic GPUs.
`boot-config`	`'BCDEDIT Output'`	Sammelt `HKEY_LOCAL_MACHINE\BCD00000000` -Hive.

Protokollgruppe	Verfügbare Protokolle	Beschreibung
`windows-update`	`'Log Files'`	Sammelt vom Windows Update generierte Protokoll dateien. **Note** In Windows Server 2016 und höher wird das Protokoll im Format Ereignisa blaufverfolgung für Windows (ETW) gesammelt.
`cloudendure`	• `'Migrate Script Logs'` • `'Driver Logs'` • `'CloudEndure File List'`	Sammelt Protokolldateien, die sich auf den CloudEndure Agenten beziehen.

EC2Rescue for Windows Server kann folgende zusätzliche Daten aus aktiven Instances sammeln.

Protokollgruppe	Verfügbare Protokolle	Beschreibung
`system-info`	`'MSInfo32 Output'`	Sammelt `MSInfo32`.
`gpresult`	`'GPResult Output'`	Erfasst einen Bericht zu einer Gruppenrichtlinie.

Die folgenden Optionen sind verfügbar:

- /output: <output FilePath > - Erforderlicher Zieldateipfad zum Speichern der gesammelten Protokolldateien im ZIP-Format.

- /no-offline – Optionales Attribut, das im Offline-Modus verwendet wird. Setzt das Volume nach Abschluss der Aktion nicht auf offline.
- /no-fix-signature – Optionales Attribut, das im Offline-Modus verwendet wird. Korrigiert eine mögliche Datenträger-Signaturkollision nach Abschluss der Aktion nicht.

Beispiele

In den folgenden Beispielen wird die EC2Rescue for Windows Server-CLI verwendet.

Beispiele für den Online-Modus

Erfassen aller verfügbaren Protokolle:

```
EC2RescueCmd /accepteula /online /collect:all /output:<outputFilePath>
```

Erfassen nur einer bestimmten Protokollgruppe:

```
EC2RescueCmd /accepteula /online /collect:ec2config /output:<outputFilePath>
```

Erfassen einzelner Protokolle in einer Protokollgruppe:

```
EC2RescueCmd /accepteula /online /collect:'ec2config.Log Files,driver-setup.SetupAPI
 Log Files' /output:<outputFilePath>
```

Beispiele für den Offline-Modus

Erfassen aller verfügbaren Protokolle in einem EBS-Volume. Das Volume wird durch den device_id-Wert angegeben.

```
EC2RescueCmd /accepteula /offline:xvdf /collect:all /output:<outputFilePath>
```

Erfassen nur einer bestimmten Protokollgruppe:

```
EC2RescueCmd /accepteula /offline:xvdf /collect:ec2config /output:<outputFilePath>
```

Rettungsaktion

EC2Rescue for Windows Server kann Probleme mit den folgenden Service-Einstellungen erkennen und beheben:

Servicegruppe	Verfügbare Aktionen	Beschreibung
`all`		
`system-time`	`'RealTimeIsUniversal'`	Systemzeit • RealTimeisUniversal - Erkennt, ob der `RealTimeisUniversal` Registrierungsschlüssel aktiviert ist. Andernfalls weicht die Windows-Systemzeit ab, wenn die Zeitzone auf einen anderen Wert als UTC eingestellt ist.
`firewall`	• `'Domain networks'` • `'Private networks'` • `'Guest or public networks'`	Windows-Firewall • Domain networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist. • Private networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist. • Guest or public networks – Erkennt, ob dieses Windows-Firewall-Profil aktiviert oder deaktiviert ist.
rdp	• `'Service Start'` • `'Remote Desktop Connections'` • `'TCP Port'`	Remotedesktop • Service Start – Erkennt, ob der Remote Desktop Service aktiviert ist.

Servicegruppe	Verfügbare Aktionen	Beschreibung
		• Remote Desktop Connections – Erkennt, ob diese Funktion aktiviert ist. • TCP Port – Erkennt, welchen Port der Remote Desktop Service überwacht.
`ec2config`	• `'Service Start'` • `'Ec2SetPassword'` • `'Ec2HandleUserData'`	EC2Config • Service Start – Erkennt, ob der EC2Config-Service aktiviert ist. • Ec2 SetPassword - Generiert ein neues Administratorkennwort. • Ec2 HandleUser Data - Ermöglicht es Ihnen, beim nächsten Start der Instance ein Benutzerdatenskript auszuführen.
`ec2launch`	`'Reset Administrator Password'`	Generiert ein neues Windows-Administratorpasswort.
`network`	`'DHCP Service Startup'`	Netzwerkschnittstelle • DHCP Service Startup – Erkennt, ob der DHCP-Service aktiviert ist.

Die folgenden Optionen sind verfügbar:

- /level:<level> – Optionales Attribut für die Prüfstufe, die durch die Aktion ausgelöst werden sollte. Die zulässigen Werte lauten: `information`, `warning`, `error`, `all`. Standardmäßig ist der Wert eingestell `error`.

- /check-only – Optionales Attribut, das einen Bericht generiert, aber keine Änderungen am Offline-Volume vornimmt.

> **Note**
>
> Wenn EC2Rescue für Windows Server eine mögliche Kollision mit der Festplattensignatur erkennt, wird die Signatur standardmäßig nach Abschluss des Offline-Vorgangs korrigiert, auch wenn Sie die Option verwenden. `/check-only` Sie müssen die `/no-fix-signature` Option verwenden, um die Korrektur zu verhindern.

- /no-offline – Optionales Attribut, das verhindert, dass das Volume nach Abschluss der Aktion auf offline gesetzt wird.
- /no-fix-signature – Optionales Attribut, das eine mögliche Datenträger-Signaturkollision nach Abschluss der Aktion nicht korrigiert.

Beispiele für Rettungen

In den folgenden Beispielen wird die EC2Rescue for Windows Server-CLI verwendet. Das Volume wird durch den device_id-Wert angegeben.

Der Versuch, alle erkannten Probleme auf einem Volume zu beheben:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:all
```

Der Versuch, alle Probleme in einer Servicegruppe auf einem Volume zu beheben:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:firewall
```

Der Versuch, ein bestimmtes Problem in einer Servicegruppe auf einem Volume zu beheben:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:rdp.'Service Start'
```

Der Versuch, mehrere Probleme anzugeben und auf einem Volume zu beheben:

```
EC2RescueCmd /accepteula /offline:xvdf /rescue:'system-
time.RealTimeIsUniversal,ec2config.Service Start'
```

Wiederherstellen-Aktion

EC2Rescue for Windows Server kann Probleme mit den folgenden Service-Einstellungen erkennen und beheben:

Servicegruppe	Verfügbare Aktionen	Beschreibung
Wiederherstellen der letzten bekannten funktionierenden Konfiguration	`lkgc`	Last Known Good Configuration – Versucht, die Instance im letzten bekannten bootfähigen Zustand zu starten.
Wiederherstellen der Windows-Registrierung aus der letzten Sicherung	`regback`	Restore registry from backup – Stellt die Registrierung aus `\Windows\System32\config\RegBack` wieder her.

Die folgenden Optionen sind verfügbar:

- /no-offline — Optionales Attribut, das verhindert, dass das Volume nach Abschluss der Aktion auf offline gesetzt wird.
- /no-fix-signature— Optionales Attribut, das eine mögliche Datenträger-Signaturkollision nach Abschluss der Aktion nicht korrigiert.

Beispiele für Wiederherstellungen

In den folgenden Beispielen wird die EC2Rescue for Windows Server-CLI verwendet. Das Volume wird durch den device_id-Wert angegeben.

Wiederherstellen der letzten bekannten funktionierenden Konfiguration für ein Volume:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:lkgc
```

Wiederherstellen der letzten Sicherung der Windows-Registrierung eines Volumes:

```
EC2RescueCmd /accepteula /offline:xvdf /restore:regback
```

Verwenden von EC2Rescue for Windows Server mit Systems Manager Run Command

AWS Support bietet Ihnen ein Systems Manager Run Command-Dokument als Schnittstelle zu Ihrer Systems Manager-fähigen Instanz, um EC2Rescue für Windows Server auszuführen. Das Run Command-Dokument hat den Namen `AWSSupport-RunEC2RescueForWindowsTool`.

Dieses Systems Manager Run Command-Dokument führt die folgenden Aufgaben aus:

- Herunterladen und Überprüfen von EC2Rescue for Windows Server
- Importiert ein PowerShell Modul, um Ihnen die Interaktion mit dem Tool zu erleichtern.
- Führt EC2 RescueCmd mit dem angegebenen Befehl und den angegebenen Parametern aus.

Das Systems Manager Run Command-Dokument akzeptiert drei Parameter:

- Command — Die EC2Rescue for Windows Server Aktion. Die aktuell zulässigen Werte sind:
  - ResetAccess— Setzt das lokale Administratorkennwort zurück. Das lokale Administratorpasswort der aktuellen Instance wird zurückgesetzt und das zufallsgeneriert Passwort wird in Parameter Store als sicher gespeicher `/EC2Rescue/Password/<INSTANCE_ID>`. Wenn Sie diese Aktion auswählen und keine Parameter angeben, werden Passwörter automatisch mit dem Standard-Verschlüsselung verschlüsselt. Sie können in den Parametern optional die ID eines Verschlüsselung angeben, um das Passwort mit einem eigenen Schlüssel zu verschlüsseln.
  - CollectLogs— Führt EC2Rescue für Windows Server mit der Aktion aus. `/collect:all` Wenn Sie diese Aktion auswählen, müssen die `Parameters` des Amazon S3-Buckets, auf den die Protokolle hochgeladen werden sollen, in den Logs enthalten sein.
  - FixAll— Führt EC2Rescue für Windows Server mit der Aktion aus. `/rescue:all` Wenn Sie diese Aktion auswählen, muss der Name des zu rettenden Blockgerätes in den `Parameters` enthalten sein.
- Parameter — Die PowerShell Parameter, die für den angegebenen Befehl übergeben werden sollen.

> **Note**
>
> Damit die ResetAccessAktion funktioniert, muss Ihrer Amazon EC2 EC2-Instance die folgende Richtlinie angehängt sein, um das verschlüsselte Passwort in den Parameter Store zu schreiben. Warten Sie ein paar Minuten, bevor Sie versuchen, das Passwort

einer Instance zurückzusetzen, nachdem Sie diese Richtlinie der zugehörigen IAM-Rolle zugeordnet haben.
Verwenden des Standard-Verschlüsselung:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
      ]
    }
  ]
}
```

Verwenden eines benutzerdefinierten Verschlüsselung:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:PutParameter"
      ],
      "Resource": [
        "arn:aws:ssm:region:account_id:parameter/EC2Rescue/
Passwords/<instanceid>"
        ]
      },
      {
      "Effect": "Allow",
      "Action": [
      "kms:Encrypt"
      ],
      "Resource": [
        "arn:aws:kms:region:account_id:key/<kmskeyid>"
```

```
      ]
    }
  ]
}
```

Im folgenden Verfahren wird beschrieben, wie Sie die JSON-Daten für diesen Dokument mit der Amazon EC2-Konsole anzeigen können.

So zeigen Sie die JSON-Daten für das Systems Manager Run Command-Dokument an

1. Öffnen Sie die Systems Manager-Konsole unter https://console.aws.amazon.com/systems-manager/home.
2. Erweitern Sie im Navigationsbereich den Abschnitt Shared Services und wählen Sie Documents aus.
3. Legen Sie in der Suchleiste Owner (Eigentümer) auf Owned by Me or Amazon (Eigentum von mir oder Amazon) und Document name prefix (Dokumentnamenpräfix) auf `AWSSupport-RunEC2RescueForWindowsTool` fest.
4. Markieren Sie das Dokument `AWSSupport-RunEC2RescueForWindowsTool`, wählen Sie die Option Contents und zeigen Sie dann die JSON-Daten an.

Beispiele

Die folgenden Beispiele zeigen, wie das Systems Manager Run Command-Dokument verwendet wird, um EC2Rescue for Windows Server mithilfe der AWS CLI auszuführen. Weitere Informationen zum Senden von Befehlen mit dem AWS CLI finden Sie in der AWS CLI Befehlsreferenz.

Der Versuch, alle erkannten Probleme auf einem Offline-Stamm-Volume zu beheben

Versuchen Sie, alle erkannten Probleme auf einem Offline-Stamm-Volume zu beheben, das einer Amazon EC2-Windows-Instance zugeordnet ist:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline volume xvdf" --parameters
 "Command=FixAll, Parameters='xvdf'" --output text
```

Erfassen von Protokollen in der aktuellen Amazon EC2-Windows-Instance

Erfassen Sie alle Protokolle von der aktuellen Online- Amazon EC2-Windows-Instance und laden Sie sie in einen Amazon S3-Bucket hoch:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online log collection to S3" --
parameters "Command=CollectLogs, Parameters='YOURS3BUCKETNAME'" --output text
```

Erfassen von Protokollen auf einem Offline-Volume einer Amazon EC2-Windows-Instance

Erfassen Sie alle Protokolle auf einem Offline-Volume, das einer Amazon EC2-Windows-Instance zugeordnet ist, und laden Sie diese mithilfe einer vorsignierten URL in Amazon S3 hoch:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue offline log collection to S3"
 --parameters "Command=CollectLogs, Parameters=\"-Offline -BlockDeviceName xvdf -
S3PreSignedUrl 'YOURS3PRESIGNEDURL'\"" --output text
```

Zurücksetzen des lokalen Administratorpassworts

In den folgenden Beispielen werden Methoden gezeigt, mit denen Sie das lokale Administratorpasswort zurücksetzen können. In der Ausgabe wird ein Link zu Parameter Store bereitgestellt, unter dem Sie das sichere, zufallsgenerierte Passwort finden können; mit diesem können Sie anschließend über RDP als lokaler Administrator auf Ihre Amazon EC2-Windows-Instance zugreifen.

Zurücksetzen des lokalen Administratorpassworts für eine Online-Instance mithilfe des AWS KMS key -Standardschlüssels alias/aws/ssm:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess" --output text
```

Zurücksetzen des lokalen Administratorpassworts für eine Online-Instance mithilfe eines Verschlüsselung:

```
aws ssm send-command --instance-ids "i-0cb2b964d3e14fd9f" --document-name "AWSSupport-
RunEC2RescueForWindowsTool" --comment "EC2Rescue online password reset" --parameters
 "Command=ResetAccess, Parameters=a133dc3c-a2g4-4fc6-a873-6c0720104bf0" --output text
```

> **Note**
>
> In diesem Beispiel lautet Verschlüsselung `a133dc3c-a2g4-4fc6-a873-6c0720104bf0`.

Serielle EC2-Konsole für Amazon EC2 EC2-Instances

Mit der seriellen EC2-Konsole haben Sie Zugriff auf den seriellen Port Ihrer Amazon EC2-Instance, den Sie zur Behebung von Boot-, Netzwerkkonfigurations- und anderen Problemen verwenden können. Die serielle Konsole erfordert nicht, dass Ihre Instance über Netzwerkfähigkeiten verfügt. Mit der seriellen Konsole können Sie Befehle für eine Instance eingeben, als ob Ihre Tastatur und Ihr Monitor direkt an die serielle Schnittstelle der Instance angeschlossen wären. Die Sitzung der seriellen Konsole dauert während des Neustarts und Stopps der Instance. Während des Neustarts können Sie alle Boot-Meldungen von Anfang an anzeigen.

Der Zugriff auf die serielle Konsole ist standardmäßig nicht verfügbar. Ihre Organisation muss Kontozugriff auf die serielle Konsole gewähren und IAM-Richtlinien konfigurieren, um Ihren Benutzern Zugriff auf die serielle Konsole zu gewähren. Der serielle Konsolenzugriff kann auf differenzierter Ebene mithilfe von Instance-IDs, RessourcenTags und anderen IAM-Hebeln gesteuert werden. Weitere Informationen finden Sie unter Konfigurieren des Zugriffs auf die serielle EC2-Konsole.

Auf die serielle Konsole kann über die EC2-Konsole oder zugegriffen werde AWS CLI.

Die serielle Konsole ist ohne zusätzliche Kosten verfügbar.

Themen

Voraussetzungen

Um eine Verbindung zur seriellen EC2-Konsole herzustellen und das von Ihnen gewählte Tool zur Fehlerbehebung zu verwenden, müssen die folgenden Voraussetzungen erfüllt sein:

- AWS-Regionen

- Wavelength-Zonen und AWS -Außenposten
- Local Zones
- Instance-Typen
- Gewähren von Zugriff
- Unterstützung für browserbasierte Clients
- Instance-Status
- Amazon EC2 Systems Manager
- SSHD-Server
- Konfigurieren des von Ihnen gewählten Tools für die Fehlerbehebung

AWS-Regionen

Wird in allen Ländern AWS-Regionen außer Kanada West (Calgary) unterstützt.

Wavelength-Zonen und AWS -Außenposten

Nicht unterstützt

Local Zones

Unterstützt in allen lokalen Zonen.

Instance-Typen

Unterstützte Instance-Typen:

- Linux
  - Alle virtualisierten Instances, die auf dem Nitro System aufgebaut sind.
  - Alle Bare-Metal-Instances außer:
    - Universell: `a1.metal`, `mac1.metal`, `mac2.metal`
    - Beschleunigte Datenverarbeitung: `g5g.metal`
    - RAM-optimiert: `u-6tb1.metal`, `u-9tb1.metal`, `u-12tb1.metal`, `u-18tb1.metal`, `u-24tb1.metal`
- Windows

  Alle virtualisierten Instances, die auf dem Nitro System aufgebaut sind. Wird nicht auf Bare-Metal-Instances unterstützt.

Gewähren von Zugriff

Sie müssen die Konfigurationsaufgaben abschließen, um Zugriff auf die serielle EC2-Konsole zu gewähren. Weitere Informationen finden Sie unter Konfigurieren des Zugriffs auf die serielle EC2-Konsole.

Unterstützung für browserbasierte Clients

Um über den browserbasierten Client eine Verbindung zur seriellen Konsole herzustellen, muss Ihr Browser dies unterstützen. WebSocket Wenn Ihr Browser dies nicht unterstützt WebSocket, stellen Sie mit Ihrem eigenen Schlüssel und einem SSH-Client eine Verbindung zur seriellen Konsole her.

Instance-Status

Der Wert muss `running` sein.

Wenn sich die Instance in den `pending`-, `stopping`-, `stopped`-, `shutting-down`- oder `terminated`-Status befindet, können Sie keine Verbindung mit der seriellen Konsole herstellen.

Weitere Informationen zum Instance-Status finden Sie unter Instance-Lebenszyklus.

Amazon EC2 Systems Manager

Wenn die Instance Amazon EC2 Systems Manager verwendet, muss SSM Agent Version 3.0.854.0 oder höher auf der Instance installiert sein. Informationen zu SSM Agent finden Sie unter Arbeiten mit SSM Agent im AWS Systems Manager -Benutzerhandbuch.

SSHD-Server

Sie benötigen keinen sshd-Server, der auf Ihrer Instance installiert oder ausgeführt wird.

Konfigurieren des von Ihnen gewählten Tools für die Fehlerbehebung

Linux-Instances

Um Fehler in Ihrer Linux-Instanz über die serielle Konsole zu beheben, können Sie GRUB oder verwenden. SysRq Bevor Sie diese Tools verwenden können, müssen Sie zunächst Konfigurationsschritte für jede Instance ausführen, auf der Sie sie verwenden möchten.

Tools

- Konfigurieren von GRUB
- Konfigurieren SysRq

Konfigurieren von GRUB

Bevor Sie GRUB über die serielle Konsole verwenden können, müssen Sie Ihre Instance so konfigurieren, dass GRUB über die serielle Konsole verwendet wird.

Um GRUB zu konfigurieren, wählen Sie eines der folgenden Verfahren basierend auf dem AMI, das zum Starten der Instance verwendet wurde.

Amazon Linux 2

So konfigurieren Sie GRUB für eine Amazon Linux 2-Instance

1. Herstellen einer Verbindung zur Linux-Instance
2. Fügen Sie die folgenden Optionen hinzu oder ändern Sie sie in `/etc/default/grub`:
   - Set `GRUB_TIMEOUT=1`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Fügen Sie `GRUB_SERIAL_COMMAND="serial --speed=115200"` hinzu.

   Es folgt ein Beispiel für `/etc/default/grub`. Möglicherweise müssen Sie die Konfiguration basierend auf Ihrem System-Setup ändern.

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.shell=0"
   GRUB_TIMEOUT=1
   GRUB_DISABLE_RECOVERY="true"
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```
3. Übernehmen Sie die aktualisierte Konfiguration, indem Sie den folgenden Befehl ausführen.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

Ubuntu

So konfigurieren Sie GRUB auf einer Ubuntu-Instance

1. Verbinden Sie sich mit der Instance.

2. Fügen Sie die folgenden Optionen hinzu oder ändern Sie sie in `/etc/default/grub.d/50-cloudimg-settings.cfg`:

   - Set `GRUB_TIMEOUT=1`.
   - Add `GRUB_TIMEOUT_STYLE=menu`.
   - Fügen Sie `GRUB_TERMINAL="console serial"` hinzu.
   - Entfernen Sie `GRUB_HIDDEN_TIMEOUT`.
   - Fügen Sie `GRUB_SERIAL_COMMAND="serial --speed=115200"` hinzu.

   Es folgt ein Beispiel für `/etc/default/grub.d/50-cloudimg-settings.cfg`. Möglicherweise müssen Sie die Konfiguration basierend auf Ihrem System-Setup ändern.

   ```
   # Cloud Image specific Grub settings for Generic Cloud Images
   # CLOUD_IMG: This file was created/modified by the Cloud Image build process

   # Set the recordfail timeout
   GRUB_RECORDFAIL_TIMEOUT=0

   # Do not wait on grub prompt
   GRUB_TIMEOUT=1
   GRUB_TIMEOUT_STYLE=menu

   # Set the default commandline
   GRUB_CMDLINE_LINUX_DEFAULT="console=tty1 console=ttyS0
    nvme_core.io_timeout=4294967295"

   # Set the grub console type
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed 115200"
   ```

3. Übernehmen Sie die aktualisierte Konfiguration, indem Sie den folgenden Befehl ausführen.

   ```
   [ec2-user ~]$ sudo update-grub
   ```

RHEL

So konfigurieren Sie GRUB auf einer RHEL-Instance

1. Verbinden Sie sich mit der Instance.

2. Fügen Sie die folgenden Optionen hinzu oder ändern Sie sie in `/etc/default/grub`:

   - Entfernen Sie `GRUB_TERMINAL_OUTPUT`.
   - Add `GRUB_TERMINAL="console serial"`.
   - Fügen Sie `GRUB_SERIAL_COMMAND="serial --speed=115200"` hinzu.

   Es folgt ein Beispiel für `/etc/default/grub`. Möglicherweise müssen Sie die Konfiguration basierend auf Ihrem System-Setup ändern.

   ```
   GRUB_TIMEOUT=1
   GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
   GRUB_DEFAULT=saved
   GRUB_DISABLE_SUBMENU=true
   GRUB_CMDLINE_LINUX="console=tty0 console=ttyS0,115200n8 net.ifnames=0
    rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto"
   GRUB_DISABLE_RECOVERY="true"
   GRUB_ENABLE_BLSCFG=true
   GRUB_TERMINAL="console serial"
   GRUB_SERIAL_COMMAND="serial --speed=115200"
   ```

3. Übernehmen Sie die aktualisierte Konfiguration, indem Sie den folgenden Befehl ausführen.

   ```
   [ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
   ```

CentOS

Für Instances, die mit einem CentOS-AMI gestartet werden, ist GRUB standardmäßig für die serielle Konsole konfiguriert.

Es folgt ein Beispiel für `/etc/default/grub`. Ihre Konfiguration kann je nach Systemeinrichtung unterschiedlich sein.

```
GRUB_TIMEOUT=1
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL="serial console"
GRUB_SERIAL_COMMAND="serial --speed=115200"
GRUB_CMDLINE_LINUX="console=tty0 crashkernel=auto console=ttyS0,115200"
```

```
GRUB_DISABLE_RECOVERY="true"
```

Konfigurieren SysRq

Zur Konfiguration SysRq aktivieren Sie die SysRq Befehle für den aktuellen Startzyklus. Um die Konfiguration dauerhaft zu machen, können Sie die SysRq Befehle auch für nachfolgende Starts aktivieren.

Um alle SysRq Befehle für den aktuellen Startzyklus zu aktivieren

1. Verbinden Sie sich mit der Instance.
2. Führen Sie den folgenden Befehl aus.

```
[ec2-user ~]$ sudo sysctl -w kernel.sysrq=1
```

> **Note**
>
> Diese Einstellung wird beim nächsten Neustart gelöscht.

Um alle SysRq Befehle für nachfolgende Starts zu aktivieren

1. Erstellen Sie die Datei `/etc/sysctl.d/99-sysrq.conf` und öffnen Sie sie in Ihrem Lieblingseditor.

```
[ec2-user ~]$ sudo vi /etc/sysctl.d/99-sysrq.conf
```

2. Fügen Sie die folgende Zeile zu.

```
kernel.sysrq=1
```

3. Starten Sie die Instance neu, um die Änderungen zu übernehmen.

```
[ec2-user ~]$ sudo reboot
```

4. Geben Sie an der `login`-Eingabeaufforderung den Benutzernamen des passwortbasierten Benutzers ein, den Sie zuvor eingerichtet haben, und drücken Sie dann die Eingabetaste.

5. Geben Sie an der `Password`-Eingabeaufforderung das Passwort ein und drücken Sie dann die Eingabetaste.

Windows-Instances

Um Probleme mit Ihrer Windows-Instance über die serielle Konsole zu beheben, können Sie die Special Admin Console (SAC) verwenden. Bevor Sie SAC verwenden können, müssen Sie SAC und das Startmenü zunächst auf jeder Instance aktivieren, auf der Sie es verwenden möchten.

Aktivieren Sie SAC und das Boot-Menü

> **Note**
>
> Wenn Sie SAC für eine Instance aktivieren, funktionieren die EC2-Services, die auf den Passwortabruf angewiesen sind, auf der Amazon-EC2-Konsole nicht. Windows auf Amazon-EC2-Launch-Agents (EC2Config, EC2Launch v1 und EC2Launch v2) verlassen sich bei der Ausführung verschiedener Aufgaben auf die serielle Konsole. Diese Aufgaben werden nicht erfolgreich ausgeführt, wenn Sie SAC für eine Instance aktivieren. Weitere Informationen zu Windows auf Amazon EC2 EC2-Start-Agenten finden Sie unterthe section called “Windows-Instanzen konfigurieren”. Wenn Sie SAC aktivieren, können Sie es später deaktivieren. Weitere Informationen finden Sie unter Deaktivieren von SAC und vom Boot-Menü.

Verwenden Sie eine der folgenden Methoden, um SAC und das Bootmenü einer Instance zu aktivieren.

PowerShell

Aktivieren von SAC und dem Boot-Menü auf einer Windows-Instance

1. Connect zu Ihrer Instance her und führen Sie die folgenden Schritte von einer PowerShell Befehlszeile mit erhöhten Rechten aus.
2. Aktivieren Sie SAC.

```
bcdedit /ems '{current}' on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Aktivieren Sie das Boot-Menü.

```
bcdedit /set '{bootmgr}' displaybootmenu yes
bcdedit /set '{bootmgr}' timeout 15
bcdedit /set '{bootmgr}' bootems yes
```

4. Wenden Sie die aktualisierte Konfiguration an, indem Sie die Instance neu starten.

```
shutdown -r -t 0
```

Command prompt

Aktivieren von SAC und dem Boot-Menü auf einer Windows-Instance

1. Stellen Sie eine Verbindung mit Ihrer Instance her und führen Sie die folgenden Schritte an der Eingabeaufforderung aus.
2. Aktivieren Sie SAC.

```
bcdedit /ems {current} on
bcdedit /emssettings EMSPORT:1 EMSBAUDRATE:115200
```

3. Aktivieren Sie das Boot-Menü.

```
bcdedit /set {bootmgr} displaybootmenu yes
bcdedit /set {bootmgr} timeout 15
bcdedit /set {bootmgr} bootems yes
```

4. Wenden Sie die aktualisierte Konfiguration an, indem Sie die Instance neu starten.

```
shutdown -r -t 0
```

Konfigurieren des Zugriffs auf die serielle EC2-Konsole

Um den Zugriff auf die serielle Konsole zu konfigurieren, müssen Sie den Zugriff auf die serielle Konsole auf Kontoebene gewähren und dann IAM-Richtlinien konfigurieren, um Ihren Benutzern Zugriff zu gewähren. Bei Linux-Instances müssen Sie außerdem auf jeder Instanz einen passwortbasierten Benutzer konfigurieren, damit Ihre Benutzer die serielle Konsole zur Fehlerbehebung verwenden können.

Überprüfen Sie vor Beginn unbedingt die Voraussetzungen.

Themen

Ebenen des Zugriffs auf die serielle EC2-Konsole

Standardmäßig gibt es auf Kontoebene keinen Zugriff auf die serielle Konsole. Sie müssen explizit Zugriff auf die serielle Konsole auf Kontoebene gewähren. Weitere Informationen finden Sie unter Verwalten des Kontozugriffs auf die serielle EC2-Konsole.

Sie können eine Service-Kontroll-Richtlinie (SCP) verwenden, um den Zugriff auf die serielle Konsole in Ihrem Unternehmen zu ermöglichen. Sie können dann eine differenzierte Zugriffskontrolle auf Benutzerebene vornehmen, indem Sie eine IAM-Richtlinie zur Zugriffskontrolle verwenden. Durch die Verwendung einer Kombination von SCP- und IAM-Richtlinien haben Sie unterschiedliche Zugriffskontrollstufen für die serielle Konsole.

Organisationsebene

Sie können eine Service-Kontroll-Richtlinie (SCP) verwenden, um Mitgliedskonten in Ihrer Organisation den Zugriff auf die serielle Konsole zu ermöglichen. Weitere Informationen zu SCPs finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.

Instance-Ebene

Sie können die Zugriffsrichtlinien für die serielle Konsole mithilfe von IAM PrincipalTag und ResourceTag Constructions konfigurieren und Instanzen anhand ihrer ID angeben. Weitere Informationen finden Sie unter Konfigurieren von IAM-Richtlinien für den Zugriff auf serielle EC2-Konsole.

Benutzerebene

Sie können den Zugriff auf die Benutzerebene konfigurieren, indem Sie eine IAM-Richtlinie konfigurieren, um einem bestimmten Benutzer die Berechtigung zu erteilen oder zu verweigern, den öffentlichen SSH-Schlüssel an den seriellen Konsolendienst einer bestimmten Instance zu übertragen. Weitere Informationen finden Sie unter Konfigurieren von IAM-Richtlinien für den Zugriff auf serielle EC2-Konsole.

Betriebssystemebene (nur Linux-Instanzen)

Sie können ein Benutzerpasswort auf der Ebene des Gastbetriebssystems festlegen. Dies ermöglicht für einige Anwendungsfälle Zugriff auf die serielle Konsole. Um die Protokolle zu überwachen, benötigen Sie jedoch keinen passwortbasierten Benutzer. Weitere Informationen finden Sie unter Legen Sie ein Betriebssystem-Benutzerkennwort für eine Linux-Instance fest.

Verwalten des Kontozugriffs auf die serielle EC2-Konsole

Standardmäßig gibt es auf Kontoebene keinen Zugriff auf die serielle Konsole. Sie müssen explizit Zugriff auf die serielle Konsole auf Kontoebene gewähren.

Themen

- Gewähren von Berechtigungen für Benutzer zur Verwaltung des Kontozugriffs
- Anzeigen des Kontozugriffsstatus für die serielle Konsole
- Erteilen des Kontozugriffs auf die serielle Konsole
- Kontozugriff auf die serielle Konsole verweigern

Gewähren von Berechtigungen für Benutzer zur Verwaltung des Kontozugriffs

Um Ihren Benutzern die Verwaltung des Kontozugriffs auf die serielle EC2-Konsole zu ermöglichen, müssen Sie ihnen die erforderlichen IAM-Berechtigungen gewähren.

Die folgende Richtlinie gewährt Berechtigungen zum Anzeigen des Kontostatus und zum Zulassen und Verhindern des Kontozugriffs auf die serielle EC2-Konsole.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:GetSerialConsoleAccessStatus",
                "ec2:EnableSerialConsoleAccess",
                "ec2:DisableSerialConsoleAccess"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

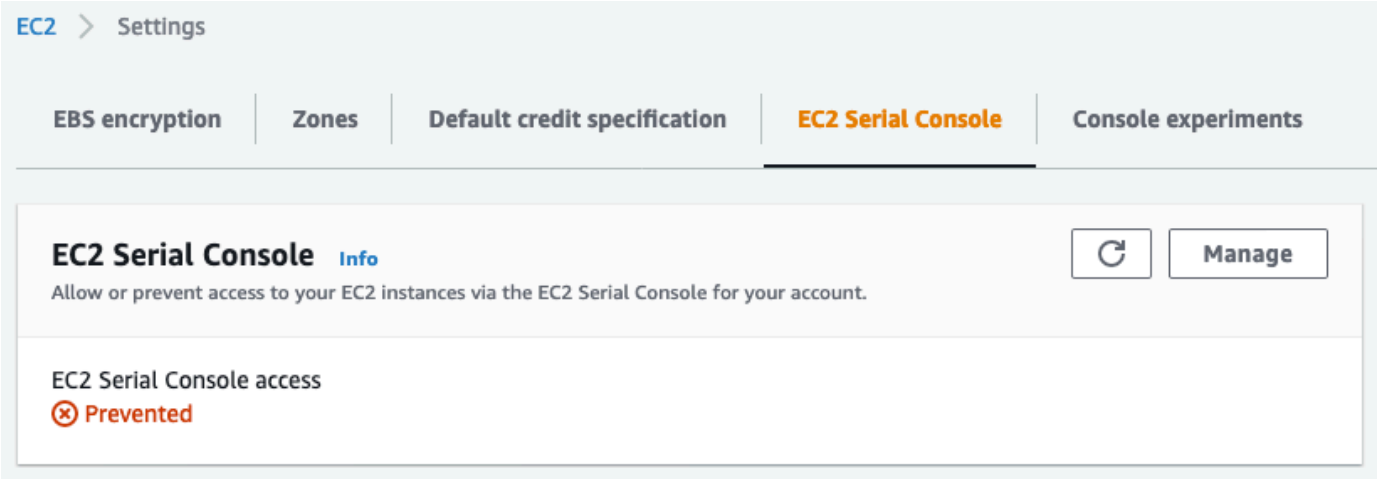
Anzeigen des Kontozugriffsstatus für die serielle Konsole

Anzeigen des Kontozugriffsstatus auf die serielle Konsole (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
3. Wählen Sie unter Kontoattribute serielle EC2-Konsole aus.

   Das Feld Zugriff auf serielle EC2-Konsole zeigt an, ob der Kontozugriff erlaubt oder verhindert ist.

   Der folgende Screenshot zeigt, dass das Konto daran gehindert wird, die serielle EC2-Konsole zu verwenden.



Anzeigen des Kontozugriffsstatus für die serielle Konsole (AWS CLI)

Verwenden Sie den Befehl get-serial-console-access-status, um den Kontozugriffsstatus auf die serielle Konsole anzuzeigen.

```
aws ec2 get-serial-console-access-status --region us-east-1
```

In der folgenden Ausgabe zeigt `true` an, dass dem Konto Zugriff auf die serielle Konsole gewährt wird.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Erteilen des Kontozugriffs auf die serielle Konsole

Gewähren des Kontozugriffs auf die serielle Konsole (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
3. Wählen Sie unter Kontoattribute serielle EC2-Konsole aus.
4. Wählen Sie Manage (Verwalten).
5. Um den Zugriff auf die serielle EC2-Konsole aller Instances im Konto zu ermöglichen, aktivieren Sie das Kontrollkästchen Zulassen.
6. Wählen Sie Update (Aktualisieren) aus.

Gewähren des Kontozugriffs auf die serielle Konsole (AWS CLI)

Verwenden Sie den Befehl enable-serial-console-access, um den Kontozugriff auf die serielle Konsole zu ermöglichen.

```
aws ec2 enable-serial-console-access --region us-east-1
```

In der folgenden Ausgabe zeigt `true` an, dass dem Konto Zugriff auf die serielle Konsole gewährt wird.

```
{
    "SerialConsoleAccessEnabled": true
}
```

Kontozugriff auf die serielle Konsole verweigern

Verweigern des Kontozugriffs auf die serielle Konsole (Konsole)

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich EC2-Dashboard aus.
3. Wählen Sie unter Kontoattribute serielle EC2-Konsole aus.

4. Wählen Sie Manage (Verwalten).
5. Um den Zugriff auf die serielle EC2-Konsole aller Instances im Konto zu verhindern, deaktivieren Sie das Kontrollkästchen Zulassen.
6. Wählen Sie Update (Aktualisieren) aus.

Verrweigern des Kontozugriffs auf die serielle Konsole (AWS CLI)

Verwenden Sie den Befehl disable-serial-console-access, um den Kontozugriff auf die serielle Konsole zu verhindern.

```
aws ec2 disable-serial-console-access --region us-east-1
```

In der folgenden Ausgabe zeigt `false` an, dass dem Konto Zugriff auf die serielle Konsole verweigert wird.

```
{
    "SerialConsoleAccessEnabled": false
}
```

Konfigurieren von IAM-Richtlinien für den Zugriff auf serielle EC2-Konsole

Standardmäßig haben Ihre Benutzer keinen Zugriff auf die serielle Konsole. Ihre Organisation muss IAM-Richtlinien konfigurieren, um Ihren Benutzern den erforderlichen Zugriff zu gewähren. Weitere Informationen finden Sie unter Erstellen von IAM-Richtlinien im IAM-Benutzerhandbuch.

Für den seriellen Konsolenzugriff erstellen Sie ein JSON-Richtliniendokument, das die `ec2-instance-connect:SendSerialConsoleSSHPublicKey`-Aktion enthält. Diese Aktion gewährt einem Benutzer die Berechtigung, den öffentlichen Schlüssel an den seriellen Konsolenservice zu übertragen, der eine serielle Konsolensitzung startet. Wir empfehlen die Einschränkung des Zugriffs auf bestimmte EC2-Instances. Andernfalls können alle Benutzer mit dieser Berechtigung eine Verbindung zur seriellen Konsole aller EC2-Instances herstellen.

IAM-Beispielrichtlinien

- Zulassen des Zugriffs auf die serielle Konsole
- Explizites Verweigern des Zugriffs auf die serielle Konsole
- Verwenden von Ressourcen-Tags (Markierungen), um den Zugriff auf die serielle Konsole zu kontrollieren

Zulassen des Zugriffs auf die serielle Konsole

Standardmäßig hat niemand Zugriff auf die serielle Konsole. Um den Zugriff auf die serielle Konsole zu gewähren, müssen Sie eine Richtlinie konfigurieren, um den Zugriff explizit zuzulassen. Wir empfehlen, eine Richtlinie zu konfigurieren, die den Zugriff auf bestimmte Instances einschränkt.

Die folgende Richtlinie ermöglicht den Zugriff auf die serielle Konsole einer bestimmten Instance, die durch ihre Instance-ID identifiziert wird.

Beachten Sie, dass die `DescribeInstances`-, `DescribeInstanceTypes`-, und `GetSerialConsoleAccessStatus`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Daher müssen alle Ressourcen, die durch ein * (Sternchen) gekennzeichnet sind, für diese Aktionen spezifiziert werden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
             "Resource": "*"
        },
        {
            "Sid": "AllowinstanceBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Explizites Verweigern des Zugriffs auf die serielle Konsole

Die folgende IAM-Richtlinie ermöglicht den Zugriff auf die serielle Konsole aller Instances, die durch das * (Sternchen) gekennzeichnet ist, und verweigert ausdrücklich den Zugriff auf die serielle Konsole einer bestimmten Instance, die durch ihre ID identifiziert wird.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DenySerialConsoleAccess",
            "Effect": "Deny",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/i-0598c7d356eba48d7"
        }
    ]
}
```

Verwenden von Ressourcen-Tags (Markierungen), um den Zugriff auf die serielle Konsole zu kontrollieren

Sie können Ressourcen-Tags (Markierungen) verwenden, um den Zugriff auf die serielle Konsole einer Instance zu steuern.

Bei der attributbasierten Zugriffskontrolle handelt es sich um eine Autorisierungsstrategie, bei der Berechtigungen auf der Grundlage von Tags definiert werden, die Benutzern und Ressourcen zugewiesen werden können. AWS Beispielsweise ermöglicht die folgende Richtlinie einem Benutzer, eine serielle Konsolenverbindung für eine Instance nur dann zu initiieren, wenn das Ressourcen-Tag

dieser Instance und das Tag des Prinzipals denselben `SerialConsole`-Wert für den Tag-Schlüssel haben.

Weitere Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf Ihre AWS Ressourcen finden Sie unter Steuern des Zugriffs auf AWS Ressourcen im IAM-Benutzerhandbuch.

Beachten Sie, dass die `DescribeInstances`-, `DescribeInstanceTypes`-, und `GetSerialConsoleAccessStatus`-Aktionen keine Berechtigungen auf Ressourcenebene unterstützen. Daher müssen alle Ressourcen, die durch ein * (Sternchen) gekennzeichnet sind, für diese Aktionen spezifiziert werden.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribeInstances",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceTypes",
                "ec2:GetSerialConsoleAccessStatus"
            ],
            "Resource": "*"
        },
        {
            "Sid": "AllowTagBasedSerialConsoleAccess",
            "Effect": "Allow",
            "Action": [
                "ec2-instance-connect:SendSerialConsoleSSHPublicKey"
            ],
            "Resource": "arn:aws:ec2:region:account-id:instance/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/SerialConsole":
 "${aws:PrincipalTag/SerialConsole}"
                }
            }
        }
    ]
}
```

Legen Sie ein Betriebssystem-Benutzerkennwort für eine Linux-Instance fest

> **Note**
>
> Dieser Abschnitt gilt nur für Linux-Instances.

Sie können sich ohne Passwort mit der seriellen Konsole verbinden. Um jedoch die serielle Konsole für die Problembehandlung einer Linux-Instanz verwenden zu können, muss die Instanz über einen kennwortbasierten Betriebssystembenutzer verfügen.

Sie können das Kennwort für jeden Betriebssystembenutzer festlegen, einschließlich des Stammbenutzers. Beachten Sie, dass der Stammbenutzer alle Dateien ändern kann, während jeder Betriebssystembenutzer möglicherweise eingeschränkte Berechtigungen hat.

Sie müssen für jede Instance, für die Sie die serielle Konsole verwenden, ein Benutzerkennwort festlegen. Dies ist eine einmalige Anforderung für jede Instance.

> **Note**
>
> Die folgenden Anweisungen gelten nur, wenn Sie Ihre Instance mit einem von bereitgestellten Linux-AMI gestartet haben, AWS da AMIs, die von bereitgestellt werden, standardmäßig nicht mit einem kennwortbasierten Benutzer konfiguriert AWS sind. Wenn Sie Ihre Instance mit einem AMI gestartet haben, für das das Root-Benutzerkennwort bereits konfiguriert ist, können Sie diese Anweisungen überspringen.

So legen Sie ein Betriebssystem-Benutzerkennwort für eine Linux-Instance fest

1. Verbinden Sie sich mit der Instance. Sie können eine beliebige Methode für die Verbindung mit Ihrer Instance verwenden, mit Ausnahme der seriellen EC2-Konsolen-Verbindungsmethode.
2. Verwenden Sie den passwd-Befehl, um das Kennwort für einen Benutzer festzulegen. Im folgenden Beispiel ist der Benutzer `root`.

   ```
   [ec2-user ~]$ sudo passwd root
   ```

   Es folgt eine Beispielausgabe.

   ```
   Changing password for user root.
   ```

```
New password:
```

3. Geben Sie an der `New password`-Eingabeaufforderung das neue Passwort ein.
4. Geben Sie an der Eingabeaufforderung das Passwort erneut ein.

Herstellen einer Verbindung zur seriellen EC2-Konsole

Sie können über die Amazon EC2-Konsole oder über SSH eine Verbindung mit der seriellen Konsole Ihrer EC2-Instance herstellen. Nachdem Sie eine Verbindung zur seriellen Konsole hergestellt haben, können Sie sie zur Fehlerbehebung bei Booten, Netzwerkkonfiguration und anderen Problemen verwenden. Weitere Informationen zur Fehlerbehebung finden Sie unter Beheben Sie Probleme mit Ihrer Amazon EC2 EC2-Instance mithilfe der seriellen EC2-Konsole.

Überlegungen

- Pro Instance wird nur 1 aktive serielle Konsolenverbindung unterstützt.
- Die Verbindung zur seriellen Konsole dauert normalerweise 1 Stunde, sofern Sie sie nicht beenden. Allerdings beendet Amazon EC2 während der Systemwartung die serielle Konsolensitzung.
- Es dauert 30 Sekunden, um eine Sitzung abzubrechen, nachdem Sie die Verbindung zur seriellen Konsole getrennt haben, um eine neue Sitzung zuzulassen.
- Unterstützte serielle Konsolenports: `ttyS0` (Linux-Instanzen) und `COM1` (Windows-Instanzen)
- Wenn Sie eine Verbindung zur seriellen Konsole herstellen, können Sie einen leichten Rückgang des Durchsatzes Ihrer Instance feststellen.

Themen

- Herstellen von Verbindungen über den browserbasierten Client
- Herstellen von Verbindungen über Ihren eigenen Schlüssel und einen SSH-Client
- Endpunkte und Fingerabdrücke der seriellen EC2-Konsole

Herstellen von Verbindungen über den browserbasierten Client

Sie können eine Verbindung mit der seriellen Konsole Ihrer EC2-Instance herstellen, indem Sie den browserbasierten Client verwenden. Dazu wählen Sie die Instance in der Amazon EC2-Konsole aus und wählen, eine Verbindung zur seriellen Konsole herzustellen. Der browserbasierte Client verarbeitet die Berechtigungen und stellt eine erfolgreiche Verbindung bereit.

Die serielle EC2-Konsole funktioniert von den meisten Browsern und unterstützt Tastatur- und Mauseingaben.

Stellen Sie vor dem Verbinden sicher, dass Sie die Voraussetzungen erfüllt haben.

So stellen Sie mithilfe des browserbasierten Clients (Amazon EC2-Konsole) eine Verbindung mit dem seriellen Port Ihrer Instance her

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Instances aus.
3. Wählen Sie die Instance und Actions (Aktionen), Monitor and troubleshoot (Überprüfen und Fehler beheben), EC2 Serial Console (Serielle EC2-Konsole), Connect (Verbinden) aus.

   Alternativ können Sie die Instance markieren und wählen Sie Connect (Verbinden), EC2 Serial Console (Serielle EC2-Konsole), Connect (Verbinden).

   Ein Terminalfenster im Browser wird geöffnet.
4. Drücken Sie die Eingabetaste. Wenn eine Anmeldeaufforderung zurückkehrt, sind Sie mit der seriellen Konsole verbunden.

   Wenn der Bildschirm schwarz bleibt, können Sie die folgenden Informationen verwenden, um Probleme bei der Verbindung mit der seriellen Konsole zu beheben:

   - Stellen Sie sicher, dass Sie den Zugriff auf die serielle Konsole konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren des Zugriffs auf die serielle EC2-Konsole.
   - (Nur Linux-Instanzen) Wird verwendet SysRq , um eine Verbindung zur seriellen Konsole herzustellen. SysRq erfordert nicht, dass Sie eine Verbindung über den browserbasierten Client herstellen. Weitere Informationen finden Sie unter Beheben Sie Probleme mit Ihrer Linux-Instance SysRq.
   - (Nur Linux-Instanzen) Starten Sie Getty neu. Wenn Sie SSH-Zugriff auf Ihre Instance haben, stellen Sie mithilfe von SSH eine Verbindung zu Ihrer Instance her und starten Sie Getty mit dem folgenden Befehl neu.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```
   - Starten Sie Ihre Instance neu. Sie können Ihre Instance neu starten, indem Sie SysRq (Linux-Instances), die EC2-Konsole oder den verwenden. AWS CLI Weitere Informationen

finden Sie unter Beheben Sie Probleme mit Ihrer Linux-Instance SysRq (Linux-Instances) oderDurchführen eines Neustarts Ihrer Instance.

5. (Nur Linux-Instanzen) Geben Sie an der **`login`** Eingabeaufforderung den Benutzernamen des kennwortbasierten Benutzers ein, den Sie zuvor eingerichtet haben, und drücken Sie dann die EINGABETASTE.
6. (Nur Linux-Instanzen) Geben Sie an der **`Password`** Eingabeaufforderung das Passwort ein, und drücken Sie dann die Eingabetaste.

Sie sind jetzt bei der Instance angemeldet und können die serielle Konsole zur Fehlerbehebung verwenden.

Herstellen von Verbindungen über Ihren eigenen Schlüssel und einen SSH-Client

Sie können mittels Ihres eigenen SSH-Schlüssels über einen SSH-Client Ihrer Wahl Verbindungen mit Ihrer Instance herstellen, während Sie die serielle Konsolen-API verwenden. Auf diese Weise können Sie die serielle Konsolenfunktion für die Push-Übergabe öffentlicher Schlüssel an Instances nutzen.

Stellen Sie vor dem Verbinden sicher, dass Sie die Voraussetzungen erfüllt haben.

So stellen Sie eine Verbindung mit der seriellen Konsole einer Instance über SSH her

1. Schieben Sie Ihren öffentlichen SSH-Schlüssel auf die Instance, um eine Sitzung der seriellen Konsole zu starten

   Übertragen Sie den öffentlichen SSH-Schlüssel mit dem Befehl send-serial-console-ssh-public-key per Push an die Instance. Dies startet eine serielle Konsolensitzung.

   Wenn für diese Instance bereits eine serielle Konsolensitzung gestartet wurde, schlägt der Befehl fehl, da Sie jeweils nur eine Sitzung geöffnet haben können. Es dauert 30 Sekunden, um eine Sitzung abzubrechen, nachdem Sie die Verbindung zur seriellen Konsole getrennt haben, um eine neue Sitzung zuzulassen.

   ```
   aws ec2-instance-connect send-serial-console-ssh-public-key \
       --instance-id i-001234a4bf70dec41EXAMPLE \
       --serial-port 0 \
       --ssh-public-key file://my_key.pub \
       --region us-east-1
   ```

2. Stellen Sie mit Ihrem privaten Schlüssel eine Verbindung zur seriellen Konsole her

   Verwenden Sie den ssh-Befehl, um eine Verbindung mit der seriellen Konsole herzustellen, bevor der öffentliche Schlüssel aus dem seriellen Konsolendienst entfernt wird. Sie haben 60 Sekunden bevor er entfernt wird.

   Verwenden Sie den privaten Schlüssel, der dem öffentlichen Schlüssel entspricht.

   Das Benutzernamenformat lautet `instance-id.port0`, das die Instance-ID und den Port 0 umfasst. Im folgenden Beispiel lautet der Benutzername `i-001234a4bf70dec41EXAMPLE.port0`.

   Der Endpunkt des seriellen Konsolendienstes ist für jede Region unterschiedlich. In der Endpunkte und Fingerabdrücke der seriellen EC2-Konsole Tabelle finden Sie die Endpunkte der einzelnen Regionen. Im folgenden Beispiel befindet sich der serielle Konsolendienst in der Region us-east-1.

   ```
   ssh -i my_key i-001234a4bf70dec41EXAMPLE.port0@serial-console.ec2-instance-connect.us-east-1.aws
   ```

3. (Optional) Überprüfen Sie den Fingerabdruck

   Wenn Sie zum ersten Mal eine Verbindung mit der seriellen Konsole herstellen, werden Sie aufgefordert, den Fingerabdruck zu überprüfen. Sie können den Fingerabdruck der seriellen Konsole mit dem Fingerabdruck vergleichen, der zur Überprüfung angezeigt wird. Wenn diese Fingerabdrücke nicht übereinstimmen, wird ggf. versucht, einen Man-In-the-Middle-Angriff durchzuführen. Wenn sie übereinstimmen, können Sie sich sicher mit der seriellen Konsole verbinden.

   Der folgende Fingerabdruck gilt für den seriellen Konsolendienst in der Region us-east-1. Informationen zu den Fingerabdrücken für die einzelnen Regionen finden Sie unter Endpunkte und Fingerabdrücke der seriellen EC2-Konsole.

   ```
   SHA256:dXwn5ma/xadVMeBZGEru5l2gx+yI5LDiJaLUcz0FMmw
   ```

> **Note**
>
> Der Fingerabdruck wird nur angezeigt, wenn Sie zum ersten Mal eine Verbindung mit der seriellen Konsole herstellen.

4. Drücken Sie die Eingabetaste. Wenn eine Eingabeaufforderung zurückkehrt, sind Sie mit der seriellen Konsole verbunden.

   Wenn der Bildschirm schwarz bleibt, können Sie die folgenden Informationen verwenden, um Probleme bei der Verbindung mit der seriellen Konsole zu beheben:

   - Stellen Sie sicher, dass Sie den Zugriff auf die serielle Konsole konfiguriert haben. Weitere Informationen finden Sie unter Konfigurieren des Zugriffs auf die serielle EC2-Konsole.
   - (Nur Linux-Instanzen) Wird verwendet SysRq , um eine Verbindung zur seriellen Konsole herzustellen. SysRq erfordert nicht, dass Sie eine Verbindung über SSH herstellen. Weitere Informationen finden Sie unter Beheben Sie Probleme mit Ihrer Linux-Instance SysRq.
   - (Nur Linux-Instanzen) Starten Sie Getty neu. Wenn Sie SSH-Zugriff auf Ihre Instance haben, stellen Sie mithilfe von SSH eine Verbindung zu Ihrer Instance her und starten Sie Getty mit dem folgenden Befehl neu.

     ```
     [ec2-user ~]$ sudo systemctl restart serial-getty@ttyS0
     ```

   - Starten Sie Ihre Instance neu. Sie können Ihre Instance neu starten, indem Sie SysRq (nur Linux-Instances), die EC2-Konsole oder den verwenden. AWS CLI Weitere Informationen finden Sie unter Beheben Sie Probleme mit Ihrer Linux-Instance SysRq (nur Linux-Instances) oderDurchführen eines Neustarts Ihrer Instance.

5. (Nur Linux-Instanzen) Geben Sie an der **`login`** Eingabeaufforderung den Benutzernamen des kennwortbasierten Benutzers ein, den Sie zuvor eingerichtet haben, und drücken Sie dann die EINGABETASTE.
6. (Nur Linux-Instanzen) Geben Sie an der **`Password`** Eingabeaufforderung das Passwort ein, und drücken Sie dann die Eingabetaste.

Sie sind jetzt bei der Instance angemeldet und können die serielle Konsole zur Fehlerbehebung verwenden.

Endpunkte und Fingerabdrücke der seriellen EC2-Konsole

Im Folgenden sind die Service-Endpunkte und Fingerabdrücke für die serielle EC2-Konsole aufgeführt. Um programmgesteuert eine Verbindung zur seriellen Konsole einer Instance herzustellen, verwenden Sie einen EC2 Serial Console-Endpunkt. Die Endpunkte und Fingerabdrücke der seriellen EC2-Konsole sind für jede AWS -Region einzigartig.

Name der Region	Region	Endpunkt	Fingerabdruck
USA Ost (Ohio)	us-east-2	serial-console.ec2-instance-connect.us-east-2.aws	SHA256: TY7TRSZZ26XBB0/HVV9JRM7MCZN0xW/D/0EhwPk TzRt
USA Ost (Nord-Virginia)	us-east-1	serial-console.ec2-instance-connect.us-east-1.aws	SHA256DiJa: DXWN5MA/XADVMEBZGERU5L2GX+YI5LLUCZ0FMMW
USA West (Nordkalifornien)	us-west-1	serial-console.ec2-instance-connect.us-west-1.aws	SHA256:OHldlcMET8u7QLSX3jmRTRAPFHVtqbyoLZBMUCqiH3Y
USA West (Oregon)	us-west-2	serial-console.ec2-instance-connect.us-west-2.aws	SHA256: EMCIe23Bi6YG dhHAVHA1O2JXVUC TqKaHainqZc MwqNk
Afrika (Kapstadt)	af-south-1	ec2-serial-console.af-south-1.api.aws	SHA256: RMWWZ2FJUQZJO5JL2KHLZ21ED00BIIWIVePe IgXsczo
Asien-Pazifik (Hongkong)	ap-east-1	ec2-serial-console.ap-east-1.api.aws	SHA256: T0Q1LPi ZXxCho P7TKM2XXV

Name der Region	Region	Endpunkt	Fingerabdruck
			IC9BJ HplnAkjb FsjYnifk
Asien-Pazifik (Hyderabad)	ap-south-2	ec2-serial-console.ap-south-2.api.aws	SHA256: WJGPBSWV4/SHN +OPIT YJ15DVW84 5JEHDKRS ValoewAu
Asien-Pazifik (Jakarta)	ap-southeast-3	ec2-serial-console.ap-southeast-3.api.aws	SHA 256:5 +LFNS32Xi TQL/4O0ZI FBX4BZGSY FQY3O8MIK ZwgrCh
Asien-Pazifik (Melbourne)	ap-southeast-4	ec2-serial-console.ap-southeast-4.api.aws	FgLvjnSHA 256: AVAQ27H 5GTSSHZ0O V7H90P0GG 46WFOET6ZJVM
Asien-Pazifik (Mumbai)	ap-south-1	serial-console.ec2-instance-connect.ap-south-1.aws	SHA256: OBL HHEBLIA H8ISO51RE ZTPISM35BSU40 XcYmklq RxEg
Asien-Pazifik (Osaka)	ap-northeast-3	ec2-serial-console.ap-northeast-3.api.aws	SHA256: AM0/ JIBK BnBu FnHr 9AXSGev3G8TU/ VVHFXE/3UCYJSQ
Asien-Pazifik (Seoul)	ap-northeast-2	serielle Konsole.ec2-instance-connect.ap-northeast-2.aws	SHA256:FoqWXNX +DZ++GuNTztg9 PK49WYMqBX +FrcZM2dSrqrI

Name der Region	Region	Endpunkt	Fingerabdruck
Asien-Pazifik (Singapur)	ap-southeast-1	serial-console.ec2-instance-connect.ap-southeast-1.aws	SHA256: PLFNN7WNC QDHX3QMWLU1GY/ O8TUX7L C6L45COY QgZua
Asien-Pazifik (Sydney)	ap-southeast-2	serial-console.ec2-instance-connect.ap-southeast-2.aws	SHA256: y uk9leuqjq troxxzun+cw9/vse9w 984cf5tgzo4 FvMw
Asien-Pazifik (Tokio)	ap-northeast-1	serielle Konsole.ec2-instance-connect.ap-northeast-1.aws	SHA256: rqfsdczt TRDV1T9EM /HMRFQE+C RLIOT5UM4K OfQawew
Kanada (Zentral)	ca-central-1	serial-console.ec2-instance-connect.ca-central-1.aws	SHA256: P2O2Jo O6YW738FIOTHDU 2GcZYMMO7S4 ZwmpMwkp TyEv
China (Beijing)	cn-north-1	ec2-serial-console .cn-north-1.api.am azonwebservices.co m.cn	SHA 256:2 GHVFY4H7U U3+WAFUXD28V/gg LgGT+Y MeqjvSlgn gpg
China (Ningxia)	cn-northwest-1	appmesh.cn-northwe st-1.api.amazonweb services.com.cn	OdVfSHA256: TDGRNZKIQ YEBUHO 4SZUA09VW I5RYOZG zu GPWMIM

Name der Region	Region	Endpunkt	Fingerabdruck
Europa (Frankfurt)	eu-central-1	serial-console.ec2-instance-connect.eu-central-1.aws	SHA256: ACMFS/Y OL8AMZ1TO E+BBNRJJ3 FY0K0DE2C IcOd OlkXv
Europa (Irland)	eu-west-1	serial-console.ec2-instance-connect.eu-west-1.aws	SHA256: H2AAGAWO4 HATHHTM6E ZS3BJ7UDGUXI2Q ZAwCW6E TrHj
Europa (London)	eu-west-2	serial-console.ec2-instance-connect.eu-west-2.aws	SHA256: RnJg A69RD5CE/ AEG4AMM53 I6LKD1ZPVS/ BCV3TTPW2 8
Europa (Mailand)	eu-south-1	ec2-serial-console.eu-south-1.api.aws	SHA256: LC0KOV BVRXN0A7N 99ECLBXSX 95CUUS7X7QK30 JnpgFy
Europa (Paris)	eu-west-3	serial-console.ec2-instance-connect.eu-west-3.aws	SHA256:q8ldnAf9pym eNe8BnFVngY3RPAr/ kxswJUzfrlxeEWs
Europa (Spanien)	eu-south-2	ec2-serial-console.eu-south-2.api.aws	SHA256: Gocw2DFRLU669Q ecsr6fzuz/4F4N7T45 NxqFx ZcwoEc

Name der Region	Region	Endpunkt	Fingerabdruck
Europa (Stockholm)	eu-north-1	serial-console.ec2-instance-connect.eu-north-1.aws	SHA256: Tkgffuvu GSS3CU8GD L6W2UI32E PNPKFKLWX84 DvocDi
Europa (Zürich)	eu-central-2	ec2-serial-console.eu-central-2.api.aws	SHA 256:8 PPx2MBMF6 0N M4/4OaxFU TQXWP6MK WdCw UlzKfw IfRz
Israel (Tel Aviv)	il-central-1	ec2-serial-console.il-central-1.api.aws	SHA256: JR6Q8V6KN NPI8+QSFQ 4DJ5DIMNM ZPTGWGSM1S U NvtYy
Naher Osten (Bahrain)	me-south-1	ec2-serial-console .me-south-1.api.aws	SHA256: NPJLLKHU2 UQ2KVARSO K5XVPJOMR JKCBZCDQC3K8 QnLd
Naher Osten (VAE)	me-central-1	ec2-serial-console .me-central-1.api.aws	SHA256: ZPB5DUKIB Z+L0D B4MP von HI/ XZXNEFSDKBVLE FwPeyyk
Südamerika (São Paulo)	sa-east-1	serielle Konsole.ec2-Instance-Connect.sa-east-1.aws	SHA256: rd2+/32og njew1y vime c +botbih62oqapdq1di NaQz

Name der Region	Region	Endpunkt	Fingerabdruck
AWS GovCloud (US-Ost)	us-gov-east-1	serial-console.ec2-instance-connect.us-gov-east-1.amazonaws.com	SHA256IkqnDc: TiWE19GWS OYLCLRTVU38YEEH +DH ZNMTEBVF28
AWS GovCloud (US-West)	us-gov-west-1	serial-console.ec2-instance-connect.us-gov-west-1.amazonaws.com	SHA256OlPf: KFOFRWLAOZFB +UTBD3BRF8 8NGO2YZLQX 5DQ Zilw

Trennen der Verbindung mit der seriellen EC2-Konsole

Wenn Sie nicht mehr mit der seriellen EC2-Konsole Ihrer Instance verbunden sein müssen, können Sie die Verbindung trennen. Wenn Sie die Verbindung zur seriellen Konsole trennen, wird jede Shell-Sitzung, die auf der Instance ausgeführt wird, weiterhin ausgeführt. Wenn Sie die Shell-Sitzung beenden möchten, müssen Sie sie beenden, bevor Sie die Verbindung zur seriellen Konsole trennen.

Überlegungen

- Die Verbindung zur seriellen Konsole dauert normalerweise 1 Stunde, sofern Sie sie nicht beenden. Allerdings beendet Amazon EC2 während der Systemwartung die serielle Konsolensitzung.
- Es dauert 30 Sekunden, um eine Sitzung abzubrechen, nachdem Sie die Verbindung zur seriellen Konsole getrennt haben, um eine neue Sitzung zuzulassen.

Die Art und Weise, wie die Verbindung zur seriellen Konsole getrennt wird, hängt vom Client ab.

Browserbasierter Client

Um die Verbindung zur seriellen Konsole zu trennen, schließen Sie das Terminalfenster der seriellen Konsole im Browser.

Standard-OpenSSH-Client

Um die Verbindung zur seriellen Konsole zu trennen, verwenden Sie den folgenden Befehl, um die SSH-Verbindung zu schließen. Dieser Befehl muss unmittelbar nach einer neuen Zeile ausgeführt werden.

```
~.
```

Der Befehl, den Sie zum Schließen einer SSH-Verbindung verwenden, kann je nach verwendetem SSH-Client unterschiedlich sein.

Beheben Sie Probleme mit Ihrer Amazon EC2 EC2-Instance mithilfe der seriellen EC2-Konsole

Mithilfe der seriellen EC2-Konsole können Sie Boot-, Netzwerkkonfigurations- und andere Probleme beheben, indem Sie eine Verbindung zum seriellen Port Ihrer Instance herstellen.

> **Note**
>
> Bevor Sie beginnen, stellen Sie sicher, dass Sie die Voraussetzungen erfüllt haben.

Linux-Instances

Themen

- Beheben Sie die Fehler Ihrer Linux-Instance mit GRUB
- Beheben Sie Probleme mit Ihrer Linux-Instance SysRq

Beheben Sie die Fehler Ihrer Linux-Instance mit GRUB

GNU GRUB (Abkürzung für GNU GRand Unified Bootloader, gemeinhin als GRUB bezeichnet) ist der Standard-Bootloader für die meisten Linux-Betriebssysteme. Im GRUB-Menü können Sie auswählen, in welchen Kernel Sie booten möchten oder Menüeinträge ändern, um den Bootvorgang des Kernels zu ändern. Dies kann bei der Problembehandlung einer fehlerhaften Instance nützlich sein.

Das GRUB-Menü wird während des Startvorgangs angezeigt. Das Menü ist nicht über normales SSH zugänglich, Sie können jedoch über die serielle EC2-Konsole darauf zugreifen.

Single user mode

Der Einzelbenutzermodus bootet den Kernel auf ein niedrigeres Runlevel. Zum Beispiel könnte es das Dateisystem einhängen, aber das Netzwerk nicht aktivieren, was Ihnen die Möglichkeit gibt, die Wartung durchzuführen, die zum Reparieren der Instance erforderlich ist.

So booten Sie in den Einzelbenutzermodus

1. Stellen Sie eine Verbindung mit der seriellen Konsole der Instance her.
2. Starten Sie die Instance mit dem folgenden Befehl neu.

```
[ec2-user ~]$ sudo reboot
```

3. Wenn während des Neustarts das GRUB-Menü angezeigt wird, drücken Sie eine beliebige Taste, um den Bootvorgang zu beenden.
4. Verwenden Sie im GRUB-Menü die Pfeiltasten, um den zu bootenden Kernel auszuwählen, und drücken Sie e auf Ihrer Tastatur.
5. Verwenden Sie die Pfeiltasten, um den Cursor in der Zeile zu finden, die den Kernel enthält. Die Zeile beginnt mit `linux` oder `linux16`, abhängig von dem AMI, das zum Starten der Instance verwendet wurde. Für Ubuntu beginnen zwei Zeilen mit `linux`, die beide im nächsten Schritt geändert werden müssen.
6. Am Ende der Zeile fügen Sie das Wort `single` hinzu.

   Im Folgenden finden Sie ein Beispiel für Amazon Linux 2.

```
linux /boot/vmlinuz-4.14.193-149.317.amzn2.aarch64 root=UUID=d33f9c9a-\
dadd-4499-938d-ebbf42c3e499 ro  console=tty0 console=ttyS0,115200n8 net.ifname\
s=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff rd.she\
ll=0 single
```

7. Drücken Sie Strg+X, um in den Einzelbenutzermodus zu starten.
8. Geben Sie an der `login`-Eingabeaufforderung den Benutzernamen des passwortbasierten Benutzers ein, den Sie zuvor eingerichtet haben, und drücken Sie dann die Eingabetaste.
9. Geben Sie an der `Password`-Eingabeaufforderung das Passwort ein und drücken Sie dann die Eingabetaste.

Emergency mode

Der Notfallmodus ähnelt dem Einzelbenutzermodus, mit der Ausnahme, dass der Kernel auf dem niedrigsten möglichen Runlevel läuft.

Um in den Notfallmodus zu starten, folgen Sie den gleichen Schritten wie im Einzelbenutzermodus, fügen Sie jedoch in Schritt 6 das Wort `emergency` anstelle von `single` hinzu.

Beheben Sie Probleme mit Ihrer Linux-Instance SysRq

Der Schlüssel System Request (SysRq), der manchmal auch als SysRq „Magic“ bezeichnet wird, kann verwendet werden, um außerhalb einer Shell direkt einen Befehl an den Kernel zu senden, und der Kernel wird antworten, unabhängig davon, was der Kernel tut. Wenn die Instanz beispielsweise nicht mehr reagiert, können Sie den SysRq Schlüssel verwenden, um dem Kernel mitzuteilen, dass er abstürzen oder neu starten soll. Weitere Informationen finden Sie unter Magic SysRq Key in Wikipedia.

Sie können SysRq Befehle im browserbasierten Client für die EC2 Serial Console oder in einem SSH-Client verwenden. Der Befehl zum Senden einer Unterbrechungsanfrage ist für jeden Client unterschiedlich.

Wählen Sie zur Verwendung SysRq je nach verwendetem Client eines der folgenden Verfahren aus.

Browser-based client

Zur Verwendung SysRq in der seriellen Konsole (browserbasierter Client)

1. Stellen Sie eine Verbindung mit der seriellen Konsole der Instance her.
2. Um eine Unterbrechungsanfrage zu senden, drücken Sie `CTRL+0` (Null). Wenn Ihre Tastatur dies unterstützt, können Sie auch eine Unterbrechungsanfrage mit der Pause- oder Break-Taste senden.

   ```
   [ec2-user ~]$ CTRL+0
   ```

3. Um einen SysRq Befehl auszuführen, drücken Sie die Taste auf Ihrer Tastatur, die dem gewünschten Befehl entspricht. Um beispielsweise eine Liste mit SysRq Befehlen anzuzeigen, drücken Sieh.

```
[ec2-user ~]$ h
```

Der h-Befehl gibt etwas Ähnliches wie das Folgende aus.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

SSH client

Zur Verwendung SysRq in einem SSH-Client

1. Stellen Sie eine Verbindung mit der seriellen Konsole der Instance her.
2. Um eine Unterbrechungsanfrage zu senden, drücken Sie ~B (Tilde, gefolgt von Großbuchstaben B).

```
[ec2-user ~]$ ~B
```

3. Um einen SysRq Befehl auszuführen, drücken Sie die Taste auf Ihrer Tastatur, die dem gewünschten Befehl entspricht. Um beispielsweise eine Liste mit SysRq Befehlen anzuzeigen, drücken Sieh.

```
[ec2-user ~]$ h
```

Der h-Befehl gibt etwas Ähnliches wie das Folgende aus.

```
[ 1169.389495] sysrq: HELP : loglevel(0-9) reboot(b) crash(c) terminate-all-
tasks(e) memory-full-oom-kill(f) kill-all-tasks(i) thaw-filesystems
(j) sak(k) show-backtrace-all-active-cpus(l) show-memory-usage(m) nice-all-RT-
tasks(n) poweroff(o) show-registers(p) show-all-timers(q) unraw(r
) sync(s) show-task-states(t) unmount(u) show-blocked-tasks(w) dump-ftrace-
buffer(z)
```

> **Note**
>
> Der Befehl, den Sie zum Senden einer Unterbrechungsanfrage verwenden, kann je nach verwendetem SSH-Client unterschiedlich sein.

Windows-Instances

Verwenden Sie SAC zur Fehlerbehebung Ihrer Windows-Instance

Die Special-Admin-Console(SAC)-Funktion von Windows bietet eine Möglichkeit zur Fehlerbehebung einer Windows-Instance. Wenn Sie eine Verbindung zur seriellen Konsole der Instance herstellen und SAC verwenden, können Sie den Startvorgang unterbrechen und Windows im abgesicherten Modus starten.

> **Note**
>
> Wenn Sie SAC für eine Instance aktivieren, funktionieren die EC2-Services, die auf den Passwortabruf angewiesen sind, auf der Amazon-EC2-Konsole nicht. Windows auf Amazon-EC2-Launch-Agents (EC2Config, EC2Launch v1 und EC2Launch v2) verlassen sich bei der Ausführung verschiedener Aufgaben auf die serielle Konsole. Diese Aufgaben werden nicht erfolgreich ausgeführt, wenn Sie SAC für eine Instance aktivieren. Weitere Informationen zu Windows auf Amazon EC2 EC2-Start-Agenten finden Sie unterthe section called “Windows-Instanzen konfigurieren”. Wenn Sie SAC aktivieren, können Sie es später deaktivieren. Weitere Informationen finden Sie unter Deaktivieren von SAC und vom Boot-Menü.

Themen

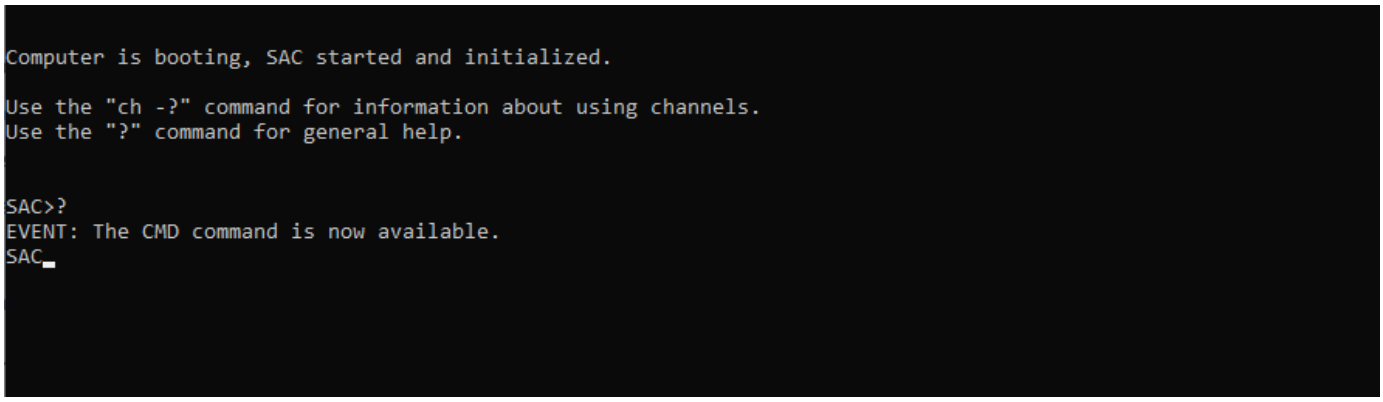
- Verwenden von SAC
- Verwenden des Boot-Menüs
- Deaktivieren von SAC und vom Boot-Menü

Verwenden von SAC

So verwenden Sie SAC

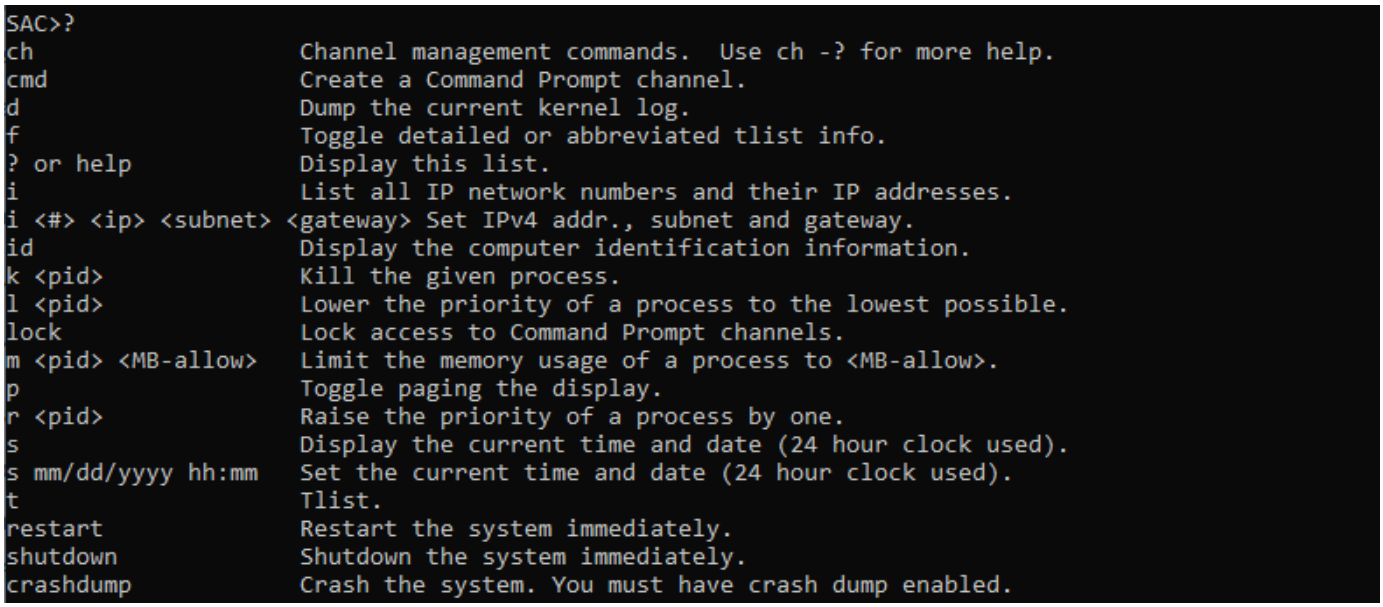
1. Stellen Sie eine Verbindung mit der seriellen Konsole her.

Wenn SAC auf der Instance aktiviert ist, zeigt die serielle Konsole die SAC>-Anfrage an.



2. Geben Sie zum Anzeigen der SAC-Befehle **?** ein und drücken Sie dann die Eingabetaste.

   Erwartete Ausgabe



3. Um einen Eingabeaufforderungskanal (z. B. `cmd0001` oder `cmd0002`) zu erstellen, geben Sie **`cmd`** ein und drücken Sie dann die Eingabetaste.
4. Um den Eingabeaufforderungskanal anzuzeigen, drücken Sie ESC und drücken Sie dann auf TAB.

   Erwartete Ausgabe

```
Name:                 Cmd0001
Description:          Command
Type:                 VT-UTF8
Channel GUID:         ef9f20a0-1287-11eb-82b0-0e4ba51872e5
Application Type GUID: 63d02271-8aa4-11d5-bccf-00b0d014a2d0

Press <esc><tab> for next channel.
Press <esc><tab>0 to return to the SAC channel.
Use any other key to view this channel.
```

5. Um Kanäle zu wechseln, drücken Sie ESC+Tab+Kanalnummer gleichzeitig. Um zum Beispiel zum `cmd0002`-Kanal (falls er erstellt wurde) zu wechseln, drücken Sie ESC+TAB+2.
6. Geben Sie die für den Eingabeaufforderungskanal erforderlichen Anmeldeinformationen ein.

```
Please enter login credentials.
Username: Administrator
Domain  : .
Password: *******
```

Die Eingabeaufforderung ist dieselbe voll funktionsfähige Command Shell, die Sie auf einem Desktop erhalten, mit der Ausnahme, dass sie das Lesen von bereits ausgegebenen Zeichen nicht zulässt.

```
Microsoft Windows [Version 10.0.17763.1457]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer: EC2AMAZ-ASR4SAI

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           30 GB      0 B
  Disk 1    Online           46 GB    46 GB

DISKPART>
```

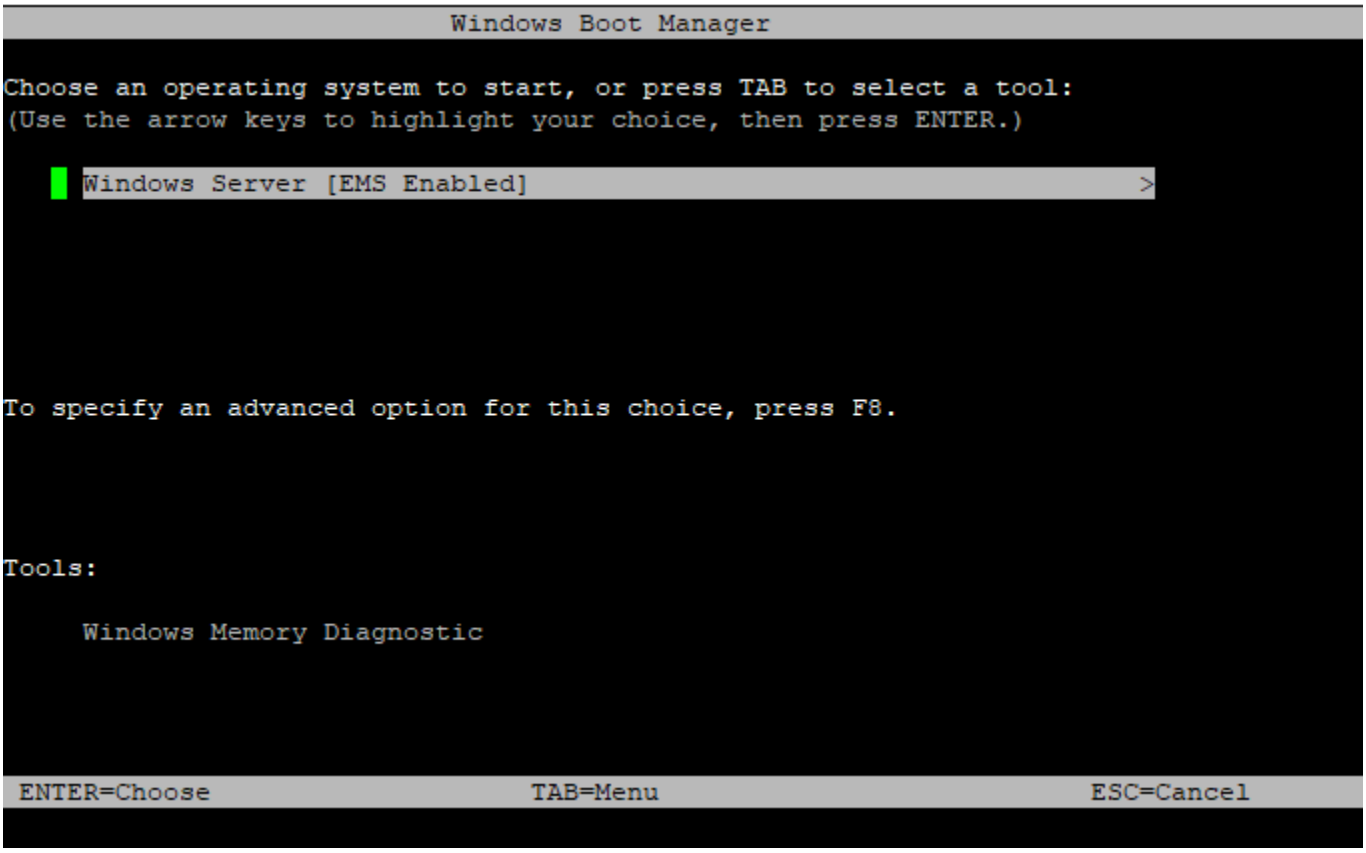
PowerShell kann auch von der Befehlszeile aus verwendet werden.

Beachten Sie, dass Sie möglicherweise die Einstellung Fortschritt auf den stillen Modus festlegen müssen.

```
PS C:\Windows\system32> $ProgressPreference="SilentlyContinue"
PS C:\Windows\system32> $computerInfo = Get-ComputerInfo
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Name
Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz
PS C:\Windows\system32> $computerInfo.Csprocessors[0].Description
Intel64 Family 6 Model 85 Stepping 4
PS C:\Windows\system32>
```

Verwenden des Boot-Menüs

Wenn für die Instance das Boot-Menü aktiviert ist und nach der Verbindung über SSH neu gestartet wird, sollten Sie das Startmenü wie folgt sehen.



Befehle im Boot-Menü

EINGEBEN

Startet den ausgewählten Eintrag des Betriebssystems.

Tabulatortaste

Wechselt zum Tools-Menü.

ESC

Bricht die Instance ab und startet sie neu.

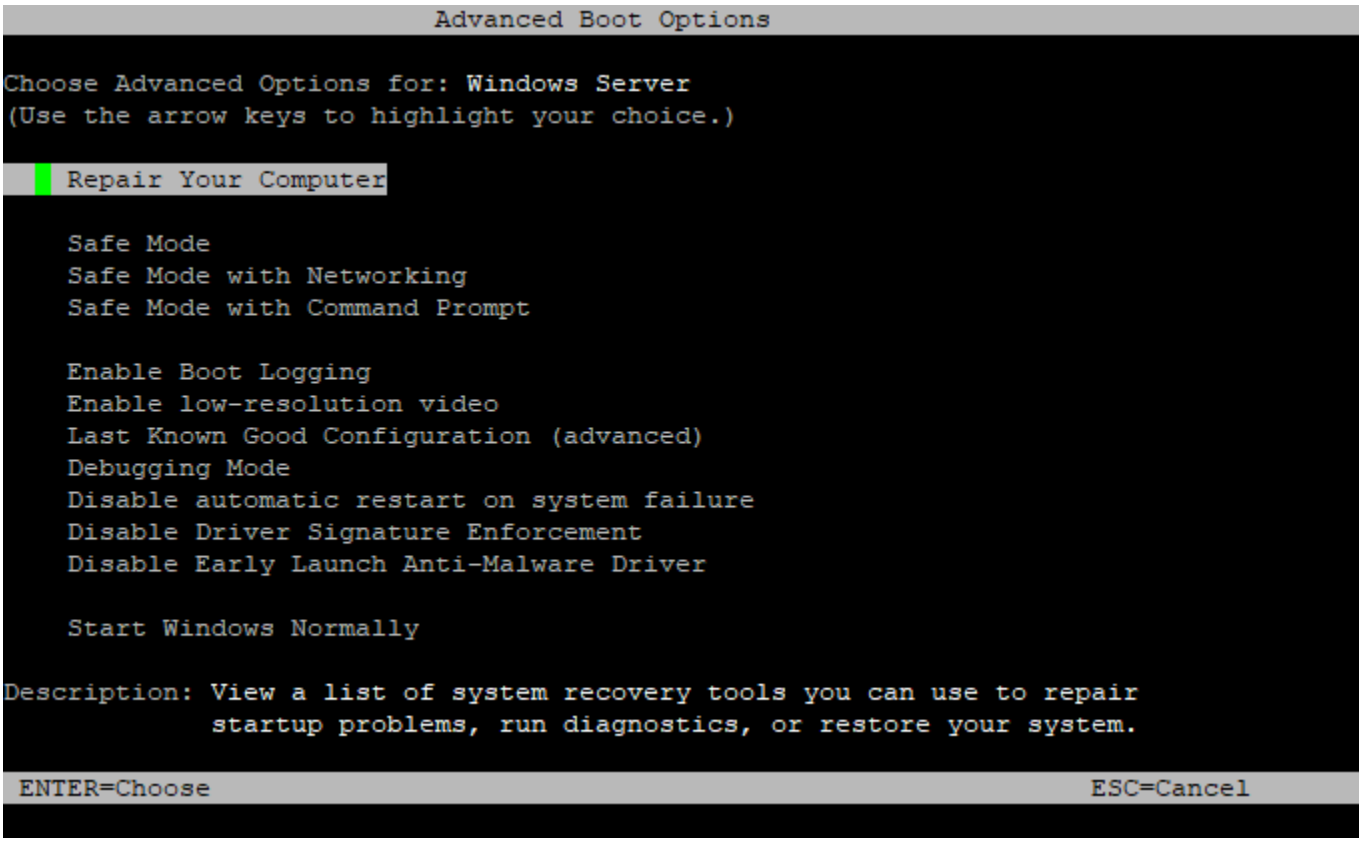
ESC, gefolgt von 8

Entspricht dem Drücken von F8. Zeigt erweiterte Optionen für das ausgewählte Element an.

ESC-Taste + linke Pfeiltaste

Geht zurück zum anfänglichen Boot-Menü.

> **Note**
>
> Die ESC-Taste allein bringt Sie nicht zurück zum Hauptmenü, da Windows darauf wartet, zu sehen, ob eine Escapesequenz läuft.



Deaktivieren von SAC und vom Boot-Menü

Wenn Sie SAC und das Boot-Menü aktivieren, können Sie diese Funktionen später deaktivieren.

Verwenden Sie eine der folgenden Methoden, um SAC und das Boot-Menü einer Instance zu deaktivieren.

PowerShell

So deaktivieren Sie SAC und das Boot-Menü auf einer Windows-Instance

1. Connect zu Ihrer Instance her und führen Sie die folgenden Schritte von einer PowerShell Befehlszeile mit erhöhten Rechten aus.
2. Deaktivieren Sie zuerst das Boot-Menü, indem Sie den Wert in no ändern.

```
bcdedit /set '{bootmgr}' displaybootmenu no
```

3. Deaktivieren Sie dann SAC, indem Sie den Wert auf `off` setzen.

```
bcdedit /ems '{current}' off
```

4. Wenden Sie die aktualisierte Konfiguration an, indem Sie die Instance neu starten.

```
shutdown -r -t 0
```

Command prompt

So deaktivieren Sie SAC und das Boot-Menü auf einer Windows-Instance

1. Stellen Sie eine Verbindung mit Ihrer Instance her und führen Sie die folgenden Schritte an der Eingabeaufforderung aus.
2. Deaktivieren Sie zuerst das Boot-Menü, indem Sie den Wert in no ändern.

```
bcdedit /set {bootmgr} displaybootmenu no
```

3. Deaktivieren Sie dann SAC, indem Sie den Wert auf `off` setzen.

```
bcdedit /ems {current} off
```

4. Wenden Sie die aktualisierte Konfiguration an, indem Sie die Instance neu starten.

```
shutdown -r -t 0
```

Senden eines Diagnose-Interrupts (für fortgeschrittene Benutzer)

> **Warning**
>
> Diagnose-Interrupts sind für fortgeschrittene Benutzer vorgesehen. Eine falsche Verwendung kann sich negativ auf Ihre Instance auswirken. Das Senden eines Diagnose-Interrupts an eine Instance kann zum Absturz und Neustart einer Instance führen, was unter Umständen den Verlust von Daten zur Folge hat.

Sie können einen Diagnose-Interrupt an eine Instanz senden, die nicht erreichbar ist oder nicht reagiert, um manuell eine Kernel-Panic für eine Linux-Instance oder einen Stop-Fehler (allgemein als Bluescreen-Fehler bezeichnet) für eine Windows-Instance auszulösen.

Linux-Instances

Linux-Betriebssysteme stürzen bei einer Kernel-Panik gewöhnlich ab und werden neu gestartet. Das spezifische Verhalten des Betriebssystems ist von seiner Konfiguration abhängig. Mit einer Kernel-Panik kann das Betriebssystem der Instance auch zum Ausführen von Aufgaben, z. B. Generieren einer Dump-Datei, veranlasst werden. Sie können dann mithilfe der Informationen in der Absturzabbilddatei eine Ursachenanalyse durchführen und die Instance debuggen. Die Absturzabbilddaten werden lokal von dem Betriebssystem auf der Instance selbst erstellt.

Windows-Instances

Im Allgemeinen stürzen Windows-Betriebssysteme ab und werden neu gestartet, wenn ein Abbruchfehler auftritt, das spezifische Verhalten hängt aber von seiner Konfiguration ab. Ein Abbruchfehler kann auch bewirken, dass das Betriebssystem Debugging-Informationen, wie z. B. ein Kernel-Speicherabbild, in einer Datei ausgibt. Sie können anhand dieser Informationen eine Ursachenanalyse durchführen, um die Instance zu debuggen. Die Speicherabbilddaten werden lokal von dem Betriebssystem auf der Instance selbst erstellt.

Bevor Sie ein Diagnose-Interrupt an Ihre Instance senden, empfehlen wir Ihnen, die Dokumentation für Ihr Betriebssystem zu konsultieren und anschließend die erforderlichen Konfigurationsänderungen vorzunehmen.

Inhalt

- Senden eines Diagnose-Interrupts

Unterstützte Instance-Typen

Der Diagnose-Interrupt wird auf allen Nitro-basierten Instance-Typen unterstützt, mit Ausnahme derjenigen, die mit Graviton-Prozessoren betrieben werden. AWS Weitere Informationen finden Sie unter Instances, die auf dem AWS Nitro System und Graviton basieren.AWS

Voraussetzungen

Bevor Sie einen Diagnose-Interrupt verwenden, müssen Sie das Betriebssystem der Instance entsprechend konfigurieren. Dadurch wird sichergestellt, dass es die Aktionen ausführt, die Sie benötigen, wenn ein Kernel-Panic (Linux-Instanzen) oder ein Stop-Fehler (Windows-Instanzen) auftritt.

Linux-Instances

So konfigurieren Sie Amazon Linux 2 zum Generieren eines Absturzabbildes bei Auftreten einer Kernel-Panik

1. Verbinden Sie sich mit der Instance.
2. Installieren Sie kexec und kdump.

   ```
   [ec2-user ~]$ sudo yum install kexec-tools -y
   ```

3. Konfigurieren Sie den Kernel zum Reservieren einer angemessenen Menge an Arbeitsspeicher für den sekundären Kernel. Die Menge an Arbeitsspeicher ist von dem insgesamt verfügbaren Arbeitsspeicher Ihrer Instance abhängig. Öffnen Sie die Datei `/etc/default/grub` in Ihrem bevorzugten Texteditor, suchen Sie die Zeile, die mit `GRUB_CMDLINE_LINUX_DEFAULT` beginnt, und fügen Sie dann den Parameter `crashkernel` im folgenden Format hinzu: `crashkernel=`*`memory_to_reserve`*. Um beispielsweise `160MB` zu reservieren, ändern Sie die Datei `grub` wie folgt ab:

   ```
   GRUB_CMDLINE_LINUX_DEFAULT="crashkernel=160M console=tty0 console=ttyS0,115200n8
    net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
    rd.shell=0"
   GRUB_TIMEOUT=0
   GRUB_DISABLE_RECOVERY="true"
   ```

4. Speichern Sie Ihre Änderungen und schließen Sie die Datei `grub`.
5. Erstellen Sie die neue GRUB2-Konfigurationsdatei.

```
[ec2-user ~]$ sudo grub2-mkconfig -o /boot/grub2/grub.cfg
```

6. Bei Instances auf Intel- und AMD-Prozessoren sendet der Befehl `send-diagnostic-interrupt` einen unbekannten nicht maskierbaren Interrupt (NMI) an die Instance. Sie müssen den Kernel so konfigurieren, dass er bei Eingang des unbekannten NMI abstürzt. Öffnen Sie die Datei `/etc/sysctl.conf` mit Ihrem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

```
kernel.unknown_nmi_panic=1
```

7. Starten Sie Ihre Instance neu und richten Sie wieder eine Verbindung zu ihr ein.
8. Vergewissern Sie sich, dass der Kernel mit dem richtigen `crashkernel`-Parameter gestartet wurde.

```
$ grep crashkernel /proc/cmdline
```

   Die folgende Beispielausgabe weist auf eine erfolgreiche Konfiguration hin.

```
BOOT_IMAGE=/boot/vmlinuz-4.14.128-112.105.amzn2.x86_64 root=UUID=a1e1011e-
e38f-408e-878b-fed395b47ad6 ro crashkernel=160M console=tty0 console=ttyS0,115200n8
 net.ifnames=0 biosdevname=0 nvme_core.io_timeout=4294967295 rd.emergency=poweroff
 rd.shell=0
```

9. Überprüfen Sie, ob der kdump-Service ausgeführt wird.

```
[ec2-user ~]$ systemctl status kdump.service
```

   Die folgende Beispielausgabe zeigt das Ergebnis, wenn der Service kdump derzeit ausgeführt wird.

```
kdump.service - Crash recovery kernel arming
   Loaded: loaded (/usr/lib/systemd/system/kdump.service; enabled; vendor preset:
 enabled)
   Active: active (exited) since Fri 2019-05-24 23:29:13 UTC; 22s ago
  Process: 2503 ExecStart=/usr/bin/kdumpctl start (code=exited, status=0/SUCCESS)
 Main PID: 2503 (code=exited, status=0/SUCCESS)
```

> **Note**
>
> Die Absturzabbilddatei wird standardmäßig in `/var/crash/` gespeichert. Um den Speicherort zu ändern, bearbeiten Sie die Datei `/etc/kdump.conf` mit Ihrem bevorzugten Texteditor.

So konfigurieren Sie Amazon Linux zum Generieren eines Absturzabbildes bei Auftreten einer Kernel-Panik

1. Verbinden Sie sich mit der Instance.
2. Installieren Sie kexec und kdump.

   ```
   [ec2-user ~]$ sudo yum install kexec-tools -y
   ```

3. Konfigurieren Sie den Kernel zum Reservieren einer angemessenen Menge an Arbeitsspeicher für den sekundären Kernel. Die Menge an Arbeitsspeicher ist von dem insgesamt verfügbaren Arbeitsspeicher Ihrer Instance abhängig.

   ```
   $ sudo grubby --args="crashkernel=memory_to_reserve" --update-kernel=ALL
   ```

   Um beispielsweise `160MB` für den Absturzkernel zu reservieren, verwenden Sie den folgenden Befehl.

   ```
   $ sudo grubby --args="crashkernel=160M" --update-kernel=ALL
   ```

4. Bei Instances auf Intel- und AMD-Prozessoren sendet der Befehl `send-diagnostic-interrupt` einen unbekannten nicht maskierbaren Interrupt (NMI) an die Instance. Sie müssen den Kernel so konfigurieren, dass er bei Eingang des unbekannten NMI abstürzt. Öffnen Sie die Datei `/etc/sysctl.conf` mit Ihrem bevorzugten Texteditor und fügen Sie Folgendes hinzu.

   ```
   kernel.unknown_nmi_panic=1
   ```

5. Starten Sie Ihre Instance neu und richten Sie wieder eine Verbindung zu ihr ein.
6. Vergewissern Sie sich, dass der Kernel mit dem richtigen `crashkernel`-Parameter gestartet wurde.

   ```
   $ grep crashkernel /proc/cmdline
   ```

Die folgende Beispielausgabe weist auf eine erfolgreiche Konfiguration hin.

```
root=LABEL=/ console=tty1 console=ttyS0 selinux=0 nvme_core.io_timeout=4294967295
 LANG=en_US.UTF-8 KEYTABLE=us crashkernel=160M
```

7. Überprüfen Sie, ob der kdump-Service ausgeführt wird.

```
[ec2-user ~]$ sudo service kdump status
```

Wenn der Service derzeit ausgeführt wird, gibt der Befehl als Antwort `Kdump is operational` zurück.

> **Note**
>
> Die Absturzabbilddatei wird standardmäßig in gespeicher `/var/crash/`. Um den Speicherort zu ändern, bearbeiten Sie die Datei `/etc/kdump.conf` mit Ihrem bevorzugten Texteditor.

So konfigurieren Sie SUSE Linux Enterprise, Ubuntu oder Red Hat Enterprise Linux

Bei Instances auf Intel- und AMD-Prozessoren sendet der Befehl `send-diagnostic-interrupt` einen unbekannten nicht maskierbaren Interrupt (NMI) an die Instance. Sie müssen den Kernel so konfigurieren, dass er abstürzt, wenn er das unbekannte NMI empfängt, indem Sie die Konfigurationsdatei für Ihr Betriebssystem anpassen. Informationen darüber, wie Sie den Kernel so konfigurieren, dass er abstürzt, finden Sie in der Dokumentation zu Ihrem Betriebssystem:

- SUSE Linux Enterprise
- Ubuntu
- Red Hat Enterprise Linux (RHEL)

Windows-Instances

So konfigurieren Sie Windows zum Generieren eines Speicherabbilds bei Auftreten von Abbruchfehlern

1. Verbinden Sie sich mit der Instance.

2. Öffnen Sie die Systemsteuerung und wählen Sie System, Erweiterte Systemeinstellungen.
3. Wählen Sie im Dialogfeld Systemeigenschaften die Registerkarte Erweitert aus.
4. Wählen Sie im Bereich Startup und Wiederherstellen die Option Einstellungen....
5. Konfigurieren Sie die Einstellungen im Bereich Systemfehler ganz nach Bedarf und wählen Sie dann OK.

Weitere Informationen zum Konfigurieren von Windows-Abbruchfehlern finden Sie unter Overview of memory dump file options for Windows.

Senden eines Diagnose-Interrupts

Nachdem Sie die erforderlichen Konfigurationsänderungen vorgenommen haben, können Sie mithilfe der AWS CLI oder der Amazon EC2 EC2-API einen Diagnose-Interrupt an Ihre Instance senden.

AWS CLI

So senden Sie einen Diagnose-Interrupt an Ihre Instance (AWS CLI)

Verwenden Sie den Befehl send-diagnostic-interrupt und geben Sie die Instance-ID an.

```
aws ec2 send-diagnostic-interrupt --instance-id i-1234567890abcdef0
```

PowerShell

So senden Sie einen Diagnose-Interrupt an Ihre Instance (AWS Tools for Windows PowerShell)

Verwenden Sie das Send-EC2DiagnosticInterruptCmdlt und geben Sie die Instance-ID an.

```
PS C:\> Send-EC2DiagnosticInterrupt -InstanceId i-1234567890abcdef0
```

Dokumentverlauf

In der folgenden Tabelle werden wichtige Ergänzungen des Amazon EC2 EC2-Benutzerhandbuchs ab 2019 beschrieben. Wir aktualisieren das Handbuch auch regelmäßig, um auf das Feedback einzugehen, das Sie uns senden.

Änderung	Beschreibung	Datum
EC2-Instance-Typ-Finder — zusätzliche Parameter	Der EC2-Instance-Typ-Finder bietet jetzt zusätzliche Parameter, mit denen Sie detailliertere Anforderungen für Ihren Workload angeben können.	5. Juni 2024
U7i-12-TB-, U7in-16-TB-, U7in-24-TB- und U7in-32-TB-Instances	Neue Instance-Typen mit hohem Speicherbedarf, die über skalierbare Intel Xeon Prozessoren der 4. Generation verfügen.	28. Mai 2024
Neue verwaltete Richtlinie für EC2 Fast Launch	Die EC2FastLaunchFullAccess Richtlinie zur Ausführung von API-Aktionen im Zusammenhang mit der EC2 Fast Launch-Funktion von einer Instance aus wurde hinzugefügt.	14. Mai 2024
AMI-Abmeldeschutz	Sie können den Abmeldeschutz für ein AMI aktivieren, um ein versehentliches oder böswilliges Löschen zu verhindern.	23. April 2024

PTP-Hardware-Uhr — Unterstützung für Instance-Typen	Die PTP-Hardwareuhr ist jetzt für die Instance-Typen C7a, C7i, M7a, M7g, M7i, R7a und R7i verfügbar.	22. April 2024
Leistungsaspekte von Nitro für verbesserte Netzwerke wurden hinzugefügt	Diese Seite konzentriert sich auf Überlegungen zum Netzwerk, die Ihnen bei der Leistungsoptimierung Ihrer Nitro-basierten Amazon EC2 EC2-Instances helfen sollen.	4. April 2024
Neue verwaltete Richtlinie für VSS-fähige EBS-Snapshots	In Amazon EC2 VSS steht eine neue IAM-verwaltete Richtlinie zur Verfügung, die Sie zu Ihrer Instance-Profilrol le hinzufügen können, um sicherzustellen, dass Ihre Berechtigungen erhalten bleiben up-to-date und die bewährten Methoden eingehalt en werden.	28. März 2024
PTP-Hardware-Uhr — USA Ost (Nord-Virginia)	Die PTP-Hardware-Uhr ist jetzt in der Region USA Ost (Nord-Virginia) verfügbar.	26. März 2024
Stellen Sie IMDSv2 als Kontostandard ein	Sie können für alle neuen EC2-Instance-Starts in Ihrem Konto festlegen, dass standardmäßig Instance Metadata Service Version 2 (IMDSv2) verwendet wird.	25. März 2024

Kennzeichnen Sie neue Linux-AMIs, die aus einem Snapshot erstellt wurden	Wenn Sie ein Linux-AMI aus einem Snapshot erstellen , können Sie das neue AMI taggen.	7. März 2024
Kennzeichnen Sie neue AMIs und Snapshots beim Kopieren	Wenn Sie ein AMI kopieren, können Sie das neue AMI und die neuen Snapshots mit denselben Tags oder mit unterschiedlichen Tags kennzeichnen.	7. März 2024
Entfernen Sie die AWS Management Pack-Seiten	Das AWS Management Pack wurde hauptsächlich mit Windows Server 2012 und früheren Versionen verwendet . Diese älteren Betriebss ystemplattformversionen werden nicht mehr unterstützt. Informationen zur Verwaltung Ihrer Serverflotte, die vor Ort und vor Ort laufen, AWS und zur Fehlerbehebung finden Sie unter AWS Systems Manager Fleet Manager.	12. Februar 2024
EC2 Instance Connect ist auf macOS-AMIs vorinstalliert	EC2 Instance Connect ist jetzt auf macOS Sonoma 14.2.1 oder höher, macOS Ventura 13.6.3 oder höher und macOS Monterey 12.7.2 oder höher AMIs vorinstalliert.	26. Januar 2024
Unterstützung von EC2 Instance Connect für CentOS, macOS und RHEL	Sie können EC2 Instance Connect jetzt auf unterstützten CentOS-, macOS- und RHEL-AMIs installieren.	6. Dezember 2023

Unterstützt Ruhezustand für C7a, C7i, R7a, R7i und R7iz	Versetzen Sie Ihre neu gestarteten Instances, die auf C7a, C7i, R7a, R7i und R7iz-Instance-Typen ausgeführt werden, in den Ruhezustand.	1. Dezember 2023
Amazon Q EC2 Instance Type Selector	Der Amazon Q EC2 Instance Type Selector berücksichtigt Ihren Anwendungsfall, Ihren Workload-Typ und die Präferenz des CPU-Herstellers sowie die Art und Weise, wie Sie Preis und Leistung priorisieren. Anschließend werden diese Daten verwendet, um Anleitungen und Vorschläge für Amazon-EC2-Instance-Typen bereitzustellen, die für Ihre neuen Workloads am besten geeignet sind.	28. November 2023
Kostenloses Kontingent für EC2	Sie können Ihre Nutzung des kostenlosen EC2-Kontingents im EC2-Dashboard verfolgen.	26. November 2023

Console-to-Code	Console-to-Code kann Ihnen zum Einstieg mit dem Automatisierungscode helfen. Console-to-Code zeichnet Ihre Konsolenaktionen auf und verwendet dann generative KI, um Code in Ihrem bevorzugten Infrastructure-as-Code-Form at vorzuschlagen. Sie können den Code als Ausgangsp unkt verwenden und ihn so anpassen, dass er für Ihren speziellen Anwendungsfall produktionsbereit ist.	26. November 2023
Konfigurierbare Timeouts für die Nachverfolgung von Leerlaufverbindungen	Im Leerlauf befindliche Sicherheitsgruppenverbindun gen können zur Erschöpfung der Kapazität der Verbindun gsnachverfolgung führen und zur Folge haben, dass Verbindungen nicht nachverfo lgt und Pakete verworfen werden. Jetzt können Sie das Timeout für die Nachverfo lgung von Sicherheitsgruppen verbindungen auf einer Elastic-Network-Schnittstelle in Sekunden festlegen.	17. November 2023

PTP-Hardware-Uhr	Unterstützte Instances verfügen jetzt über eine Precision Time Protocol (PTP)-Hardware-Uhr. Die PTP-Hardware-Uhr unterstützt entweder NTP oder eine direkte PTP-Verbindung.	16. November 2023
Ändern Sie den Instance-Typ der Instance, die für den Ruhezustand aktiviert ist	Sie können jetzt den Instance-Typ einer Instance mit Ruhezustands-Unterstützung ändern, wenn sie sich im Zustand `stopped` befindet.	16. November 2023
Instance-Topologie	Sie können die DescribeInstanceTopology API verwenden, um den Standort Ihrer Instances zu ermitteln, und diese Informationen dann verwenden, um HPC- und ML-Jobs zu optimieren, indem Sie sie auf Instances ausführen, die physisch näher beieinander liegen.	13. November 2023
Gemeinsame AMI-Unterstützung für EC2 Fast Launch	Sie können jetzt EC2 Fast Launch auf einem AMI aktivieren, das mit Ihnen geteilt wurde. Wenn Sie EC2 Fast Launch auf einem gemeinsam genutzten AMI aktivieren, werden die vorab bereitgestellten Snapshots für einen schnelleren Start in Ihrem Konto erstellt.	6. November 2023

Kapazitätsblöcke für ML	Sie können GPU-Instances jetzt für einen späteren Zeitpunkt reservieren, um Ihre kurzfristigen Machine-L earning-Workloads (ML) zu unterstützen.	31. Oktober 2023
Spot-Instance-Ruhezustand	Sie können Ihre Spot Instances jetzt in den Ruhezustand versetzen und dabei das gleiche Ruhezusta ndserlebnis und die gleichen Instance-Familien nutzen, die derzeit für On-Demand-Instances verfügbar sind.	24. Oktober 2023
Standardeinstellungen zum Blockieren des öffentlichen Zugriffs für AMIs	Das Blockieren des öffentlic hen Zugriffs für AMIs ist jetzt standardmäßig für alle neuen Konten und für bestehende Konten ohne öffentliche AMIs aktiviert.	20. Oktober 2023
Amazon EC2 Global View	Amazon EC2 Global View unterstützt zusätzliche Ressourcentypen und anpassbare Anzeigeoptionen.	18. Oktober 2023
Unterstützung des Ruhezusta nds für Ubuntu 22.04.2 LTS (Jammy Jellyfish)	Versetzen Sie Ihre neu gestarteten Instances, die vom AMI mit Ubuntu 22.04.2 LTS (Jammy Jellyfish) gestartet wurden, in den Ruhezustand.	16. Oktober 2023

Deaktivieren eines AMIs	Sie können ein AMI deaktivieren, um zu verhindern, dass es für Instance-Starts verwendet wird.	12. Oktober 2023
Verknüpfte EBS-Statusprüfungen	Sie können die verknüpften EBS-Statusprüfungen verwenden, um zu überwachen, ob die mit einer Instance verknüpften Amazon EBS-Volumes erreichbar sind.	11. Oktober 2023
Hibernation-Unterstützung für Red Hat Enterprise Linux 9	Versetzen Sie Ihre neu gestarteten Instances, die von Red Hat Enterprise Linux 9 AMI gestartet wurden, in den Ruhezustand.	02. Oktober 2023
Hibernation-Unterstützung für Microsoft Windows Server 2022	Versetzen Sie Ihre neu gestarteten Instances, die von Microsoft Windows Server 2022 AMI gestartet wurden, in den Ruhezustand.	2. Oktober 2023
Ruhezustands-Unterstützung für AL2023	Versetzen Sie Ihre neu gestarteten Instances, die aus dem AL2023 AMI gestartet wurden, in den Ruhezustand.	02. Oktober 2023
Initiieren der Unterbrechung von Spot-Instances in einer Spot-Flotte	Sie können eine Spot-Flotte in der Amazon-EC2-Konsole auswählen und eine Unterbrechung von Spot Instances in der Flotte zu initiieren, um zu testen, wie die Anwendungen auf Ihren Spot Instances mit Unterbrechungen umgehen.	21. September 2023

Blockieren des öffentlichen Zugriffs auf AMIs	Sie können die Sperrung des öffentlichen Zugriffs für AMIs auf Kontoebene aktivieren, um alle Versuche zu blockieren, Ihre AMIs öffentlich zugänglich zu machen.	12. September 2023
Unterstützung des Ruhezustands für M7i und M7i-flex	Versetzen Sie neu gestartete Instances, die auf Instances vom Typ M7i und M7i-flex ausgeführt werden, in den Ruhezustand.	22. August 2023
EC2-Classic ist veraltet	Mit EC2-Classic wurden EC2-Instances in einem einzigen, flachen Netzwerk ausgeführt, das mit anderen Kunden geteilt wurde. Amazon VPC ersetzt EC2-Classic. Mit Amazon VPC werden Ihre Instances in einer Virtual Private Cloud (VPC) ausgeführt, die logisch von Ihrem AWS-Konto isoliert ist.	08. August 2023
Dedicated Hosts	Sie können Dedicated Hosts bestimmten Hardware-Assets auf einem Outpost zuweisen.	20. Juni 2023
EC2-Instance-Verbindungsendpunkt	Sie können jetzt über SSH oder RDP eine Verbindung zu einer Instance herstellen, ohne dass die Instance eine öffentliche IPv4-Adresse haben muss.	13. Juni 2023

IMDS-Paket-Analysator	Sie können jetzt den IMDS-Paket-Analysator verwenden, um Quellen von IMDSv1-Aufrufen auf Ihren EC2-Instances zu identifizieren.	01. Juni 2023
Bare-Metal-Instances der seriellen EC2-Konsole	Die serielle EC2-Konsole unterstützt jetzt die Konnektivität zur seriellen Schnittstelle ausgewählter Bare-Metal-Instances.	11. April 2023
Quotas für Startvorlagen	Sie können jetzt Ihre Kontingente für Startvorlagen und Startvorlagenversionen in der Service-Quotas-Konsole und mithilfe der Service-Quotas-CLI anzeigen.	03. April 2023
Benachrichtigungen zur Auslastung der Kapazitätsreservierung	AWS Health sendet jetzt Benachrichtigungen, wenn die Kapazitätsauslastung für Kapazitätsreservierungen in Ihrem Konto unter 20 Prozent fällt.	03. April 2023
Kapazitätsreservierungs-Gruppen	Sie können jetzt Kapazitätsreservierungen, die für Sie freigegeben sind, zu Kapazitätsreservierungsgruppen hinzufügen, die Sie besitzen.	30. März 2023
Modifizieren von Instance-Metadatenoptionen	Sie können jetzt die Amazon-EC2-Konsole zum Ändern von Instance-Metadatenoptionen verwenden.	20. März 2023

Direkte Updates für das macOS-Betriebssystem	Sie können jetzt Apple macOS-Betriebssystem-Updates auf M1-Mac-Instances direkt durchführen.	14. März 2023
UEFI Preferred	Sie können jetzt ein einziges AMI erstellen, das sowohl den Unified Extensible Firmware Interface (UEFI) als auch den Legacy BIOS-Startmodus unterstützt.	03. März 2023
Modifizieren eines AMI für IMDSv2	Modifizieren Sie Ihr bestehendes AMI so, dass über das AMI gestartete Instances standardmäßig IMDSv2 erfordern.	28. Februar 2023
Auf Windows-Virtualisierung basierende Sicherheit – Credential Guard	Sie können Credential Guard, ein virtualisierungsbasiertes Sicherheitsfeature (VBS), auf unterstützten Amazon-EC2-Instances aktivieren.	31. Januar 2023
AMI-Alias in Startvorlagen	Sie können in Ihren Startvorlagen einen AWS Systems Manager Parameter anstelle der AMI-ID angeben, um zu vermeiden, dass Sie die Vorlagen jedes Mal aktualisieren müssen, wenn sich die AMI-ID ändert.	19. Januar 2023

Ruhezustand-Unterstützung für C6i, I3en und M6i	Versetzen Sie Ihre neu gestarteten Instances, die auf C6i-, I3en- und M6i-Instance-Typen ausgeführt werden, in den Ruhezustand.	19. Dezember 2022
Torn-Write-Prävention	Verbessern Sie die Leistung Ihrer I/O-intensiven relationalen Datenbank-Workloads und reduzieren Sie die Latenz, ohne die Datenstabilität zu beeinträchtigen, indem Sie das Blockspeicherfeature Torn-Write-Prävention verwenden.	29. November 2022
ENA Express	Erhöhen Sie mit ENA Express den Durchsatz und minimieren Sie die Latenz des Netzwerkverkehrs zwischen EC2-Instances.	28. November 2022
Sperrung der Aufbewahrungsregel für den Papierkorb	Sie können Aufbewahrungsregeln sperren, um sie vor versehentlichen oder böswilligen Änderungen und Löschungen zu schützen.	23. November 2022
Kopieren von AMI-Tags	Wenn Sie ein AMI kopieren, können Sie gleichzeitig Ihre benutzerdefinierten AMI-Tags kopieren.	18. November 2022

AMI-Größe für Speichern und Wiederherstellen	Die Größe eines AMI (vor der Komprimierung), das in und von einem Amazon-S3-Bucket gespeichert und wiederher gestellt werden kann, kann jetzt bis zu 5 000 GB betragen.	16. November 2022
priceCapacityOptimizedZuweisungsstrategie für Spot-Instances	Eine Spot-Flotte, die die `priceCapacityOptimized` -Zuweisungsstrategie verwendet, berücksichtigt sowohl den Preis als auch die Kapazität, um die Pools mit Spot Instances auszuwählen, bei denen die Wahrscheinlichkeit einer Unterbrechung am geringsten ist und die den niedrigstmöglichen Preis haben.	10. November 2022
price-capacity-optimizedZuweisungsstrategie für Spot-Instances	Eine EC2-Flotte, die die `price-capacity-optimized` -Zuweisungsstrategie verwendet, berücksichtigt sowohl den Preis als auch die Kapazität, um die Pools mit Spot Instances auszuwählen, bei denen die Wahrscheinlichkeit einer Unterbrechung am geringsten ist und die den niedrigstmöglichen Preis haben.	10. November 2022

Aufheben der Freigabe eines AMI für Ihr Konto	Wenn ein AMI mit Ihrem geteilt wurde AWS-Konto und Sie nicht mehr möchten, dass es mit Ihrem Konto geteilt wird, können Sie Ihr Konto aus den Startberechtigungen des AMI entfernen.	04. November 2022
Übertragen von Elastic-IP-Adressen	Sie können jetzt Elastic IP-Adressen von einer AWS-Konto zur anderen übertragen.	31. Oktober 2022
Ersetzen von Stamm-Volume	Sie können das Stamm-Amazon-EBS-Volume für eine ausgeführte Instance durch ein AMI ersetzen.	27. Oktober 2022
Automatisches Verbinden einer Instance mit der Datenbank	Verwenden Sie das automatische Verbindungsfeature, um eine oder mehrere EC2-Instances schnell mit einer RDS-Datenbank zu verbinden, um Datenverkehr zwischen ihnen zuzulassen.	10. Oktober 2022
AMI-Kontingente	Kontingente gelten jetzt für das Erstellen und Freigeben von AMIs.	10. Oktober 2022
Konfigurieren von AMI für IMDSv2	Konfigurieren Sie Ihr AMI so, dass über das AMI gestartete Instances standardmäßig IMDSv2 erfordern.	3. Oktober 2022

Initiieren einer Spot-Instance-Unterbrechung	Sie können eine Spot Instance in der Amazon-EC2-Konsole auswählen und eine Unterbrechung initiieren, um zu testen, wie die Anwendungen auf Ihren Spot Instances mit Unterbrechungen umgehen.	26. September 2022
Verifizierter AMI-Anbieter	In der Amazon EC2-Konsole werden öffentliche AMIs, die Amazon oder einem verifizierten Amazon-Partner gehören, mit Verifizierter Anbieter gekennzeichnet.	22. Juli 2022
Platzierungsgruppen auf AWS Outposts	Host-Spread-Strategie für Platzierungsgruppen auf einem Outpost hinzugefügt.	30. Juni 2022
Bedingungsschlüssel für den Papierkorb	Sie können die Bedingungsschlüssel `rbin:Request/ResourceType` und `rbin:Attribute/ResourceType` zum Filtern des Zugriffs auf Papierkorb-Anforderungen verwenden.	14. Juni 2022
`io2`-Block-Express-Volumes	Sie können die Größe und die bereitgestellten IOPS von `io2`-Block-Express-Volumes ändern und Sie können sie für eine schnelle Snapshot-Wiederherstellung aktivieren.	31. Mai 2022
Dedizierte Hosts auf AWS Outposts	Sie können Dedicated Hosts auf AWS Outposts zuweisen.	31. Mai 2022

Beendungsschutz der Instances	Wenn Sie verhindern möchten, dass Ihre Instance versehentlich gestoppt wird, können Sie den Stopp-Schutz für die Instance aktivieren.	24. Mai 2022
UEFI Secure Boot	UEFI Secure Boot baut auf dem langjährigen sicheren Startprozess von Amazon EC2 auf und bietet zusätzliche Funktionen, mit defense-in-depth denen Kunden Software vor Bedrohungen schützen können, die auch nach Neustarts bestehen.	10. Mai 2022
NitroTPM	Das Nitro Trusted Platform Module (NitroTPM) ist ein virtuelles Gerät, das vom AWS Nitro-System bereitgestellt wird und der TPM 2.0-Spezifikation entspricht.	10. Mai 2022
AMI-Status-Änderungsereignisse	Amazon EC2 generiert jetzt ein Ereignis, wenn ein AMI den Status ändert. Sie können Amazon verwenden EventBridge , um diese Ereignisse zu erkennen und darauf zu reagieren.	9. Mai 2022
Beschreiben öffentlicher Schlüssel	Sie können den öffentlichen Schlüssel und das Erstellungsdatum eines Amazon-EC2-Schlüsselpaares abfragen.	28. April 2022

Erstellen von Schlüsselpaaren	Sie können das Schlüsselformat (PEM oder PPK) angeben, wenn Sie ein neues Schlüsselpaar erstellen.	28. April 2022
Bereitstellen von Amazon-FSx-Dateisystemen beim Start	Sie können ein neues oder vorhandenes Amazon FSx for NetApp ONTAP- oder Amazon FSx for OpenZFS-Dateisystem beim Start mithilfe des Assistenten für neue Instances bereitstellen.	12. April 2022
Neuer Launch Instance Wizard	Eine neue und verbesserte Start-Erfahrung in der Amazon-EC2-Konsole mit einer schnelleren und einfacheren Möglichkeit, EC2-Instances zu starten.	5. April 2022
Öffentliche AMIs automatisch als veraltet kennzeichnen	Standardmäßig ist das Veralterungsdatum aller öffentlichen AMIs auf zwei Jahre ab dem AMI-Erstellungsdatum festgelegt.	31. März 2022
Kategorie Instance-Metadaten: Autoscaling/Target-Lebenszyklusstatus	Wenn Sie Auto-Scaling-Gruppen verwenden, können Sie über die Instance-Metadaten auf den Target-Lebenszyklusstatus einer Instance zugreifen.	24. März 2022
Zeitpunkt des letzten AMI-Starts	`lastLaunchedTime` gibt an, wann Ihr AMI zuletzt zum Starten einer Instance verwendet wurde.	28. Februar 2022

Papierkorb für AMIs	Über den Papierkorb können Sie versehentlich gelöschte AMIs wiederherstellen.	3. Februar 2022
ED25519-Schlüssel	ED25519-Schlüssel werden jetzt für die EC2-Instance Connect und die serielle EC2-Konsole unterstützt.	20. Januar 2022
Weitere RHEL-Plattformen für Kapazitätsreservierungen	Weitere Red Hat Enterprise Linux-Plattformen für Kapazität sreservierungen on demand.	11. Januar 2022
Konfigurieren von Windows-AMIs für schnelleres Starten	Konfigurieren Sie Windows-AMIs so, dass Instances mit vorab bereitgestellten Snapshots bis zu 65 % schneller gestartet werden.	10. Januar 2022
Instance-Tags in Instance-Metadaten	Sie können über die Instance-Metadaten auf die Tags einer Instance zugreifen.	6. Januar 2022
Kapazitätsreservierungen in Cluster-Placement-Gruppen	Sie können Kapazitätsreservierungen in Cluster-Placement-Gruppen erstellen.	6. Januar 2022
Papierkorb für Amazon-EBS-Snapshots	Der Papierkorb für Amazon-EBS-Snapshots ist ein Snapshot-Wiederherstellungsfeature, mit dem Sie versehentlich gelöschte Snapshots wiederherstellen können.	29. November 2021

Spot-Flotte launch-before-terminate	Die Spot-Flotte kann die Spot-Instances beenden, die eine Neuausgleichsbenachrichtigung erhalten, nachdem neue Ersatz-Spot-Instances gestartet wurden.	4. November 2021
EC2-Flotte launch-before-terminate	Die EC2-Flotte kann die Spot-Instances beenden, die eine Neuausgleichsmeldung erhalten, nachdem neue Ersatz-Spot-Instances gestartet wurden.	4. November 2021
Vergleichen von Zeitstempeln	Sie können den tatsächlichen Zeitpunkt eines Ereignisses ermitteln, indem Sie den Zeitstempel Ihrer Amazon EC2 EC2-Linux-Instance mit vergleichen. ClockBound	2. November 2021
Gemeinsame AMIs mit Organisationen und OEs	Sie können AMIs jetzt mit den folgenden AWS Ressourcen teilen: Organisationen und Organisationseinheiten (OUs).	29. Oktober 2021
Spot-Platzierungsbewertung	Holen Sie sich eine Empfehlung für eine AWS Region oder Availability Zone auf der Grundlage Ihrer Spot-Kapazitätsanforderungen.	27. Oktober 2021
Attributbasierte Instance-Typauswahl für Spot-Flotte	Geben Sie die Attribute an, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen.	27. Oktober 2021

Attributbasierte Auswahl von Instance-Typen für EC2-Flotte	Geben Sie die Attribute an, die eine Instance haben muss, und Amazon EC2 identifiziert alle Instance-Typen mit diesen Attributen.	27. Oktober 2021
On-Demand-Kapazitätsreservierungsflotte	Sie können eine Kapazitätsreservierungsflotte verwenden, um eine Gruppe oder Flotte von Kapazitätsreservierungen zu starten.	5. Oktober 2021
Unterstützung des Ruhezustands für Ubuntu 20.04 LTS (Focal)	Versetzen Sie Ihre neu gestarteten Instances, die vom AMI mit Ubuntu 20.04 LTS (Focal) gestartet wurden, in den Ruhezustand.	4. Oktober 2021
EC2-Flottenreservierungen und gezielte On-Demand-Kapazitätsreservierungen	EC2-Flotte kann On-Demand-Instances in `targeted`-Kapazitätsreservierungen starten.	22. September 2021
T3-Instances auf Dedicated Hosts	Support für T3-Instances auf Amazon-EC2-Dedicated-Host.	14. September 2021
Ruhezustand-Support für RHEL, Fedora und CentOS	Versetzen Sie Ihre neu gestarteten Instances, die von RHEL-, Fedora- und CentOS-AMIs gestartet wurden, in den Ruhezustand.	9. September 2021
Amazon EC2 Global View	Mit Amazon EC2 Global View können Sie VPCs, Subnetze, Instances, Sicherheitsgruppen und Volumes in mehreren AWS Regionen in einer einzigen Konsole anzeigen.	1. September 2021

Unterstützung für AMI-Veralterung für Amazon Data Lifecycle Manager	Von Amazon Data Lifecycle Manager EBS-unterstützte AMI-Richtlinien können AMIs veralten. Die AWSDataLifecycleManagerServiceRoleForAMIManagement AWS verwaltete Richtlinie wurde aktualisiert, um diese Funktion zu unterstützen.	23. August 2021
Ruhezustand-Unterstützung für C5d, M5d und R5d	Versetzen Sie Ihre neu gestarteten Instances, die auf C5d-, M5d- und R5d-Instance-Typen ausgeführt werden, in den Ruhezustand.	19. August 2021
Amazon-EC2-Schlüsselpaare	Amazon EC2 unterstützt jetzt ED25519-Schlüssel auf Linux- und Mac-Instances.	17. August 2021
Präfixe für Netzwerkschnittstellen	Sie können Ihren Netzwerkschnittstellen einen privaten IPv4- oder IPv6-CIDR-Bereich entweder automatisch oder manuell zuweisen.	22. Juli 2021
Ereignisfenster	Sie können benutzerdefinierte, wöchentlich wiederkehrende Ereignisfenster für geplante Ereignisse definieren, die Ihre Amazon-EC2-Instances neu starten, anhalten oder beenden.	15. Juli 2021

Unterstützung für Ressourcen-IDs und Markierung bei Sicherheitsgruppenregeln	Sie können auf Sicherheitsgruppenregeln nach Ressourcen-ID verweisen. Sie können Ihren Sicherheitsgruppenregeln auch Tags hinzufügen.	7. Juli 2021
AMI als veraltet kennzeichnen	Sie können jetzt angeben, wann ein AMI veraltet ist.	11. Juni 2021
Sekundengenaue Abrechnung für Windows	Amazon EC2 rechnet die Windows- und SQL-Server-basierte Nutzung sekundengenau ab; es wird eine Mindestgebühr von einer Minute berechnet.	10. Juni 2021
Kapazitätsreservierungen am AWS Outposts	Sie können jetzt Kapazitätsreservierungen auf AWS Outposts nutzen.	24. Mai 2021
Freigabe einer Kapazitätsreservierung	Sie können jetzt in Local Zones und Wavelength Zones erstellte Kapazitätsreservierungen freigeben.	24. Mai 2021
Root-Volume-Ersatz	Sie können jetzt die Aufgaben Stammvolumenersatz verwenden, um das EBS-Stammvolumen für laufende Instances zu ersetzen.	22. April 2021
Speichern und Wiederherstellen eines AMI mit S3	Speichern Sie EBS-gestützte AMIs in S3 und stellen Sie sie aus S3 wieder her, um das partitionsübergreifende Kopieren von AMIs zu ermöglichen.	6. April 2021

Serielle EC2-Konsole	Beheben Sie Probleme mit dem Start und der Netzwerkkonnektivität, indem Sie eine Verbindung zum seriellen Port einer Instance herstellen.	30. März 2021
Startmodi	Amazon EC2 unterstützt jetzt UEFI-Boot auf ausgewählten AMD- und Intel-basierten EC2-Instances.	22. März 2021
Erstellen eines Reverse-DNS-Datensatzes	Sie können jetzt DNS-Rückwärtssuche für Ihre Elastic IP-Adressen einrichten.	3. Februar 2021
Markieren von AMIs und Snapshots bei AMI-Erstellung	Wenn Sie ein AMI erstellen, können Sie das AMI und die Snapshots mit denselben Tags (Markierungen) markieren oder sie mit verschiedenen Tags (Markierungen) markieren.	4. Dezember 2020
Verwenden Sie Amazon EventBridge , um Spot-Flottenereignisse zu überwachen	Erstellen Sie EventBridge Regeln, die als Reaktion auf Statusänderungen und Fehler von Spot Fleet programmatische Aktionen auslösen.	20. November 2020
Verwenden Sie Amazon EventBridge , um EC2-Flottenereignisse zu überwachen	Erstellen Sie EventBridge Regeln, die als Reaktion auf Statusänderungen und Fehler der EC2-Flotte programmgesteuerte Aktionen auslösen.	20. November 2020

Löschen von instant-Flotten	Löschen Sie einen EC2-Flotte vom Typ `instant` und beenden Sie alle Instances in der Flotte in einem einzigen API-Aufruf.	18. November 2020
Ruhezustand-Unterstützung für T3 und T3a	Versetzen Ihre neu gestarteten Instances, die auf T3- und T3a-Instance-Typen ausgeführt werden, in den Ruhezustand.	17. November 2020
Amazon EFS Quick Create	Mit Amazon EFS Quick Create können Sie beim Start ein Amazon EFS-Dateisystem erstellen und in eine Instance einbinden.	9. November 2020
Kategorie der Instance-Metadaten: events/recommendations/rebalance	Die ungefähre Zeit in UTC, zu der die Empfehlungsbenachrichtigung des EC2-Instance-Neuausgleichs für die Instance ausgesendet wird.	4. November 2020
Empfehlung zum Ausgleich von EC2-Instance	Ein Signal, das Sie benachrichtigt, wenn eine Spot-Instance ein erhöhtes Unterbrechungsrisiko hat.	4. November 2020
Kapazitätsreservierungen in Wavelength-Zonen	Kapazitätsreservierungen kann nun erstellt und in den Wavelength Zones verwendet werden.	4. November 2020

Kapazitätsausgleich	Konfigurieren Sie eine Spot-Flotte oder eine EC2-Flotte, um eine Ersatz-Spot-Instance zu starten, wenn Amazon EC2 eine Empfehlung zum Neuausgleich ausgibt.	4. November 2020
Ruhezustand-Unterstützung für I3, M5ad und R5ad	Versetzen Sie Ihre neu gestarteten Instances, die auf I3-, M5ad- und R5ad-Instance-Typen ausgeführt werden, in den Ruhezustand.	21. Oktober 2020
vCPU-Limits für Spot-Instances	Spot-Instance-Limits werden nun in Bezug auf die Anzahl der vCPUs verwaltet, die Ihre ausgeführten Spot-Instances entweder verwenden oder bis zur Erfüllung offener Anforderungen verwenden werden.	1. Oktober 2020
Kapazitätsreservierungen in Local Zones	Kapazitätsreservierungen kann nun in Local Zones erstellt und verwendet werden.	30. September 2020
Ruhezustand-Unterstützung für M5a und R5a	Versetzen Sie Ihre neu gestarteten Instances, die auf M5a- und R5a-Instance-Typen ausgeführt werden, in den Ruhezustand.	28. August 2020
Instance-Metadaten bieten Informationen zu Speicherort und Platzierung	Neue Instance-Metadatenfelder unter der Kategorie `placement` : Region, Placement-Gruppennname, Partitionsnummer, Host-ID und Availability Zone-ID.	24. August 2020

Kapazitätsreservierungs-Gruppen	Sie können AWS Resource Groups verwenden, um logische Sammlungen von Kapazitätsreservierungen zu erstellen und dann Zielinstanzen in diesen Gruppen zu starten.	29. Juli 2020
EC2Launch v2	Sie können EC2Launch v2 zum Ausführen von Aufgaben während des Instance-Startups verwenden, wenn eine Instance gestoppt und später gestartet wird, wenn eine Instance neu gestartet wird, sowie bei Bedarf. EC2Launch v2 unterstützt alle Versionen von Windows Server und ersetzt EC2Launch und EC2Config.	30. Juni 2020
Mitbringen der eigenen IPv6-Adressen	Sie können Ihren IPv6-Adressbereich ganz oder teilweise aus Ihrem lokalen Netzwerk auf Ihr AWS Konto übertragen.	21. Mai 2020
Starten von Instances mithilfe eines Systems-Manager-Parameters	Sie können einen AWS Systems Manager Parameter anstelle eines AMI angeben, wenn Sie eine Instance starten.	5. Mai 2020

Anpassen geplanter Ereignisbenachrichtigungen	Sie können geplante Ereignisbenachrichtigungen so anpassen, dass Tags (Markierungen) in die E-Mail-Benachrichtigung aufgenommen werden.	4. Mai 2020
Amazon-Linux-2-Kernel-Live-Patching	Kernel-Live-Patching für Amazon Linux 2 ermöglicht es Ihnen, Patches für Schwachstellen und kritische Fehler auf einen laufenden Linux-Kernel anzuwenden, ohne Neustarts oder Unterbrechungen der laufenden Anwendungen.	28. April 2020
Windows Server auf Dedicated Hosts	Sie können Windows Server-AMIs verwenden, die von Amazon bereitgestellt werden, um die neuesten Versionen von Windows Server auf Dedicated Hosts auszuführen.	7. April 2020
Stoppen und Starten einer Spot-Instance	Stoppen Sie Ihre von Amazon EBS unterstützten Spot-Instances und starten Sie sie nach Belieben, anstatt sich auf das Stop-Unterbrechungsverhalten zu verlassen.	13. Januar 2020

Ressourcen-Markierung	Sie können Internet-Gateways nur für ausgehend en Datenverkehr, lokale Gateways, Routing-Tabellen für lokale Gateways, virtuelle Schnittstellen von lokalen Gateways, virtuelle Schnittst ellengruppen von lokalen Gateways, VPC-Zuordnungen von Routing-Tabellen für lokale Gateways mit Tags (Markierungen) versehen.	10. Januar 2020
Verbinden mit Instance über Session Manager	Sie können eine Session Manager-Sitzung mit einer Instance über die Amazon EC2-Konsole starten.	18. Dezember 2019
Dedicated Hosts und Hostressourcengruppen	Dedicated Hosts kann nun mit Hostressourcengruppen verwendet werden.	02. Dezember 2019
Dedicated-Host-Freigabe	Sie können Ihre Dedicated Hosts jetzt für mehrere AWS Konten gemeinsam nutzen.	02. Dezember 2019
Standardmäßige Guthaben-Spezifikation auf Kontoebene	Sie können die Standard-Kreditspezifikation pro Instance-Familie mit Burstable -Performance auf Kontoebene pro AWS Region festlegen.	25. November 2019
Erkennung von Instance-Typen	Sie können einen Instance-Typ finden, der Ihren Anforderungen entspricht.	22. November 2019

Dedicated Hosts	Sie können nun einen Dedicated Host konfigurieren, um mehrere Instance-Typen in einer Instance-Familie zu unterstützen.	21. November 2019
Instance Metadata Service Version 2	Sie können Instance-Metadatenservice Version 2 verwenden. Es handelt sich um eine sitzungsorientierte Methode zum Anfordern von Instance-Metadaten.	19. November 2019
Elastic Fabric Adapter	Elastic Fabric-Adapter können jetzt auch mit Intel MPI 2019 Update 6 verwendet werden.	15. November 2019
Ruhezustand-Unterstützung für On-Demand-Windows-Instances	Sie können On-Demand-Windows-Instances in den Ruhezustand versetzen.	14. Oktober 2019
In die Warteschlange gestellte Käufe von Reserved Instances	Sie können den Kauf einer Reserved Instance bis zu drei Jahre im Voraus in die Warteschlange einstellen.	4. Oktober 2019
Diagnose-Interrupt	Sie können einen Diagnose-Interrupt an eine unerreich bare oder nicht reagierende Instance senden, um eine Kernel-Panik auszulösen.	14. August 2019
Kapazitätsoptimierte Zuweisungsstrategie	Mithilfe von EC2-Flotten oder Spot-Flotten können Sie Spot-Instances aus Spot-Pools mit optimaler Kapazität für die gestartete Anzahl von Instances starten.	12. August 2019

On-Demand-Kapazitätsreservierungs-Freigabe	Sie können Ihre Kapazitätsreservierungen jetzt für mehrere AWS Konten gemeinsam nutzen.	29. Juli 2019
Elastic Fabric Adapter	EFA unterstützt jetzt Open MPI 3.1.4 und Intel MPI 2019 Update 4.	26. Juli 2019
EC2 Instance Connect	EC2 Instance Connect bietet mit Secure Shell (SSH) eine einfache und sichere Möglichkeit, eine Verbindung zu Ihren Instances herzustellen.	27. Juni 2019
Host-Wiederherstellung	Starten Sie Ihre Instance bei einem unerwarteten Hardware-Ausfall auf einem Dedicated Host auf einem neuen Host neu.	5. Juni 2019
Anwendungskonsistente VSS-Snapshots	Erstellen Sie mit Run Command anwendungskonsistente Snapshots aller Amazon EBS-Volumes, die an Ihre Windows-Instances angehängt sind. AWS Systems Manager	13. Mai 2019
Assistent zum Ändern der Plattform von Windows auf Linux für Microsoft SQL Server-Datenbanken	Verschieben Sie vorhandene Microsoft SQL Server-Workloads von einem Windows- zu einem Linux-Betriebssystem.	8. Mai 2019

Automatisiertes Windows-Upgrade	Führen Sie automatisierte Upgrades von EC2-Windows-Instances durch mit. AWS Systems Manager	6. Mai 2019
Elastic Fabric Adapter	Sie können einen Elastic Fabric Adapter an Ihre Instances anfügen, um High Performance Computing (HPC)-Anwendungen zu beschleunigen.	29. April 2019

Informationen zu den Instance-Typ-Releases für Amazon EC2 finden Sie unter Dokumentverlauf im Amazon EC2 Instance Types Guide.

Historie für 2018 und früher

In der folgenden Tabelle werden wichtige Ergänzungen des Amazon EC2 EC2-Benutzerhandbuchs im Jahr 2018 und in früheren Jahren beschrieben.

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Partitions-Placement-Gruppen	15.11.2016	Partitions-Placement-Gruppen verteilen Instances über logische Partitionen. Sie gewährleisten dabei, dass Instances in einer Partition keine zugrunde liegende Hardware mit Instances in anderen Partitionen teilen. Weitere Informationen finden Sie unter Partitions-Placement-Gruppen.	20. Dezember 2018
Ruhezustand bei EC2 Linux-Instances	15.11.2016	Sie können eine Linux-Instance nur dann in den Ruhezustand versetzen, wenn sie für den Ruhezustsand aktiviert ist und die Vorausset	28. November 2018

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
		zungen für den Ruhezustand erfüllt. Weitere Informationen finden Sie unter Versetzen Sie Ihre Amazon EC2 EC2-Instance in den Ruhezustand.	
Amazon Elastic Inference Accelerators	15.11.2016	Sie können Ihren Instances einen Amazon EI-Accelerator hinzufügen, um GPU-gesteuerte Beschleunigung zu nutzen und dadurch die Kosten für die Ausführung von Deep Learning-Inferenz zu senken.	28. November 2018
Spot-Konsole empfiehlt eine Flotte von Instances	15.11.2016	Die Spot-Konsole empfiehlt eine Flotte von Instances, die auf den bewährten Methoden für Spot basieren (Instance-Diversifizierung), um die minimalen Hardwarespezifikationen (vCPUs, Arbeitsspeicher und Speicherplatz) für Ihre Anwendung zu erfüllen. Weitere Informationen finden Sie unter Erstellen eine Spot-Flotten-Anforderung.	20. November 2018
Neuer EC2-Flotte-Typ der Anforderung: instant	15.11.2016	EC2-Flotte unterstützt nun einen neuen Typ der Anforderung, `instant`. Damit können Sie Kapazitäten über Instance-Typen und Einkaufsmodelle hinweg synchron bereitstellen. Die `instant`-Anforderung gibt die gestarteten Instances in der API-Antwort zurück und führt keine weiteren Aktionen durch, sodass Sie steuern können, ob und wann Instances gestartet werden. Weitere Informationen finden Sie unter EC2-Flotte-Anforderungstypen.	14. November 2018

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Informationen zu Spot-Einsparungen	15.11.2016	Sie können die Einsparungen anzeigen, die durch die Verwendung von Spot-Instances für eine einzelne Spot-Flotte oder für alle Spot-Instances erzielt wurden. Weitere Informationen finden Sie unter Einsparungen durch den Spot-Instances-Einkauf.	5. November 2018
Konsolenunterstützung zur Optimierung der CPU-Optionen	15.11.2016	Wenn Sie eine Instance starten, können Sie die CPU-Optionen mithilfe der Amazon EC2-Konsole für bestimmte Workloads oder Geschäftsanforderungen optimieren. Weitere Informationen finden Sie unter CPU-Optionen optimieren.	31. Oktober 2018
Konsolenunterstützung zum Erstellen einer Startvorlage anhand einer Instance	15.11.2016	Mithilfe der Amazon EC2-Konsole können Sie eine Startvorlage über eine Instance als Grundlage für eine neue Startvorlage anlegen. Weitere Informationen finden Sie unter Erstellen einer Startvorlage.	30. Oktober 2018
On-Demand Capacity Reservations	15.11.2016	Sie können Kapazität für Ihre Amazon EC2-Instances in einer bestimmten Availability Zone für einen beliebigen Zeitraum reservieren. Auf diese Weise können Sie Kapazitätsreservierungen unabhängig von den Abrechnungsrabatten der Reserved Instances (RI) anlegen und verwalten. Weitere Informationen finden Sie unter On-Demand Capacity Reservations.	25. Oktober 2018

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Eigene IP-Adressen mitbringen (BYOIP)	15.11.2016	Sie können Ihren öffentlichen IPv4-Adressbereich ganz oder teilweise aus Ihrem lokalen Netzwerk auf Ihr Konto übertragen. AWS Nachdem Sie den Adressbereich auf übertragen haben AWS, wird er in Ihrem Konto als Adresspool angezeigt. Sie können eine elastische IP-Adresse aus Ihrem Adresspool erstellen und diese mit Ihren AWS -Ressourcen verwenden. Weitere Informationen finden Sie unter Bring Your Own IP Addresses (BYOIP) in Amazon EC2.	23. Oktober 2018
Dedicated Host-Tags (Markierungen) beim Erstellen und Konsolenunterstützung	15.11.2016	Sie können Ihre Dedicated Hosts bei der Erstellung markieren und Ihre Dedicated Host-Tags (Markierungen) mithilfe der Amazon EC2-Konsole verwalten. Weitere Informationen finden Sie unter Zuordnen von Dedicated Hosts.	08. Oktober 2018
Konsolenunterstützung für geplante Skalierungsaktionen für Spot-Flotten	15.11.2016	Erhöhen oder Verringern der aktuellen Kapazität der Flotte auf Grundlage von Datum und Zeit. Weitere Informationen finden Sie unter Skalieren der Spot-Flotte mit geplanter Skalierung.	20. September 2018

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Zuweisungsstrategien für EC2-Flotten	15.11.2016	Sie können angeben, ob die On-Demand-Kapazität nach Preis (niedrigster Preis an erster Stelle) oder nach Priorität (höchste Priorität an erster Stelle) erfüllt wird. Sie können die Anzahl der Spot-Pools angeben, über die Ihre Spot-Zielkapazität zugewiesen werden soll. Weitere Informationen finden Sie unter Zuweisungsstrategien für Spot-Instances.	26. Juli 2018
Zuweisungsstrategien für Spot-Flotten	15.11.2016	Sie können angeben, ob die On-Demand-Kapazität nach Preis (niedrigster Preis an erster Stelle) oder nach Priorität (höchste Priorität an erster Stelle) erfüllt wird. Sie können die Anzahl der Spot-Pools angeben, über die Ihre Spot-Zielkapazität zugewiesen werden soll. Weitere Informationen finden Sie unter Zuweisungsstrategien für Spot-Instances.	26. Juli 2018
Automatisieren des Snapshot-Lebenszyklus	15.11.2016	Sie können mit Amazon Data Lifecycle Manager das Erstellen und Löschen von Snapshots für Ihre EBS-Volumes automatisieren. Weitere Informationen finden Sie unter Amazon Data Lifecycle Manager.	12. Juli 2018
CPU-Optionen für Startvorlagen	15.11.2016	Wenn Sie unter Verwendung der Befehlszeilen-Tools eine Vorlage starten, können Sie die CPU-Optionen für bestimmte Workloads oder Geschäftsanforderungen optimieren. Weitere Informationen finden Sie unter Erstellen einer Startvorlage.	11. Juli 2018

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Dedicated Hosts markieren	15.11.2016	Sie können Ihre Dedicated Hosts markieren. Weitere Informationen finden Sie unter Dedicated Hosts markieren.	3. Juli 2018
Abrufen der neuesten Konsolenausgabe	15.11.2016	Sie können die neueste Konsolenausgabe für einige Instance-Typen abrufen, wenn Sie den Befehl AWS CLI get-console-output verwenden.	9. Mai 2018
CPU-Optionen optimieren	15.11.2016	Wenn Sie eine Instance starten, können Sie die CPU-Optionen für bestimmte Workloads oder Geschäftsanforderungen optimieren. Weitere Informationen finden Sie unter CPU-Optionen optimieren.	8. Mai 2018
EC2 Fleet	15.11.2016	Sie können EC2 Fleet verwenden, um eine Gruppe von Instances über verschiedene EC2-Instance-Typen und Availability Zones sowie über On-Demand-Instance-, Reserved-Instance- und Spot-Instance-Kaufmodelle hinweg zu starten. Weitere Informationen finden Sie unter EC2-Flotte.	2. Mai 2018
On-Demand-Instances in Spot-Flotten	15.11.2016	Sie können eine Anforderung nach On-Demand-Kapazität in Ihre Spot-Flotten-Anforderung aufnehmen, um sicherzustellen, dass Sie immer über Instance-Kapazität verfügen. Weitere Informationen finden Sie unter Spot-Flotte.	2. Mai 2018

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
EBS-Snapshots bei der Erstellung mit Tags (Markierungen) versehen	15.11.2016	Sie können Snapshots während der Erstellung mit Tags (Markierungen) versehen.	2. April 2018
Placement-Gruppen ändern	15.11.2016	Sie können eine Instance in oder aus einer Platzierungsgruppe verschieben oder deren Platzierungsgruppe ändern. Weitere Informationen finden Sie unter Ändern der Platzierungsgruppe für eine Instance.	1. März 2018
Längere Ressourcen-IDs	15.11.2016	Sie können das längere ID-Format für weitere Ressourcentypen aktivieren. Weitere Informationen finden Sie unter Ressourcen-IDs.	9. Februar 2018
Verbesserungen der Netzwerkleistung	15.11.2016	Instances außerhalb einer Cluster Placement-Gruppe können jetzt von einer erhöhten Bandbreite profitieren, wenn sie Netzwerkverkehr zwischen anderen Instances oder Amazon S3 senden oder empfangen.	24. Januar 2018
Elastic IP-Adressen markieren	15.11.2016	Sie können Ihre Elastic IP-Adressen markieren. Weitere Informationen finden Sie unter Markieren einer Elastic IP-Adresse.	21. Dezember 2017
Amazon Time Sync Service	15.11.2016	Sie können den Amazon Time Sync Service verwenden, um zuverlässige Zeiteinstellungen für Ihre Instance zu gewährleisten. Weitere Informationen finden Sie unter Stellen Sie die Zeit für Ihre Amazon EC2 EC2-Instance ein.	29. November 2017

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
T2 Unlimited	15.11.2016	T2 Unlimited-Instances können die Leistung so lange, wie nötig, über die Baseline hinaus steigern. Weitere Informationen finden Sie unter Burstable Performance Instances.	29. November 2017
Startvorlagen	15.11.2016	Eine Startvorlage kann alle oder einige der Parameter zum Starten einer Instance enthalten. Auf diese Weise müssen Sie sie nicht jedes Mal angeben, wenn Sie eine Instance starten. Weitere Informationen finden Sie unter Starten einer Instance über eine Startvorlage.	29. November 2017
Spread Placement	15.11.2016	Spread Placement-Gruppen werden für Anwendungen mit einer geringen Anzahl kritischer Instances empfohlen, die getrennt voneinander gehalten werden sollten. Weitere Informationen finden Sie unter Spread Placement-Gruppen.	29. November 2017
Spot-Instance-Ruhezustand	15.11.2016	Der Spot-Service kann Spot-Instances im Falle einer Unterbrechung in den Ruhezustand versetzen. Weitere Informationen finden Sie unter Unterbrochene Spot-Instances in den Ruhezustand versetzen.	28. November 2017
Spot-Flotten-Zielverfolgung	15.11.2016	Sie können Skalierungsrichtlinien für die Zielverfolgung für Ihre Spot-Flotte einrichten. Weitere Informationen finden Sie unter Skalieren der Spot-Flotte anhand einer Zielverfolgungsrichtlinie.	17. November 2017

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Spot-Flotten können in Elastic Load Balancing integriert werden.	15.11.2016	Sie können einen oder mehrere Load Balancer an eine Spot-Flotte anfügen.	10. November 2017
Zusammenführen und Teilen von Convertible Reserved Instances	15.11.2016	Sie können zwei oder mehrere Convertible Reserved Instances durch eine neue Convertible Reserved Instance ersetzen (bzw. in einer neuen zusammenführen). Außerdem können Sie eine Convertible Reserved Instance durch diesen Prozess in kleinere Reservierungen aufteilen. Weitere Informationen finden Sie unter Austauschen von Convertible Reserved Instances.	6. November 2017
Ändern der VPC-Tenancy	15.11.2016	Das Attribut für die Instance-Tenancy einer VPC kann von `dedicated` in `default` geändert werden. Weitere Informationen finden Sie unter Ändern der Tenancy einer VPC.	16. Oktober 2017
Sekundengenaue Abrechnung	15.11.2016	Amazon EC2 rechnet die Linux-basierte Nutzung sekundengenau ab; es wird eine Mindestgebühr von einer Minute berechnet.	2. Oktober 2017
Stopp bei Unterbrechungen	15.11.2016	Sie können angeben, ob Amazon EC2 angehalten werden oder Spot-Instances beenden soll, wenn diese unterbrochen werden. Weitere Informationen finden Sie unter Verhalten von Spot-Instance-Unterbrechungen.	18. September 2017

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Markieren von NAT-Gateways	15.11.2016	Sie können Ihren NAT-Gateway markieren. Weitere Informationen finden Sie unter Markieren Ihrer -Ressourcen mit Tags (Markierungen).	7. September 2017
Beschreibungen der Sicherheitsgruppenregel	15.11.2016	Sie können Ihren Sicherheitsgruppenregeln Beschreibungen hinzufügen. Weitere Informationen finden Sie unter Sicherheitsgruppenregeln.	31. August 2017
Elastic Graphics	15.11.2016	Fügen Sie Ihren Instances Elastic Graphics-Accelerators hinzu, um die Grafikleistung Ihrer Anwendungen zu verbessern.	29. August 2017
Wiederherstellen von Elastic IP-Adressen	15.11.2016	Wenn Sie eine Elastic IP-Adresse für die Verwendung in einer VPC freigeben, können Sie sie möglicherweise wiederherstellen. Weitere Informationen finden Sie unter Wiederherstellen einer Elastic-IP-Adresse.	11. August 2017
Markieren von Spot-Flotten-Instances	15.11.2016	Sie können Ihre Spot-Flotte so konfigurieren, dass die gestarteten Instances automatisch markiert werden.	24. Juli 2017

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Zuordnung von Tags (Markierungen) zu Ressourcen während der Erstellung	15.11.2016	Sie können Instances und Volumes zum Zeitpunkt der Erstellung Tags (Markierungen) zuordnen. Weitere Informationen finden Sie unter Markieren Ihrer -Ressourcen mit Tags (Markierungen). Darüber hinaus können Sie Tag (Markierung)-basierte Berechtigungen auf Ressourcenebene dazu verwenden, die Tags (Markierungen) zu kontrollieren, die angewendet werden. Weitere Informationen finden Sie unter Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.	28. März 2017
Durchführen von Modifikationen bei angefügten EBS-Volumes	15.11.2016	Bei den meisten an EC2-Instances angefügten EBS-Volumes können Sie Volume-Größe, -Typ und -IOPS modifizieren, ohne das Volume zu trennen oder die Instance anzuhalten.	13. Februar 2017
Hinzufügen einer IAM-Rolle	15.11.2016	Sie können eine IAM-Rolle zu einer bestehenden Instance hinzufügen, sie von der Instance trennen oder sie ersetzen. Weitere Informationen finden Sie unter IAM-Rollen für Amazon EC2.	9. Februar 2017
Dedicated Spot Instances	15.11.2016	Sie können Spot-Instances auf Single-Tenant-Hardware in einer Virtual Private Cloud (VPC) ausführen. Weitere Informationen finden Sie unter Angeben einer Tenancy für Ihre Spot-Instances.	19. Januar 2017

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
IPv6-Support	15.11.2016	Sie können Ihrer VPC und den Subnetzen einen IPv6 CIDR-Block zuordnen und den Instances in der VPC IPv6-Adressen zuweisen. Weitere Informationen finden Sie unter IP-Adressierung von Amazon EC2-Instances.	1. Dezember 2016
Automatische Skalierung für Spot-Flotten		Sie können jetzt Skalierungsrichtlinien für Ihre Spot-Flotte einrichten. Weitere Informationen finden Sie unter Automatische Skalierung für Spot-Flotten.	1. September 2016
Elastic Network Adapter (ENA)	01.04.2016	Sie können ENA jetzt für Enhanced Networking verwenden. Weitere Informationen finden Sie unter Unterstützung von Enhanced Networking.	28. Juni 2016
Erweiterte Unterstützung für das Anzeigen und Ändern längerer IDs	01.04.2016	Sie können jetzt längere ID-Einstellungen für andere IAM-Benutzer, IAM-Rollen oder den Stammbenutzer anzeigen und ändern. Weitere Informationen finden Sie unter Ressourcen-IDs.	23. Juni 2016
Verschlüsselte Amazon EBS-Snapshots zwischen Konten kopieren AWS	01.04.2016	Sie können jetzt verschlüsselte EBS-Snapshots zwischen Konten kopieren. AWS	21. Juni 2016
Aufnehmen eines Screenshots einer Instance-Konsole	01.10.2015	Sie können jetzt zusätzliche Informationen erhalten, wenn Sie ein Debugging bei Instances vornehmen, die nicht erreichbar sind. Weitere Informationen finden Sie unter Aufnehmen eines Screenshots einer nicht erreichbaren Instance.	24. Mai 2016

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Zwei neue EBS-Volume-Typen	01.10.2015	Sie können jetzt Throughput Optimized HDD(st1)- und Cold HDD(sc1)-Volumes erstellen.	19. April 2016
Neue NetworkPacketsIn und NetworkPacketsOut Metriken für Amazon EC2 hinzugefügt		Neue NetworkPacketsIn und NetworkPacketsOut Metriken für Amazon EC2 hinzugefügt. Weitere Informationen finden Sie unter Instance-Metriken.	23. März 2016
CloudWatch Metriken für Spot Fleet		Sie können jetzt CloudWatch Metriken für Ihre Spot-Flotte abrufen. Weitere Informationen finden Sie unter CloudWatch Metriken für Spot Fleet.	21. März 2016
Geplante Instances	01.10.2015	Geplante Reserved Instances (geplante Instances) ermöglichen Ihnen, Kapazitätsreservierungen, die täglich, wöchentlich oder monatlich wiederkehren, mit Angabe von Startzeit und Dauer zu kaufen.	13. Januar 2016
Längere Ressourcen-IDs	01.10.2015	Wir führen schrittweise längere IDs für manche Amazon EC2- und Amazon EBS-Ressourcentypen ein. Während des Übergangszeitraums können Sie das längere ID-Format für unterstützte Ressourcentypen aktivieren. Weitere Informationen finden Sie unter Ressourcen-IDs.	13. Januar 2016

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
ClassicLink DNS-Unterstützung	01.10.2015	Sie können die ClassicLink DNS-Unterstützung für Ihre VPC aktivieren, sodass DNS-Hostnamen, die zwischen verknüpften EC2-Classic-Instances und Instances in der VPC adressiert werden, in private IP-Adressen und nicht in öffentliche IP-Adressen aufgelöst werden.	11. Januar 2016
Dedicated Hosts	01.10.2015	Ein Amazon EC2 Dedicated Host ist ein physischer Server mit EC2-Instance-Kapazität, der ausschließlich von Ihnen genutzt wird. Weitere Informationen finden Sie unter Dedicated Hosts.	23. November 2015
Spot-Instance-Dauer	01.10.2015	Sie können jetzt eine Dauer für Ihre Spot-Instances festlegen. Spot-Blocks werden nicht unterstützt (Januar 2023).	6. Oktober 2015
Anforderung zur Änderung einer Spot-Flotte	01.10.2015	Sie können jetzt die Zielkapazität Ihrer Spot-Flotten-Anforderung ändern. Weitere Informationen finden Sie unter Ändern einer Spot-Flotten-Anforderung.	29. September 2015
Diversifizierte Zuordnungsstrategie für Spot-Flotten	15.04.2015	Sie können jetzt Spot-Instances in mehreren Spot-Pools mithilfe einer einzigen Spot-Flotten-Anforderung zuordnen. Weitere Informationen finden Sie unter Zuweisungsstrategien für Spot-Instances.	15. September 2015

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Instance-Gewichtung für Spot-Flotten	15.04.2015	Sie können jetzt Kapazitätseinheiten definieren, die jeder Instance-Typ zur Leistung Ihrer Anwendung beiträgt, und Ihren Gebotspreis für Spot-Instances jeden Spot-Pool entsprechend anpassen. Weitere Informationen finden Sie unter Instance-Gewichtung für Spot-Flotten.	31. August 2015
Neue Neustart-Alarmaktion und neue IAM-Rolle für die Verwendung mit Alarmaktionen		Neustart-Alarmaktion und neue IAM-Rolle für die Verwendung mit Alarmaktionen hinzugefügt. Weitere Informationen finden Sie unter Erstellen von Alarmen, mit denen eine Instance angehalten, beendet, neu gestartet oder wiederhergestellt wird.	23. Juli 2015
Spot Fleets	15.04.2015	Sie können eine Sammlung oder Flotte von Spot-Instances verwalten, anstatt getrennte Spot-Instance-Anforderungen verwalten zu müssen. Weitere Informationen finden Sie unter Spot-Flotte.	18. Mai 2015
Migrieren von Elastic IP-Adressen zu EC2-Classic	15.04.2015	Sie können eine elastische IP-Adresse, die Sie zur Verwendung in EC2-Classic zugewiesen haben, zur Verwendung in einer VPC migrieren.	15. Mai 2015
Importieren von VMs mit mehreren Laufwerken als AMIs	01.03.2015	Der VM Import-Prozess unterstützt jetzt das Importieren von VMs mit mehreren Laufwerken als AMIs. Weitere Informationen finden Sie unter Importieren einer VM als Image mithilfe von VM Import/Export im VM Import/Export-Benutzerhandbuch.	23. April 2015

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Systems Manager		Mit Systems Manager können Sie Ihre EC2-Instances konfigurieren und verwalten.	17. Februar 2015
Systems Manager for Microsoft SCVMM 1.5		Sie können jetzt Systems Manager for Microsoft SCVMM dazu verwenden, eine Instance zu starten und eine VM von SCVMM nach Amazon EC2 zu importieren.	21. Januar 2015
Automatische Wiederherstellung für EC2-Instances		Sie können einen CloudWatch Amazon-Alarm erstellen, der eine Amazon EC2-Instance überwacht und die Instance automatisch wiederherstellt, wenn sie aufgrund eines zugrunde liegenden Hardwarefehlers oder eines Problems, das eine Reparatur erfordert AWS , beeinträchtigt wird. Eine wiederhergestellte Instance ist mit der ursprünglichen Instance identisch. Dies schließt auch die Instance-ID, IP-Adressen und alle Instance-Metadaten mit ein. Weitere Informationen finden Sie unter Resilienz der Instanz.	12. Januar 2015
ClassicLink	01.10.2014	ClassicLink ermöglicht es Ihnen, Ihre EC2-Classic-Instance mit einer VPC in Ihrem Konto zu verknüpfen. Sie können der EC2-Classic-Instance VPC-Sicherheitsgruppen zuordnen, um Kommunikation zwischen der EC2-Classic-Instance und Instances innerhalb Ihrer VPC mit privaten IP-Adressen zu ermöglichen.	07. Januar 2015

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Benachrichtigungen über Spot-Instance-Unterbrechungen		Am besten können Sie Ihre Anwendung vor einer Spot-Instance-Unterbrechung schützen, indem Sie sie so konzipieren, dass sie fehlertolerant ist. Darüber hinaus können Sie Benachrichtigungen über Spot-Instance-Unterbrechungen nutzen. Diese stellen zwei Minuten, bevor Amazon EC2 Ihre Spot-Instance beenden muss, eine Warnmeldung bereit. Weitere Informationen finden Sie unter Spot-Instance-Unterbrechungsbenachrichtigungen.	5. Januar 2015
Systems Manager for Microsoft SCVMM		Systems Manager for Microsoft SCVMM bietet eine einfache easy-to-use Oberfläche für die Verwaltung von AWS Ressourcen wie EC2-Instances von Microsoft SCVMM aus.	29. Oktober 2014
`DescribeVolumes` Paginierungsunterstützung	01.09.2014	Der API-Aufruf `DescribeVolumes` unterstützt jetzt die Paginierung von Ergebnissen mit den Parametern `MaxResults` und `NextToken`. Weitere Informationen finden Sie DescribeVolumesin der Amazon EC2 API-Referenz.	23. Oktober 2014

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Unterstützung für Amazon CloudWatch Logs hinzugefügt		Sie können Amazon CloudWatch Logs verwenden, um Ihre System-, Anwendungs- und benutzerdefinierten Protokolldateien von Ihren Instances oder anderen Quellen aus zu überwachen, zu speichern und darauf zuzugreifen. Anschließend können Sie die zugehörigen Protokolldaten mithilfe der CloudWatch Amazon-Konsole, der CloudWatch Logs-Befehle in der AWS CLI oder des CloudWatch Logs-SDK aus CloudWatch Logs abrufen.	10. Juli 2014
Neue EC2 Service Limits-Seite		Auf der Seite EC2 Service Limits in der Amazon EC2-Konsole können Sie die aktuellen Limits für Ressourcen anzeigen, die von Amazon EC2 und Amazon VPC pro Region bereitgestellt werden.	19. Juni 2014
Amazon EBS-Allzweck-SSD-Volumes	01.05.2014	Allzweck-SSD-Volumes bieten kostengünstigen Speicher, der für ein breites Spektrum an Workloads gedacht ist. Diese Volumes bieten Latenzen im einstelligen Millisekundenbereich, die Möglichkeit, für längere Zeiträume auf 3 000 IOPS zu beschleunigen und eine Basisleistung von 3 IOPS/GiB. Universelle SSD-Volumes verfügen über Größen von 1 GiB bis 1 TiB.	16. Juni 2014
AWS Management Pack		AWS Das Management Pack unterstützt jetzt System Center Operations Manager 2012 R2.	22. Mai 2014

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Amazon EBS encryption	01.05.2014	Amazon EBS-Verschlüsselung bietet nahtlose Verschlüsselung von EBS-Daten-Volumes und Snapshots, wodurch die Notwendigkeit entfällt, eine sichere Infrastruktur zur Schlüsselverwaltung aufzubauen und zu unterhalten. Die EBS-Verschlüsselung gewährleistet die Sicherheit gespeicherter Daten, indem Ihre Daten mithilfe von Von AWS verwaltete Schlüssel verschlüsselt werden. Die Verschlüsselung erfolgt auf den Servern, die EC2-Instances hosten, was für die Verschlüsselung von Daten sorgt, die zwischen EC2-Instances und EBS-Speicher übertragen werden.	21. Mai 2014
Amazon EC2-Nutzungsberichte		Amazon EC2-Nutzungsberichte sind ein Satz von Berichten, der Kosten- und Nutzungsdaten für Ihre Nutzung von EC2 anzeigt.	28. Januar 2014
Importieren virtueller Maschinen mit Linux-Betriebssystem	15.10.2013	Der VM Import-Prozess unterstützt jetzt den Import von Linux-Instances. Weitere Informationen finden Sie im VM Import/Export-Benutzerhandbuch.	16. Dezember 2013
Berechtigungen auf Ressourcenebene für RunInstances	15.10.2013	Sie können jetzt Richtlinien erstellen, AWS Identity and Access Management um Berechtigungen auf Ressourcenebene für die Amazon EC2 RunInstances EC2-API-Aktion zu kontrollieren. Weitere Informationen und Beispielrichtlinien finden Sie unter Identity and Access Management für Amazon EC2.	20. November 2013

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Starten einer Instance von AWS Marketplace		Sie können jetzt eine Instance AWS Marketplace mithilfe des Amazon EC2 EC2-Startassistenten starten. Weitere Informationen finden Sie unter Starten Sie eine AWS Marketplace Instanz.	11. November 2013
Neuer Launch Wizard		Es gibt einen neuen und überarbeiteten EC2-Launch Wizard. Weitere Informationen finden Sie unter Starten einer Instance mit dem alten Launch Instance Wizard.	10. Oktober 2013
Instance-Typen von Reserved Instances ändern	01.10.2013	Sie können jetzt den Instance-Typ von Linux-Reserved Instances innerhalb derselben Familie ändern (z. B. M1, M2, M3, C1). Weitere Informationen finden Sie unter Ändern von Reserved Instances.	09. Oktober 2013
Ändern von Amazon EC2 Reserved Instances	15.08.2013	Sie können jetzt Reserved Instances in einer Region ändern. Weitere Informationen finden Sie unter Ändern von Reserved Instances.	11. September 2013
Zuweisen einer öffentlichen IP-Adresse	15.07.2013	Sie können jetzt eine öffentliche IP-Adresse zuweisen, wenn Sie eine Instance in einer VPC starten. Weitere Informationen finden Sie unter Zuweisen einer öffentlichen IPv4-Adresse beim Start einer Instance.	20. August 2013
Gewähren von Berechtigungen auf Ressourcenebene	15.06.2013	Amazon EC2 unterstützt neue Amazon-Ressourcennamen (ARNs) und Bedingungsschlüssel. Weitere Informationen finden Sie unter IAM-Richtlinien für Amazon EC2.	8. Juli 2013

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Inkrementelle Snapshot-Kopien	01.02.2013	Sie können jetzt inkrementelle Snapshot-Kopien erstellen.	11. Juni 2013
AWS Management Pack		Das AWS Management Pack verknüpft Amazon EC2 EC2-Instances und die darin ausgeführten Windows- oder Linux-Betriebssysteme. Das AWS Management Pack ist eine Erweiterung für Microsoft System Center Operations Manager.	8. Mai 2013
Neue Tags-Seite		Es gibt eine neue Tags-Seite in der Amazon EC2-Konsole. Weitere Informationen finden Sie unter Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).	04. April 2013
Kopieren eines AMI von einer Region in eine andere	01.02.2013	Sie können ein AMI von einer Region in eine andere kopieren, sodass Sie schnell und einfach konsistente Instances in mehr als einer AWS Region starten können. Weitere Informationen finden Sie unter Kopieren eines AMI.	11. März 2013
Starten von Instances in einer Standard-VPC	01.02.2013	Ihr AWS Konto ist in der Lage, Instances entweder in EC2-Classic oder einer VPC oder nur in einer VPC auf einer Basis zu starten. region-by-region Falls Sie Instances nur in der VPC starten können, erstellen wir eine standardmäßige VPC für Sie. Wir starten Ihre Instance dann in Ihrer standardmäßigen VPC, sofern Sie keine nicht standardmäßige VPC erstellt und beim Start der Instance angegeben haben.	11. März 2013

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
EBS-Snapshot-Kopie	01.12.2012	Sie können Snapshot-Kopien zum Erstellen von Daten-Backups, neuen Amazon EBS-Volumes oder Amazon Machine Images (AMIs) verwenden.	17. Dezember 2012
Aktualisierte EBS-Metriken und Statusprüfungen für Provisioned IOPS SSD-Volumes	01.10.2012	EBS-Metriken wurden aktualisiert, um zwei neue Metriken für Provisioned IOPS SSD-Volumes aufzunehmen. Außerdem wurden neue Statusprüfungen für Provisioned IOPS SSD-Volumes hinzugefügt.	20. November 2012
Status von Spot-Instance-Anforderungen	01.10.2012	Mit der Spot-Instance-Statusabfrage lässt sich der Status Ihrer Spot-Anforderungen leicht ermitteln.	14. Oktober 2012
Amazon EC2 Reserved Instance Marketplace	15.08.2012	Im Reserved Instance Marketplace werden Verkäufer, die über nicht mehr benötigte Amazon EC2 Reserved Instances verfügen, mit Käufern zusammengebracht, die zusätzliche Kapazität kaufen möchten. Reserved Instances, die über den Reserved Instance Marketplace gekauft und verkauft werden, funktionieren so wie andere Reserved Instances, mit der Ausnahme, dass sie möglicherweise nicht mehr die volle Standardlaufzeit bieten und zu anderen Preisen verkauft werden können.	11. September 2012
Provisioned IOPS SSD für Amazon EBS	20.07.2012	Provisioned IOPS SSD-Volumes liefern eine kalkulierbare, hohe Leistung für I/O-intensive Workloads, z. B. Datenbankanwendungen, für die konsistente und schnelle Reaktionszeiten erforderlich sind.	31. Juli 2012

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
IAM-Rollen auf Amazon EC2-Instances	01.06.2012	IAM-Rollen für Amazon EC2 bieten Folgendes: • AWS Zugriffsschlüssel für Anwendungen, die auf Amazon EC2 EC2-Instances ausgeführt werden. • Automatische Rotation der AWS Zugriffsschlüssel auf der Amazon EC2 EC2-Instance. • Granulare Berechtigungen für Anwendungen, die auf Amazon EC2 EC2-Instances ausgeführt werden und Anfragen an Ihre AWS Services stellen.	11. Juni 2012

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Spot-Instance-Features, die es einfacher machen, erste Schritte zu unternehmen und das Störungspotenzial zu bewältigen.		Sie können Ihre Spot-Instances jetzt wie folgt verwalten: • Definieren Sie unter Verwendung der Auto Scaling Startkonfigurationen ein Gebot für Spot-Instances. Erstellen Sie einen Zeitplan für die Definition des Gebots, das Sie für Spot-Instances abgeben möchten. Weitere Informationen finden Sie unter Starten von Spot-Instances in Ihrer Auto Scaling-Gruppe im Amazon EC2 Auto Scaling-Benutzerhandbuch. • Erhalten von Benachrichtigungen, wenn Instances gestartet oder beendet werden. • Verwenden Sie AWS CloudFormation Vorlagen, um Spot-Instances in einem Stapel mit AWS Ressourcen zu starten.	7. Juni 2012
EC2-Instance-Export und Zeitstempel für Statusprüfungen für Amazon EC2	01.05.2012	Zuvor in EC2 importierte Windows Server-Instances können nun exportiert werden. Unterstützung für Zeitstempel für Instance- und Systemstatus wurde hinzugefügt, um das Datum und den Zeitpunkt anzuzeigen, zu dem eine Statusprüfung fehlgeschlagen ist.	25. Mai 2012

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
EC2-Instance-Export und Zeitstempel in Instance- und Systemstatusprüfungen für Amazon VPC	01.05.2012	EC2-Instances können nun nach Citrix Xen, Microsoft Hyper-V und VMware vSphere exportiert werden. Unterstützung für Zeitstempel in Instance- und Systemstatusprüfungen wurde hinzugefügt.	25. Mai 2012
AWS Marketplace AMIs	01.04.2012	Unterstützung für AWS Marketplace AMIs hinzugefügt.	19. April 2012
Preisstufen für Reserved Instances	15.12.2011	Ein neuer Abschnitt wurde hinzugefügt, in dem behandelt wird, wie die Rabatte genutzt werden können, die in die Preisstufen für Reserved Instances integriert sind.	5. März 2012
Elastic Network-Schnittstellen (ENIs) für EC2-Instances in Amazon Virtual Private Cloud	01.12.2011	Ein neuer Abschnitt über Elastic-Network-Schnittstellen (ENIs) für EC2-Instances in einer VPC wurde hinzugefügt. Weitere Informationen finden Sie unter Elastic-Network-Schnittstelle.	21. Dezember 2011
Neue Angebotstypen für Amazon EC2 Reserved Instances	01.11.2011	Sie können aus einer Vielzahl von Reserved Instance-Angeboten auswählen, die auf Ihre projizierte Nutzung der Instance abgestimmt sind.	01. Dezember 2011

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Amazon EC2-Instance-Status	01.11.2011	Sie können zusätzliche Informationen zum Status Ihrer Instances einsehen, einschließlich der geplanten Ereignisse AWS , die sich auf Ihre Instances auswirken könnten. Zu diesen Betriebsaktivitäten gehören Instance-Neustarts , die zur Anwendung von Software-Updates oder Sicherheits-Patches erforderlich sind oder Instance-Aussonderungen, die im Falle von Hardware-Problemen erforderlich sind. Weitere Informationen finden Sie unter Überwachen des Status Ihrer Instances.	16. November 2011
Spot Instances in Amazon VPC	15.07.2011	Es wurden Informationen über die Unterstützung für Spot-Instances in Amazon VPC hinzugefügt. Mit diesem Update können die Benutzer Spot-Instances in einer Virtual Private Cloud (VPC) starten. Durch Starten von Spot-Instances in einer VPC kommen die Verwender von Spot-Instances in den Genuss der Vorteile von Amazon VPC.	11. Oktober 2011
Vereinfachter VM Import-Prozess für Benutzer von CLI-Tools	15.07.2011	Der VM Import-Prozess wird mit der verbesserten Funktionalität von `ImportInstance` und `ImportVolume` vereinfacht, die jetzt den Upload der Images nach Amazon EC2 durchführt, nachdem die Importaufgabe erstellt wurde. Außerdem können die Benutzer mit der Einführung von `ResumeImport` einen unvollständigen Upload an dem Punkt neu starten, an dem die Aufgabe gestoppt wurde.	15. September 2011

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Unterstützung für den Import in das VHD-Dateiformat		VM Import kann jetzt Image-Dateien virtueller Maschinen im VHD-Format importieren. Das VHD-Dateiformat ist mit den Citrix Xen- und Microsoft Hyper-V-Virtualisierungsplattformen kompatibel. Ab dieser Version unterstützt VM Import Images in den Formaten RAW, VHD und VMDK (VMware ESX-kompatibel). Weitere Informationen finden Sie im VM Import/Export-Benutzerhandbuch.	24. August 2011
Aktualisierung auf den Amazon EC2 VM Import Connector für VMware vCenter		Es wurden Informationen über die Version 1.1 des Amazon EC2 VM Import Connector für die virtuelle Appliance VMware vCenter (Connector) hinzugefügt. Diese Aktualisierung beinhaltet Proxy-Unterstützung für den Internetzugriff, bessere Fehlerbehandlung, verbesserte Genauigkeit des Aufgaben-Fortschrittsbalkens und verschiedene Fehlerbehebungen.	27. Juni 2011
Preisänderungen bei Spot-Instances in bestimmten Availability Zones	15.05.2011	Es wurden Informationen über das Preise-Feature für Spot-Instances in bestimmten Availability Zones hinzugefügt. In dieser Veröffentlichung haben wir im Rahmen der Informationen, die zurückgegeben werden, wenn Sie Spot-Instance-Anforderungen und den Spot-Preisverlauf abfragen, neue Preisoptionen für Availability Zones hinzugefügt. Diese zusätzlichen Informationen machen es einfacher, den Preis für das Starten einer Spot-Instance in einer bestimmten Availability Zone zu ermitteln.	26. Mai 2011

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
AWS Identity and Access Management		Es wurden Informationen über AWS Identity and Access Management (IAM) hinzugefügt, mit denen Benutzer angeben können, welche Amazon EC2 EC2-Aktionen ein Benutzer mit Amazon EC2 EC2-Ressourcen im Allgemeinen verwenden kann. Weitere Informationen finden Sie unter Identity and Access Management für Amazon EC2.	26. April 2011
Dedicated Instances		Dedicated Instances werden innerhalb Ihrer Amazon Virtual Private Cloud (Amazon VPC) gestartet. Dabei handelt es sich um Instances, die physisch auf Host-Hardware-Ebene isoliert sind. Mit Dedicated Instances können Sie die Vorteile von Amazon VPC und der AWS Cloud nutzen. Zu den Vorteilen gehört die flexible Bereitstellung auf Abruf. Sie zahlen nur für das, was Sie tatsächlich nutzen, während Sie Ihre Amazon EC2 EC2-Recheninstanzen auf Hardwareebene isolieren. Weitere Informationen finden Sie unter Dedicated Instances.	27. März 2011
Reserved Instances -Updates für die Management Console AWS		Aktualisierungen der AWS Management Console erleichtern es Benutzern, ihre Reserved Instances einzusehen und zusätzliche Reserved Instances, einschließlich Dedicated Reserved Instances, zu erwerben.	27. März 2011

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
Metadaten-Informationen	01.01.2011	Es wurden Informationen über Metadaten hinzugefügt, um Änderungen für Version 2011-01-01 zu berücksichtigen. Weitere Informationen finden Sie unter Arbeiten mit Instance-Metadaten und Instance-Metadaten kategorien.	11. März 2011
Amazon EC2 VM Import Connector für VMware vCenter		Es wurden Informationen über den Amazon EC2 VM Import Connector für die virtuelle Anwendung VMware vCenter (Connector) hinzugefügt. Der Connector ist ein Plug-in für VMware vCenter, das in VMware vSphere Client integriert wird und eine Benutzeroberfläche bereitstellt, die Sie zum Importieren Ihrer virtuellen VMware-Maschinen in Amazon EC2 verwenden können.	3. März 2011
Erzwungene Volume-Trennung		Sie können jetzt den verwenden AWS Management Console , um die Trennung eines Amazon EBS-Volumes von einer Instance zu erzwingen.	23. Februar 2011
Beendigungsschutz für Instances		Sie können jetzt die AWS Management Console verwenden, um zu verhindern, dass eine Instance beendet wird. Weitere Informationen finden Sie unter Aktivieren des Beendigungsschutzes.	23. Februar 2011

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
VM Import	15.11.2010	Es wurden Informationen über VM Import hinzugefügt, so dass Sie jetzt eine virtuelle Maschine oder ein Volume in Amazon EC2 importieren können. Weitere Informationen finden Sie im VM Import/Export-Benutzerhandbuch.	15. Dezember 2010
Grundlegende Überwachung für Instances	31.08.2010	Es wurden Informationen über eine grundlegende Überwachung für EC2-Instances hinzugefügt.	12. Dezember 2010
Filter und Tags (Markierungen)	31.08.2010	Es wurden Informationen über das Auflisten, Filtern und Markieren von Ressourcen hinzugefügt. Weitere Informationen finden Sie unter Auflisten und Filtern Ihrer Ressourcen und Markieren Ihrer Amazon-EC2-Ressourcen mit Tags (Markierungen).	19. September 2010
Idempotenter Instance-Start	31.08.2010	Es wurden Informationen über das Sicherstellen von Idempotenz beim Ausführen von Instances hinzugefügt.	19. September 2010
AWS Identity and Access Management für Amazon EC2		Amazon EC2 ist jetzt in AWS Identity and Access Management (IAM) integriert. Weitere Informationen finden Sie unter Identity and Access Management für Amazon EC2.	2. September 2010
IP-Adressenangabe in Amazon VPC	15.06.2010	Amazon VPC-Benutzer können jetzt die IP-Adresse angeben, um eine Instance zuzuweisen, die in einer VPC gestartet wurde.	12. Juli 2010

Funktion	API-Version	Beschreibung	Datum der Veröffentlichung
CloudWatch Amazon-Überwachung für Amazon EBS-Volumes		Die CloudWatch Amazon-Überwachung ist jetzt automatisch für Amazon EBS-Volumes verfügbar.	14. Juni 2010
Reserved Instances mit Windows		Amazon EC2 unterstützt jetzt Reserved Instances mit Windows.	22. Februar 2010

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.