aws

Benutzerhandbuch

Amazon Virtual Private Cloud

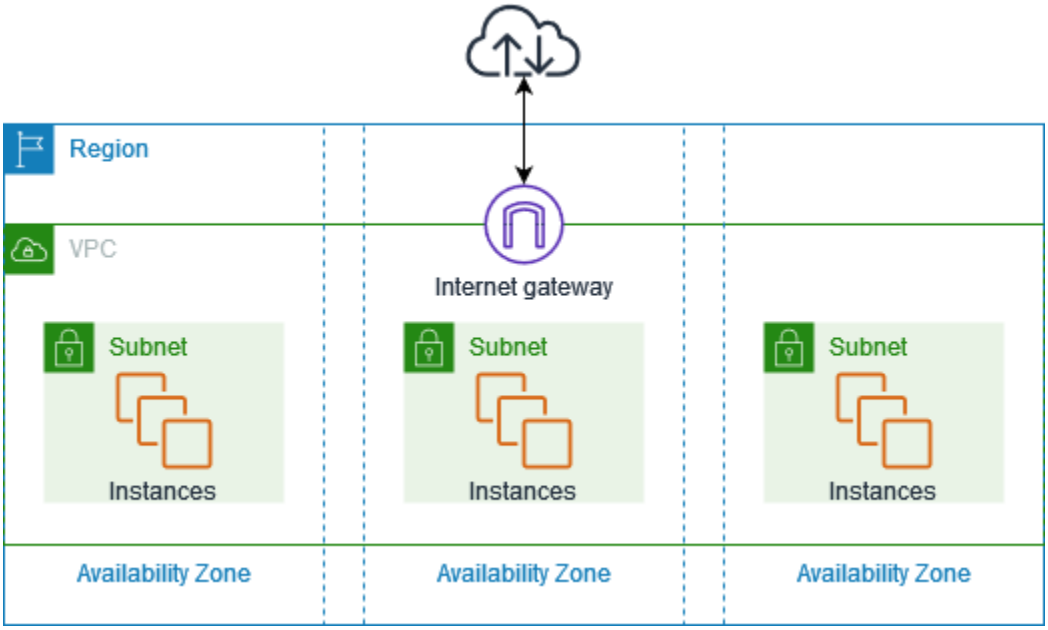
Amazon Virtual Private Cloud: Benutzerhandbuch

Table of Contents

Was ist Amazon VPC?

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

Das folgende Diagramm zeigt eine Beispiel-VPC. Die VPC umfasst ein Subnetz in jeder der Availability Zones in der Region, EC2-Instances in jedem Subnetz und ein Internet-Gateway, das die Kommunikation zwischen den Ressourcen in Ihrer VPC und dem Internet ermöglicht.



Weitere Informationen finden Sie unter Amazon Virtual Private Cloud (Amazon VPC).

Features

Die folgenden Funktionen helfen Ihnen bei der Konfiguration einer VPC, um die Konnektivität bereitzustellen, die Ihre Anwendungen benötigen:

Virtual Private Cloudc (VPCs)

> Eine VPC ist ein virtuelles Netzwerk, das einem herkömmlichen Netzwerk, das Sie in Ihrem eigenen Rechenzentrum betreiben würden, sehr ähnlich ist. Nachdem Sie eine VPC erstellt haben, können Sie Subnetze hinzufügen.

Subnetze

Ein Subnetz ist ein Bereich an IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden. Nachdem Sie Subnetze hinzugefügt haben, können Sie AWS Ressourcen in Ihrer VPC bereitstellen.

IP-Adressierung

Sie können Ihren VPCs und Subnetzen IP-Adressen IPv4 und IPv6 zuordnen. Sie können Ihre öffentlichen IPv4-Adressen und IPv6-GUA-Adressen auch Ressourcen in Ihrer VPC wie EC2-Instances, NAT-Gateways AWS und Network Load Balancers zuordnen und sie ihnen zuweisen.

Routing

Verwenden Sie Routing-Tabellen, um zu bestimmen, wohin der Netzwerkverkehr von Ihrem Subnetz oder Gateway geleitet wird.

Gateways und Endpunkte

Ein Gateway verbindet Ihre VPC mit einem anderen Netzwerk. Verwenden Sie zum Beispiel ein Internet-Gateway um Ihre VPC mit dem Internet zu verbinden. Verwenden Sie einen VPC-Endpunkt, um eine AWS-Services private Verbindung herzustellen, ohne ein Internet-Gateway oder ein NAT-Gerät zu verwenden.

Peering-Verbindungen

Verwenden Sie eine VPC-Peering-Verbindung, um den Datenverkehr zwischen den Ressourcen in zwei VPCs zu leiten.

Datenverkehrsspiegelung

Kopieren Sie den Netzwerkverkehr von den Netzwerkschnittstellen und senden Sie es zur eingehenden Paketprüfung an Sicherheits- und Überwachungsgeräte.

Transit Gateways

Verwenden Sie ein Transit-Gateway, das als zentraler Hub fungiert, um den Verkehr zwischen Ihren VPCs, VPN-Verbindungen und AWS Direct Connect Verbindungen weiterzuleiten.

VPC Flow Logs

Ein Ablaufprotokoll erfasst Informationen zum IP-Verkehr, der zu und von Netzwerkschnittstellen in Ihrer VPC geht.

VPN-Verbindungen

Verbinden Sie Ihre VPCs mit Ihren On-Premises-Netzwerken mithilfe von AWS Virtual Private Network (AWS VPN).

Erste Schritte mit Amazon VPC

Ihre AWS-Konto enthält jeweils AWS-Region eine Standard-VPC. Ihre Standard-VPCs sind so konfiguriert, dass Sie sofort mit dem Start und der Verbindung zu EC2-Instances beginnen können. Weitere Informationen finden Sie unter Erste Schritte.

Sie können zusätzliche VPCs mit den Subnetzen, IP-Adressen, Gateways und Routing erstellen, die Sie benötigen. Weitere Informationen finden Sie unter the section called “Erstellen einer VPC”.

Arbeiten mit Amazon VPC

Sie können Ihre VPCs mithilfe einer der folgenden Schnittstellen erstellen und verwalten:

- AWS Management Console — Bietet eine Webschnittstelle für den Zugriff auf Ihre VPCs.
- AWS Command Line Interface (AWS CLI) — Stellt Befehle für eine Vielzahl von AWS Diensten bereit, darunter Amazon VPC, und wird unter Windows, Mac und Linux unterstützt. Weitere Informationen finden Sie unter AWS Command Line Interface.
- AWS SDKs — Stellt sprachspezifische APIs bereit und kümmert sich um viele Verbindungsdetails, wie z. B. die Berechnung von Signaturen, die Bearbeitung von Wiederholungsversuchen von Anfragen und die Fehlerbehandlung. Weitere Informationen finden Sie unter AWS -SDKs.
- Abfrage-API – Bietet API-Aktionen auf niedriger Ebene, die Sie mithilfe von HTTPS-Anforderungen aufrufen. Die Verwendung der Abfrage-API ist die direkteste Möglichkeit für den Zugriff auf die Amazon VPC. Allerdings müssen dann viele technische Abläufe, wie beispielsweise das Erzeugen des Hashwerts zum Signieren der Anforderung und die Fehlerbehandlung in der Anwendung durchgeführt werden. Weitere Informationen finden Sie unter Amazon-VPC-Aktionen in der Referenz zur Amazon-EC2-API.

Preise für Amazon VPC

Für VPC fallen keine zusätzlichen Gebühren an. Für einige VPC-Komponenten wie NAT-Gateways, IP Address Manager, Traffic Mirroring, Reachability Analyzer und Network Access Analyzer fallen jedoch Gebühren an. Weitere Informationen dazu finden Sie unter Amazon VPC – Preise.

Fast alle Ressourcen, die Sie in Ihrer Virtual Private Cloud (VPC) starten, stellen Ihnen eine IP-Adresse für die Konnektivität zur Verfügung. Die überwiegende Mehrheit der Ressourcen in Ihrer VPC verwendet private IPv4-Adressen. Ressourcen, die direkten Zugriff auf das Internet über IPv4 benötigen, verwenden jedoch öffentliche IPv4-Adressen.

Preise für öffentliche IPv4-Adressen

Eine öffentliche IPv4-Adresse ist eine IPv4-Adresse, die vom Internet aus routbar ist. Eine öffentliche IPv4-Adresse ist erforderlich, damit eine Ressource im Internet direkt über IPv4 erreichbar ist.

Wenn Sie bereits Kunde oder neuer Kunde des AWS kostenlosen Kontingents sind, können Sie öffentliche IPv4-Adressen für 750 Stunden kostenlos nutzen. Wenn Sie das AWS kostenlose Kontingent nicht nutzen, werden öffentliche IPv4-Adressen in Rechnung gestellt. Spezifische Preisinformationen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse unter Amazon VPC – Preise.

Private IPv4-Adressen (RFC 1918) werden nicht in Rechnung gestellt. Weitere Informationen darüber, wie öffentliche IPv4-Adressen für gemeinsam genutzte VPCs berechnet werden, finden Sie unter Abrechnung und Abrechnung für den Eigentümer und die Teilnehmer.

Öffentliche IPv4-Adressen haben die folgenden Typen:

- Elastische IP-Adressen (EIPs): Von Amazon bereitgestellte statische, öffentliche IPv4-Adressen, die Sie einer EC2-Instance, einer elastic network interface oder einer Ressource zuordnen können. AWS
- Öffentliche EC2-IPv4-Adressen: Öffentliche IPv4-Adressen, die von Amazon einer EC2-Instance zugewiesen werden (wenn die EC2-Instance in einem Standardsubnetz oder in einem Subnetz gestartet wird, das zur automatischen Zuweisung einer öffentlichen IPv4-Adresse konfiguriert ist).
- BYOIPv4-Adressen: Öffentliche IPv4-Adressen im IPv4-Adressbereich, zu denen Sie AWS mithilfe von Bring Your Own IP Addresses (BYOIP) gewechselt haben.
- Vom Dienst verwaltete IPv4-Adressen: Öffentliche IPv4-Adressen, die automatisch auf Ressourcen bereitgestellt und von einem Dienst verwaltet werden. AWS AWS Zum Beispiel öffentliche IPv4-Adressen auf Amazon ECS, Amazon RDS oder Amazon WorkSpaces.

Die folgende Liste zeigt die gängigsten AWS Dienste, die öffentliche IPv4-Adressen verwenden können.

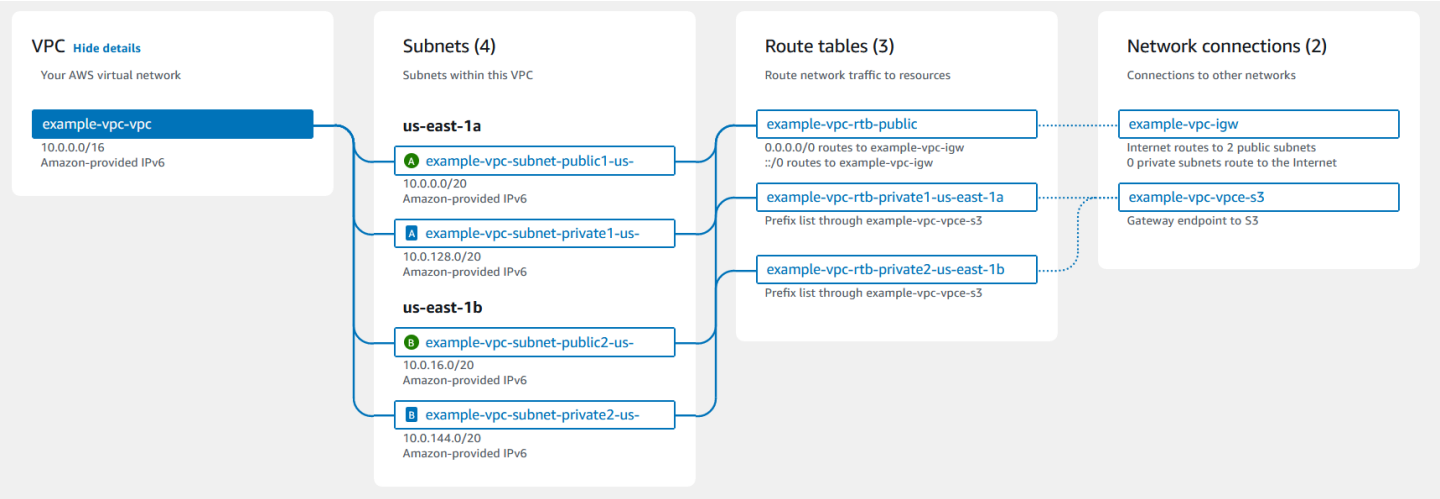
- Amazon AppStream 2.0

- AWS Client VPN
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- Amazon GameLift
- AWS Global Accelerator
- AWS Mainframe Modernization
- Amazon Managed Streaming für Apache Kafka
- Amazon MQ
- Amazon RDS
- Amazon-Redshift
- AWS Site-to-Site VPN
- Amazon-VPC-NAT-Gateway
- Amazon WorkSpaces
- Elastic Load Balancing

Funktionsweise von Amazon VPC

Mit Amazon Virtual Private Cloud (Amazon VPC) können Sie AWS Ressourcen in einem von Ihnen definierten logisch isolierten virtuellen Netzwerk starten. Dieses virtuelle Netzwerk entspricht weitgehend einem herkömmlichen Netzwerk, wie Sie es in Ihrem Rechenzentrum betreiben, kann jedoch die Vorzüge der skalierbaren Infrastruktur von AWS nutzen.

Im Folgenden finden Sie eine visuelle Darstellung einer VPC und ihrer Ressourcen aus der Vorschau, die angezeigt wird, wenn Sie eine VPC mithilfe von AWS Management Console erstellen. Bei einer vorhandenen VPC können Sie auf diese Visualisierung auf der Registerkarte Ressourcenkarte zugreifen. Dieses Beispiel zeigt die Ressourcen, die auf der Seite VPC erstellen zunächst ausgewählt werden, wenn Sie sich entscheiden, die VPC sowie andere Netzwerkressourcen zu erstellen. Diese VPC ist mit einem IPv4-CIDR und einem von Amazon bereitgestellten IPv6-CIDR, Subnetzen in zwei Availability Zones, drei Routing-Tabellen, einem Internet-Gateway und einem Gateway-Endpunkt konfiguriert. Da wir das Internet-Gateway ausgewählt haben, zeigt die Visualisierung, dass der Datenverkehr von den öffentlichen Subnetzen ins Internet geleitet wird, da die entsprechende Routing-Tabelle den Datenverkehr an das Internet-Gateway weiterleitet.



Konzepte

- VPCs und Subnetze
- Standardmäßige und nicht standardmäßige VPCs
- Routing-Tabellen
- Zugriff auf das Internet
- Zugriff auf ein Unternehmens- oder Heimnetzwerk
- Verbinden von VPCs und Netzwerken

- AWS Privates globales Netzwerk

VPCs und Subnetze

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk für Ihr AWS -Konto. Es ist logisch von anderen virtuellen Netzwerken in der AWS Cloud isoliert. Sie können einen IP-Adressbereich für die VPC festlegen, Subnetze und Gateways hinzufügen und Sicherheitsgruppen zuordnen.

Ein Subnetz ist ein Bereich an IP-Adressen in Ihrer VPC. Sie können AWS -Ressourcen, wie z. B. Amazon-EC2-Instances, in Ihren Subnetzen starten. Sie können ein Subnetz mit dem Internet, anderen VPCs und Ihren eigenen Rechenzentren verbinden und den Verkehr zu und von Ihren Subnetzen mithilfe von Routing-Tabellen leiten.

Weitere Informationen

- IP-Adressierung
- Virtual Private Clouds
- Subnetze

Standardmäßige und nicht standardmäßige VPCs

Wenn Ihr Konto nach dem 04.12.2013 erstellt wurde, verfügt es über eine Standard-VPC in jeder Region. Eine Standard-VPC ist konfiguriert und kann von Ihnen verwendet werden. Beispielsweise verfügen die Daten über ein Standardsubnetz in jeder Availability Zone in der Region, ein angeschlossenes Internet-Gateway, eine Route in der Haupt-Routing-Tabelle, die den gesamten Datenverkehr an das Internet-Gateway sendet, und DNS-Einstellungen, die Instances mit öffentlichen IP-Adressen automatisch öffentliche DNS-Hostnamen zuordnen und DNS-Auflösung über den von Amazon bereitgestellten DNS-Server ermöglichen (siehe DNS-Attribute in Ihrer VPC). Daher hat eine EC2-Instance, die in einem Standardsubnetz gestartet wird, automatisch Zugang zum Internet. Wenn Sie eine Standard-VPC in einer Region haben und beim Starten einer EC2-Instance in dieser Region kein Subnetz angeben, wählen wir eines der Standard-Subnetze und starten die Instance in diesem Subnetz.

Sie können auch eine eigene VPC erstellen und sie nach Bedarf konfigurieren. Dies wird als eine nicht standardmäßige VPC bezeichnet. Subnetze, die Sie in Ihrer nicht standardmäßigen VPC erstellen, und zusätzliche Subnetze, die Sie in Ihrer standardmäßigen VPC erstellen, werden als nicht standardmäßige Subnetze bezeichnet.

Weitere Informationen

- the section called “Standard-VPCs”
- the section called “Erstellen einer VPC”

Routing-Tabellen

Eine Routing-Tabelle enthält eine Reihe von Regeln, so genannte Routen, die festlegen, wohin der Netzwerkdatenverkehr aus Ihrer VPC gelenkt wird. Sie können ein Subnetz einer bestimmten Routing-Tabelle explizit zuordnen. Andernfalls wird das Subnetz implizit der Haupt-Routing-Tabelle zugeordnet.

Jede Route in einer Routing-Tabelle gibt den Bereich der IP-Adressen an, in den der Datenverkehr gehen soll (den Empfänger), und das Gateway, die Netzwerkschnittstelle oder die Verbindung, über die der Datenverkehr gesendet werden soll (das Ziel).

Weitere Informationen

- Konfigurieren von Routing-Tabellen

Zugriff auf das Internet

Sie steuern, wie die Instances, die Sie in einer VPC starten, auf Ressourcen außerhalb der VPC zugreifen.

Eine Standard-VPC umfasst ein Internet-Gateway und jedes Standardsubnetz ist ein öffentliches Subnetz. Jede Instance, die Sie innerhalb eines Standardsubnetz starten, umfasst eine private IPv4-Adresse und eine öffentliche IPv4-Adresse. Diese Instances können über das Internet-Gateway mit dem Internet kommunizieren. Ein Internet-Gateway ermöglicht es Ihren Instances, sich über den Amazon EC2-Netzwerk-Edge mit dem Internet zu verbinden.

Standardmäßig verfügt jede von Ihnen in ein nicht standardmäßiges Subnetz gestartete Instance zwar über eine private IPv4-Adresse, aber nicht über eine öffentliche IPv4-Adresse. Hierfür müssen Sie entweder beim Start ausdrücklich eine öffentliche IPv4-Adresse zuordnen oder das Attribut für die öffentliche IP-Adresse des Subnetzes ändern. Diese Instances können zwar miteinander, aber nicht mit dem Internet kommunizieren.

Sie können den Internetzugriff für eine Instance, die in einem nicht standardmäßigen Subnetz gestartet wurde, aktivieren, indem Sie ihrer VPC ein Internet-Gateway anfügen (solange es sich

bei der VPC nicht um eine standardmäßige VPC handelt) und der Instance eine Elastic IP-Adresse zuweisen.

Um einer Instance in Ihrer VPC die Initiierung ausgehender Verbindungen zum Internet zu erlauben, aber unaufgeforderte eingehende Verbindungen zu verhindern, können Sie alternativ ein NAT-Gerät verwenden. NAT ordnet einer einzelnen öffentlichen IPv4-Adresse mehrere private IPv4-Adressen zu. Sie können das NAT-Gerät mit einer Elastic-IP-Adresse konfigurieren und es über ein Internet-Gateway mit dem Internet verbinden. Dadurch kann eine Instance in einem privaten Subnetz über das NAT-Gerät eine Verbindung zum Internet herstellen, wobei der Datenverkehr von der Instance zum Internet-Gateway und alle Antworten an die Instance geleitet werden.

Wenn Sie Ihrer VPC einen IPv6-CIDR-Block zuordnen und Ihren Instances IPv6-Adressen zuweisen, können Instances über ein Internet-Gateway unter Verwendung von IPv6 eine Verbindung zum Internet herstellen. Alternativ können Instances ausgehende Verbindungen zum Internet über IPv6 mithilfe eines nur für ausgehenden Verkehr zuständigen Internet-Gateways initiieren. IPv6-Datenverkehr fließt getrennt vom IPv4-Datenverkehr, daher müssen Ihre Routing-Tabellen getrennte Routen für den IPv6-Datenverkehr aufweisen.

Weitere Informationen

- Herstellen einer Internetverbindung über ein Internet-Gateway
- Aktivieren von ausgehendem IPv6-Datenverkehr mit einem Internet-Gateway, das nur ausgehenden Verkehr zulässt
- Herstellen einer Verbindung mit dem Internet oder anderen Netzwerken über NAT-Geräte

Zugriff auf ein Unternehmens- oder Heimnetzwerk

Sie können Ihre VPC optional über eine IPsec- AWS Site-to-Site VPN Verbindung mit Ihrem eigenen Unternehmensrechenzentrum verbinden, wodurch die - AWS Cloud zu einer Erweiterung Ihres Rechenzentrums wird.

Eine Site-to-Site-VPN-Verbindung besteht aus zwei VPN-Tunneln zwischen einem Virtual Private Gateway oder Transit-Gateway auf der - AWS Seite und einem Kunden-Gateway-Gerät in Ihrem Rechenzentrum. Ein Kunden-Gateway-Gerät ist ein physisches Gerät oder eine Softwareanwendung, die auf Ihrer Seite der Site-to-Site VPN-Verbindung konfiguriert wird.

Weitere Informationen

- AWS Site-to-Site VPN Benutzerhandbuch

- Amazon VPC Transit Gateways

Verbinden von VPCs und Netzwerken

Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs, die den privaten Datenverkehr zwischen diesen beiden VPCs ermöglicht. Instances in jeder der VPCs können so miteinander kommunizieren, als befänden sie sich im selben Netzwerk.

Sie können auch ein Transit-Gateway erstellen und damit Ihre VPCs und On-Premises-Netzwerke miteinander verbinden. Das Transit-Gateway fungiert als regionaler virtueller Router für den Datenverkehr zwischen seinen Anhängen, der VPCs, VPN-Verbindungen, AWS Direct Connect Gateways und Transit-Gateway-Peering-Verbindungen umfassen kann.

Weitere Informationen

- Amazon VPC Peering Guide
- Amazon VPC Transit Gateways

AWS Privates globales Netzwerk

AWS bietet ein privates Netzwerk mit hoher Leistung und geringer Latenz, das eine sichere Cloud-Computing-Umgebung bereitstellt, um Ihre Netzwerkanforderungen zu erfüllen. AWS Die Regionen sind mit mehreren Internetdienstanbietern sowie einem privaten Netzwerk-Backbone verbunden, die die Netzwerkleistung des durch die Kunden erzeugten regionsübergreifenden Datenverkehrs verbessern.

Beachten Sie die folgenden Überlegungen:

- Datenverkehr, der sich in einer Availability Zone oder zwischen Availability Zones in allen Regionen befindet, wird über das AWS private globale Netzwerk geleitet.
- Datenverkehr, der sich zwischen -Regionen befindet, wird immer über das AWS private globale Netzwerk geleitet, mit Ausnahme der Regionen in China.

Verschiedene Faktoren können einen Netzwerkpaketverlust verursachen, darunter Netzwerkflusskollisionen, Low-Level-Fehler (Layer 2) und andere Netzwerkfehler. Wir konstruieren und betreiben unsere Netzwerke so, dass der Paketverlust minimiert wird. Wir messen die Paketverlustrate (Paket-Loss Rate, PLR) über das globale Backbone, das die AWS Regionen

verbindet. Wir betreiben unser Backbone-Netzwerk mit dem Ziel von p99 der stündlichen PLR von weniger als 0,0001 %.

Erste Schritte mit Amazon VPC

Führen Sie die folgenden Aufgaben aus, um die Erstellung und Verbindung Ihrer VPCs vorzubereiten. Wenn Sie fertig sind, sind Sie bereit, Ihre Anwendung auf AWS bereitzustellen.

Aufgaben

- Melde dich an für ein AWS-Konto
- Überprüfen der Berechtigungen
- Ermitteln Sie Ihre IP-Adressbereiche
- Wählen Sie Ihre Availability Zones
- Planen Sie Ihre Internetverbindung
- Erstellen Sie Ihre VPC
- Bereitstellen der Anwendung

Melde dich an für ein AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

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

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

   Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontoswird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu https://aws.amazon.com/ auf und klicken Sie auf Mein Konto.

Überprüfen der Berechtigungen

Um Amazon VPC verwenden zu können, benötigen Sie die erforderlichen Berechtigungen. Weitere Informationen finden Sie unter Identity and Access Management für Amazon VPC und Beispiele für Amazon VPC-Richtlinien.

Ermitteln Sie Ihre IP-Adressbereiche

Die Ressourcen in Ihrer VPC kommunizieren untereinander und mit Ressourcen im Internet über IP-Adressen. Wenn Sie VPCs und Subnetze erstellen, können Sie deren IP-Adressbereiche auswählen. Wenn Sie Ressourcen in einem Subnetz bereitstellen, z. B. EC2-Instances, erhalten diese IP-Adressen aus dem IP-Adressbereich des Subnetzes. Weitere Informationen finden Sie unter IP-Adressierung.

Überlegen Sie sich bei der Auswahl der Größe für Ihre VPC, wie viele IP-Adressen Sie für Ihre AWS-Konten und VPCs benötigen. Stellen Sie sicher, dass sich die IP-Adressbereiche Ihrer VPCs nicht mit den IP-Adressbereichen Ihres eigenen Netzwerks überschneiden. Wenn Sie Konnektivität zwischen mehreren VPCs benötigen, müssen Sie sicherstellen, dass diese keine überlappenden IP-Adressen haben.

IP Address Manager (IPAM) erleichtert die Planung, Verfolgung und Überwachung der IP-Adressen für Ihre Anwendung. Weitere Informationen finden Sie unter Handbuch für IP Address Manager.

Wählen Sie Ihre Availability Zones

Eine AWS Region ist ein physischer Standort, an dem wir Rechenzentren gruppieren, sogenannte Availability Zones. Jede Availability Zone verfügt über eine unabhängige Stromversorgung, Kühlung und physische Sicherheit mit redundanter Stromversorgung, Vernetzung und Konnektivität. Die Availability Zones in einer Region sind physisch durch eine bedeutende Entfernung getrennt und über Netzwerke mit hoher Bandbreite und niedriger Latenz miteinander verbunden. Sie können Ihre Anwendung so gestalten, dass sie in mehreren Availability Zones ausgeführt wird, um eine noch höhere Fehlertoleranz zu erreichen.

Produktionsumgebung

Für eine Produktionsumgebung empfehlen wir, dass Sie mindestens zwei Availability Zones auswählen und Ihre AWS Ressourcen gleichmäßig in jeder aktiven Availability Zone einsetzen.

Entwicklungs- oder Testumgebung

Bei einer Entwicklungs- oder Testumgebung können Sie Geld sparen, indem Sie Ihre Ressourcen in nur einer Availability Zone bereitstellen.

Planen Sie Ihre Internetverbindung

Planen Sie, jede VPC je nach Ihren Konnektivitätsanforderungen in Subnetze zu unterteilen. Beispielsweise:

- Wenn Sie über Webserver verfügen, die Datenverkehr von Clients im Internet empfangen, erstellen Sie in jeder Availability Zone ein Subnetz für diese Server.
- Wenn Sie auch Server haben, die nur Datenverkehr von anderen Servern in der VPC empfangen, erstellen Sie für diese Server in jeder Availability Zone ein eigenes Subnetz.
- Wenn Sie Server haben, die den Datenverkehr nur über eine VPN-Verbindung zu Ihrem Netzwerk empfangen, erstellen Sie für diese Server in jeder Availability Zone ein eigenes Subnetz.

Wenn Ihre Anwendung Datenverkehr aus dem Internet empfängt, muss die VPC über ein Internet-Gateway verfügen. Durch das Anhängen eines Internet-Gateways an eine VPC werden Ihre Instances nicht automatisch über das Internet zugänglich. Zusätzlich zum Anhängen des Internet-Gateways müssen Sie die Subnetz-Routing-Tabelle mit einer Route zum Internet-Gateway aktualisieren. Darüber hinaus müssen Sie sicherstellen, dass die Instances über öffentliche IP-Adressen verfügen und einer Sicherheitsgruppe zugeordnet sind, die Datenverkehr aus dem Internet über bestimmte, für die Anwendung erforderliche Ports und Protokolle zulässt.

Alternativ können Sie Ihre Instances bei einem Load Balancer mit Internetanschluss registrieren. Der Load Balancer empfängt Datenverkehr von den Clients und verteilt ihn auf die registrierten Instances in einer oder mehreren Availability Zones. Weitere Informationen finden Sie unter Elastic Load Balancing. Um Instances in einem privaten Subnetz den Zugriff auf das Internet zu ermöglichen (z. B. um Updates herunterzuladen), ohne unerwünschte eingehende Verbindungen aus dem Internet zuzulassen, fügen Sie in jeder aktiven Availability Zone ein öffentliches NAT-Gateway hinzu und aktualisieren Sie die Routing-Tabelle, um Internetverkehr an das NAT-Gateway zu senden. Weitere Informationen finden Sie unter the section called “Zugriff auf das Internet von einem privaten Subnetz”.

Erstellen Sie Ihre VPC

Nachdem Sie festgelegt haben, wie viele VPCs und Subnetze Sie benötigen, welche CIDR-Blöcke Ihren VPCs und Subnetzen zugewiesen werden sollen und wie Sie Ihre VPC mit dem

Internet verbinden, können Sie Ihre VPC erstellen. Wenn Sie Ihre VPC mithilfe der erstellen AWS Management Console und öffentliche Subnetze in Ihre Konfiguration einbeziehen, erstellen wir eine Routentabelle für das Subnetz und fügen die Routen hinzu, die für den direkten Zugriff auf das Internet erforderlich sind. Weitere Informationen finden Sie unter the section called “Erstellen einer VPC”.

Bereitstellen der Anwendung

Nachdem Sie Ihre VPC erstellt haben, können Sie Ihre Anwendung bereitstellen.

Produktionsumgebung

In einer Produktionsumgebung können Sie mit einem der folgenden Services Server in mehreren Availability Zones bereitstellen, um die Skalierung so zu konfigurieren, dass Sie die für die Anwendung erforderliche Mindestanzahl von Servern beibehalten, und um die Server zur gleichmäßigen Verteilung des Datenverkehrs bei einem Load Balancer zu registrieren.

- Amazon EC2 Auto Scaling
- EC2-Flotte
- Amazon Elastic Container Service (Amazon ECS)

Entwicklungs- oder Testumgebung

Für eine Entwicklungs- oder Testumgebung können Sie sich dafür entscheiden, eine einzelne EC2-Instance zu starten. Weitere Informationen finden Sie unter Erste Schritte mit Amazon EC2 im Amazon-EC2-Benutzerhandbuch.

IP-Adressierung für Ihre VPCs und Subnetze

IP-Adressen ermöglichen es Ressourcen in Ihrer VPC untereinander und mit Ressourcen im Internet zu kommunizieren.

Die CIDR-Notation (Classless Inter-Domain Routing) ist eine Möglichkeit, eine IP-Adresse und ihre Netzwerkmaske darzustellen. Diese Adressen haben folgendes Format:

- Eine einzelne IPv4-Adresse hat 32 Bits, mit 4 Gruppen mit bis zu 3 Dezimalstellen. Zum Beispiel 10.0.1.0.
- Ein IPv4-CIDR-Block hat vier Gruppen von bis zu drei Dezimalziffern, 0–255, die durch Punkte getrennt sind, gefolgt von einem Schrägstrich und einer Zahl von 0 bis 32. Beispiel: 10.0.0.0/16.
- Eine einzelne IPv6-Adresse besteht aus 128 Bits, mit 8 Gruppen von 4 hexadezimalen Ziffern. Zum Beispiel: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
- Ein IPv6-CIDR-Block hat vier Gruppen von bis zu vier hexadezimalen Ziffern, die durch Doppelpunkte getrennt sind, gefolgt von einem doppelten Doppelpunkt, gefolgt von einem Schrägstrich und einer Zahl von 1 bis 128. Zum Beispiel 2001:db8:1234:1a00::/56.

Weitere Informationen finden Sie unter Was ist CIDR?

Inhalt

Vergleich von IPv4 und IPv6

Die folgende Tabelle bietet eine Übersicht über die Unterschiede zwischen IPv4 und IPv6 unter Amazon EC2 und Amazon VPC. Eine Liste der AWS Dienste, die Dual-Stack-Konfigurationen (IPv4 und IPv6) und reine IPv6-Konfigurationen unterstützen, finden Sie unter. Services, die IPv6 unterstützen

Merkmal	IPv4	IPv6
VPC-Größe	Bis zu 5 CIDRs von /16 bis /28. Dieses Kontingent ist einstellbar.	Bis zu 5 CIDRs von /44 bis /60 in Schritten von /4. Dieses Kontingent ist einstellbar.
Subnetzgröße	Von /16 bis /28	Von /44 bis /64 in Schritten von /4.
Auswahl der Adresse	Sie können den IPv4-CIDR-Block für Ihre VPC auswählen oder einen CIDR-Block aus Amazon VPC IP Address Manager (IPAM) zuweisen. Weitere Informationen zu IPAM finden Sie unter Was ist IPAM? im Benutzerhandbuch von Amazon VPC IPAM.	Sie können Ihren eigenen IPv6-CIDR -Block AWS für Ihre VPC verwenden , einen von Amazon bereitgestellten IPv6-CIDR-Block wählen oder einen CIDR-Block von Amazon VPC IP Address Manager (IPAM) zuweisen. Weitere Informationen zu IPAM finden Sie unter Was ist IPAM? im Benutzerhandbuch von Amazon VPC IPAM.
Internetzugang	Erfordert ein Internet-Gateway.	Erfordert ein Internet-Gateway. Unterstützt nur ausgehende Kommunikation über ein Internet-Gateway für ausgehenden Verkehr.
Elastic-IP-Adressen	Unterstützt. Gibt einer EC2-Instance eine permanente, statische öffentlic he IPv4-Adresse.	Nicht unterstützt EIPs halten die öffentliche IPv4-Adresse einer Instance bei deren Neustart statisch. IPv6-Adressen sind standardmäßig statisch.

Merkmal	IPv4	IPv6
NAT gateways (NAT-Gateways)	Unterstützt. Instances in privaten Subnetzen können über ein öffentliches NAT-Gateway eine Verbindung zum Internet oder über ein privates NAT-Gateway eine Verbindung zu Ressourcen in anderen VPCs herstellen.	Unterstützt. Sie können ein NAT-Gateway mit NAT64 verwenden, um Instances in reinen IPv6-Netzwerken die Kommunikation mit reinen IPv4-Ressourcen innerhalb von VPCs, zwischen VPCs, in On-Premises-Netzwerken oder über das Internet zu ermöglichen.
DNS-Namen	Instances erhalten von Amazon bereitgestellte IPBN- oder RBN-basierte DNS-Namen. Der DNS-Name wird in die für die Instance ausgewählten DNS-Datensätze aufgelöst.	Instances erhalten von Amazon bereitgestellte IPBN- oder RBN-basierte DNS-Namen. Der DNS-Name wird in die für die Instance ausgewählten DNS-Datensätze aufgelöst.

Private IPv4-Adressen

Private IPv4-Adressen (in diesem Thema auch als private IP-Adressen bezeichnet) können nicht über das Internet erreicht werden. Sie können für die Kommunikation zwischen Instances in Ihrer VPC verwendet werden. Beim Start einer Instance in Ihrer VPC, wird der Standardnetzwerkschnittstelle (eth0) der Instance eine primäre private IP-Adresse aus dem IPv4-Adressbereich des Subnetzes zugeordnet. Darüber hinaus wird jeder Instance auch ein privater (interner) DNS-Hostname gegeben, der zur privaten IP-Adresse der Instance wird. Der Hostname kann zwei Arten haben: ressourcenbasiert oder IP-basiert. Weitere Informationen finden Sie unter EC2-Instance-Bennenung. Wenn Sie keine primäre private IP-Adresse angeben, wählen wir eine verfügbare IP-Adresse im Subnetzbereich für Sie aus. Weitere Informationen zu Netzwerkschnittstellen finden Sie unter Elastic Network Interfaces im Amazon EC2 EC2-Benutzerhandbuch.

Sie können den in der VPC ausgeführten Instances noch zusätzliche private IP-Adressen, auch sekundäre private IP-Adressen genannt, zuweisen. Im Gegensatz zu privaten IP-Adressen können Sie sekundäre private IP-Adressen erneut einer anderen Netzwerkschnittstelle zuweisen. Die Zuordnung der privaten IP-Adresse mit der Netzwerkschnittstelle bleibt bestehen, wenn die Instance angehalten und neu gestartet wird. Sie wird erst freigegeben, wenn die Instance beendet wird.

Weitere Informationen zu primären und sekundären IP-Adressen finden Sie unter Mehrere IP-Adressen im Amazon EC2 EC2-Benutzerhandbuch.

Wir bezeichnen private IP-Adressen als IP-Adressen, die innerhalb des IPv4-CIDR-Bereichs in der VPC liegen. Die meisten VPC IP-Adressbereiche fallen innerhalb des privaten (nicht öffentlich routingfähigen) IP-Adressbereichs, wie in RFC 1918 angegeben. Sie können jedoch auch öffentlich routingfähige CIDR-Blöcke für Ihre VPC verwenden. Unabhängig vom IP-Adressbereich Ihrer VPC unterstützen wir nicht den direkten Zugriff auf das Internet vom CIDR-Block Ihrer VPC, einschließlich einem öffentlich routingfähigen CIDR-Block. Sie müssen den Internetzugang über ein Gateway einrichten, z. B. ein Internet-Gateway, ein virtuelles privates Gateway, eine AWS Site-to-Site VPN Verbindung oder AWS Direct Connect.

Wir geben niemals den IPv4-Adressbereich eines Subnetzes ggü. dem Internet bekannt.

Öffentliche IPv4-Adressen

Alle Subnetze verfügen über ein Attribut, über das festlegt wird, ob eine in einem Subnetz erstellte Netzwerkschnittstelle automatisch eine öffentliche IPv4-Adresse (in diesem Thema auch als öffentliche IP-Adresse bezeichnet) erhält. Wenn Sie daher eine Instance in einem Subnetz starten, in dem dieses Attribut aktiviert ist, wird der primären Netzwerkschnittstelle (eth0), die für die Instance erstellt wurde, eine öffentliche IP-Adresse zugewiesen. Der primären privaten IP-Adresse wird über eine Netzwerkadressenübersetzung (Network Address Translation, NAT) eine öffentliche IP-Adresse zugewiesen.

> **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.

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 Ihres Subnetzes.

- Aktivieren oder Deaktivieren des öffentlichen IP-Adressierungsfeatures während des Starts einer Instance, wodurch das öffentliche IP-Adressierungsattribut des Subnetzes überschrieben wird.
- 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. Weitere Informationen finden Sie unter IP-Adressen verwalten im Amazon EC2 EC2-Benutzerhandbuch.

Eine öffentliche IP-Adresse wird von Amazons öffentlichem IP-Adresspool zugewiesen. Sie ist nicht mit Ihrem Konto verknüpft. Wenn eine öffentliche IP-Adresse von Ihrer Instance getrennt wurde, wird sie an den Pool zurückgegeben und steht Ihnen nicht länger zur Verfügung. In bestimmten Fällen geben wir die öffentliche IP-Adresse Ihrer Instance frei oder weisen ihr eine neue zu. Weitere Informationen finden Sie unter Öffentliche IP-Adressen im Amazon EC2 EC2-Benutzerhandbuch.

Wenn Sie für Ihr Konto eine persistente öffentliche IP-Adresse benötigen, die Instances nach Bedarf zugeordnet oder von diesen entfernt werden kann, verwenden Sie stattdessen eine Elastic-IP-Adresse. Weitere Informationen finden Sie unter Zuordnen von elastischen IP-Adressen zu Ressourcen in Ihrer VPC.

Wenn Ihre VPC DNS-Hostnamen unterstützt, wird jeder Instance, die eine öffentliche IP-Adresse oder eine Elastic-IP-Adresse erhält, auch ein öffentlicher DNS-Hostname zugewiesen. Wir ordnen den öffentlichen DNS-Hostnamen der öffentlichen IP-Adresse der Instance außerhalb des Instance-Netzwerks bzw. der privaten IP-Adresse der Instance innerhalb des Instance-Netzwerks zu. Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC.

IPv6-Adressen

Optional können Sie Ihrer VPC auch einen IPv6 CIDR-Block und Ihren Subnetzen IPv6 CIDR-Blöcke zuweisen. Weitere Informationen finden Sie unter den folgenden Themen:

- Hinzufügen eines IPv6-CIDR-Blocks zu Ihrer VPC
- Hinzufügen eines IP6-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 Ihres Subnetzes.
- 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 im Amazon EC2 EC2-Benutzerhandbuch.
- 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 und Verwalten von IP-Adressen im Amazon EC2 EC2-Benutzerhandbuch.

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 Richtlinie für den Datenverkehr zwischen Netzwerken in Amazon VPC.

Weitere Informationen über reservierte IPv6-Adressbereiche finden Sie unter IANA IPv6 Special-Purpose Address Registry und RFC4291.

Verwenden Sie Ihre eigenen IP-Adressen

Sie können Ihren eigenen öffentlichen IPv4-Adressbereich oder IPv6-Adressbereich ganz oder teilweise auf Ihr Konto übertragen. AWS Der Adressbereich gehört weiterhin Ihnen, wird jedoch von AWS standardmäßig im Internet veröffentlicht. Nachdem Sie den Adressbereich auf übertragen haben AWS, wird er in Ihrem Konto als Adresspool angezeigt. Sie können eine Elastic-IP-Adresse aus Ihrem IPv4-Adresspool erstellen und einen IPv6-CIDR-Block aus Ihrem IPv6-Adresspool mit einer VPC verknüpfen.

Weitere Informationen finden Sie unter Bring Your Own IP Addresses (BYOIP) im Amazon EC2 EC2-Benutzerhandbuch.

Amazon VPC IP Address Manager

Amazon VPC IP Address Manager (IPAM) ist eine VPC-Funktion, die es Ihnen erleichtert, IP-Adressen für Ihre Workloads zu planen, nachzuverfolgen und zu überwachen. AWS Sie können IPAM verwenden, um VPCs mithilfe bestimmter Geschäftsregeln IP-Adress-CIDRs zuzuweisen.

Weitere Informationen zu IPAM finden Sie unter Was ist IPAM? im Benutzerhandbuch von Amazon VPC IPAM.

VPC-CIDR-Blöcke

Die IP-Adressen für Ihre Virtual Private Cloud (VPC) werden in der CIDR-Notation (Classless Inter-Domain Routing) dargestellt. Einer VPC muss ein IPv4-CIDR-Block zugeordnet sein. Sie können optional zusätzliche IPv4-CIDR-Blöcke und einen oder mehrere IPv6-CIDR-Blöcke zuordnen. Weitere Informationen finden Sie unter IP-Adressierung für Ihre VPCs und Subnetze.

Inhalt

IPv4-VPC-CIDR-Blöcke

Beim Erstellen einer VPC müssen Sie einen IPv4-CIDR-Block für die VPC angeben. Die zugelassene Blockgröße liegt zwischen einer /16 Netzwerkmaske (65536 IP-Adressen) und einer /28 Netzwerkmaske (16 IP-Adressen). Nachdem Sie Ihre VPC erstellt haben, können Sie zusätzliche IPv4-CIDR-Blöcke der VPC zuordnen. Weitere Informationen finden Sie unter Hinzufügen eines IP4-CIDR-Blocks zu Ihrer VPC.

Wenn Sie eine VPC erstellen, empfehlen wir Ihnen, einen CIDR-Block aus den privaten IPv4-Adressbereichen festzulegen, wie unter RFC 1918 dargelegt.

Bereich RFC 1918	Beispiel-CIDR-Block
10.0.0.0 - 10.255.255.255 (10/8 Präfix)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16/12 Präfix)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168/16 Präfix)	192.168.0.0/20

Important

Einige AWS Dienste verwenden den CIDR-Bereich. `172.17.0.0/16` Verwenden Sie diesen Bereich beim Erstellen Ihrer VPC nicht, um zukünftige Konflikte zu vermeiden. Beispielsweise SageMaker kann es bei Diensten wie AWS Cloud9 oder Amazon zu IP-Adresskonflikten kommen, wenn der `172.17.0.0/16` IP-Adressbereich bereits irgendwo in Ihrem Netzwerk verwendet wird. Weitere Informationen finden Sie unter Verbindung zur EC2-Umgebung nicht möglich, da die IP-Adressen von VPC von Docker verwendet werden im AWS Cloud9 - Benutzerhandbuch.

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 IP-Adressen die IPv4-Adressen, die innerhalb des CIDR-Bereichs Ihrer VPC liegen.

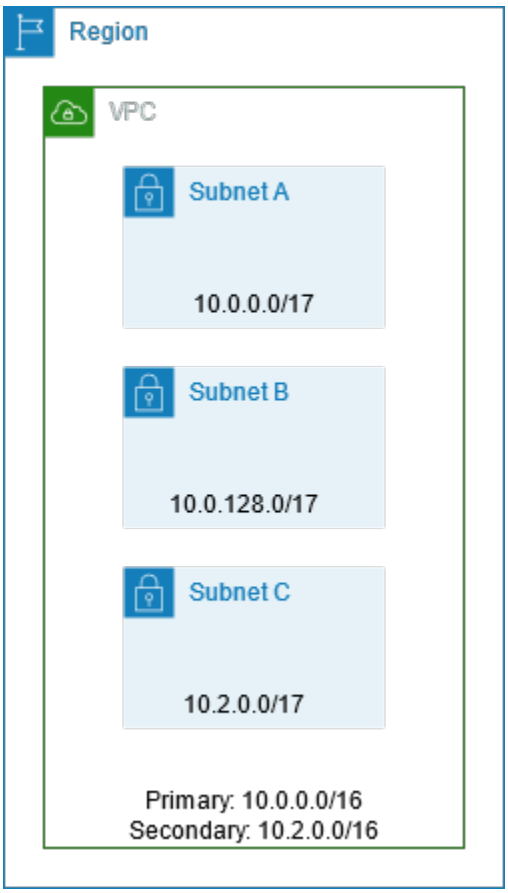
Wenn Sie eine VPC für die Verwendung mit einem AWS Service erstellen, überprüfen Sie in der Servicedokumentation, ob bestimmte Anforderungen für die Konfiguration gelten.

Wenn Sie eine VPC mit einem Befehlszeilen-Tool oder der Amazon-EC2-API erstellen, wird der CIDR-Block automatisch in seine kanonische Form geändert. Wenn Sie beispielsweise 100.68.0.18/18 für den CIDR-Block angeben, erstellen wir den CIDR-Block 100.68.0.0/18.

Verwalten von IPv4-CIDR-Blöcken für eine VPC

Sie können Ihrer VPC sekundäre IPv4-CIDR-Blöcke zuordnen. Wenn Sie Ihrer VPC einen CIDR-Block zuordnen, wird Ihren VPC-Routing-Tabellen automatisch eine Route hinzugefügt, um ein Routing innerhalb der VPC zu unterstützen (das Ziel ist der CIDR-Block, der Empfänger ist `local`).

Im folgenden Beispiel weist die VPC sowohl einen primären als auch einen sekundären CIDR-Block auf. Die CIDR-Blöcke für Subnetz A und Subnetz B stammen aus dem primären CIDR-Block der VPC. Der CIDR-Block für Subnetz C stammt aus dem sekundären CIDR-Block der VPC.



Die folgende Routing-Tabelle zeigt die lokalen Routen für die VPC.

Bestimmungsort	Ziel
10.0.0.0/16	Local

Bestimmungsort	Ziel
10.2.0.0/16	Local

Beim Hinzufügen eines CIDR-Blocks zu Ihrer VPC gelten die folgenden Regeln:

- Die zugelassene Blockgröße liegt zwischen der Netzwerkmaske `/28` und der Netzwerkmaske `/16`.
- Der CIDR-Block darf sich nicht mit vorhandenen CIDR-Blöcken überlappen, die der VPC zugeordnet sind.
- Es gibt Einschränkungen im Hinblick auf die IPv4-Adressbereiche, die Sie verwenden können. Weitere Informationen finden Sie unter Einschränkungen bei der Zuordnung von IPv4-CIDR-Blöcken.
- Sie können die Größe eines vorhandenen CIDR-Blocks nicht vergrößern oder verkleinern.
- Es gibt ein Kontingent für die Anzahl an CIDR-Blöcken, die Sie einer VPC zuordnen können, ebenso wie für die Anzahl der Routen, die Sie einer Routing-Tabellen hinzufügen können. Sie können einen CIDR-Block nicht zuordnen, wenn Sie dadurch Ihre Kontingente überschreiten würden. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.
- Der CIDR-Block darf nicht gleich dem oder größer als der CIDR-Zielbereich in einer Route in einer der VPC-Routing-Tabellen sein. In einer VPC, in der der primäre CIDR-Block beispielsweise `10.2.0.0/16` lautet, verfügen Sie über eine vorhandene Route in einer Routing-Tabelle mit dem Ziel `10.0.0.0/24` zu einem Virtual Private Gateway. Sie möchten einen sekundären CIDR-Block im Bereich `10.0.0.0/16` zuordnen. Aufgrund der vorhandenen Route können Sie den CIDR-Block `10.0.0.0/24` oder größere Blöcke nicht zuordnen. Sie können jedoch den sekundären CIDR-Block `10.0.0.0/25` oder kleiner zuordnen.
- Beim Hinzufügen von IPv4 CIDR-Blöcken zu einer VPC, die Teil einer VPC-Peering-Verbindung ist, gelten die folgenden Regeln:
  - Wenn die VPC-Peering-Verbindung `active` ist, können Sie einer VPC CIDR-Blöcke zuordnen, vorausgesetzt, diese überlappen sich nicht mit einem CIDR-Block der Peer-VPC.
  - Wenn die VPC-Peering-Verbindung `pending-acceptance` ist, kann der Eigentümer der anfordernden VPC der VPC keinen CIDR-Block hinzufügen, unabhängig davon, ob sich dieser mit dem CIDR-Block der entgegennehmenden VPC überlappt. Entweder muss der Eigentümer der entgegennehmenden VPC die Peering-Verbindung annehmen, oder der Eigentümer der anfordernden VPC muss die Anforderung der VPC-Peering-Verbindung löschen, den CIDR-Block hinzufügen und dann eine neue VPC-Peering-Verbindung anfordern.

  - Wenn die VPC-Peering-Verbindung `pending-acceptance` ist, kann der Eigentümer der entgegennehmenden VPC der VPC CIDR-Blöcke hinzufügen. Wenn sich ein sekundärer CIDR-Block mit einem CIDR-Block der anfordernden VPC überlappt, schlägt die Anforderung der VPC-Peering-Verbindung fehl und sie kann nicht angenommen werden.
- Wenn Sie über ein Direct Connect-Gateway eine Verbindung AWS Direct Connect zu mehreren VPCs Connect, dürfen die VPCs, die dem Direct Connect-Gateway zugeordnet sind, keine überlappenden CIDR-Blöcke haben. Wenn Sie einer der VPCs, die einem Direct Connect-Gateway zugeordnet ist, einen CIDR-Block hinzufügen, vergewissern Sie sich, dass der neue CIDR-Block nicht mit einem bestehenden CIDR-Block für eine andere VPC überlappt. Weitere Informationen finden Sie unter Direct Connect-Gateways im AWS Direct Connect -Benutzerhandbuch.
- Wenn Sie einen CIDR-Block hinzufügen oder entfernen, kann dieser verschiedene Status durchlaufen: `associating` | `associated` | `disassociating` | `disassociated` | `failing` | `failed`. Der CIDR-Block ist bereit für die Verwendung, wenn er sich im Status `associated` befindet.

Sie können die Zuordnung eines CIDR-Blocks aufheben, den Sie Ihrer VPC zugeordnet haben. Sie können jedoch nicht die Zuordnung des CIDR-Blocks aufheben, mit der Sie die VPC ursprünglich erstellt haben (den primären CIDR-Block). Um das primäre CIDR für Ihre VPC in der Amazon VPC-Konsole anzuzeigen, wählen Sie Your VPCs (Ihre VPCs), aktivieren Sie das Kontrollkästchen für Ihre VPC und wählen Sie die Registerkarte CIDRs. Um das primäre CIDR mithilfe von anzuzeigen, verwenden Sie den Befehl AWS CLI describe-vpcs wie folgt. Das primäre CIDR wird im obersten `CidrBlock element` zurückgegeben.

```
aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d --query Vpcs[*].CidrBlock --output text
```

Es folgt eine Beispielausgabe.

```
10.0.0.0/16
```

Einschränkungen bei der Zuordnung von IPv4-CIDR-Blöcken

Die folgende Tabelle gibt einen Überblick über zulässige und eingeschränkte VPC-CIDR-Blockzuordnungen. Der Grund für die Einschränkungen liegt darin, dass einige AWS Dienste VPC- und kontoübergreifende Funktionen verwenden, für die auf der Dienstseite keine Konflikte verursachende CIDR-Blöcke erforderlich sind. AWS

IP-Adressbereich	Beschränkte Verknüpfungen	Zugelassene Verknüpfungen
10.0.0.0/8	CIDR-Blöcke aus anderen RFC 1918*-Bereichen (172.16.0.0/12 und 192.168.0.0/16). Wenn einer der mit dem VPC verbundenen CIDR-Blöcke aus dem Bereich 10.0.0.0/15 (10.0.0.0 bis 10.1.255.255) stammt, können Sie keinen CIDR-Block aus dem Bereich 10.0.0.0/16 (10.0.0.0 bis 10.0.255.255) hinzufügen. Ein CIDR-Block aus dem Bereich 198.19.0.0/16.	Jeder andere CIDR-Block aus dem Bereich 10.0.0.0/8 zwischen einer /16-Netzmaske und einer /28-Netzmaske, der nicht eingeschränkt ist. Jeder öffentlich routbare IPv4-CIDR-Block (nicht RFC 1918) zwischen einer /16-Netzmaske und /28-Netzmaske oder ein CIDR-Block zwischen einer /16-Netzmaske und einer /28-Netzmaske aus dem Bereich 100.64.0.0/10.
169.254.0.0/16	CIDR-Blöcke aus dem Block „Link Local“ sind wie in RFC 5735 beschrieben reserviert und können VPCs nicht zugewiesen werden.	
172.16.0.0/12	CIDR-Blöcke aus anderen RFC 1918*-Bereichen (10.0.0.0/8 und 192.168.0.0/16). CIDR-Blöcke aus dem Bereich 172.31.0.0/16. CIDR-Blöcke aus dem Bereich 198.19.0.0/16.	Jeder andere CIDR-Block aus dem Bereich 172.16.0.0/12 zwischen einer /16-Netzmaske und einer /28-Netzmaske, der nicht eingeschränkt ist. Jeder öffentlich routbare IPv4-CIDR-Block (nicht RFC 1918) zwischen einer /16-Netzmaske und /28-Netzmaske oder ein CIDR-Block zwischen einer /16-Netzmaske und einer /28-Netzmaske aus dem Bereich 100.64.0.0/10.

IP-Adressbereich	Beschränkte Verknüpfungen	Zugelassene Verknüpfungen
192.168.0.0/16	CIDR-Blöcke aus anderen RFC 1918*-Bereichen (10.0.0.0/8 und 172.16.0.0/12). Ein CIDR-Block aus dem Bereich 198.19.0.0/16.	Jeder andere CIDR-Block aus dem Bereich 192.168.0.0/16 zwischen einer /16-Netzmaske und einer /28-Netzmaske. Jeder öffentlich routbare IPv4-CIDR-Block (nicht RFC 1918) zwischen einer /16-Netzmaske und /28-Netzmaske oder ein CIDR-Block aus dem 100.64.0.0/10-Bereich zwischen einer /16-Netzmaske und einer /28-Netzmaske.
198.19.0.0/16	CIDR-Blöcke aus den RFC 1918*-Bereichen.	Jeder öffentlich routbare IPv4-CIDR-Block (nicht RFC 1918) zwischen einer /16-Netzmaske und /28-Netzmaske oder ein CIDR-Block aus dem 100.64.0.0/10-Bereich zwischen einer /16-Netzmaske und einer /28-Netzmaske.
Öffentlich weiterleitbarer CIDR-Block (nicht RFC 1918), oder ein CIDR-Block aus dem Bereich 100.64.0.0/10	CIDR-Blöcke aus den RFC 1918*-Bereichen. Ein CIDR-Block aus dem Bereich 198.19.0.0/16.	Jeder andere öffentlich routbare IPv4-CIDR-Block (nicht RFC 1918) zwischen einer /16-Netzmaske und /28-Netzmaske oder ein CIDR-Block zwischen einer /16-Netzmaske und einer /28-Netzmaske aus dem Bereich 100.64.0.0/10.

*RFC 1918-Bereiche sind die privaten IPv4-Adressbereiche, die in RFC 1918 angegeben sind.

IPv6-VPC-CIDR-Blöcke

Sie können einen einzelnen IPv6 CIDR-Block zuordnen, wenn Sie eine neue VPC erstellen, oder Sie können bis zu fünf IPv6 CIDR-Blöcke von `/44` bis `/60` in Schritten von `/4` zuordnen. Sie können einen IPv6-CIDR-Block aus dem IPv6-Adresspool von Amazon anfordern. Weitere Informationen finden Sie unter Hinzufügen eines IPv6-CIDR-Blocks zu Ihrer VPC.

Wenn Sie Ihrer VPC einen IPv6-CIDR-Block zugewiesen haben, können Sie auch einem vorhandenen Subnetz in Ihrer VPC einen IPv6-CIDR-Block zuweisen oder ihn beim Erstellen eines neuen Subnetzes verknüpfen. Weitere Informationen finden Sie unter the section called “Dimensionierung der Subnetze für IPv6”.

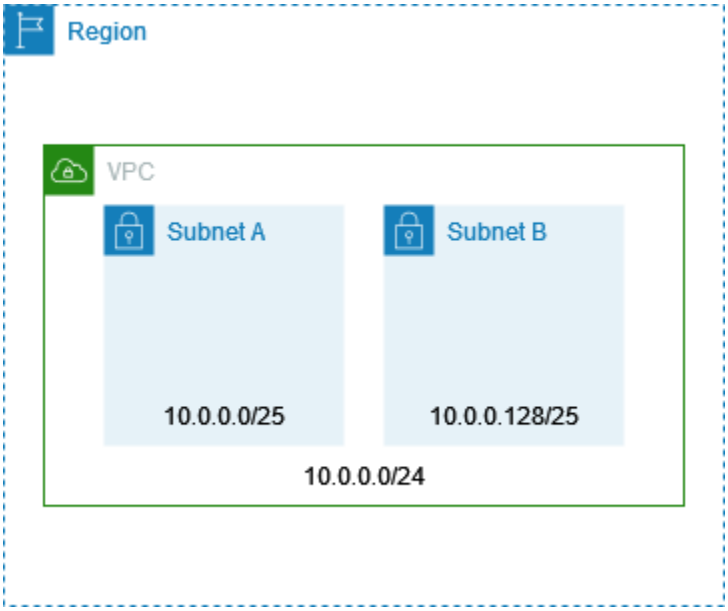
Wenn Sie beispielsweise eine VPC erstellen und angeben, dass Sie dieser VPC einen von Amazon bereitgestellten IPv6 CIDR-Block zuweisen möchten, dann weist Amazon Ihrer VPC den folgenden IPv6 CIDR-Block zu: `2001:db8:1234:1a00::/56`. Sie können den Bereich der IP-Adressen nicht selbst auswählen. Sie können ein Subnetz erstellen und einen IPv6 CIDR-Block aus diesem Bereich zuweisen, zum Beispie, `2001:db8:1234:1a00::/64`.

Die Zuordnung eines IPv6-CIDR-Blocks zu einer VPC lässt sich aufheben. Wenn Sie die Zuordnung eines IPv6 CIDR-Blocks zu einer VPC aufheben, können Sie nicht erwarten, bei einer späteren erneuten Zuordnung eines IPv6 CIDR-Blocks zu Ihrer VPC das gleiche CIDR zu erhalten.

Subnetz-CIDR-Blöcke

Die IP-Adressen für Ihre Subnetze werden in der CIDR-Notation (Classless Inter-Domain Routing) dargestellt. Der CIDR-Block eines Subnetzes kann mit dem CIDR-Block der VPC übereinstimmen (zum Erstellen eines einzelnen Subnetzes in der VPC) oder eine Teilmenge des CIDR-Blocks für die VPC sein (zum Erstellen mehrerer Subnetze in der VPC). Wenn Sie mehr als ein Subnetz in einer VPC erstellen, dürfen sich die CIDR-Blöcke der Subnetze nicht überlappen.

Wenn Sie beispielsweise eine VPC mit dem CIDR-Block `10.0.0.0/24` erstellt haben, unterstützt er 256 IP-Adressen. Sie können diesen CIDR-Block in zwei Subnetze aufteilen, die jeweils 128 IP-Adressen unterstützen. Ein Subnetz verwendet den CIDR-Block `10.0.0.0/25` (für die Adressen `10.0.0.0` – `10.0.0.127`) und das andere verwendet den CIDR-Block `10.0.0.128/25` (für die Adressen `10.0.0.128` – `10.0.0.255`).



Im Internet stehen Tools zur Verfügung, mit denen Sie IPv4- und IPv6-Subnetz-CIDR-Blöcke berechnen und erstellen können. Sie können Tools finden, die Ihren Bedürfnissen entsprechen, indem Sie nach Begriffen wie „Subnetzrechner“ oder „CIDR-Rechner“ suchen. Darüber hinaus kann Ihnen die Netzwerk-Engineering-Gruppe dabei behilflich sein, die IPv4- und IPv6-CIDR-Blöcke zu ermitteln, die Sie für Ihre Subnetze festlegen sollten.

Dimensionierung der Subnetze für IPv4

Die zugelassene IPv4- und IPv6-Blockgröße liegt zwischen der Netzmaske `/28` und der Netzmaske `/16`. Die ersten vier IP-Adressen und die letzte IP-Adresse in jedem Subnetz-CIDR-Block stehen nicht zu Ihrer Verfügung und können daher keiner Ressource wie etwa einer EC2-Instance zugewiesen werden. So sind beispielsweise in einem Subnetz mit dem CIDR-Block `10.0.0.0/24` die folgenden fünf IP-Adressen reserviert:

- 10.0.0.0: Netzwerkadresse.
- 10.0.0.1: Reserviert von AWS für den VPC-Router.
- 10.0.0.2: Reserviert von. AWS Die IP-Adresse des DNS-Servers ist die Basis des VPC-Netzwerkbereichs plus zwei. Für VPCs mit mehreren CIDR-Blöcken befindet sich die IP-Adresse des DNS-Servers im primären CIDR. Wir reservieren auch die Basis jedes Subnetzbereichs plus zwei für alle CIDR-Blöcke in der VPC. Weitere Informationen finden Sie unter Amazon DNS-Server.
- 10.0.0.3: AWS Für die future Verwendung reserviert.
- 10.0.0.255: Broadcast Adresse des Netzwerks. Wir unterstützen nicht die Broadcasting-Funktion in einer VPC, daher reservieren wir diese Adresse.

Wenn Sie ein Subnetz mit einem Befehlszeilen-Tool oder der Amazon-EC2-API erstellen, wird der CIDR-Block automatisch in seine kanonische Form geändert. Wenn Sie beispielsweise 100.68.0.18/18 für den CIDR-Block angeben, erstellen wir den CIDR-Block 100.68.0.0/18.

Wenn Sie AWS mithilfe von BYOIP einen IPv4-Adressbereich verwenden, können Sie alle IP-Adressen im Bereich verwenden, einschließlich der ersten Adresse (der Netzwerkadresse) und der letzten Adresse (der Broadcast-Adresse).

Dimensionierung der Subnetze für IPv6

Wenn Sie Ihrer VPC einen IPv6 CIDR-Block zugewiesen haben, können Sie auch einem vorhandenen Subnetz in Ihrer VPC einen IPv6 CIDR-Block zuweisen oder ihn beim Erstellen eines neuen Subnetzes verknüpfen. Mögliche IPv6-Netzmaskenlängen liegen zwischen `/44` und `/64` in Schritten von `/4`.

Im Internet stehen Tools zur Verfügung, mit denen Sie IPv6-Subnetz-CIDR-Blöcke berechnen und erstellen können. Sie können Tools finden, die Ihren Bedürfnissen entsprechen, indem Sie nach Begriffen wie „IPv6-Subnetzrechner“ oder „IPv6-CIDR-Rechner“ suchen. Darüber hinaus kann Ihnen Ihre Netzwerk-Engineering-Gruppe dabei behilflich sein, die IPv6-CIDR-Blöcke zu ermitteln, die Sie für Ihre Subnetze festlegen sollten.

Die ersten vier IPv6-Adressen und die letzte IPv6-Adresse in jedem Subnetz-CIDR-Block stehen nicht zu Ihrer Verfügung und können daher keiner EC2-Instance zugewiesen werden. So sind beispielsweise in einem Subnetz mit dem CIDR-Block `2001:db8:1234:1a00/64` die folgenden fünf IP-Adressen reserviert:

- `2001:db8:1234:1a00::`
- `2001:db8:1234:1a00::1`: Reserviert von AWS für den VPC-Router.
- `2001:db8:1234:1a00::2`
- `2001:db8:1234:1a00::3`
- `2001:db8:1234:1a00:ffff:ffff:ffff:ffff`

Zusätzlich zu der IP-Adresse, die im obigen Beispiel AWS für den VPC-Router reserviert wurde, sind die folgenden IPv6-Adressen für den Standard-VPC-Router reserviert:

- Eine Link-lokale IPv6-Adresse im FE80::/10-Bereich, die mit EUI-64 generiert wurde. Weitere Informationen zu Link-lokalen Adressen finden Sie unter Link-lokale Adresse.

- Die Link-lokale IPv6-Adresse `FE80:ec2::1`.

Wenn Sie über IPv6 mit dem VPC-Router kommunizieren müssen, können Sie Ihre Anwendungen so konfigurieren, dass sie mit der Adresse kommunizieren, die Ihren Anforderungen am besten entspricht.

Gruppieren von CIDR-Blöcken mit verwalteten Präfixlisten

Eine verwaltete Präfixliste ist ein Satz von einem oder mehreren CIDR-Blöcken. Sie können Präfixlisten verwenden, um die Konfiguration und Pflege Ihrer Sicherheitsgruppen und Routing-Tabellen zu vereinfachen. Sie können eine Präfixliste aus den IP-Adressen erstellen, die Sie häufig verwenden, und sie als Satz in Sicherheitsgruppenregeln und -Routen referenzieren, anstatt sie einzeln zu referenzieren. Sie können beispielsweise Sicherheitsgruppenregeln mit verschiedenen CIDR-Blöcken, aber demselben Port und demselben Protokoll in einer einzigen Regel konsolidieren, die eine Präfixliste verwendet. Wenn Sie Ihr Netzwerk skalieren und den Datenverkehr von einem anderen CIDR-Block zulassen müssen, können Sie die entsprechende Präfixliste aktualisieren und alle Sicherheitsgruppen, die die Präfixliste verwenden, werden aktualisiert. Sie können verwaltete Präfixlisten auch mit anderen AWS Konten verwenden, die Resource Access Manager (RAM) verwenden.

Es gibt zwei Arten von Präfixlisten:

- Vom Kunden verwaltete Präfixlisten – Sätze von IP-Adressbereichen, die Sie definieren und verwalten. Sie können Ihre Präfixliste für andere AWS Konten freigeben, sodass diese Konten in ihren eigenen Ressourcen auf die Präfixliste verweisen können.
- Von AWS verwaltete Präfixlisten – Satz von IP-Adressbereichen für - AWS Services. Sie können eine von AWS verwaltete Präfixliste nicht erstellen, ändern, freigeben oder löschen.

Inhalt

Konzepte und Regeln für Präfixlisten

Eine Präfixliste besteht aus Einträgen. Jeder Eintrag besteht aus einem CIDR-Block und optional einer Beschreibung für den CIDR-Block.

Vom Kunden verwaltete Präfixlisten

Für vom Kunden verwaltete Präfixlisten gelten die folgenden Regeln:

- Eine Präfixliste unterstützt nur einen einzigen IP-Adresstyp (IPv4 oder IPv6). Sie können IPv4- und IPv6-CIDR-Blöcke nicht in einer einzigen Präfixliste kombinieren.
- Eine Präfixliste gilt nur für die Region, in der Sie sie erstellt haben.
- Wenn Sie eine Präfixliste erstellen, müssen Sie die maximale Anzahl von Einträgen angeben, die die Präfixliste unterstützen kann.
- Wenn Sie in einer Ressource auf eine Präfixliste verweisen, zählt die maximale Anzahl von Einträgen für die Präfixlisten zu, Kontingent für die Einträge für die Ressource. Wenn Sie beispielsweise eine Präfixliste mit maximal 20 Einträgen erstellen und in einer Sicherheitsgruppenregel auf diese Präfixliste verweisen, zählt dies als 20 Regeln für die Sicherheitsgruppe.
- Wenn Sie in einer Routing-Tabelle auf eine Präfixliste verweisen, gelten die Routingprioritätsregeln. Weitere Informationen finden Sie unter Routenpriorität und Präfixlisten.
- Sie können eine Präfixliste erstellen. Wenn Sie Einträge hinzufügen oder entfernen, erstellen wir eine neue Version der Präfixliste. Ressourcen, die auf das Präfix verweisen, verwenden stets die aktuelle (neueste) Version. Sie können die Einträge aus einer früheren Version der Präfixliste wiederherstellen, wodurch auch eine neue Version erstellt wird.
- Präfixlisten unterliegen Kontingenten. Weitere Informationen finden Sie unter Vom Kunden verwaltete Präfixlisten.
- Vom Kunden verwaltete Präfixlisten sind in allen kommerziellen AWS Regionen (einschließlich GovCloud (USA) und China) verfügbar.

AWS Von verwaltete Präfixlisten

Die folgenden Regeln gelten für von AWS verwaltete Präfixlisten:

- Sie können eine von AWS verwaltete Präfixliste nicht erstellen, ändern, freigeben oder löschen.
- Verschiedene von AWS verwaltete Präfixlisten haben eine andere Gewichtung, wenn Sie sie verwenden. Weitere Informationen finden Sie unter Von AWS verwaltete Präfixlistengewicht.

- Sie können die Versionsnummer einer von AWS verwalteten Präfixliste nicht anzeigen.

Identitäts- und Zugriffsverwaltung für Präfixlisten

Standardmäßig sind -Benutzer nicht berechtigt, Präfixlisten zu erstellen, anzuzeigen, zu ändern oder zu löschen. Sie können eine IAM-Richtlinie erstellen und sie einer Rolle anfügen, die Benutzern erlaubt, mit Präfixlisten zu arbeiten.

Eine Liste der Amazon VPC-Aktionen und der Ressourcen und Bedingungsschlüssel, die Sie in einer IAM-Richtlinie verwenden können, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2 im IAM-Benutzerhandbuch.

Mit der folgenden Beispielrichtlinie können Benutzer nur die Präfixliste `pl-123456abcde123456` anzeigen und mit ihr arbeiten. Benutzer können keine Präfixlisten erstellen oder löschen.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:ModifyManagedPrefixList",
        "ec2:RestoreManagedPrefixListVersion"
      ],
      "Resource": "arn:aws:ec2:region:account:prefix-list/pl-123456abcde123456"
    },
    {
      "Effect": "Allow",
      "Action": "ec2:DescribeManagedPrefixLists",
      "Resource": "*"
    }
   ]
}
```

Weitere Informationen über die Arbeit mit IAM in Amazon VPC finden Sie unter Identity and Access Management für Amazon VPC.

Arbeiten mit vom Kunden verwalteten Präfixlisten

Sie können vom Kunden verwaltete Präfixlisten erstellen und verwalten. Sie können von AWS verwaltete Präfixlisten anzeigen.

Aufgaben

- Erstellen einer Präfixliste
- Anzeigen der Präfixliste
- Anzeigen der Einträge für eine Präfixliste
- Anzeigen von Zuordnungen (Referenzen) für Ihre Präfixliste
- Ändern einer Präfixliste
- Größe einer Präfixliste ändern
- Wiederherstellen einer früheren Version einer Präfixliste
- Löschen einer Präfixliste

Erstellen einer Präfixliste

Wenn Sie eine Präfixliste erstellen, müssen Sie die maximale Anzahl von Einträgen angeben, die die Präfixliste unterstützen kann.

Einschränkung

Sie können einer Sicherheitsgruppenregel keine Präfixliste hinzufügen, wenn die Anzahl der Regeln plus die maximalen Einträge für die Präfixliste das Kontingent für Regeln pro Sicherheitsgruppe für Ihr Konto übersteigt.

So erstellen Sie eine Präfixliste mit der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Wählen Sie Create prefix list (Präfixliste erstellen).
4. Geben Sie für Prefix list name (Name der Präfixliste) einen Namen für die Präfixliste ein.
5. Geben Sie für Max entries (Max. Einträge) die maximale Anzahl von Einträgen für die Präfixliste ein.
6. Wählen Sie unter Address family (Adressfamilie) aus, ob die Präfixliste IPv4- oder IPv6-Einträge unterstützt.

7. Wählen Sie für Prefix list entries (Präfixlisteneinträge) Add new entry (Neuen Eintrag hinzufügen) und geben Sie den CIDR-Block und eine Beschreibung für den Eintrag ein. Wiederholen Sie diesen Schritt für jeden Eintrag.
8. (Optional) Fügen Sie unter Tags der Präfixliste Tags hinzu, damit Sie sie später identifizieren können.
9. Wählen Sie Create prefix list (Präfixliste erstellen).

So erstellen Sie eine Präfixliste mit der AWS CLI

Verwenden Sie den create-managed-prefix-list-Befehl.

Anzeigen der Präfixliste

Sie können Ihre Präfixlisten, für Sie freigegebene Präfixlisten und AWS-verwaltete Präfixlisten anzeigen.

So zeigen Sie Präfixlisten mit der Konsole an:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. In der Spalte Besitzer-ID wird die AWS Konto-ID des Besitzers der Präfixliste angezeigt. Bei von AWS verwalteten Präfixlisten lautet die Besitzer-ID AWS.

So zeigen Sie Präfixlisten mit der an AWS CLI

Verwenden Sie den describe-managed-prefix-lists-Befehl.

Anzeigen der Einträge für eine Präfixliste

Sie können die Einträge für Ihre Präfixlisten, für Sie freigegebenen Präfixlisten und von AWS verwalteten Präfixlisten anzeigen.

So zeigen Sie die Einträge für eine Präfixliste mit der Konsole an:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Aktivieren Sie das Kontrollkästchen für die Präfixliste.

4. Wählen Sie im unteren Bereich Entries (Einträge), um die Einträge für die Präfixliste anzuzeigen.

So zeigen Sie die Einträge für eine Präfixliste mit der an AWS CLI

Verwenden Sie den Befehl get-managed-prefix-list-entries.

Anzeigen von Zuordnungen (Referenzen) für Ihre Präfixliste

Sie können die IDs und Besitzer der Ressourcen anzeigen, die Ihrer Präfixliste zugeordnet sind. Zugeordnete Ressourcen sind Ressourcen, die in ihren Einträgen oder Regeln auf Ihre Präfixliste verweisen.

Einschränkung

Sie können keine zugehörigen Ressourcen für eine von AWS verwaltete Präfixliste anzeigen.

So zeigen Sie Präfixlistenzuordnungen mit der Konsole an:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Aktivieren Sie das Kontrollkästchen für die Präfixliste.
4. Wählen Sie im unteren Bereich Associations (Zuordnungen), um die Ressourcen anzuzeigen, die auf die Präfixliste verweisen.

So zeigen Sie Präfixlistenzuordnungen mit der an AWS CLI

Verwenden Sie den Befehl get-managed-prefix-list-associations.

Ändern einer Präfixliste

Sie können den Namen der Präfixliste ändern und Einträge hinzufügen oder entfernen. Um die maximale Anzahl von Einträgen zu ändern, siehe Größe einer Präfixliste ändern.

Durch das Aktualisieren der Einträge einer Präfixliste wird eine neue Version der Präfixliste erstellt. Durch das Aktualisieren des Namens oder der maximalen Anzahl von Einträgen für eine Präfixliste wird keine neue Version der Präfixliste erstellt.

Überlegungen

- Sie können eine von AWS verwaltete Präfixliste nicht ändern.

- Wenn Sie die maximale Anzahl von Einträgen in einer Präfixliste erhöhen, wird die erhöhte maximale Größe auf das Kontingent von Einträgen für die Ressourcen angewendet, die auf die Präfixliste verweisen. Wenn eine dieser Ressourcen die erhöhte maximale Größe nicht unterstützen kann, schlägt der Änderungsvorgang fehl und die vorherige maximale Größe wird wiederhergestellt.

So ändern Sie eine Präfixliste mit der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Aktivieren Sie das Kontrollkästchen für die Präfixliste und wählen Sie Aktionen, Präfixliste ändern.
4. Geben Sie unter Prefix list name (Name der Präfixliste) einen neuen Namen für die Präfixliste ein.
5. Wählen Sie für Prefix list entries (Präfixlisteneinträge) Remove (Entfernen), um einen vorhandenen Eintrag zu entfernen. Um einen neuen Eintrag hinzuzufügen, wählen Sie Add new entry (Neuen Eintrag hinzufügen) und geben Sie den CIDR-Block und eine Beschreibung für den Eintrag ein.
6. Wählen Sie Save prefix list (Präfixliste speichern).

So ändern Sie eine Präfixliste mithilfe der AWS CLI

Verwenden Sie den modify-managed-prefix-list-Befehl.

Größe einer Präfixliste ändern

Sie können die Größe und die maximale Anzahl von Einträgen einer Präfixliste auf bis zu 1.000 ändern. Weitere Informationen zu den Kontingenten der vom Kunden verwalteten Schlüssel finden Sie unter Vom Kunden verwaltete Präfixlisten.

So ändern Sie die Größe einer Präfixliste mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Wählen Sie das Kontrollkästchen für die Präfixliste aus, und wählen Sie Aktionen, Größe der Präfixliste ändern.

4. Geben Sie für Neue max. Einträge einen Wert ein.
5. Wählen Sie Resize (Größe ändern) aus.

So ändern Sie die Größe einer Präfixliste mithilfe der AWS CLI

Verwenden Sie den modify-managed-prefix-list-Befehl.

Wiederherstellen einer früheren Version einer Präfixliste

Sie können die Einträge aus einer früheren Version Ihrer Präfixliste wiederherstellen. Dadurch wird eine neue Version der Präfixliste erstellt.

Wenn Sie die Größe der Präfixliste verkleinert haben, müssen Sie sicherstellen, dass die Präfixliste groß genug ist, um die Einträge aus der vorherigen Version zu enthalten.

So stellen Sie eine frühere Version einer Präfixliste mithilfe der Konsole wieder her:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Wählen Sie das Kontrollkästchen für die Präfixliste aus, und wählen Sie Actions (Aktionen), Restore prefix list (Präfixliste wiederherstellen).
4. Wählen Sie für Version der Präfixliste auswählen eine frühere Version aus. Die Einträge für die ausgewählte Version werden in den Einträgen der Präfixliste angezeigt.
5. Wählen Sie Restore prefix list (Präfixliste wiederherstellen).

So stellen Sie eine frühere Version einer Präfixliste mithilfe der wieder her AWS CLI

Verwenden Sie den Befehl restore-managed-prefix-list-version.

Löschen einer Präfixliste

Um eine Präfixliste zu löschen, müssen Sie zunächst alle Verweise darauf in Ihren Ressourcen entfernen (z. B. in den Routing-Tabellen). Wenn Sie die Präfixliste mit AWS RAM freigegeben haben, müssen alle Verweise in benutzereigenen Ressourcen zuerst entfernt werden.

Einschränkung

Sie können eine von AWS verwaltete Präfixliste nicht löschen.

So löschen Sie eine Präfixliste mit der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Wählen Sie die Präfixliste aus, und wählen Sie Actions (Aktionen), Delete prefix list (Präfixliste löschen).
4. Geben Sie in das Bestätigungsfeld `delete` ein, und wählen Sie dann Delete (Löschen).

So löschen Sie eine Präfixliste mithilfe der AWS CLI

Verwenden Sie den delete-managed-prefix-list-Befehl.

Arbeiten mit von AWS verwalteten Präfixlisten

AWS Von verwaltete Präfixlisten sind Gruppen von IP-Adressbereichen für - AWS Services.

Inhalt

Verwenden einer von AWS verwalteten Präfixliste

AWS Von verwaltete Präfixlisten werden von erstellt und verwaltet AWS und können von jedem mit einem - AWS Konto verwendet werden. Sie können eine von AWS verwaltete Präfixliste nicht erstellen, ändern, freigeben oder löschen.

Wie bei vom Kunden verwalteten Präfixlisten können Sie von verwaltete Präfixlisten mit AWS Ressourcen wie Sicherheitsgruppen und Routing AWS-Tabellen verwenden. Weitere Informationen finden Sie unter Referenz-Präfix-Listen in Ihren AWS -Ressourcen.

Von AWS verwaltete Präfixlistengewicht

Die Gewichtung einer von AWS verwalteten Präfixliste bezieht sich auf die Anzahl der Einträge, die sie in einer Ressource aufnimmt.

Die Gewichtung einer von Amazon CloudFront verwalteten Präfixliste beträgt beispielsweise 55. So wirkt sich dies auf Ihre Amazon VPC-Kontingente aus:

- Sicherheitsgruppen – Das Standardkontingent beträgt 60 Regeln, so dass nur 5 zusätzliche Regeln in einer Sicherheitsgruppe möglich sind. Sie können eine Erhöhung dieses Kontingents beantragen.
- Routing-Tabellen – Das Standardkontingent beträgt 50 Routen. Sie müssen also eine Kontingenterhöhung beantragen, bevor Sie die Präfixliste zu einer Routing-Tabelle hinzufügen können.

Verfügbare von AWS verwaltete Präfixlisten

Die folgenden Services stellen von AWS verwaltete Präfixlisten bereit.

AWS-Service	Name der Präfixliste	Gewicht
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing	55
Amazon DynamoDB	com.amazonaws.*region*.dynamodb	1
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws.*region*.ipv6.route53-healthchecks	25
	com.amazonaws.*region*.route53-healthchecks	25
Amazon S3	com.amazonaws.*region*.s3	1
Amazon S3 Express One Zone	com.amazonaws.*region*.s3express	6
Amazon VPC Lattice	com.amazonaws.*region*.vpc-lattice	10
	com.amazonaws.*region*.ipv6.vpc-lattice	10

So zeigen Sie die von AWS verwalteten Präfixlisten mit der Konsole an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Fügen Sie im Suchfeld den Filter Eigentümer-ID: AWS hinzu.

So zeigen Sie die von AWS verwalteten Präfixlisten mit der an AWS CLI

Verwenden Sie den describe-managed-prefix-lists-Befehl wie folgt:

```
aws ec2 describe-managed-prefix-lists --filters Name=owner-id,Values=AWS
```

Arbeiten mit freigegebenen Präfixlisten

Mit AWS Resource Access Manager (AWS RAM) kann der Besitzer einer Präfixliste eine Präfixliste für Folgendes freigeben:

- Spezifische AWS Konten innerhalb oder außerhalb seiner Organisation in AWS Organizations
- Eine Organisationseinheit innerhalb ihrer Organisation in AWS Organizations
- Eine gesamte Organisation in AWS Organizations

Konsumenten, für die eine Präfixliste freigegeben wurde, können die Präfixliste und ihre Einträge anzeigen und in ihren AWS Ressourcen auf die Präfixliste verweisen.

Weitere Informationen zu AWS RAM finden Sie im AWS RAM -Benutzerhandbuch.

Inhalt

Voraussetzungen für die Freigabe von Präfixlisten

- Um eine Präfixliste freizugeben, müssen Sie diesen besitzen. Sie können eine für Sie freigegebene Präfixliste nicht freigeben. Sie können eine von AWS verwaltete Präfixliste nicht freigeben.

- Um eine Präfixliste für Ihre Organisation oder eine Organisationseinheit in AWS Organizations freigeben zu können, müssen Sie die Freigabe mit AWS Organizations aktivieren. Weitere Informationen finden Sie unter Freigabe für AWS Organizations aktivieren im AWS RAM - Benutzerhandbuch.

Teilen einer Präfixliste

Um eine Präfixliste freizugeben, müssen Sie sie einer Ressourcenfreigabe hinzufügen. Wenn Sie keine Ressourcenfreigabe haben, müssen Sie zuerst mit der AWS RAM -Konsole eine Ressourcenfreigabe erstellen.

Wenn Sie Teil einer Organisation in sind AWS Organizations und die Freigabe innerhalb Ihrer Organisation aktiviert ist, wird Konsumenten in Ihrer Organisation automatisch Zugriff auf die freigegebene Präfixliste gewährt. Andernfalls erhalten Konsumenten eine Einladung zur Teilnahme an der Ressourcenfreigabe, und nach Annahme der Einladung wird ihnen Zugriff auf die freigegebene Präfixliste gewährt.

Sie können mit der AWS RAM -Konsole oder der AWS CLI eine Ressourcenfreigabe erstellen und eine Präfixliste freigeben, deren Eigentümer Sie sind.

So erstellen Sie mit der AWS RAM -Konsole eine Ressourcenfreigabe und geben eine Präfixliste frei:

Führen Sie die Schritte unter Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch aus. Wählen Sie unter Select resource type (Ressourcentyp auswählen) die Option Prefix Lists (Präfixlisten) aus, und markieren Sie dann das Kontrollkästchen für die Präfixliste.

So fügen Sie einer vorhandenen Ressourcenfreigabe mithilfe der AWS RAM -Konsole eine Präfixliste hinzu:

Um einer vorhandenen Ressourcenfreigabe ein verwaltetes Präfix hinzuzufügen, dessen Eigentümer Sie sind, führen Sie die Schritte unter Aktualisieren einer Ressourcenfreigabe im AWS RAM - Benutzerhandbuch durch. Wählen Sie unter Select resource type (Ressourcentyp auswählen) die Option Prefix Lists (Präfixlisten) aus, und markieren Sie dann das Kontrollkästchen für die Präfixliste.

So geben Sie eine Präfixliste in Ihrem Besitz mithilfe der frei AWS CLI

Verwenden Sie zum Erstellen und Aktualisieren einer Ressourcenfreigabe die folgenden Befehle:

- create-resource-share

- associate-resource-share
- update-resource-share

Identifizieren einer freigegebenen Präfixliste

Besitzer und Verbraucher können freigegebene Präfixlisten mit der Amazon VPC-Konsole oder der AWS CLI identifizieren.

So identifizieren Sie eine freigegebene Präfixliste mit der Amazon VPC-Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Auf der Seite werden die Präfixlisten angezeigt, deren Besitzer Sie sind, sowie die Präfixlisten, die für Sie freigegeben wurden. In der Spalte Owner ID (Besitzer-ID) wird die AWS -Konto-ID des Besitzers der Präfixliste angezeigt.
4. Um die Informationen zur Ressourcenfreigabe für eine Präfixliste anzuzeigen, wählen Sie die Präfixliste aus, und wählen Sie im unteren Bereich die Option Sharing (Freigeben) .

So identifizieren Sie eine freigegebene Präfixliste mithilfe der AWS CLI

Verwenden Sie den describe-managed-prefix-lists-Befehl. Der Befehl gibt die Präfixlisten zurück, die Sie besitzen, und die Präfixlisten, die für Sie freigegeben werden. `OwnerId` zeigt die AWS Konto-ID des Besitzers der Präfixliste an.

Identifizieren von Verweisen auf eine freigegebene Präfixliste

Besitzer können die verbrauchereigenen Ressourcen identifizieren, die auf eine freigegebene Präfixliste verweisen.

So identifizieren Sie Verweise auf eine freigegebene Präfixliste mit der Amazon VPC-Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Managed Prefix Lists (Verwaltete Präfixlisten) aus.
3. Wählen Sie die Präfixliste aus, und wählen Sie im unteren Bereich Associations (Zuordnungen).
4. Die IDs der Ressourcen, die auf die Präfixliste verweisen, werden in der Spalte Resource ID (Ressourcen-ID) aufgeführt. Die Besitzer der Ressourcen werden in der Spalte Resource Owner (Ressourcenbesitzer) aufgeführt.

So identifizieren Sie Verweise auf eine freigegebene Präfixliste mithilfe der AWS CLI

Verwenden Sie den Befehl get-managed-prefix-list-associations.

Aufheben der Freigabe einer freigegebenen Präfixliste

Wenn Sie die Freigabe einer Präfixliste aufheben, können Konsumenten die Präfixliste oder ihre Einträge in ihrem Konto nicht mehr anzeigen, und sie können nicht auf die Präfixliste in ihren Ressourcen verweisen. Wenn auf die Präfixliste bereits in den Ressourcen des Konsumenten verwiesen wird, funktionieren diese Verweise weiterhin normal, und Sie können diese Referenzen weiterhin anzeigen. Wenn Sie die Präfixliste auf eine neue Version aktualisieren, verwenden die Verweise die neueste Version.

Um die Freigabe einer freigegebenen Präfixliste in Ihrem Besitz aufzuheben, müssen Sie sie mithilfe von aus der Ressourcenfreigabe entfernen AWS RAM.

So heben Sie die Freigabe einer freigegebenen Präfixliste in Ihrem Besitz mithilfe der AWS RAM Konsole auf

Siehe Aktualisieren einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

So heben Sie die Freigabe einer freigegebenen Präfixliste in Ihrem Besitz mithilfe der auf AWS CLI

Verwenden Sie den disassociate-resource-share-Befehl.

Berechtigungen für freigegebene Präfixlisten

Berechtigungen für Besitzer

Besitzer sind für die Verwaltung einer freigegebenen Präfixliste und ihrer Einträge verantwortlich. Besitzer können die IDs der AWS Ressourcen anzeigen, die auf die Präfixliste verweisen. Sie können jedoch keine Verweise auf eine Präfixliste in AWS Ressourcen hinzufügen oder entfernen, die Konsumenten gehören.

Besitzer können eine Präfixliste nicht löschen, wenn auf die Präfixliste in einer Ressource verwiesen wird, deren Besitzer ein Konsument ist.

Berechtigungen für Konsumenten

Konsumenten können die Einträge in einer freigegebenen Präfixliste anzeigen und in ihren AWS Ressourcen auf eine freigegebene Präfixliste verweisen. Konsumenten können jedoch eine freigegebene Präfixliste nicht ändern, wiederherstellen oder löschen.

Fakturierung und Messung

Für die Freigabe von Präfixlisten fallen keine zusätzlichen Gebühren an.

Kontingente für AWS RAM

Weitere Informationen finden Sie unter Servicekontingente.

Referenz-Präfix-Listen in Ihren AWS -Ressourcen

Sie können in den folgenden AWS Ressourcen auf eine Präfixliste verweisen.

Ressourcen

- VPC-Sicherheitsgruppen
- Subnetz-Routingtabellen
- Transit-Gateway-Routing-Tabellen
- AWS Network Firewall Regelgruppen
- Netzwerkzugriffkontrolle von Amazon Managed Grafana
- AWS Outposts Lokale -Rack-Gateways

VPC-Sicherheitsgruppen

Sie können eine Präfixliste als Quelle für eine eingehende Regel oder als Ziel für eine ausgehende Regel angeben. Weitere Informationen finden Sie unter Sicherheitsgruppen.

So verweisen Sie mit der Konsole auf eine Präfixliste in einer Sicherheitsgruppenregel:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Security Groups (Sicherheitsgruppen) aus.
3. Wählen Sie die Sicherheitsgruppe aus, die aktualisiert werden soll.
4. Wählen Sie Actions (Aktionen), Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) oder Actions (Aktionen), Edit outbound rules (Regeln für ausgehenden Datenverkehr bearbeiten).
5. Wählen Sie Regel hinzufügen aus. Wählen Sie unter Type (Typ) den Verkehrstyp aus. Wählen Sie für Source (Quelle) (eingehende Regeln) oder Destination (Ziel) (ausgehende Regeln) die ID der Präfixliste aus.
6. Wählen Sie Save rules (Regeln speichern) aus.

So verweisen Sie mit der auf eine Präfixliste in einer Sicherheitsgruppenregel AWS CLI

Verwenden Sie die authorize-security-group-egress Befehle authorize-security-group-ingress und . Geben Sie für den `--ip-permissions`-Parameter die ID der Präfixliste mit `PrefixListIds` an.

Subnetz-Routingtabellen

Sie können eine Präfixliste als Ziel für den Routing-Tabelleneintrag angeben. Sie können nicht auf Präfixliste in einer Gateway-Routing-Tabelle verweisen. Weitere Informationen über die Routing-Tabellen finden Sie unter Konfigurieren von Routing-Tabellen.

So verweisen Sie auf eine Präfixliste in einer Routing-Tabelle mit der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie Actions (Aktionen) und dann Edit routes (Routen bearbeiten).
4. Um eine Route hinzuzufügen, wählen Sie Add route (Route hinzufügen).
5. Geben Sie unter Destination (Ziel) die ID einer Präfixliste ein.
6. Wählen Sie unter Target (Ziel) ein Ziel aus.
7. Wählen Sie Änderungen speichern aus.

So verweisen Sie mit der auf eine Präfixliste in einer Routing-Tabelle AWS CLI

Verwenden Sie den Befehl create-route (AWS CLI). Verwenden Sie den `--destination-prefix-list-id`-Parameter, um die ID einer Präfixliste anzugeben.

Transit-Gateway-Routing-Tabellen

Sie können eine Präfixliste als Ziel für eine Route angeben. Weitere Informationen finden Sie unter Verweise auf Präfixlisten in Amazon VPC Transit Gateways.

AWS Network Firewall Regelgruppen

Eine - AWS Network Firewall Regelgruppe ist ein wiederverwendbarer Satz von Kriterien für die Überprüfung und Handhabung des Netzwerkverkehrs. Wenn Sie Suricata-kompatible statusbehaftete Regelgruppen in erstellen AWS Network Firewall, können Sie auf eine Präfixliste aus der Regelgruppe verweisen. Weitere Informationen finden Sie unter Verweisen auf Amazon-

VPC-Präfixlisten und Erstellen einer zustandsbehafteten Regelgruppe im AWS Network Firewall - Entwicklerhandbuch.

Netzwerkzugriffkontrolle von Amazon Managed Grafana

Sie können eine oder mehrere Präfixlisten als eingehende Regel für Anfragen an Amazon-Managed-Grafana-Workspaces angeben. Weitere Informationen zur Netzwerkzugriffskontrolle für Grafana-Workspaces oder zum Verweis auf Präfixlisten finden Sie unter Verwalten des Netzwerkzugriffs im Amazon-Managed-Grafana-Benutzerhandbuch.

AWS Outposts Lokale -Rack-Gateways

Jedes AWS Outposts Rack bietet ein lokales Gateway, mit dem Sie Ihre Outpost-Ressourcen mit Ihren On-Premises-Netzwerken verbinden können. Sie können CIDRs gruppieren, die Sie häufig in einer Präfixliste verwenden, und diese Liste als Routenziel in Ihrer Routing-Tabelle des lokalen Gateways referenzieren. Weitere Informationen finden Sie unter Verwalten von Routing-Tabellenrouten für lokale Gateways im AWS Outposts Benutzerhandbuch für Racks.

AWS IP-Adressbereiche

AWS veröffentlicht seine aktuellen IP-Adressbereiche im JSON-Format. Anhand dieser Informationen können Sie den Verkehr von identifizieren AWS. Sie können diese Informationen auch verwenden, um den Verkehr zu oder von einigen AWS Diensten zuzulassen oder zu verweigern.

> **Note**
>
> - Nur einige AWS Service-IP-Adressbereiche werden in ip-ranges.json veröffentlicht. Wir veröffentlichen die IP-Adressbereiche für Dienste, für die Kunden häufig Ausgangsfilterung durchführen möchten.
> - Dienste können die IP-Adressbereiche verwenden, um mit anderen Diensten zu kommunizieren, oder Dienste können die IP-Bereiche verwenden, um mit einem Kundennetzwerk zu kommunizieren.

Um die aktuellen Bereiche anzuzeigen, laden Sie die `.json`-Datei herunter. Um einen Verlauf zu pflegen, speichern Sie nachfolgende Versionen der `.json`-Datei in Ihrem System. Um festzustellen, ob seit der letzten Speicherung der Datei Änderungen vorgenommen wurden, prüfen Sie den

Zeitpunkt der letzten Veröffentlichung in der aktuellen Datei und vergleichen Sie ihn mit dem Zeitpunkt der Veröffentlichung in der letzten Datei, die Sie gespeichert haben.

Die IP-Adressbereiche, zu denen Sie AWS über Bring Your Own IP Addresses (BYOIP) gelangen, sind nicht in der `.json` Datei enthalten.

Alternativ veröffentlichen einige Dienste ihre Adressbereiche mithilfe von AWS-verwalteten Präfixlisten. Weitere Informationen finden Sie unter the section called “Verfügbare von AWS verwaltete Präfixlisten”.

Inhalt

Herunterladen

Laden Sie ip-ranges.json herunter.

Wenn Sie auf diese Datei programmgesteuert zugreifen, liegt es in Ihrer Verantwortung sicherzustellen, dass die Anwendung die Datei erst herunterlädt, nachdem das vom Server bereitgestellte TLS-Zertifikat erfolgreich überprüft wurde.

Syntax

Die Syntax von `ip-ranges.json` ist wie folgt:

```
{
  "syncToken": "0123456789",
  "createDate": "yyyy-mm-dd-hh-mm-ss",
  "prefixes": [
    {
      "ip_prefix": "cidr",
```

```
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ],
  "ipv6_prefixes": [
    {
      "ipv6_prefix": "cidr",
      "region": "region",
      "network_border_group": "network_border_group",
      "service": "subset"
    }
  ]
}
```

syncToken

Zeitpunkt der Veröffentlichung (als Zeit seit Unix-Epoche)

Typ: Zeichenfolge

Beispiel: `"syncToken": "1416435608"`

createDate

Datum und Uhrzeit der Veröffentlichung im UTC-Format YY-MM-DD-. hh-mm-ss

Typ: Zeichenfolge

Beispiel: `"createDate": "2014-11-19-23-29-02"`

prefixes

Die IP-Präfixe für die IPv4-Adressbereiche

Typ: Array

ipv6_prefixes

Die IP-Präfixe für die IPv6-Adressbereiche

Typ: Array

ip_prefix

Der öffentliche IPv4-Adressbereich, in CIDR-Notation. Beachten Sie, dass ein Präfix AWS möglicherweise in spezifischeren Bereichen angekündigt wird. Zum Beispiel könnte der Präfix

96.127.0.0/17 in der Datei als 96.127.0.0/21, 96.127.8.0/21, 96.127.32.0/19 und 96.127.64.0/18 angekündigt werden.

Typ: Zeichenfolge

Beispiel: `"ip_prefix": "198.51.100.2/24"`

ipv6_prefix

Der öffentliche IPv6-Adressbereich, in CIDR-Notation. Beachten Sie, dass AWS möglicherweise ein Präfix in spezifischeren Bereichen angekündigt wird.

Typ: Zeichenfolge

Beispiel: `"ipv6_prefix": "2001:db8:1234::/64"`

network_border_group

Der Name der Netzwerkgrenzgruppe, bei der es sich um eine eindeutige Gruppe von Availability Zones oder Local Zones handelt, aus AWS denen IP-Adressen bekannt gegeben werden, oder`GLOBAL`. Der Datenverkehr für `GLOBAL` Dienste kann von mehreren (bis zu allen) Availability Zones oder Local Zones, aus denen IP-Adressen AWS beworben werden, angelockt werden oder von diesen stammen.

Typ: Zeichenfolge

Beispiel: `"network_border_group": "us-west-2-lax-1"`

Region

Die AWS Region oder`GLOBAL`. Der Verkehr für `GLOBAL` Dienstleistungen kann aus mehreren (bis zu allen) AWS Regionen stammen oder aus diesen stammen.

Typ: Zeichenfolge

Zulässige Werte: `af-south-1` | `ap-east-1` | `ap-northeast-1` | `ap-northeast-2` | `ap-northeast-3` | `ap-south-1` | `ap-south-2` | `ap-southeast-1` | `ap-southeast-2` | `ap-southeast-3` | `ap-southeast-4` | `ca-central-1` | `cn-north-1` | `cn-northwest-1` | `eu-central-1` | `eu-central-2` | `eu-north-1` | `eu-south-1` | `eu-south-2` | `eu-west-1` | `eu-west-2` | `eu-west-3` | `me-central-1` | `me-south-1` | `sa-east-1` | `us-east-1` | `us-east-2` | `us-gov-east-1` | `us-gov-west-1` | `us-west-1` | `us-west-2` | `GLOBAL`

Beispiel: `"region": "us-east-1"`

Service nicht zulässig

Die Untergruppe der IP-Adressbereiche. Die aufgelisteten Adressen für `API_GATEWAY` sind nur Egress. Geben Sie `AMAZON` an, um alle IP-Adressbereiche abzurufen (d. h. die jeweiligen Teilmengen sind auch in der `AMAZON`-Teilmenge enthalten). Einige IP-Adressbereiche sind jedoch nur in der `AMAZON`-Teilmenge (d. h. in keiner weiteren Teilmenge) enthalten.

Typ: Zeichenfolge

Gültige Werte: `AMAZON` `AMAZON_APPFLOW` | `AMAZON_CONNECT` | `API_GATEWAY` | `CHIME_MEETINGS` | `CHIME_VOICECONNECTOR` | `CLOUD9` | `CLOUDFRONT` | `CLOUDFRONT_ORIGIN_FACING` | `CODEBUILD` | `DYNAMODB` | `EBS` | `EC2` | `EC2_INSTANCE_CONNECT` | `GLOBALACCELERATOR` | `IVS_REALTIME` | `KINESIS_VIDEO_STREAMS` | `MEDIA_PACKAGE_V2` | `ROUTE53` | `ROUTE53_HEALTHCHECKS` | `ROUTE53_HEALTHCHECKS_PUBLISHING` | `ROUTE53_RESOLVER` | `S3` | `WORKSPACES_GATEWAYS`

Beispiel: `"service": "AMAZON"`

Bereich überschneidet sich

Die von einem Servicecode zurückgegebenen IP-Adressbereiche werden auch vom `AMAZON`-Servicecode zurückgegeben. Zum Beispiel werden alle Adressbereiche, die vom `S3`-Servicecode zurückgegeben werden, auch vom `AMAZON`-Servicecode zurückgegeben.

Wenn Service A Ressourcen von Service B verwendet, gibt es IP-Adressbereiche, die von den Servicecodes für Service A und Service B zurückgegeben werden. Diese IP-Adressbereiche werden jedoch ausschließlich von Service A verwendet und können nicht von Service B genutzt werden. Amazon S3 verwendet beispielsweise Ressourcen von Amazon EC2, daher gibt es IP-Adressbereiche, die vom `S3`- und vom `EC2`-Servicecode zurückgegeben werden. Diese IP-Adressbereiche werden jedoch ausschließlich von Amazon S3 genutzt. Daher gibt der `S3`-Servicecode alle IP-Adressbereiche zurück, die ausschließlich von Amazon S3 verwendet werden. Um die IP-Adressbereiche zu ermitteln, die ausschließlich von Amazon EC2 genutzt werden, suchen Sie nach den IP-Adressbereichen, die vom `EC2`-Servicecode, aber nicht vom `S3`-Servicecode zurückgegeben werden.

Filtern der JSON-Datei

Sie können ein Befehlszeilen-Tool herunterladen, um die Informationen so zu filtern, dass Sie nur die gewünschten Informationen erhalten.

Windows

AWS Tools for Windows PowerShell enthält ein Cmdlet (`Get-AWSPublicIpAddressRange`) für die Analyse dieser JSON-Datei. Die folgenden Beispiele zeigen, wie Sie das Cmdlet verwenden. Weitere Informationen finden Sie unter Abfragen der öffentlichen IP-Adressbereiche für AWS und Get- AWSPublicIpAddressRange.

Example 1. Abrufen des Erstellungsdatums

```
PS C:\> Get-AWSPublicIpAddressRange -OutputPublicationDate

Wednesday, August 22, 2018 9:22:35 PM
```

Example 2. Abrufen der Informationen für eine bestimmte Region

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1

IpPrefix        Region      NetworkBorderGroup         Service
--------        ------       -------                   -------
23.20.0.0/14    us-east-1    us-east-1                 AMAZON
50.16.0.0/15    us-east-1    us-east-1                 AMAZON
50.19.0.0/16    us-east-1    us-east-1                 AMAZON
...
```

Example 3. Abrufen aller IP-Adressen

```
PS C:\> (Get-AWSPublicIpAddressRange).IpPrefix
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
2406:da00:ff00::/64
2600:1fff:6000::/40
2a01:578:3::/64
2600:9000::/28
```

Example 4. Abrufen aller IPv4-Adressen

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv4"} | select
 IpPrefix
```

```
IpPrefix
--------
23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

Example 5. Abrufen aller IPv6-Adressen

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.IpAddressFormat -eq "Ipv6"} | select
 IpPrefix

IpPrefix
--------
2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Example 6. Abrufen aller IP-Adressen für einen bestimmten Service

```
PS C:\> Get-AWSPublicIpAddressRange -ServiceKey CODEBUILD | select IpPrefix

IpPrefix
--------
52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
...
```

Linux

Die folgenden Beispielbefehle verwenden das jq-Tool, um eine lokale Kopie der JSON-Datei zu analysieren.

Example 1. Abrufen des Erstellungsdatums

```
$ jq .createDate < ip-ranges.json

"2016-02-18-17-22-15"
```

Example 2. Abrufen der Informationen für eine bestimmte Region

```
$ jq '.prefixes[] | select(.region=="us-east-1")' < ip-ranges.json

{
  "ip_prefix": "23.20.0.0/14",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.16.0.0/15",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
{
  "ip_prefix": "50.19.0.0/16",
  "region": "us-east-1",
  "network_border_group": "us-east-1",
  "service": "AMAZON"
},
...
```

Example 3. Abrufen aller IPv4-Adressen

```
$ jq -r '.prefixes | .[].ip_prefix' < ip-ranges.json

23.20.0.0/14
27.0.0.0/22
43.250.192.0/24
...
```

Example 4. Abrufen aller IPv6-Adressen

```
$ jq -r '.ipv6_prefixes | .[].ipv6_prefix' < ip-ranges.json

2a05:d07c:2000::/40
2a05:d000:8000::/40
2406:dafe:2000::/40
...
```

Example 5. Abrufen aller IPv4-Adressen für einen bestimmten Service

```
$ jq -r '.prefixes[] | select(.service=="CODEBUILD") | .ip_prefix' < ip-ranges.json

52.47.73.72/29
13.55.255.216/29
52.15.247.208/29
...
```

Example 6. Abrufen aller IPv4-Adressen für einen bestimmten Service in einer bestimmten Region

```
$ jq -r '.prefixes[] | select(.region=="us-east-1") | select(.service=="CODEBUILD")
 | .ip_prefix' < ip-ranges.json

34.228.4.208/28
```

Example 7. Abrufen von Informationen für eine bestimmte Netzwerkgrenzgruppe

```
$ jq -r '.prefixes[] | select(.region=="us-west-2") |
 select(.network_border_group=="us-west-2-lax-1") | .ip_prefix' < ip-ranges.json
70.224.192.0/18
52.95.230.0/24
15.253.0.0/16
...
```

Implementieren der Kontrolle ausgehenden Datenverkehrs

Damit Ressourcen, die Sie mit einem AWS Dienst erstellt haben, nur auf andere AWS Dienste zugreifen können, können Sie die IP-Adressbereichsinformationen in der Datei ip-ranges.json verwenden, um eine Ausgangsfilterung durchzuführen. Stellen Sie sicher, dass die Sicherheitsgruppenregeln ausgehenden Datenverkehr zu den CIDR-Blöcken in der AMAZON-Liste zulassen. Es gibt Quotas für Sicherheitsgruppen. Abhängig von der Anzahl der IP-Adressbereiche in jeder Region benötigen Sie möglicherweise mehrere Sicherheitsgruppen pro Region.

> **Note**
>
> Einige AWS Dienste basieren auf EC2 und verwenden den EC2-IP-Adressraum. Wenn Sie den Verkehr zur EC2-IP-Adressumgebung blockieren, blockieren Sie auch den Verkehr zu diesen Nicht-EC2-Diensten.

AWS Benachrichtigungen über IP-Adressbereiche

Immer wenn sich die AWS IP-Adressbereiche ändern, senden wir Benachrichtigungen an Abonnenten des `AmazonIpSpaceChanged` Themas. Die Nutzlast enthält Informationen im folgenden Format:

```
{
  "create-time":"yyyy-mm-ddThh:mm:ss+00:00",
  "synctoken":"0123456789",
  "md5":"6a45316e8bc9463c9e926d5d37836d33",
  "url":"https://ip-ranges.amazonaws.com/ip-ranges.json"
}
```

create-time

Datum und Zeitpunkt der Erstellung

Es kann vorkommen, dass Benachrichtigungen nicht in der richtigen Reihenfolge versandt werden. Daher wird empfohlen, die Zeitstempel zu überprüfen, um für die richtige Reihenfolge zu sorgen.

synctoken

Zeitpunkt der Veröffentlichung (als Zeit seit Unix-Epoche)

md5

Der kryptografische Hash-Wert der Datei `ip-ranges.json`. Sie können diesen Wert verwenden, um zu überprüfen, ob die heruntergeladene Datei beschädigt ist.

URL

Der Speicherort der Datei `ip-ranges.json`

Wenn Sie bei jeder Änderung der AWS IP-Adressbereiche benachrichtigt werden möchten, können Sie den Empfang von Benachrichtigungen über Amazon SNS wie folgt abonnieren.

Um Benachrichtigungen über den AWS IP-Adressbereich zu abonnieren

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. Kopieren Sie für Topic ARN den folgenden Amazon-Ressourcennamen (ARN):

   ```
   arn:aws:sns:us-east-1:806199016981:AmazonIpSpaceChanged
   ```

   b. Wählen Sie für Protocol das zu verwendende Protokoll aus (z. B. `Email`).

   c. Geben Sie für den Endpoint den Endpunkt ein, an den die Benachrichtigung zugestellt werden soll (z. B. Ihre E-Mail-Adresse).

   d. Wählen Sie Create subscription (Abonnement erstellen) aus.
6. Sie werden über den angegebenen Endpunkt kontaktiert und gebeten, Ihr Abonnement zu bestätigen. Wenn Sie beispielsweise eine E-Mail-Adresse angegeben haben, erhalten Sie eine E-Mail-Nachricht mit der Betreffzeile `AWS Notification - Subscription Confirmation`. Befolgen Sie die Anweisungen, um Ihr Abonnement zu bestätigen.

Benachrichtigungen hängen von der Verfügbarkeit des Endpunkts ab. Aus diesem Grund sollten Sie die JSON-Datei regelmäßig überprüfen, um sicherzustellen, dass Sie über die neuesten Bereiche verfügen. Weitere Informationen zur Zuverlässigkeit von Amazon SNS erhalten Sie unter https://aws.amazon.com/sns/faqs/#Reliability.

Wenn Sie diese Benachrichtigungen nicht mehr erhalten möchten, führen Sie die folgenden Schritte aus, um sich abzumelden.

Um Benachrichtigungen über AWS IP-Adressbereiche abzubestellen

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.
4. Wählen Sie Actions und dann Delete subscriptions.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Weitere Informationen zu Amazon SNS finden Sie im Amazon-Simple-Notification-Service-Entwicklerhandbuch.

Versionshinweise

Die folgende Tabelle beschreibt Aktualisierungen der Syntax von `ip-ranges.json`. Wir fügen außerdem neue Regionscodes bei jedem Regionsstart hinzu.

Beschreibung	Datum der Veröffentlichung
Der `IVS_REALTIME` -Servicecode wurde hinzugefügt.	11. Juni 2024
Der `MEDIA_PACKAGE_V2` -Servicecode wurde hinzugefügt.	9. Mai 2023
Der `CLOUDFRONT_ORIGIN_FACING` -Servicecode wurde hinzugefügt.	12. Oktober 2021
Der `ROUTE53_RESOLVER` -Servicecode wurde hinzugefügt.	24. Juni 2021
Der `EBS`-Servicecode wurde hinzugefügt.	12. Mai 2021
Der `KINESIS_VIDEO_STREAMS` -Servicecode wurde hinzugefügt.	19. November 2020
Die `CHIME_MEETINGS` - und `CHIME_VOICECONNECTOR` -Dienstcodes und wurden hinzugefügt.	19. Juni 2020
Der `AMAZON_APPFLOW` -Servicecode wurde hinzugefügt.	9. Juni 2020
Fügen Sie Unterstützung für die Netzwerkgrenzgruppe hinzu.	7. April 2020
Der `WORKSPACES_GATEWAYS` -Servicecode wurde hinzugefügt.	30. März 2020

Beschreibung	Datum der Veröffentlichung
Der ROUTE53_HEALTHCHECK_PUBLISHING -Servicecode wurde hinzugefügt.	30. Januar 2020
Der API_GATEWAY -Servicecode wurde hinzugefügt.	26. September 2019
Der EC2_INSTANCE_CONNECT -Servicecode wurde hinzugefügt.	26. Juni 2019
Der DYNAMODB-Servicecode wurde hinzugefügt.	25. April 2019
Der GLOBALACCELERATOR -Servicecode wurde hinzugefügt.	20. Dezember 2018
Der AMAZON_CONNECT -Servicecode wurde hinzugefügt.	20. Juni 2018
Der CLOUD9-Servicecode wurde hinzugefügt.	20. Juni 2018
Der CODEBUILD -Servicecode wurde hinzugefügt.	19. April 2018
Der S3-Servicecode wurde hinzugefügt.	28. Februar 2017
Unterstützung für IPv6-Adressbereiche hinzugefügt.	22. August 2016
Erstversion	19. November 2014

Weitere Informationen

- AMAZON_APPFLOW – IP-Adressbereiche
- AMAZON_CONNECT – Einrichten Ihres Netzwerks
- CHIME_MEETINGS – Konfiguration für Medien und Signalisierung
- CLOUDFRONT— Standorte und IP-Adressbereiche von CloudFront Edge-Servern

- `DYNAMODB` – IP-Adressbereiche
- `EC2` – Öffentliche IPv4-Adressen
- `EC2_INSTANCE_CONNECT` – Voraussetzungen für EC2 Instance Connect
- `GLOBALACCELERATOR` – Standort und IP-Adressbereiche von Global-Accelerator-Edge-Servern
- `ROUTE53` – IP-Adressbereiche von Amazon-Route-53-Servern
- `ROUTE53_HEALTHCHECKS` – IP-Adressbereiche von Amazon-Route-53-Servern
- `ROUTE53_HEALTHCHECKS_PUBLISHING` – IP-Adressbereiche von Amazon-Route-53-Servern
- `WORKSPACES_GATEWAYS` – PCoIP-Gatewayserver

Fügen Sie Ihrer VPC IPv6-Unterstützung hinzu

Wenn Sie über eine bestehende VPC verfügen, die nur IPv4 unterstützt, und über Ressourcen in Ihrem Subnetz, die nur für die Verwendung von IPv4 konfiguriert sind, können Sie IPv6-Unterstützung für Ihre VPC und Ressourcen hinzufügen. Ihre VPC kann im Dual-Stack-Modus betrieben werden: Ihre Ressourcen können über IPv4, über IPv6 oder über beide kommunizieren. Die IPv4- und IPv6-Kommunikation sind voneinander unabhängig.

Sie können die IPv4-Unterstützung für Ihre VPC und die Subnetze deaktivieren (das standardmäßige IP-Adresssystem für Amazon VPC und Amazon EC2).

Überlegungen

- Derzeit gibt es keinen Migrationspfad von Nur-IPv4-Subnetzen zu Nur-IPv6-Subnetzen.
- In diesem Beispiel wird davon ausgegangen, dass Sie über eine vorhandene VPC mit öffentlichen und privaten Subnetzen verfügen. Weitere Informationen zum Erstellen einer VPC zur Verwendung mit IPv6 finden Sie unter the section called “Erstellen einer VPC”.
- Bevor Sie mit der Verwendung von IPv6 beginnen, stellen Sie sicher, dass Sie die Funktionen der IPv6-Adressierung für Amazon VPC gelesen haben:. Vergleich von IPv4 und IPv6

Prozess

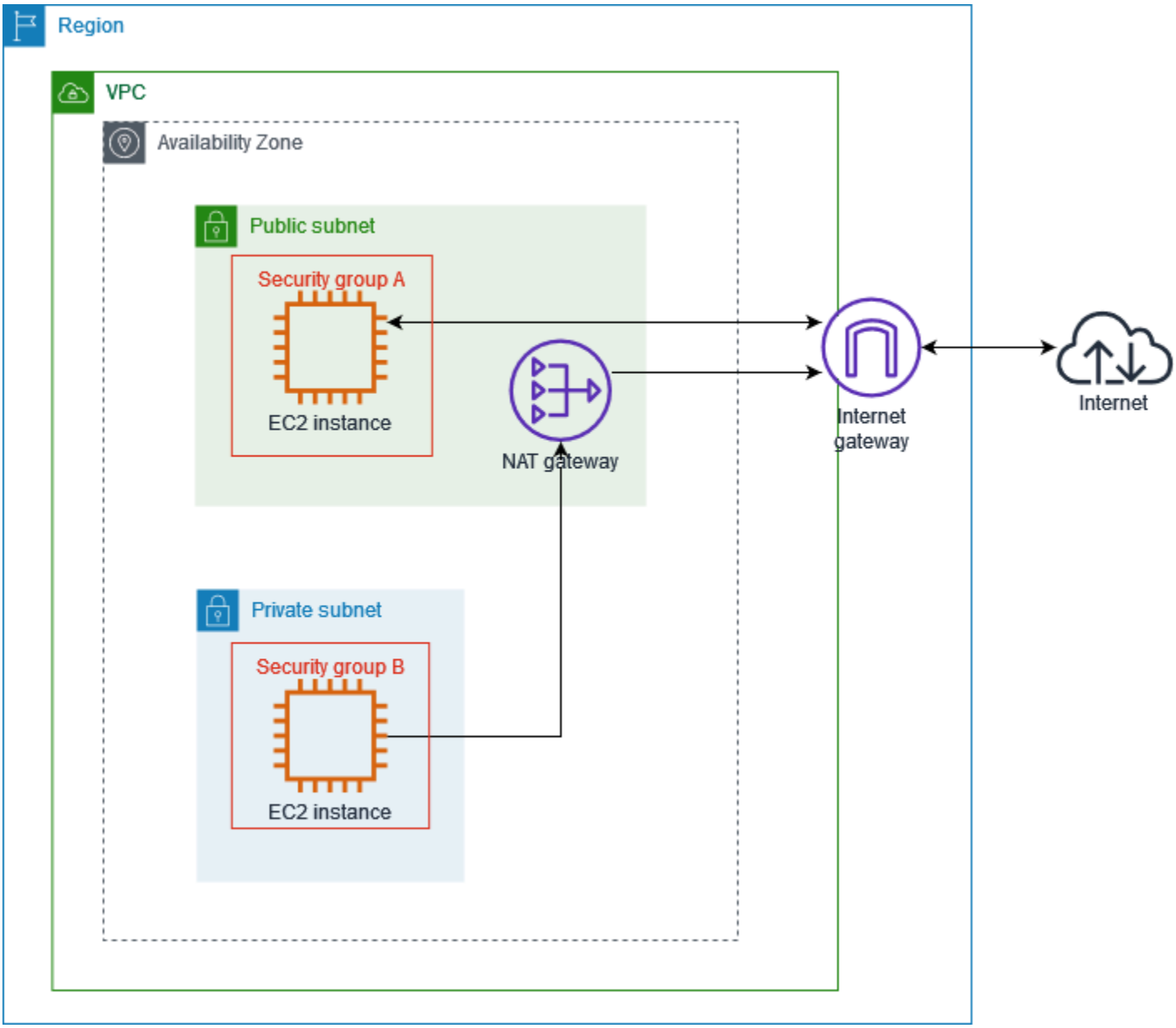
Die folgende Tabelle bietet eine Übersicht des Ablaufs zum Aktivieren von IPv6 für Ihre VPC.

Schritt	Hinweise
Schritt 1: Ordnen Sie Ihrer VPC und den Subnetzen einen IPv6-CIDR-Block zu.	Ordnen Sie einen von Amazon bereitgestellten oder einen eigenen IPv6-CIDR-Block Ihrer VPC und Ihren Subnetzen zu.
Schritt 2: Aktualisieren Sie Ihre Routing-Tabellen.	Aktualisieren Sie Ihre Routing-Tabellen für das Routen von IPv6-Datenverkehr. Erstellen Sie für ein öffentliches Subnetz eine Route, die den gesamten IPv6-Datenverkehr vom Subnetz an das Internet-Gateway routet. Erstellen Sie für ein privates Subnetz eine Route, die den gesamten IPv6-Datenverkehr aus dem Subnetz an ein Internet-Gateway für ausgehenden Datenverkehr routet.
Schritt 3: Aktualisieren Sie Ihre Sicherheitsgruppenregeln.	Fügen Sie Ihren Sicherheitsgruppenregeln Regeln für IPv6-Adressen hinzu. So sorgen Sie für die Übertragung von IPv6-Datenverkehr von und zu Ihren Instances. Wenn Sie angepasste Netzwerk-ACL-Regeln zur Steuerung der Übertragung von Datenverkehr von und zu Ihrem Subnetz erstellt haben, müssen Sie entsprechende Regeln für IPv6-Datenverkehr einfügen.
Schritt 4: Ihren Instances IPv6-Adressen zuweisen	Weisen Sie aus dem IPv6-Adressbereich Ihres Subnetzes IPv6-Adressen zu Ihren Instances zu.

Beispiel: Aktivieren von IPv6 in einer VPC mit einem öffentlichen und privaten Subnetz

In diesem Beispiel hat Ihre VPC ein öffentliches und ein privates Subnetz. Sie haben eine Datenbank-Instance in Ihrem privaten Subnetz, für das die ausgehende Kommunikation mit dem Internet über ein NAT-Gateway in Ihrer VPC läuft. Sie haben in Ihrem öffentlichen Subnetz mit Internetzugriff über das

Internet-Gateway einen öffentlich erreichbaren Webserver. Das folgende Diagramm zeigt die VPC-Architektur.



Die Sicherheitsgruppe für Ihren Webserver (z. B. mit der Sicherheitsgruppen-ID `sg-11aa22bb11aa22bb1`) hat die folgenden Zugangsregeln:

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Kommentar
Gesamter Datenverkehr	Alle	Alle	sg-33cc44 dd33cc44dd3	Lässt den eingehend

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Kommentar
				en Zugriff für den gesamten Datenverkehr von Instances in Verbindung mit sg-33cc44 dd33cc44dd3 (der Datenbank-Instance) zu.
HTTP	TCP	80	0.0.0.0/0	Lässt eingehend en Datenverkehr aus dem Internet über HTTP zu.
HTTPS	TCP	443	0.0.0.0/0	Lässt eingehend en Datenverkehr aus dem Internet über HTTPS zu.
SSH	TCP	22	203.0.113 .123/32	Lässt eingehend en SSH-Zugriff von Ihrem lokalen Computer zu (z. B., wenn Sie sich mit der Instance verbinden müssen, um administrative Aufgaben durchzuführen).

Die Sicherheitsgruppe für Ihre Datenbank-Instance (z. B. mit der Sicherheitsgruppen-ID `sg-33cc44dd33cc44dd3`) hat die folgende Zugangsregeln:

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Kommentar
MySQL	TCP	3306	sg-11aa22 bb11aa22bb1	Lässt den eingehend en Zugriff für MySQL-Dat enverkehr von Instances in Verbindung mit sg-11aa22 bb11aa22bb1 (der Webserver-Instance) zu.

Beide Sicherheitsgruppen haben eine standardmäßige ausgehende Regel, die sämtlichen ausgehenden IPv4-Datenverkehr zulässt. Es gibt keine weiteren ausgehenden Regeln.

Ihr Webserver ist vom Instance-Typ `t2.medium`. Ihr Datenbankserver hat den Instance-Typ `m3.large`.

Sie möchten, dass Ihre VPC und die Ressourcen IPv6 nutzen. Sie möchten ferner, dass sie im Dual-Stack-Modus arbeiten (sie sollen also zwischen den Ressourcen in Ihrer VPC und Ressourcen im Internet IPv6 und IPv4 verwenden).

Schritt 1: Ordnen Sie Ihrer VPC und den Subnetzen einen IPv6-CIDR-Block zu.

Sie können Ihrer VPC einen IPv6 CIDR-Block zuweisen. Dann ordnen Sie jedem Subnetz einen `/64` CIDR-Block aus dem Bereich zu.

So ordnen Sie einen IPv6 CIDR-Block zu einer VPC zu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs.

3. Wählen Sie Ihre VPC aus.
4. Wählen Sie Aktionen, CIDRs bearbeiten und dann Neuen IPv6-CIDR hinzufügen.
5. Wählen Sie eine der folgenden Optionen und klicken Sie dann auf CIDR auswählen:

   - Von Amazon bereitgestellter IPv6-CIDR-Block: Verwendet einen IPv6-CIDR-Block aus dem IPv6-Adresspool von Amazon. Wählen Sie für Network Border Group die Gruppe aus, aus der IP-Adressen AWS beworben werden.
   - IPAM-zugewiesener IPv6-CIDR-Block – Weist einen IPv6-CIDR-Block aus einem IPAM-Pool zu. Wählen Sie den IPAM-Pool und den IPv6-CIDR-Block.
   - Mein IPv6-CIDR – Weist einen IPv6-CIDR-Block aus Ihrem IPv6-Adresspool (BYOIP) zu. Wählen Sie den IPv6-Adresspool und den IPv6-CIDR-Block.
6. Klicken Sie auf Schließen.

So ordnen Sie einen IPv6 CIDR-Block zu einem Subnetz zu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Wählen Sie ein Subnetz aus.
4. Wählen Sie Aktionen, IPv6-CIDRs bearbeiten und dann IPv6-CIDR hinzufügen.
5. Bearbeiten Sie den CIDR-Block nach Bedarf (ersetzen Sie z. B. den `00`).
6. Wählen Sie Speichern.
7. Wiederholen Sie diesen Vorgang für alle anderen Subnetze in Ihrer VPC.

Weitere Informationen finden Sie unter IPv6-VPC-CIDR-Blöcke.

Schritt 2: Aktualisieren Sie Ihre Routing-Tabellen.

Wenn Sie Ihrer VPC einen IPv6-CIDR-Block zuordnen, fügen wir automatisch eine lokale Route zu jeder Routing-Tabelle für die VPC hinzu, die IPv6-Datenverkehr innerhalb der VPC zulassen.

Für Ihre öffentlichen Subnetze müssen Sie die Routing-Tabellen aktualisieren, damit Instances (wie Webserver) das Internet-Gateway für IPv6-Datenverkehr nutzen können. Für Ihre privaten Subnetze müssen Sie die Routing-Tabellen aktualisieren, damit Instances (wie Datenbank-Instances) ein Internet-Gateway für ausgehenden Verkehr für IPv6-Datenverkehr nutzen können, da NAT-Gateways IPv6 nicht unterstützen.

So aktualisieren Sie die Routing-Tabelle für ein öffentliches Subnetz

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. Wählen Sie das öffentliche Subnetz aus. Wählen Sie auf der Registerkarte Routing-Tabelle die Routing-Tabellen-ID aus, um die Detailseite für die Routing-Tabelle zu öffnen.
3. Wählen Sie die -Routing-Tabelle aus. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten).
4. Wählen Sie Add Route (Route hinzufügen) aus. Wählen Sie `::/0` als Ziel. Wählen Sie die ID für das Internet-Gateway als Ziel aus.
5. Wählen Sie Änderungen speichern aus.

So aktualisieren Sie die Routing-Tabelle für ein privates Subnetz

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Internet-Gateways für ausgehenden Datenverkehr. Klicken Sie auf Internet-Gateway für ausgehenden Datenverkehr erstellen. Wählen Sie Ihre VPC aus VPC und dann Internet-Gateway für ausgehenden Datenverkehr erstellen aus.

   Weitere Informationen finden Sie unter Aktivieren von ausgehendem IPv6-Datenverkehr mit einem Internet-Gateway, das nur ausgehenden Verkehr zulässt.
3. Wählen Sie im Navigationsbereich Subnetze aus. Wählen Sie das private Subnetz aus. Wählen Sie auf der Registerkarte Routing-Tabelle die Routing-Tabellen-ID aus, um die Detailseite für die Routing-Tabelle zu öffnen.
4. Wählen Sie die -Routing-Tabelle aus. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten).
5. Wählen Sie Add Route (Route hinzufügen) aus. Wählen Sie `::/0` als Ziel. Wählen Sie die ID Internet-Gateways für ausgehenden Datenverkehr als Ziel.
6. Wählen Sie Änderungen speichern aus.

Weitere Informationen finden Sie unter Beispiele für Routing-Optionen.

Schritt 3: Aktualisieren Sie Ihre Sicherheitsgruppenregeln.

Damit Ihre Instances Datenverkehr über IPv6 senden und empfangen können, müssen Sie Ihre Sicherheitsgruppenregeln aktualisieren und Regeln für IPv6-Adressen hinzufügen. Im obigen

Beispiel können Sie beispielsweise die Webserver-Sicherheitsgruppe (`sg-11aa22bb11aa22bb1`) aktualisieren, um Regeln hinzuzufügen, die eingehenden HTTP-, HTTPS- und SSH-Zugriff von IPv6-Adressen erlauben. Sie müssen für Ihre Datenbank-Sicherheitsgruppe keine Änderungen an den eingehenden Regeln vornehmen. Die Regel lässt die gesamte eingehende Kommunikation von `sg-11aa22bb11aa22bb1` zu. Dies schließt auch die IPv6-Kommunikation mit ein.

So aktualisieren Sie Ihre Regeln der Sicherheitsgruppe für eingehenden Datenverkehr

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen und anschließend die Webserver-Sicherheitsgruppe aus.
3. Wählen Sie auf der Registerkarte Regeln für eingehenden Datenverkehr die Option Regeln für eingehenden Datenverkehr bearbeiten.
4. Wählen Sie für jede Regel, die IPv4-Verkehr zulässt, die Option Regel hinzufügen aus und konfigurieren Sie die Regel so, dass der entsprechende IPv6-Verkehr zugelassen wird. Um beispielsweise eine Regel hinzuzufügen, die den gesamten HTTP-Verkehr über IPv6 erlaubt, wählen Sie als Typ HTTP und `::/0` als Quelle.
5. Wenn Sie mit dem Hinzufügen der Tags fertig sind, wählen Sie Regeln speichern.

So aktualisieren Sie Ihre Regeln der Sicherheitsgruppe für ausgehenden Datenverkehr

Wenn Sie einen IPv6-CIDR-Block mit Ihrer VPC verknüpfen, fügen wir automatisch eine Regel zu den Sicherheitsgruppen für ausgehenden Datenverkehr zu der VPC hinzu, die den gesamten IPv6-Datenverkehr zulässt. Wenn Sie die ursprünglichen Regeln für den ausgehenden Datenverkehr für Ihre Sicherheitsgruppe jedoch verändert haben, wird die Regel nicht automatisch hinzugefügt. In diesem Fall müssen Sie entsprechende ausgehende Regeln für den IPv6-Datenverkehr hinzufügen.

Aktualisieren Ihrer Netzwerk-ACL-Regeln

Wenn Sie einer VPC einen IPv6 CIDR-Block zuweisen und die standardmäßigen Regeln nicht verändert haben, fügen wir automatisch Regeln zur standardmäßigen Netzwerk-ACL hinzu, die IPv6-Datenverkehr zulässt. Wenn Sie jedoch Ihre standardmäßige Netzwerk-ACL geändert haben oder eine angepasste Netzwerk-ACL erstellt haben, müssen Sie manuell Regeln für den IPv6-Datenverkehr hinzufügen. Weitere Informationen finden Sie unter Arbeiten mit Netzwerk-ACLs.

Schritt 4: Ihren Instances IPv6-Adressen zuweisen

Alle Instance-Typen der aktuellen Generation unterstützen IPv6. Wenn Ihr Instance-Typ IPv6 nicht unterstützt, müssen Sie den Instance-Typ auf einen unterstützten Instance-Typ skalieren, bevor Sie eine IPv6-Adresse zuweisen können. Welches Verfahren Sie verwenden werden, hängt davon ab, ob der von Ihnen gewählte neue Instance-Typ mit dem aktuellen Instance-Typ kompatibel ist. Weitere Informationen finden Sie unter Ändern des Instance-Typs im Amazon EC2 EC2-Benutzerhandbuch. Wenn Sie eine Instance aus einem neuen AMI starten müssen, um IPv6 zu unterstützen, können Sie Ihrer Instance beim Start eine IPv6-Adresse zuweisen.

Nachdem Sie überprüft haben, ob Ihr Instance-Typ IPv6 unterstützt, können Sie über die Amazon EC2-Konsole IPv6-Adressen zu Ihrer Instance zuweisen. Die IPv6-Adresse wird zur primären Netzwerkschnittstelle (eth0) der Instance zugewiesen. Weitere Informationen finden Sie unter Zuweisen einer IPv6-Adresse zu einer Instance im Amazon EC2 EC2-Benutzerhandbuch.

Sie können über ihre IPv6-Adresse eine Verbindung zu einer Instance herstellen. Weitere Informationen finden Sie unter Connect zu Ihrer Linux-Instance mithilfe eines SSH-Clients im Amazon EC2 EC2-Benutzerhandbuch oder Herstellen einer Verbindung zu einer Windows-Instance mithilfe ihrer IPv6-Adresse im Amazon EC2 EC2-Benutzerhandbuch.

Wenn Sie Ihre Instance mit einem AMI für eine aktuelle Version Ihres Betriebssystems gestartet haben, ist Ihre Instance für IPv6 konfiguriert. Wenn Sie eine IPv6-Adresse von Ihrer Instance aus nicht anpingen können, finden Sie Informationen zur Konfiguration von IPv6 in der Dokumentation zu Ihrem Betriebssystem.

AWS Dienste, die IPv6 unterstützen

Computer und Smart-Geräte verwenden IP-Adressen, um über das Internet und andere Netzwerke miteinander zu kommunizieren. Mit dem weiteren Wachstum des Internets steigt auch der Bedarf an IP-Adressen. Das gebräuchlichste Format für IP-Adressen ist IPv4. Das neue Format für IP-Adressen ist IPv6, das einen größeren Adressraum als IPv4 bietet.

AWS-Services Die Unterstützung für IPv6 umfasst die Unterstützung von Dual-Stack-Konfigurationen (IPv4 und IPv6) oder reinen IPv6-Konfigurationen. Eine Virtual Private Cloud (VPC) ist beispielsweise ein logisch isolierter Bereich, AWS Cloud in dem Sie Ressourcen starten AWS können. Innerhalb einer VPC können Sie Subnetze erstellen, die nur IPv4, Dual-Stack oder nur IPv6 sind.

AWS-Services unterstützt den Zugriff über öffentliche Endpunkte. Einige unterstützen AWS-Services auch den Zugriff über private Endpunkte, die von betrieben werden. AWS PrivateLink AWS-

Services können IPv6 über ihre privaten Endpunkte unterstützen, auch wenn sie IPv6 nicht über ihre öffentlichen Endpunkte unterstützen. Endpunkte, die IPv6 unterstützen, können auf DNS-Abfragen mit AAAA-Datensätzen antworten.

Services, die IPv6 unterstützen

In der folgenden Tabelle sind diejenigen aufgeführt AWS-Services , die Dual-Stack-Unterstützung, nur IPv6-Unterstützung und Endpunkte bieten, die IPv6 unterstützen. Wir werden diese Tabelle aktualisieren, sobald weitere Services IPv6-Unterstützung bekommen. Weitere Informationen zur Unterstützung von IPv6 durch einen Service finden Sie in der Dokumentation des Service.

Service-Name	Unterstützung von Dual-Stack	Unterstützung ausschließlich von IPv6	Öffentliche Endpunkte unterstützen IPv6	Private Endgeräte unterstützen IPv6 1
AWS App Mesh	Ja	Ja	Ja	Nein
Amazon AppStream 2.0	Ja	Nein	Nein	Nein
Amazon Athena	Ja	Nein	Ja	Ja
Amazon Aurora	Ja	Nein	Ja	Nein

Service-Name	Unterstützung von Dual-Stack	Unterstützung ausschließlich von IPv6	Öffentliche Endpunkte unterstützen IPv6	Private Endgeräte unterstützen IPv6 1
AWS Cloud9	 Ja	 Nein	 Ja	
Amazon CloudFront	 Ja	 Nein	 Nein	
CloudWatch Amazon-Protokolle	 Ja	 Nein	 Ja	 Nein
AWS Cloud Map	 Ja	 Ja	 Ja	 Ja
AWS Cloud-WAN	 Ja	 Nein	 Ja	 Nein
Amazon Cognito	 Ja	 Nein	 Ja	

Service-Name	Unterstützung von Dual-Stack	Unterstützung ausschließlich von IPv6	Öffentliche Endpunkte unterstützen IPv6	Private Endgeräte unterstützen IPv6 1
AWS Database Migration Service	 Ja	 Nein	 Nein	 Nein
AWS Direct Connect	 Ja	 Ja	 Nein	
Amazon EC2	 Ja	 Ja	 Ja	 Nein
Amazon ECS	 Ja	 Nein	 Nein	 Nein
Amazon EKS	Knoten: Ja// Pods: Nein	Pods: Ja// Nodes: Nein	 Nein	 Nein
Elastic Load Balancing	Load Balancer: Ja Zielgruppen: Nein	Load Balancer: Nein Zielgruppen: Ja	 Nein	 Nein

Service-Name	Unterstützung von Dual-Stack	Unterstützung ausschließlich von IPv6	Öffentliche Endpunkte unterstützen IPv6	Private Endgeräte unterstützen IPv6 1
Amazon ElastiCache	 Ja	 Ja	 Nein	 Nein
AWS Fargate	 Ja	 Nein	 Nein	 Nein
AWS Global Accelerator	 Ja	 Nein	 Nein	
AWS Glue	 Nein	 Nein	 Nein	 Ja
AWS IoT	 Ja	 Nein	 Ja	 Nein
AWS Lake Formation	 Nein	 Nein	 Nein	 Ja

Service-Name	Unterstützung von Dual-Stack	Unterstützung ausschließlich von IPv6	Öffentliche Endpunkte unterstützen IPv6	Private Endgeräte unterstützen IPv6 1
AWS Lambda	 Ja	 Nein	 Ja	 Nein
Amazon Lightsail	 Ja	 Ja	 Nein	
AWS Network Firewall	 Ja	 Ja	 Nein	
OpenSearch Amazon-Dienst	 Ja	 Nein	 Ja	 Nein
AWS PrivateLink	 Ja	 Ja	 Ja	
Amazon RDS	 Ja	 Nein	 Ja	 Nein

Service-Name	Unterstützung von Dual-Stack	Unterstützung ausschließlich von IPv6	Öffentliche Endpunkte unterstützen IPv6	Private Endgeräte unterstützen IPv6 1
Amazon Route 53	 Ja	 Ja	 Nein	
Amazon S3	 Ja	 Nein	 Ja	 Nein
AWS Secrets Manager	 Ja	 Nein	 Ja	 Nein
AWS Shield	 Ja	 Ja	 Nein	
AWS Site-to-Site VPN	 Ja	 Nein	 Ja	 Nein
AWS Transit Gateway	 Ja	 Nein	 Ja	 Nein

Service-Name	Unterstützung von Dual-Stack	Unterstützung ausschließlich von IPv6	Öffentliche Endpunkte unterstützen IPv6	Private Endgeräte unterstützen IPv6 [1]
Amazon VPC	 Ja	 Ja	 Ja	 Nein
AWS WAF	 Ja	 Ja	 Nein	
Amazon WorkSpaces	 Ja	 Nein	 Nein	 Nein

[1] Eine leere Zelle bedeutet, dass der Service nicht integriert AWS PrivateLink werden kann.

Zusätzliche Unterstützung von IPv6

Datenverarbeitung

- Amazon EC2 unterstützt das Starten von Instances, die auf dem Nitro-System basieren, in reinen IPv6-Subnetzen.
- Amazon EC2 bietet IPv6-Endpunkte für Instance Metadata Service (IMDS) und Amazon Time Sync Service.

Netzwerk und Bereitstellung von Inhalten

- Amazon VPC unterstützt die Erstellung von reinen IPv6-Subnetzen.
- Amazon VPC unterstützt IPv6-Ressourcen bei der Kommunikation mit AWS IPv4-Ressourcen, indem es DNS64 in Ihren Subnetzen und NAT64 auf Ihren NAT-Gateways unterstützt.

Sicherheit, Identität und Compliance

- AWS Identity and Access Management (IAM) unterstützt IPv6-Adressen in IAM-Richtlinien.
- Amazon Macie unterstützt IPv6-Adressen in persönlich identifizierbaren Informationen (PII).

Verwaltung und Governance

- AWS CloudTrail Datensätze enthalten IPv6-Quellinformationen.
- AWS CLI v2 unterstützt das Herunterladen über IPv6-Verbindungen für reine IPv6-Clients.

Weitere Informationen

- IPv6 auf AWS
- Dual-Stack- und IPv6-only-Amazon-VPC-Referenzarchitekturen (PDF)

Virtual Private Cloudc (VPCs)

Eine Virtual Private Cloud (VPC – virtuelle private Cloud) ist ein virtuelles Netzwerk für Ihren AWS-Konto. Es ist von anderen virtuellen Netzwerken in der AWS Cloud getrennt. Sie können Ihre AWS-Ressourcen, z. B. Amazon-EC2-Instances, in Ihrer VPC starten.

Ihr Konto enthält eine Standard-VPC für jede AWS-Region. Sie können auch zusätzliche VPCs erstellen.

Inhalt

VPC-Grundlagen

Eine VPC umfasst alle Availability Zones einer Region. Nach dem Erstellen einer VPC können Sie in jeder Availability Zone einzelne oder mehrere Subnetze hinzufügen. Weitere Informationen finden Sie unter Subnetze.

Inhalt

IP-Adressbereich der VPC

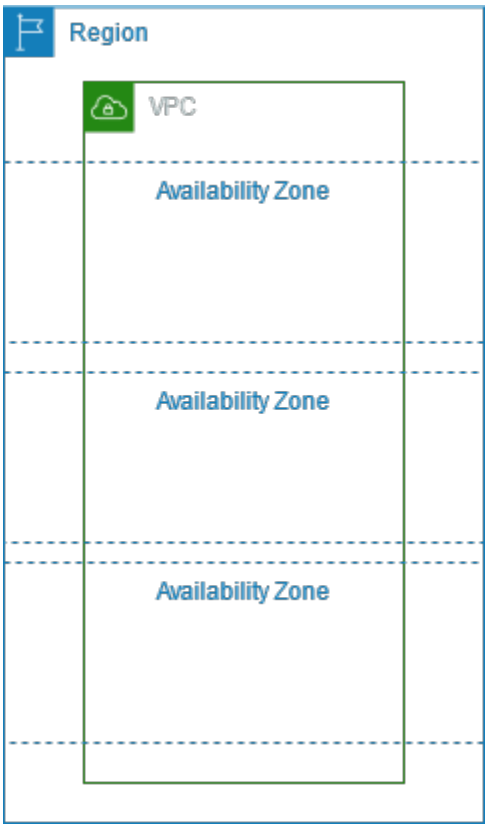
Wenn Sie eine VPC erstellen, legen Sie die IP-Adressen wie folgt fest:

- Nur IPv4 – Das Subnetz besitzt einen IPv4-CIDR-Block, besitzt jedoch keinen IPv6-CIDR-Block.
- Dual-Stack – Das Subnetz besitzt sowohl einen IPv4-CIDR-Block als auch einen IPv6-CIDR-Block.

Weitere Informationen finden Sie unter IP-Adressierung für Ihre VPCs und Subnetze.

VPC-Diagramm

Im folgenden Diagramm ist eine VPC ohne zusätzliche VPC-Ressourcen dargestellt. Beispielkonfigurationen finden Sie unter Beispiele.



VPC-Ressourcen

Jede VPC enthält automatisch die folgenden Ressourcen:

- Standardmäßiger DHCP-Optionssatz
- Standardnetzwerk-ACL

- Standardsicherheitsgruppen
- Haupt-Routing-Tabelle

Sie können die folgenden Ressourcen für Ihre VPC erstellen:

- Netzwerk-ACLs
- Benutzerdefinierte Routing-Tabellen
- Sicherheitsgruppen
- Internet-Gateway
- NAT-Gateways

Standard-VPCs

Wenn Sie beginnen Amazon VPC zu verwenden, verfügen Sie bereits über eine Standard-VPC in jeder AWS-Region: Eine Standard-VPC umfasst ein öffentliches Subnetz in jeder Availability Zone, ein Internet-Gateway und Einstellungen zum Aktivieren der DNS-Auflösung. Daher können Sie umgehend Amazon-EC2-Instances in einer Standard-VPC starten. Sie können auch Services wie Elastic Load Balancing, Amazon RDS und Amazon EMR in Ihrer Standard-VPC verwenden.

Eine Standard-VPC hilft, schnell mit der Arbeit beginnen zu können, und um öffentliche Instances zu starten, wie beispielsweise einen Blog oder eine einfache Website. Sie können die Komponenten Ihrer Standard-VPC nach Bedarf ändern.

Sie können Ihrer Standard-VPC Subnetze hinzufügen. Weitere Informationen finden Sie unter the section called “Erstellen eines Subnetzes”.

Inhalt

- Komponenten von Standard-VPCs
- Standard-Subnetze
- Anzeigen Ihrer Standard-VPC und Standardsubnetze
- Erstellen einer Standard-VPC
- Erstellen eines Standardsubnetzes
- Löschen Ihrer Standardsubnetze und der Standard-VPC

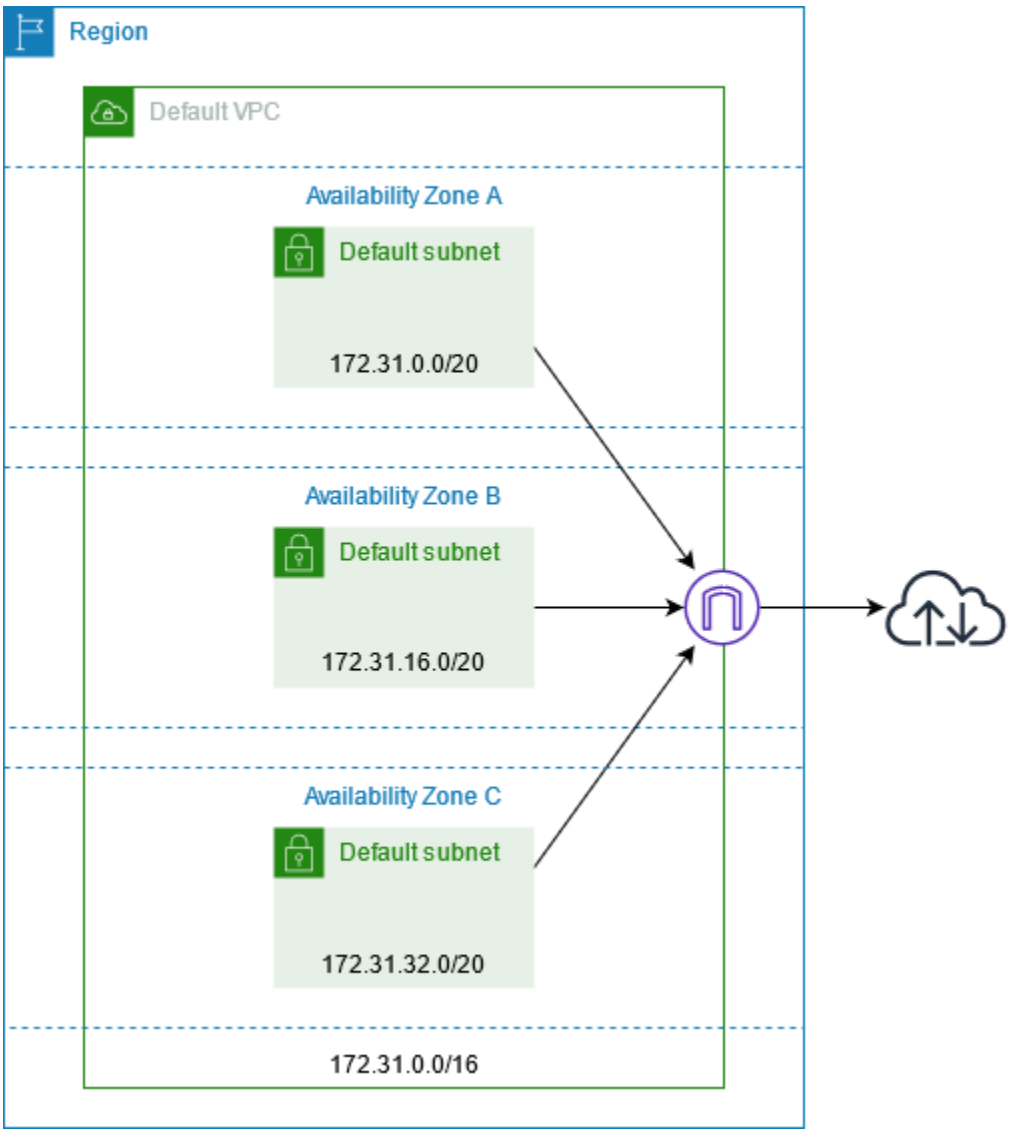
Komponenten von Standard-VPCs

Wenn wir eine Standard-VPC erstellen, werden folgende Vorgänge zur Einrichtung ausgeführt:

- Erstellen einer VPC mit einem IPv4-CIDR-Block der Größe `/16` (`172.31.0.0/16`). So sind bis zu 65.536 private IPv4-Adressen verfügbar.
- Erstellen eines Standardsubnetzes der Größe `/20` in jeder Availability Zone. Damit stehen bis zu 4.096 Adressen pro Subnetz zur Verfügung, von denen ein paar für die Nutzung durch uns reserviert sind.
- Erstellen eines Internet-Gateways und Herstellen einer Verbindung mit der Standard-VPC
- Fügen Sie der Haupt-Routingtabelle eine Route hinzu, die den gesamten Datenverkehr (`0.0.0.0/0`) an das Internet-Gateway weiterleitet.
- Erstellung einer Standardsicherheitsgruppe und Verknüpfen dieser Gruppe mit Ihrer Standard-VPC
- Erstellung einer Standardnetzwerkzugriffskontrollliste (ACL) und Verknüpfen mit Ihrer Standard-VPC
- Verknüpfung der DHCP-Standardoptionen für Ihr AWS-Konto mit Ihrer Standard-VPC

> **Note**
>
> Amazon erstellt die oben genannten Ressourcen für Sie. IAM-Richtlinien gelten für diese Aktionen nicht, da Sie diese Aktionen nicht ausführen. Wenn Sie beispielsweise über eine IAM-Richtlinie verfügen, die die Möglichkeit zum Aufrufen von CreateInternetGateway ablehnt und Sie dann CreateDefaultVpc aufrufen, wird das Internet-Gateway in der Standard-VPC dennoch erstellt.

Die folgende Abbildung zeigt die Hauptkomponenten, die wir für Ihre Standard-VPC einrichten.



Die folgende Tabelle zeigt die Routen in der Haupt-Routing-Tabelle für die Standard-VPC.

Ziel	Ziel
172.31.0.0/16	Lokal
0.0.0.0/0	*internet_gateway_id*

Sie können eine Standard-VPC wie jede andere VPC verwenden:

- Hinzufügen zusätzlicher benutzerdefinierter Subnetze.
- Ändern der Haupt-Routing-Tabelle.

- Hinzufügen zusätzlicher Routing-Tabellen.
- Zuordnung zusätzlicher Sicherheitsgruppen.
- Aktualisieren der Regeln für die Standardsicherheitsgruppe.
- Hinzufügen von AWS Site-to-Site VPN-Verbindungen.
- Hinzufügen weiterer IPv4-CIDR-Blöcke.
- Greifen Sie mithilfe eines Direct Connect-Gateways auf VPCs in einer entfernten Region zu. Weitere Informationen zu Direct Connect-Gateways finden Sie unter Direct Connect-Gateways im AWS Direct Connect -Benutzerhandbuch.

Sie können ein Standardsubnetz so nutzen wie jedes andere Subnetz: benutzerdefinierte Routing-Tabellen hinzufügen und Netzwerk-ACLs festlegen. Wenn Sie eine EC2 Instance starten, können Sie außerdem ein spezifisches Standardsubnetz festlegen.

Optional können Sie Ihrer Standard-VPC einen IPv6 CIDR-Block zuweisen.

Standard-Subnetze

Standardmäßig ist ein Standardsubnetz ein öffentliches Subnetz. Dies liegt daran, dass die Haupt-Routing-Tabelle den Datenverkehr des Subnetzes in das Internet über das Internet-Gateway sendet. Sie können ein Standardsubnetz zu einem privaten Subnetz machen, indem Sie die Route vom Ziel 0.0.0.0/0 zum Internet-Gateway verschieben. Wenn Sie so vorgehen, können EC2-Instances im betreffenden Subnetz jedoch nicht mehr auf das Internet zugreifen.

Instances, die Sie in einem Standard-Subnetz starten, erhalten sowohl eine öffentliche IPv4-Adresse, als auch eine private IPv4-Adresse, und sowohl öffentliche, als auch private DNS-Hostnamen. Instances, die Sie innerhalb eines nicht standardmäßigen Subnetzes in einer Standard-VPC starten, erhalten keine öffentliche IPv4-Adresse oder einen DNS-Hostnamen. Sie können das Standardverhalten für die öffentliche IP-Adressierung Ihres Subnetzes ändern. Weitere Informationen finden Sie unter Ändern des öffentlichen IPv4-Adressierungsattributs Ihres Subnetzes.

Von Zeit zu Zeit fügt AWS möglicherweise eine neue Availability Zone zu einer Region hinzu. In den meisten Fällen erstellen wir in dieser Availability Zone innerhalb weniger Tage automatisch ein neues Standardsubnetz für Ihre Standard-VPC. Wenn Sie Ihre Standard-VPC bearbeitet haben, fügen wir jedoch kein neues Standardsubnetz hinzu. Wenn Sie ein Standardsubnetz für die neue Availability Zone benötigten, können Sie dieses selbst erstellen. Weitere Informationen finden Sie unter Erstellen eines Standardsubnetzes.

Anzeigen Ihrer Standard-VPC und Standardsubnetze

Sie können Ihre Standard-VPC und die Subnetze mit der Amazon VPC-Konsole oder der Befehlszeilenschnittstelle anzeigen.

Anzeige Ihrer Standard-VPC und der Subnetze mit Hilfe der -Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Suchen Sie in der Spalte Default VPC nach dem Wert Yes. Merken Sie sich die ID der Standard-VPC.
4. Wählen Sie im Navigationsbereich Subnets aus.
5. Geben Sie in die Suchleiste die ID der Standard-VPC ein. Die zurückgegebenen Subnetze sind Subnetze in Ihrer Standard-VPC.
6. Um zu überprüfen, welche Subnetze Standard-Subnetze sind, suchen Sie in der Spalte Default Subnet nach dem Wert Yes.

Beschreiben Ihrer Standard-VPC unter Verwendung der Befehlszeile

- Verwenden von describe-vpcs (AWS CLI)
- Verwenden von Get-EC2Vpc (AWS Tools for Windows PowerShell)

Verwenden Sie die Befehle mit dem `isDefault`-Filter und setzen Sie den Filterwert auf `true`.

Beschreiben Ihrer Standard-Subnetze unter Verwendung der Befehlszeile

- Verwenden von describe-subnets (AWS CLI)
- Verwenden von Get-EC2Subnet (AWS Tools for Windows PowerShell)

Verwenden Sie die Befehle mit dem `vpc-id`-Filter und setzen Sie den Filterwert auf die ID der Standard-VPC. In der Ausgabe ist für Standard-Subnetze das `DefaultForAz`-Feld auf `true` gesetzt.

Erstellen einer Standard-VPC

Wenn Sie Ihre Standard-VPC löschen, können Sie eine neue erstellen. Sie können ein vorhergehendes Standard-VPC, das Sie gelöscht haben, nicht wiederherstellen, und Sie können keine vorhandene benutzerdefinierte VPC als Standard-VPC markieren.

Wenn Sie eine Standard-VPC erstellen, wird diese mit den Standardkomponenten einer Standard-VPC erstellt, einschließlich eines Standard-Subnetzes in jeder Availability Zone. Sie können keine eigenen Komponenten spezifizieren. Die Subnetz-CIDR-Blöcke Ihrer neuen Standard-VPC werden möglicherweise nicht auf dieselben Availability Zones abgebildet wie Ihre vorherige Standard-VPC. Wurde das Subnetz mit CIDR-Block `172.31.0.0/20` beispielsweise in `us-east-2a` in Ihrer vorhergehenden Standard-VPC erstellt, wird es in Ihrem neuen Standard-VPC möglicherweise in `us-east-2b` erstellt.

Wenn Sie bereits eine Standard-VPC in der Region haben, können Sie keine weitere dort erstellen.

Erstellen einer Standard-VPC unter Verwendung der -Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Wählen Sie Actions und Create Default VPC.
4. Wählen Sie Erstellen aus. Schließen Sie den Bestätigungsbildschirm.

Erstellen einer Standard-VPC unter Verwendung der Befehlszeile

Sie können den -Befehl create-default-vpcAWS CLI verwenden. Dieser Befehl hat keine Eingabeparameter.

```
aws ec2 create-default-vpc
```

Es folgt eine Beispielausgabe.

```
{
    "Vpc": {
        "VpcId": "vpc-3f139646",
        "InstanceTenancy": "default",
        "Tags": [],
        "Ipv6CidrBlockAssociationSet": [],
        "State": "pending",
```

```
        "DhcpOptionsId": "dopt-61079b07",
        "CidrBlock": "172.31.0.0/16",
        "IsDefault": true
    }
}
```

Alternativ können Sie Befehl New-EC2DefaultVpc in den Tools for Windows PowerShell oder die Aktion CreateDefaultVpc der Amazon EC2-API verwenden.

Erstellen eines Standardsubnetzes

Sie können ein Standardsubnetz in einer Availability Zone erstellen, in der es noch kein solches gibt. Beispielsweise könnten Sie ein Standard-Subnetz erstellen, wenn Sie ein Standard-Subnetz gelöscht haben, oder wenn AWS eine neue Availability Zone hinzugefügt hat und nicht automatisch ein Standard-Subnetz für dies Zone in Ihrer Standard-VPC erstellt hat.

Wenn Sie ein Standard-Subnetz erstellt haben, wird es mit einem IPv4-CIDR-Block der Größe `/20` im nächsten verfügbaren fortlaufenden Speicherplatz Ihrer Standard-VPC erstellt Es gelten die folgenden Regeln:

- Sie können den CIDR-Block nicht selbst festlegen.
- Sie können ein zuvor gelöschtes Standard-Subnetz nicht wiederherstellen.
- Sie können nur ein Standardsubnetz pro Availability Zone haben.
- Sie können kein Standardsubnetze in einem nicht standardmäßigen VPC erstellen.

Falls in Ihrer Standard-VPC nicht genügend Adressraum für das Erstellen eines CIDR-Blocks der Größe `/20` vorhanden ist, schlägt die Anfrage fehl. Wenn Sie mehr Adressraum benötigen, können Sie Ihrer VPC einen IPv4-CIDR-Block hinzufügen.

Wenn Sie Ihrer Standard-VPC einen IPv6 CIDR-Block zugeordnet haben, erhält das neue Standard-Subnetz nicht automatisch einen IPv6 CIDR-Block. Stattdessen können Sie dem Standard-Subnetz nach dem Erstellen einen IPv6 CIDR-Block zuordnen. Weitere Informationen finden Sie unter Hinzufügen eines IP6-CIDR-Blocks zu Ihrem Subnetz.

Sie können kein Standard-Subnetz mit der AWS Management Console erstellen.

So erstellen Sie ein Standard-Subnetz mit der AWS CLI

Führen Sie den AWS CLI-Befehl create-default-subnet aus und geben Sie die Availability Zone an, in der das Subnetz erstellt werden soll.

```
aws ec2 create-default-subnet --availability-zone us-east-2a
```

Es folgt eine Beispielausgabe.

```
{
    "Subnet": {
        "AvailabilityZone": "us-east-2a",
        "Tags": [],
        "AvailableIpAddressCount": 4091,
        "DefaultForAz": true,
        "Ipv6CidrBlockAssociationSet": [],
        "VpcId": "vpc-1a2b3c4d",
        "State": "available",
        "MapPublicIpOnLaunch": true,
        "SubnetId": "subnet-1122aabb",
        "CidrBlock": "172.31.32.0/20",
        "AssignIpv6AddressOnCreation": false
    }
}
```

Weitere Informationen zur Einrichtung der AWS CLI finden Sie im AWS Command Line Interface-Benutzerhandbuch.

Alternativ können Sie Befehl New-EC2DefaultSubnet in den Tools for Windows PowerShell oder die Aktion CreateDefaultSubnet der Amazon EC2-API verwenden.

Löschen Ihrer Standardsubnetze und der Standard-VPC

Sie können Standardsubnetze oder Standard-VPCs genauso löschen wie alle anderen Subnetze oder VPCs. Wenn Sie jedoch Ihre Standardsubnetze oder Standard-VPC löschen, müssen Sie beim Starten von Instances explizit ein Subnetz in einer Ihrer VPCs angeben. Wenn Sie noch nicht über eine andere VPC verfügen, müssen Sie eine VPC mit einem Subnetz in mindestens einer Availability Zone erstellen. Weitere Informationen finden Sie unter Erstellen einer VPC.

Wenn Sie Ihre Standard-VPC löschen, können Sie eine neue erstellen. Weitere Informationen finden Sie unter Erstellen einer Standard-VPC.

Wenn Sie ein Standard-Subnetz löschen, können Sie eine neue erstellen. Weitere Informationen finden Sie unter Erstellen eines Standardsubnetzes. Um sicherzustellen, dass Ihr neues Standard-Subnetz wie erwartet arbeitet, bearbeiten Sie das Subnet-Attribut und weisen Sie öffentliche IP-

Adressen zu Instances zu, die in dem entsprechenden Subnetz gestartet sind. Weitere Informationen finden Sie unter Ändern des öffentlichen IPv4-Adressierungsattributs Ihres Subnetzes. Sie können nur ein Standardsubnetz pro Availability Zone haben. Sie können kein Standardsubnetze in einem nicht standardmäßigen VPC erstellen.

Erstellen einer VPC

Mithilfe der folgenden Verfahren können Sie eine Virtual Private Cloud (VPC) erstellen. Eine VPC muss über zusätzliche Ressourcen wie Subnetze, Routentabellen und Gateways verfügen, bevor Sie AWS -Ressourcen in der VPC erstellen können.

Inhalt

Informationen zum Anzeigen oder Ändern einer VPC finden Sie unter the section called “Konfigurieren Ihrer VPC”.

VPC-Konfigurationsoptionen

Sie können die folgenden Konfigurationsoptionen angeben, wenn Sie eine VPC erstellen.

Availability Zones

Mehrere eigenständige Rechenzentren mit redundanter Stromversorgung, Vernetzung und Konnektivität in einer AWS -Region. Sie können mehrere AZs nutzen, um Produktionsanwendungen und Datenbanken zu betreiben, die hochverfügbarer, fehlertoleranter und skalierbarer sind, als dies in einem einzelnen Rechenzentrum möglich wäre. Wenn Sie Anwendungen in Subnetzen auf mehrere AZs verteilt partitionieren, erreichen Sie eine bessere Isolation und sind besser vor Problemen wie z. B. Stromausfällen, Blitzeinschlägen, Tornados und Erdbeben geschützt.

CIDR-Blöcke

Sie müssen IP-Adressbereiche für Ihre VPC und Subnetze angeben. Weitere Informationen finden Sie unter IP-Adressierung für Ihre VPCs und Subnetze.

DNS-Optionen

Wenn Sie öffentliche IPv4-DNS-Hostnamen für die in Ihren Subnetzen gestarteten EC2-Instances benötigen, müssen Sie beide DNS-Optionen aktivieren. Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC.

- DNS-Hostnamen aktivieren: Die in der VPC gestarteten EC2-Instances erhalten einen öffentlichen DNS-Hostnamen, der mit ihren öffentlichen IPv4-Adressen übereinstimmt.
- DNS-Auflösung aktivieren: Die DNS-Auflösung für private DNS-Hostnamen wird für die VPC vom Amazon-DNS-Server, dem Route 53 Resolver, bereitgestellt.

Internet-Gateway

Verbindet Ihre VPC mit dem Internet. Die Instances in einem öffentlichen Subnetz können auf das Internet zugreifen, da die Subnetz-Routing-Tabelle eine Route enthält, die Datenverkehr an das Internet-Gateway sendet. Wenn ein Server nicht direkt über das Internet erreichbar sein muss, sollten Sie ihn nicht in einem öffentlichen Subnetz bereitstellen. Weitere Informationen finden Sie unter Internet-Gateways.

Name

Die Namen, die Sie für die VPC und die anderen VPC-Ressourcen angeben, werden verwendet, um Namenstags zu erstellen. Wenn Sie das Feature zur automatischen Generierung von Namenstags in der Konsole verwenden, haben die Tag-Werte das Format *Name*-*Ressource*.

NAT gateways (NAT-Gateways)

Ermöglicht es Instances in einem privaten Subnetz, ausgehenden Datenverkehr an das Internet zu senden, verhindert jedoch, dass Ressourcen im Internet auf diese Instances zugreifen. In der Produktion empfehlen wir Ihnen, in jedem aktiven AZ ein NAT-Gateway zu implementieren. Weitere Informationen finden Sie unter NAT-Gateways.

Routing-Tabellen

Enthält Regeln, sogenannte Routen, die festlegen, wohin der Netzwerkverkehr von Ihrem Subnetz oder Gateway gelenkt wird. Weitere Informationen finden Sie unter Routing-Tabellen.

Subnetze

Ein Bereich von IP-Adressen in Ihrer VPC. Sie können AWS Ressourcen wie EC2-Instances in Ihren Subnetzen starten. Jedes Subnetz befindet sich vollständig innerhalb einer Availability Zone. Indem Instances in separaten Availability Zones gestartet werden, können Sie Ihre Anwendungen vor dem Ausfall einer einzelnen Zone schützen.

Ein öffentliches Subnetz verfügt über eine direkte Route zu einem Internet-Gateway. Ressourcen in einem öffentlichen Subnetz können auf das öffentliche Internet zugreifen. Ein privates Subnetz hat keine Weiterleitung an das Internet-Gateway. Ressourcen in einem privaten Subnetz benötigen zum Beispiel ein NAT-Gerät, um auf das öffentliche Internet zugreifen zu können.

Weitere Informationen finden Sie unter Subnetze.

Tenancy

Diese Option definiert, ob in der VPC gestartete EC2-Instances auf Hardware ausgeführt werden, die gemeinsam mit anderen AWS-Konten genutzt wird, oder auf Hardware, die ausschließlich für Ihre Verwendung bestimmt ist. Wenn Sie die Tenancy der VPC als Tenancy wählen, verwenden EC2-Instances*`Default`*, die in dieser VPC gestartet werden, das Tenancy-Attribut, das Sie beim Starten der Instance angegeben haben. Weitere Informationen finden Sie unter Starten einer Instance mit definierten Parametern im Amazon EC2 EC2-Benutzerhandbuch. Wenn Sie für die Tenancy der VPC `Dedicated` auswählen, werden die Instances immer als Dedicated Instances auf Hardware ausgeführt, die für Ihre Verwendung bestimmt ist. Wenn du AWS Outposts verwendest, benötigt dein Outpost private Konnektivität; du musst Tenancy verwenden`Default`.

Erstellen Sie eine VPC und andere VPC-Ressourcen

Gehen Sie wie folgt vor, um eine VPC sowie die zusätzlichen VPC-Ressourcen zu erstellen, die Sie zum Ausführen Ihrer Anwendung benötigen, z. B. Subnetze, Routing-Tabellen, Internet-Gateways und NAT-Gateways. Beispielkonfigurationen finden Sie unter Beispiele.

So erstellen Sie eine VPC, Subnetze und weitere VPC-Ressourcen mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie auf dem VPC-Dashboard Create VPC (VPC erstellen) aus.
3. Wählen Sie unter Zu erstellende Ressourcen die Option VPC und mehr aus.
4. Lassen Sie die automatische Generierung von Namenstags aktiviert, um Namenstags für die VPC-Ressourcen zu erstellen, oder deaktivieren Sie die Option, um Ihre eigenen Namenstags für die VPC-Ressourcen bereitzustellen.
5. Geben Sie für den IPv4-CIDR-Block einen IPv4-Adressbereich für die VPC ein. Eine VPC muss einen IPv4-Adressbereich aufweisen.
6. (Optional) Um IPv6-Datenverkehr zu unterstützen, wählen Sie IPv6-CIDR-Block, Von Amazon bereitgestellter IPv6-CIDR-Block.

7. Wählen Sie eine Tenancy-Option aus. Diese Option definiert, ob in der VPC gestartete EC2-Instances auf Hardware ausgeführt werden, die gemeinsam mit anderen AWS-Konten genutzt wird, oder auf Hardware, die ausschließlich für Ihre Verwendung bestimmt ist. Wenn Sie die Tenancy der VPC als Tenancy wählen, verwenden EC2-Instances`Default`, die in dieser VPC gestartet werden, das Tenancy-Attribut, das Sie beim Starten der Instance angegeben haben. Weitere Informationen finden Sie unter Starten einer Instance mithilfe definierter Parameter im Amazon EC2 EC2-Benutzerhandbuch. Wenn Sie für die Tenancy der VPC `Dedicated` auswählen, werden die Instances immer als Dedicated Instances auf Hardware ausgeführt, die für Ihre Verwendung bestimmt ist. Wenn du AWS Outposts verwendest, benötigt dein Outpost private Konnektivität; du musst Tenancy verwenden`Default`.
8. Für die Anzahl der Availability Zones (AZs) empfiehlt es sich, Subnetze in mindestens zwei Availability Zones für eine Produktionsumgebung bereitzustellen. Um die AZs für Ihre Subnetze auszuwählen, erweitern Sie die Option AZs anpassen. Andernfalls lassen Sie uns sie AWS für Sie auswählen.
9. Um Ihre Subnetze zu konfigurieren, wählen Sie Werte für Anzahl der öffentlichen Subnetze und Anzahl der privaten Subnetze. Um die IP-Adressbereiche für Ihre Subnetze auszuwählen, erweitern Sie die Option CIDR-Blöcke für Subnetze anpassen. Andernfalls lassen Sie uns sie für Sie AWS auswählen.
10. (Optional) Falls Ressourcen in einem privaten Subnetz Zugang zum öffentlichen Internet über IPv4 benötigen, bestimmen Sie für NAT-Gateways die Anzahl der AZs, in denen NAT-Gateways erstellt werden sollen. In der Produktion empfehlen wir, in jeder AZ ein NAT-Gateway mit Ressourcen bereitzustellen, die Zugriff auf das öffentliche Internet benötigen. Beachten Sie, dass für NAT-Gateways Kosten anfallen. Weitere Informationen finden Sie unter Preisgestaltung.
11. (Optional) Wenn Ressourcen in einem privaten Subnetz über IPv6 Zugriff auf das öffentliche Internet benötigen, wählen Sie bei Internet-Gateway nur für ausgehenden Verkehr die Option Ja aus.
12. (Optional) Wenn Sie direkt von Ihrer VPC aus auf Amazon S3 zugreifen müssen, wählen Sie VPC-Endpunkte, S3 Gateway. Dadurch wird ein Gateway-VPC-Endpunkt für Amazon S3 erstellt. Weitere Informationen finden Sie unter Gateway-VPC-Endpunkte im AWS PrivateLink -Leitfaden.
13. (Optional) Für DNS-Optionen sind beide Optionen für die Auflösung von Domainnamen standardmäßig aktiviert. Wenn die Standardeinstellung Ihren Anforderungen nicht entspricht, können Sie diese Optionen deaktivieren.
14. (Optional) Um ein Tag zu Ihrer VPC hinzuzufügen, erweitern Sie Zusätzliche Tags, wählen Sie Neues Tag hinzufügen, und geben Sie einen Tag-Schlüssel und einen Tag-Wert ein.

15. Im Vorschau-Bereich können Sie die Beziehungen zwischen Ressourcen, die Sie konfiguriert haben, innerhalb einer VPC visualisieren. Durchgezogene Linien stellen die Beziehungen zwischen Ressourcen dar. Gepunktete Linien stellen den Netzwerkverkehr zu NAT-Gateways, Internet-Gateways und Gateway-Endpunkten dar. Sobald Sie die VPC erstellt haben, können Sie die Ressourcen in Ihrer VPC in diesem Format jederzeit über die Registerkarte Ressourcenkarte visualisieren. Weitere Informationen finden Sie unter Visualisierung der Ressourcen in Ihrer VPC.
16. Wählen Sie VPC erstellen aus, sobald Sie mit der Konfiguration Ihrer VPC fertig sind.

Ausschließliches Erstellen einer VPC

Verwenden Sie das folgende Verfahren, um mithilfe der Amazon-VPC-Konsole eine VPC ohne zusätzliche VPC-Ressourcen zu erstellen.

Erstellen einer VPC ohne zusätzliche VPC-Ressourcen mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie auf dem VPC-Dashboard Create VPC (VPC erstellen) aus.
3. Wählen Sie unter Zu erstellende Ressourcen die Option Nur VPC aus.
4. (Optional) Geben Sie unter Namenstag einen Namen für Ihre VPC ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
5. Führen Sie für IPv4 CIDR block (IPv4-CIDR-Block) einen der folgenden Schritte aus:
   - Wählen Sie die manuelle IPv4-CIDR-Eingabe und geben Sie einen IPv4-Adressbereich für Ihre VPC ein.
   - Wählen Sie IPAM-zugewiesenen IPv4-CIDR-Block, wählen Sie Ihren Amazon VPC IP Address Manager (IPAM)-IPv4-Adresspool und eine Netzmaske aus. Die Größe des CIDR-Blocks ist durch die Zuordnungsregeln für den IPAM-Pool begrenzt. IPAM ist eine VPC-Funktion, die es Ihnen erleichtert, IP-Adressen für Ihre AWS Workloads zu planen, zu verfolgen und zu überwachen. Weitere Informationen finden Sie im Amazon VPC IPAM-Benutzerhandbuch.

     Wenn Sie IPAM zur Verwaltung Ihrer IP-Adressen verwenden, empfehlen wir Ihnen, diese Option zu wählen. Andernfalls könnte sich der CIDR-Block, den Sie für Ihre VPC angeben, mit einer IPAM-CIDR-Zuordnung überschneiden.
6. (Optional) Um eine Dual-Stack-VPC zu erstellen, geben Sie einen IPv6-Adressbereich für Ihre VPC an. Führen Sie für IPv6 CIDR block (IPv6-CIDR-Block) einen der folgenden Schritte aus:

- Wählen Sie IPAM-zugewiesener IPv6-CIDR-Block, wenn Sie Amazon VPC IP Address Manager verwenden und ein IPv6-CIDR aus einem IPAM-Pool bereitstellen möchten. Sie haben zwei Möglichkeiten, der VPC einen IP-Adressbereich unter dem CIDR-Block bereitzustellen:
  - Netzmaskenlänge: Wählen Sie diese Option, um eine Netzmaskenlänge für den CIDR auszuwählen. Führen Sie eine der folgenden Aktionen aus:
    - Wenn für den IPAM-Pool eine Standard-Netzmaskenlänge ausgewählt wurde, können Sie die Standardlänge der IPAM-Netzmaske wählen, um die vom IPAM-Administrator für den IPAM-Pool festgelegte Standard-Netzmaskenlänge zu verwenden. Weitere Informationen zur optionalen Standardregel für die Zuweisung von Netzmaskenlänge finden Sie unter Erstellen eines regionalen IPv6-Pools im Amazon-VPC-IPAM-Benutzerhandbuch.
    - Wenn keine Standard-Netzmaskenlänge für den IPAM-Pool ausgewählt wurde, wählen Sie eine Netzmaskenlänge, die spezifischer ist als die Netzmaskenlänge des IPAM-Pool-CIDR. Wenn der IPAM-Pool-CIDR beispielsweise /50 ist, können Sie für die VPC eine Netzmaskenlänge zwischen /52 und /60 wählen. Mögliche Netzmaskenlängen liegen zwischen /44 und /60 in Schritten von /4.
  - Einen CIDR wählen: Wählen Sie diese Option, um eine IPv6-Adresse manuell einzugeben. Sie können nur eine Netzmaskenlänge wählen, die spezifischer als die Netzmaskenlänge des IPAM-Pool-CIDR ist. Wenn der IPAM-Pool-CIDR beispielsweise /50 ist, können Sie für die VPC eine Netzmaskenlänge zwischen /52 und /60 wählen. Mögliche IPv6-Netzmaskenlängen liegen zwischen /44 und /60 in Schritten von /4.
- Wählen Sie von Von Amazon bereitgestellter IPv6-CIDR-Block aus, um einen IPv6-CIDR-Block aus dem IPv6-Adresspool von Amazon anzufordern. Wählen Sie für Network Border Group die Gruppe aus, aus der IP-Adressen AWS beworben werden. Amazon bietet eine feste IPv6-CIDR-Blockgröße von /56.
- Wählen Sie IPv6-CIDR im Besitz von mir) aus, um ein IPv6-CIDR bereitzustellen, das Sie bereits in AWS eingebunden haben. Weitere Informationen zum Herstellen eigener IP-Adressbereiche finden Sie unter Bring your own IP Addresses (BYOIP) im Amazon EC2 EC2-Benutzerhandbuch. AWS Sie können einen IP-Adressbereich für die VPC bereitstellen, indem Sie die folgenden Optionen für den CIDR-Block verwenden:
  - Keine Präferenz: Wählen Sie diese Option, um die Netzmaskenlänge /56 zu verwenden.
  - CIDR auswählen: Wählen Sie diese Option, um eine IPv6-Adresse manuell einzugeben und eine Netzmaskenlänge zu wählen, die spezifischer ist als die Größe des BYOIP-CIDR. Wenn der BYOIP-Pool-CIDR beispielsweise /50 ist, können Sie für die VPC eine

Netzmaskenlänge zwischen /52 und /60 wählen. Mögliche IPv6-Netzmaskenlängen liegen zwischen /44 und /60 in Schritten von /4.

7. (Optional) Wählen Sie eine Tenancy-Option aus. Diese Option definiert, ob in der VPC gestartete EC2-Instances auf Hardware ausgeführt werden, die gemeinsam mit anderen AWS-Konten genutzt wird, oder auf Hardware, die ausschließlich für Ihre Verwendung bestimmt ist. Wenn Sie die Tenancy der VPC als Tenancy wählen, verwenden EC2-Instances`Default`, die in dieser VPC gestartet werden, das Tenancy-Attribut, das Sie beim Starten der Instance angegeben haben. Weitere Informationen finden Sie unter Starten einer Instance mit definierten Parametern im Amazon EC2 EC2-Benutzerhandbuch. Wenn Sie für die Tenancy der VPC `Dedicated` auswählen, werden die Instances immer als Dedicated Instances auf Hardware ausgeführt, die für Ihre Verwendung bestimmt ist. Wenn du AWS Outposts verwendest, benötigt dein Outpost private Konnektivität; du musst Tenancy verwenden`Default`.
8. (Optional) Sie fügen ein Tag hinzu, indem Sie Neuen Tag hinzufügen auswählen und den Tag-Schlüssel und -Wert eingeben.
9. Wählen Sie VPC erstellen aus.
10. Nachdem Sie eine VPC erstellt haben, können Sie Subnetze hinzufügen. Weitere Informationen finden Sie unter Erstellen eines Subnetzes.

Erstellen Sie eine VPC mit dem AWS CLI

Das folgende Verfahren enthält AWS CLI Beispielbefehle zum Erstellen einer VPC sowie die zusätzlichen VPC-Ressourcen, die zum Ausführen einer Anwendung erforderlich sind. Wenn Sie alle Befehle in diesem Verfahren ausführen, erstellen Sie eine VPC, ein öffentliches Subnetz, ein privates Subnetz, eine Routing-Tabelle für jedes Subnetz, ein Internet-Gateway, ein Internet-Gateway nur für ausgehenden Verkehr und ein öffentliches NAT-Gateway. Wenn Sie nicht alle diese Ressourcen benötigen, können Sie nur die Beispielbefehle verwenden, die Sie benötigen.

Voraussetzungen

Bevor Sie beginnen, installieren und konfigurieren Sie die AWS CLI. Wenn Sie das konfigurieren AWS CLI, werden Sie zur AWS Eingabe von Anmeldeinformationen aufgefordert. In den Beispielen in diesem Tutorial wird davon ausgegangen, dass Sie eine Standardregion konfiguriert haben. Andernfalls fügen Sie für jeden Befehl die `--region`-Option hinzu. Informationen finden Sie unter Installieren und Aktualisieren der AWS CLI und Konfigurieren der AWS CLI.

Tagging

Sie können einer Ressource Tags hinzufügen, nachdem Sie sie mit dem Befehl create-tags erstellt haben. Alternativ können Sie die `--tag-specification`-Option wie folgt zum Erstellungsbefehl für die Ressource hinzufügen.

```
--tag-specifications ResourceType=vpc,Tags=[{Key=Name,Value=my-project}]
```

So erstellen Sie eine VPC plus VPC-Ressourcen mit dem AWS CLI

1. Verwenden Sie den folgenden create-vpc, um eine VPC mit dem angegebenen IPv4-CIDR-Block zu erstellen.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --query Vpc.VpcId --output text
   ```

   Um eine Dual-Stack-VPC zu erstellen, fügen Sie alternativ die `--amazon-provided-ipv6-cidr-block`-Option hinzu, u, einen von Amazon bereitgestellten IPv6-CIDR-Block hinzuzufügen, wie im folgenden Beispiel gezeigt.

   ```
   aws ec2 create-vpc --cidr-block 10.0.0.0/24 --amazon-provided-ipv6-cidr-block --
   query Vpc.VpcId --output text
   ```

   Der Befehl gibt die ID der neuen VPC zurück. Im Folgenden wird ein Beispiel gezeigt.

   ```
   vpc-1a2b3c4d5e6f1a2b3
   ```

2. [Dual-Stack-VPC] Rufen Sie den IPv6-CIDR-Block ab, der mit der VPC verknüpft ist, indem Sie den folgenden Befehl describe-vpcs verwenden.

   ```
   aws ec2 describe-vpcs --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
    Vpcs[].Ipv6CidrBlockAssociationSet[].Ipv6CidrBlock --output text
   ```

   Es folgt eine Beispielausgabe.

   ```
   2600:1f13:cfe:3600::/56
   ```

3. Erstellen Sie ein oder mehrere Subnetze, je nach Anwendungsfall. In der Produktion empfehlen wir Ihnen, Ressourcen in mindestens zwei Availability Zones zu starten. Führen Sie einen der folgenden Befehle zum Erstellen jedes Subnetzes aus.

- Nur IPv4-Subnetz – Um ein Subnetz mit einem bestimmten IPv4-CIDR-Block zu erstellen, verwenden Sie den folgenden Befehl create-subnet aus.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --availability-zone us-east-2a --query Subnet.SubnetId --output text
```

- Dual-Stack-Subnetz – Wenn Sie eine Dual-Stack-VPC erstellt haben, können Sie die `--ipv6-cidr-block`-Option verwenden, um ein Dual-Stack-Subnetz zu erstellen, wie im folgenden Befehl gezeigt.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --cidr-block 10.0.1.0/20
 --ipv6-cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --
query Subnet.SubnetId --output text
```

- Nur IPv6-Subnetz – Wenn Sie eine Dual-Stack-VPC erstellt haben, können Sie die `--ipv6-native`-Option verwenden, um ein Nur-IPv6-Subnetz zu erstellen, wie im folgenden Befehl gezeigt.

```
aws ec2 create-subnet --vpc-id vpc-1a2b3c4d5e6f1a2b3 --ipv6-native --ipv6-
cidr-block 2600:1f13:cfe:3600::/64 --availability-zone us-east-2a --query
 Subnet.SubnetId --output text
```

Der Befehl gibt die ID des neuen Subnetzes zurück. Im Folgenden wird ein Beispiel gezeigt.

```
subnet-1a2b3c4d5e6f1a2b3
```

4. Wenn Sie ein öffentliches Subnetz für Ihre Webserver oder für ein NAT-Gateway benötigen, gehen Sie wie folgt vor:

   a. Erstellen Sie ein Internet-Gateway mithilfe des folgenden Befehls create-internet-gateway. Der Befehl gibt die ID des neuen Internet-Gateways zurück.

```
aws ec2 create-internet-gateway --query InternetGateway.InternetGatewayId --
output text
```

   b. Hängen Sie das Internet-Gateway aus dem vorherigen Schritt mit dem folgenden Befehl attach-internet-gateway an die VPC an. Verwenden Sie die Internet-Gateway-ID, die Sie aus dem vorherigen Schritt erhalten.

```
aws ec2 attach-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --internet-
gateway-id igw-id
```

c. Erstellen Sie mit dem folgenden Befehl create-route-table eine benutzerdefinierte Routing-Tabelle für die VPC. Der Befehl gibt die ID der neuen Routung-Tabelle zurück.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Erstellen Sie mit dem folgenden Befehl create-route eine Route in der Routing-Tabelle, die den gesamten IPv4-Datenverkehr an das Internet-Gateway sendet. Verwenden Sie die ID der Routing-Tabelle für das öffentliche Subnetz.

```
aws ec2 create-route --route-table-id rtb-id-public --destination-cidr-block
 0.0.0.0/0 --gateway-id igw-id
```

e. Ordnen Sie die Routing-Tabelle mithilfe des folgenden Befehls associate-route-table dem öffentlichen Subnetz zu. Verwenden Sie die ID der Routing-Tabelle für das öffentliche Subnetz und die ID des öffentlichen Subnetzes.

```
aws ec2 associate-route-table --route-table-id rtb-id-public --subnet-
id subnet-id-public-subnet
```

5. [IPv6] Sie können ein reines Ausgangs-Internet-Gateway hinzufügen, damit Instances in einem privaten Subnetz über IPv6 auf das Internet zugreifen können (z. B. um Software-Updates zu erhalten), aber Hosts im Internet können nicht auf Ihre Instances zugreifen.

a. Erstellen Sie ein Internet-Gateway für ausgehenden Verkehr mithilfe des folgenden Befehls create-egress-only-internet-gateway. Der Befehl gibt die ID des neuen Internet-Gateways zurück.

```
aws ec2 create-egress-only-internet-gateway --vpc-id vpc-1a2b3c4d5e6f1a2b3 --
query EgressOnlyInternetGateway.EgressOnlyInternetGatewayId --output text
```

b. Erstellen Sie eine benutzerdefinierte Routing-Tabelle für das private Subnetz mit dem folgenden Befehl create-route-table. Der Befehl gibt die ID der neuen Routung-Tabelle zurück.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

c. Erstellen Sie mit dem folgenden Befehl create-route eine Route in der Routing-Tabelle für das private Subnetz, die den gesamten IPv6-Verkehr an das Internet-Gateway für ausgehenden Verkehr sendet. Verwenden Sie die ID der Routing-Tabelle, die im vorherigen Schritt zurückgegeben wurde.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block ::/0 --egress-only-internet-gateway eigw-id
```

d. Ordnen Sie die Routing-Tabelle mithilfe des folgenden Befehls associate-route-table dem privatem Subnetz zu.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

6. Wenn Sie ein NAT-Gateway für Ihre Ressourcen in einem privaten Subnetz benötigen, gehen Sie wie folgt vor:

a. Erstellen Sie mit dem folgenden Befehl allocate-address eine elastische IP-Adresse für das NAT-Gateway.

```
aws ec2 allocate-address --domain vpc --query AllocationId --output text
```

b. Erstellen Sie das NAT-Gateway im öffentlichen Subnetz mit dem folgenden Befehl create-nat-gateway. Verwenden Sie die Zuordnungs-ID aus dem vorherigen Schritt.

```
aws ec2 create-nat-gateway --subnet-id subnet-id-public-subnet --allocation-
id eipalloc-id
```

c. (Optional) Wenn Sie in Schritt 5 bereits eine Routing-Tabelle für das private Subnetz erstellt haben, überspringen Sie diesen Schritt. Erstellen Sie andernfalls eine benutzerdefinierte Routing-Tabelle für Ihr privates Subnetz mit dem folgenden Befehl create-route-table. Der Befehl gibt die ID der neuen Routung-Tabelle zurück.

```
aws ec2 create-route-table --vpc-id vpc-1a2b3c4d5e6f1a2b3 --query
 RouteTable.RouteTableId --output text
```

d. Erstellen Sie mit dem folgenden Befehl create-route eine Route in der Routing-Tabelle für das private Subnetz, die den gesamten IPv4-Verkehr an das NAT-Gateway sendet. Verwenden Sie die ID der Routing-Tabelle für das private Subnetz, die Sie entweder in diesem Schritt oder in Schritt 5 erstellt haben.

```
aws ec2 create-route --route-table-id rtb-id-private --destination-cidr-
block 0.0.0.0/0 --gateway-id nat-id
```

e. (Optional) Wenn Sie in Schritt 5 bereits eine Routing-Tabelle für das private Subnetz zugeordnet haben, überspringen Sie diesen Schritt. Andernfalls ordnen Sie die Routing-Tabelle mithilfe des folgenden Befehls associate-route-table dem privatem Subnetz zu. Verwenden Sie die ID der Routing-Tabelle für das private Subnetz, die Sie entweder in diesem Schritt oder in Schritt 5 erstellt haben.

```
aws ec2 associate-route-table --route-table-id rtb-id-private --subnet-
id subnet-id-private-subnet
```

Konfigurieren Ihrer VPC

Mithilfe der folgenden Verfahren können Sie Virtual Private Clouds (VPC) erstellen und konfigurieren.

Aufgaben

- Anzeigen von Details zu Ihrer VPC
- Visualisierung der Ressourcen in Ihrer VPC
- Hinzufügen eines IP4-CIDR-Blocks zu Ihrer VPC
- Hinzufügen eines IPv6-CIDR-Blocks zu Ihrer VPC
- Entfernen Sie einen IPv4-CIDR-Block von Ihrer VPC
- Entfernen Sie einen IPv6-CIDR-Block von Ihrer VPC

Weitere Informationen zum Erstellen oder Löschen einer VPC finden Sie unter the section called “Erstellen einer VPC” oder the section called “Löschen der VPC”.

Anzeigen von Details zu Ihrer VPC

Führen Sie die folgenden Schritte aus, um die Details zu Ihren VPCs anzuzeigen.

So können Sie sich die VPC-Details mithilfe der Konsole anzeigen lassen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich VPCs aus.
3. Wählen Sie die VPC und dann Details anzeigen aus, um die Konfigurationsdetails Ihrer VPC anzuzeigen.

Um eine VPC mit dem zu beschreiben AWS CLI

Verwenden Sie den Befehl describe-vpcs.

So zeigen Sie alle VPCs in verschiedenen Regionen an

Öffnen Sie die Amazon EC2 Global View-Konsole unter https://console.aws.amazon.com/ec2globalview/home. Weitere Informationen finden Sie unter Ressourcen mithilfe von Amazon EC2 Global View auflisten und filtern im Amazon EC2 EC2-Benutzerhandbuch.

Visualisierung der Ressourcen in Ihrer VPC

Gehen Sie wie folgt vor, um eine visuelle Darstellung der Ressourcen in Ihrer VPC mithilfe der Registerkarte Ressourcenkarte anzuzeigen. Die folgenden Ressourcen sind in der Ressourcenkarte sichtbar:

- VPC
- Subnetze
  - Die Availability Zone wird durch einen Buchstaben dargestellt.
  - Öffentliche Subnetze sind grün.
  - Private Subnetze sind blau.
- Routing-Tabellen
- Internet-Gateways
- Internet-Gateways nur für ausgehenden Datenverkehr
- NAT gateways (NAT-Gateways)
- Gateway-Endpunkte (Amazon S3 und Amazon DynamoDB)

Die Ressourcenkarte zeigt die Beziehungen zwischen den Ressourcen innerhalb einer VPC und den Fluss des Datenverkehrs von Subnetzen zu NAT-Gateways, Internet-Gateways und Gateway-Endpunkten.

Sie können die Ressourcenkarte verwenden, um die Architektur einer VPC zu verstehen, um anzuzeigen, wie viele Subnetze sie enthält, welche Subnetze mit welchen Routing-Tabellen verknüpft sind und welche Routing-Tabellen Routen zu NAT-Gateways, Internet-Gateways und Gateway-Endpunkten haben.

Sie können die Ressourcenkarte auch verwenden, um unerwünschte oder falsche Konfigurationen zu erkennen, z. B. private Subnetze, die von NAT-Gateways getrennt sind, oder private Subnetze mit einer Route direkt zum Internet-Gateway. Sie können Ressourcen innerhalb der Ressourcenkarte auswählen, z. B. Routing-Tabellen, und die Konfigurationen für diese Ressourcen bearbeiten.

So zeigen Sie die Ressourcen in Ihrer VPC an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich VPCs aus.
3. Wählen Sie die VPC aus.
4. Wählen Sie die Registerkarte Ressourcenkarte aus, um eine Visualisierung der Ressourcen anzuzeigen.
5. Wählen Sie Details anzeigen, um zusätzlich zu den standardmäßig angezeigten Ressourcen-IDs und Zonen weitere Details anzuzeigen.

   - VPC: Die IPv4- und IPv6-CIDR-Bereiche, die der VPC zugewiesen sind.
   - Subnetze: Die IPv4- und IPv6-CIDR-Bereiche, die jedem Subnetz zugewiesen sind.
   - Routing-Tabellen: Die Subnetzzuordnungen und die Anzahl der Routen in der Routing-Tabelle.
   - Netzwerkverbindungen: Die Details zu den einzelnen Verbindungstypen:
     - Wenn in der VPC öffentliche Subnetze vorhanden sind, gibt es eine Internet-Gateway-Ressource mit der Anzahl der Routen sowie den Quell- und Ziel-Subnetzen für den Datenverkehr über das Internet-Gateway.
     - Wenn ein Internet-Gateway nur für ausgehenden Datenverkehr vorhanden ist, gibt es eine Internet-Gateway-Ressource nur für ausgehenden Datenverkehr. Dieser beinhaltet die Anzahl der Routen und den Quell- und Zielsubnetzen für den Datenverkehr, der das Internet-Gateway nur für ausgehenden Datenverkehr verwendet.

- Wenn ein NAT-Gateway vorhanden ist, gibt es eine NAT-Gateway-Ressource mit der Anzahl der Netzwerkschnittstellen und Elastic IP-Adressen für das NAT-Gateway.
- Wenn es einen Gateway-Endpunkt gibt, gibt es eine Gateway-Endpunktressource mit dem Namen des AWS Dienstes (Amazon S3 oder Amazon DynamoDB), zu der Sie über den Endpunkt eine Verbindung herstellen können.

6. Bewegen Sie den Mauszeiger über eine Ressource, um die Beziehung zwischen den Ressourcen anzuzeigen. Durchgezogene Linien stellen die Beziehungen zwischen Ressourcen dar. Gepunktete Linien stellen den Netzwerkverkehr zu Netzwerkverbindungen dar.

Hinzufügen eines IP4-CIDR-Blocks zu Ihrer VPC

Sie können Ihrer VPC standardmäßig bis zu fünf IPv4-CIDR-Blöcke hinzufügen, aber das Limit ist einstellbar. Weitere Informationen finden Sie unter Amazon VPC-Kontingente. Informationen zu Einschränkungen für IPv4-CIDR-Blöcke für eine VPC finden Sie unter VPC-CIDR-Blöcke.

Hinzufügen eines IPv4-CIDR-Blocks zu einer VPC unter Verwendung der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Wählen Sie die VPC und dann unter Actions (Aktionen) die Option Edit CIDRs (CIDRs bearbeiten) aus.
4. Wählen Sie Add new IPv4-CIDR (Neues IPv4-CIDR hinzufügen) aus.
5. Führen Sie für IPv4 CIDR block (IPv4-CIDR-Block) einen der folgenden Schritte aus:
   - Wählen Sie IPv4 CIDR manual input (Manuelle IPv4-CIDR-Eingabe) und geben Sie einen IPv4-CIDR-Block ein.
   - Wählen Sie IPAM-allocated IPv4 CIDR (IPAM-zugewiesene IPv4-CIDR) und wählen Sie ein CIDR aus einem IPv4-IPAM-Pool aus.
6. Wählen Sie Speichern und dann Schließen.
7. Nachdem Sie den benötigten IPv4-CIDR-Block hinzugefügt haben, können Sie Subnetze erstellen, die den neuen CIDR-Block verwenden. Weitere Informationen finden Sie unter Erstellen eines Subnetzes.

Um einen IPv4-CIDR-Block mit einer VPC zu verknüpfen, verwenden Sie AWS CLI

Verwenden Sie den Befehl associate-vpc-cidr-block.

Hinzufügen eines IPv6-CIDR-Blocks zu Ihrer VPC

Sie können Ihrer VPC standardmäßig bis zu fünf IPv6-CIDR-Blöcke hinzufügen, aber das Limit ist einstellbar. Weitere Informationen finden Sie unter Amazon VPC-Kontingente. Informationen zu Einschränkungen für IPv6-CIDR-Blöcke für eine VPC finden Sie unter VPC-CIDR-Blöcke.

Hinzufügen eines IPv6-CIDR-Blocks zu einer VPC unter Verwendung der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Wählen Sie die VPC und dann unter Actions (Aktionen) die Option Edit CIDRs (CIDRs bearbeiten) aus.
4. Wählen Sie Add new IPv6 CIDR (Neue IPv6 CIDR hinzufügen) aus.
5. Führen Sie für IPv6 CIDR block (IPv6-CIDR-Block) einen der folgenden Schritte aus:

   - Wählen Sie IPAM-zugewiesener IPv6-CIDR-Block, wenn Sie Amazon VPC IP Address Manager verwenden und ein IPv6-CIDR aus einem IPAM-Pool bereitstellen möchten. Sie haben zwei Möglichkeiten, der VPC einen IP-Adressbereich unter dem CIDR-Block bereitzustellen:
     - Netzmaskenlänge: Wählen Sie diese Option, um eine Netzmaskenlänge für den CIDR auszuwählen. Führen Sie eine der folgenden Aktionen aus:
       - Wenn für den IPAM-Pool eine Standard-Netzmaskenlänge ausgewählt wurde, können Sie die Standardlänge der IPAM-Netzmaske wählen, um die vom IPAM-Administrator für den IPAM-Pool festgelegte Standard-Netzmaskenlänge zu verwenden. Weitere Informationen zur optionalen Standardregel für die Zuweisung von Netzmaskenlänge finden Sie unter Erstellen eines regionalen IPv6-Pools im Amazon-VPC-IPAM-Benutzerhandbuch.
       - Wenn keine Standard-Netzmaskenlänge für den IPAM-Pool ausgewählt wurde, wählen Sie eine Netzmaskenlänge, die spezifischer ist als die Netzmaskenlänge des IPAM-Pool-CIDR. Wenn der IPAM-Pool-CIDR beispielsweise /50 ist, können Sie für die VPC eine Netzmaskenlänge zwischen /52 und /60 wählen. Mögliche Netzmaskenlängen liegen zwischen /44 und /60 in Schritten von /4.
     - Einen CIDR wählen: Wählen Sie diese Option, um eine IPv6-Adresse manuell einzugeben. Sie können nur eine Netzmaskenlänge wählen, die spezifischer als die Netzmaskenlänge des IPAM-Pool-CIDR ist. Wenn der IPAM-Pool-CIDR beispielsweise /50 ist, können Sie für die VPC eine Netzmaskenlänge zwischen /52 und /60 wählen. Mögliche IPv6-Netzmaskenlängen liegen zwischen /44 und /60 in Schritten von /4.

- Wählen Sie von Von Amazon bereitgestellter IPv6-CIDR-Block aus, um einen IPv6-CIDR-Block aus dem IPv6-Adresspool von Amazon anzufordern. Wählen Sie für Network Border Group die Gruppe aus, aus der IP-Adressen bekannt gegeben werden AWS . Amazon bietet eine feste IPv6-CIDR-Blockgröße von /56.
- Wählen Sie IPv6-CIDR im Besitz von mir) aus, um ein IPv6-CIDR bereitzustellen, das Sie bereits in AWS eingebunden haben. Weitere Informationen zum Herstellen eigener IP-Adressbereiche finden Sie unter Bring your own IP Addresses (BYOIP) in Amazon EC2 im Amazon EC2 EC2-Benutzerhandbuch. AWS Sie haben zwei Möglichkeiten, der VPC einen IP-Adressbereich unter dem CIDR-Block bereitzustellen:
  - Keine Präferenz: Wählen Sie diese Option, um die Netzmaskenlänge /56 zu verwenden.
  - CIDR auswählen: Wählen Sie diese Option, um eine IPv6-Adresse manuell einzugeben und eine Netzmaskenlänge zu wählen, die spezifischer ist als die Größe des BYOIP-CIDR. Wenn der BYOIP-Pool-CIDR beispielsweise /50 ist, können Sie für die VPC eine Netzmaskenlänge zwischen /52 und /60 wählen. Mögliche IPv6-Netzmaskenlängen liegen zwischen /44 und /60 in Schritten von /4.

6. Wählen Sie CIDR auswählen und dann Schließen aus.
7. Nachdem Sie einen IPv6-CIDR-Block hinzugefügt haben, können Sie Subnetze erstellen, die den neuen CIDR-Block verwenden. Weitere Informationen finden Sie unter Erstellen eines Subnetzes.

Um einen IPv6-CIDR-Block mit einer VPC zu verknüpfen, verwenden Sie AWS CLI

Verwenden Sie den Befehl associate-vpc-cidr-block.

Entfernen Sie einen IPv4-CIDR-Block von Ihrer VPC

Wenn Ihrer VPC mehrere IPv4-CIDR-Blöcke zugeordnet sind, können Sie einen IPv4-CIDR-Blocks von der VPC entfernen. Es ist nicht möglich, den primären IPv4-CIDR-Blocks zu entfernen. Sie können nur einen vollständigen CIDR-Blocks entfernen. Es ist nicht möglich, die Zuordnung einer Untermenge eines CIDR-Blocks oder eines kombinierten CIDR-Blockbereichs aufzuheben. Sie müssen zuerst alle Subnetze in dem CIDR-Block löschen.

Einen CIDR-Block aus einer VPC mithilfe der Konsole entfernen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.

3. Wählen Sie die VPC und unter Actions die Option Edit CIDRs aus.
4. Entfernen Sie unter VPC-IPv4-CIDRs den CIDR, indem Sie Entfernen wählen.
5. Klicken Sie auf Schließen.

Um einen IPv4-CIDR-Block von einer VPC zu trennen, verwenden Sie den AWS CLI

Verwenden Sie den Befehl disassociate-vpc-cidr-block.

Entfernen Sie einen IPv6-CIDR-Block von Ihrer VPC

Wenn Sie IPv6 in Ihrer VPC nicht mehr unterstützen möchten, die VPC aber weiterhin für die Erstellung von IPv4-Ressourcen und für die Kommunikation mit ihnen verwenden möchten, können Sie den IPv6-CIDR-Blocks entfernen.

Um den IPv6-Blocks zu entfernen, müssen Sie zunächst die Zuordnung aller IPv6-Adressen zu Instances in Ihrem Subnetz aufheben.

Durch die Entfernung eines IPv6-CIDR-Blocks werden die Sicherheitsgruppenregeln, Netzwerk-ACL-Regeln oder Routen der Routing-Tabelle, die Sie für das IPv6-Netzwerk konfiguriert haben, nicht automatisch gelöscht. Sie müssen diese Regeln oder Routen manuell ändern oder löschen.

Einen IPv6-CIDR-Block aus einer VPC mithilfe der Konsole entfernen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Wählen Sie Ihre VPC und unter Actions die Option Edit CIDRs aus.
4. Entfernen Sie unter IPv6-CIDRs den IPv6-CIDR, indem Sie Entfernen wählen.
5. Klicken Sie auf Schließen.

Um einen IPv6-CIDR-Block von einer VPC zu trennen, verwenden Sie AWS CLI

Verwenden Sie den Befehl disassociate-vpc-cidr-block.

DHCP-Optionssätze in Amazon VPC

Netzwerkgeräte in Ihrer VPC verwenden das Dynamic Host Configuration Protocol (DHCP). Sie können DHCP-Optionssätze verwenden, um die folgenden Aspekte der Netzwerkkonfiguration in Ihrem virtuellen Netzwerk zu steuern:

- Die DNS-Server, Domain-Namen oder NTP-Server (Network Time Protocol), die von den Geräten in Ihrer VPC verwendet werden.
- Ob die DNS-Auflösung in Ihrer VPC aktiviert ist.

Inhalt

Was ist DHCP?

Jedes Gerät in einem TCP/IP-Netzwerk benötigt eine IP-Adresse, um m Netzwerk kommunizieren zu können. In der Vergangenheit mussten IP-Adressen den einzelnen Geräten im Netzwerk manuell zugewiesen werden. Heute werden IP-Adressen dynamisch von DHCP-Servern mithilfe des Dynamic Host Configuration Protocol (DHCP) zugewiesen.

Anwendungen, die auf EC2-Instances ausgeführt werden, können bei Bedarf mit Amazon-DHCP-Servern kommunizieren, um ihren IP-Adresslease oder andere Netzwerkkonfigurationsinformationen (z. B. die IP-Adresse eines Amazon-DNS-Servers oder die IP-Adresse des Routers in Ihrer VPC) abzurufen.

Sie können die Netzwerkkonfigurationen, die von Amazon-DHCP-Servern bereitgestellt werden, mit Hilfe von DHCP-Optionssätzen festlegen.

Wenn Sie über eine VPC-Konfiguration verfügen, bei der Ihre Anwendungen direkte Anfragen an den Amazon-IPv6-DHCP-Server stellen müssen, beachten Sie Folgendes:

- Eine EC2-Instance in einem Dual-Stack-Subnetz kann die eigene IPv6-Adresse nur vom IPv6-DHCP-Server abrufen. Zusätzliche Netzwerkkonfigurationen wie DNS-Servernamen oder Domänennamen kann sie hingegen nicht vom IPv6-DHCP-Server abrufen.
- Eine EC2-Instance in einem reinen IPv6-Subnetz kann die eigene IPv6-Adresse und kann zusätzliche Informationen zur Netzwerkkonfiguration wie DNS-Servernamen und Domänennamen vom IPv6-DHCP-Server abrufen.
- Für eine EC2-Instance in einem reinen IPv6-Subnetz gibt der IPv4-DHCP-Server 169.254.169.253 als Nameserver zurück, wenn „DNS“ ausdrücklich im DHCP-Optionssatz erwähnt wird. AmazonProvided Wenn "AmazonProvidedDNS“ im Optionssatz fehlt, gibt der IPv4-DHCP-Server

keine Adresse zurück, unabhängig davon, ob andere IPv4-Nameserver im Optionssatz erwähnt werden oder nicht.

Die Amazon DHCP-Server können auch ein vollständiges IPv4- oder IPv6-Präfix für eine Netzwerkschnittstelle in Ihrer VPC mithilfe der Präfix-Delegierung bereitstellen (siehe Zuweisen von Präfixen zu Amazon EC2 EC2-Netzwerkschnittstellen im Amazon EC2 EC2-Benutzerhandbuch). Die IPv4-Präfix-Delegation ist in DHCP-Antworten nicht vorgesehen. IPv4-Präfixe, die der Schnittstelle zugewiesen wurden, können mithilfe von IMDS abgerufen werden (siehe Kategorien von Instance-Metadaten im Amazon EC2 EC2-Benutzerhandbuch).

DHCP-Optionssatzkonzepte

Ein DHCP-Optionssatz ist eine Gruppe von Netzwerkeinstellungen, die von Ressourcen in Ihrer VPC, z. B. EC2-Instances, zur Kommunikation über Ihr virtuelles Netzwerk verwendet werden.

In jeder Region gibt es Standard-DHCP-Optionssatz. Jede VPC verwendet den standardmäßigen DHCP-Optionssatz für ihre Region, sofern Sie nicht entweder einen benutzerdefinierten DHCP-Optionssatz erstellen und der VPC zuweisen oder die VPC ohne DHCP-Optionssatz konfigurieren.

Wenn für Ihre VPC kein DHCP-Optionssatz konfiguriert ist:

- AWS Wird für EC2-Instances, die auf dem Nitro-System basieren, `169.254.169.253` als Standard-Domain-Namenserver konfiguriert.
- Für EC2-Instances, die auf Xen basieren, werden keine Domainnamenserver konfiguriert, und da Instances in der VPC keinen Zugriff auf einen DNS-Server haben, können sie auch nicht auf das Internet zugreifen.

Sie können einen DHCP-Optionssatz mehreren VPCs zuweisen, aber jeder VPC kann nur einen zugewiesenen DHCP-Optionssatz haben.

Wenn Sie eine VPC löschen, wird die Zuordnung des der VPC zugewiesenen DHCP-Optionssatzes aufgehoben.

Inhalt

Standardmäßiger DHCP-Optionssatz

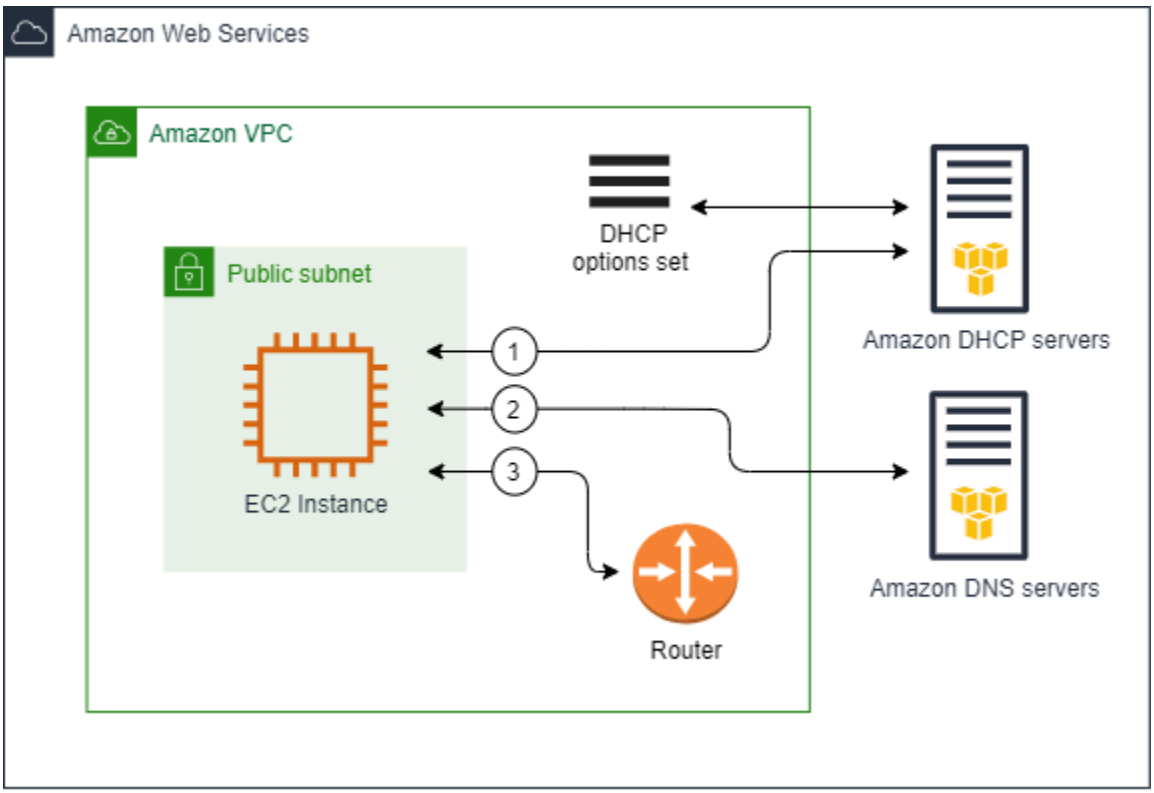
Der Standard-DHCP-Optionssatz enthält die folgenden Einstellungen:

- Domain-Namenserver: Die DNS-Server, die die Netzwerkschnittstellen zur Auflösung von Domain-Namen verwenden. Für einen standardmäßigen DHCP-Optionssatz ist dies immer `AmazonProvidedDNS`. Weitere Informationen finden Sie unter Amazon DNS-Server.
- Domain-Name: Der Domain-Name, den ein Client beim Auflösen von Hostnamen über das Domain Name System (DNS) verwenden sollte. Weitere Informationen zu den für EC2-Instances verwendeten Domain-Namen finden Sie unter Amazon-EC2-Instance-Hostnamen.
- IPv6-Preferred Lease Time: Wie oft eine laufende Instance, der ein IPv6 zugewiesen ist, eine DHCPv6-Lease-Verlängerung durchläuft. Die Standard-Leasingzeit beträgt 140 Sekunden. Die Leasingverlängerung erfolgt in der Regel, wenn die Hälfte der Leasingdauer abgelaufen ist.

Wenn Sie einen standardmäßigen DHCP-Optionssatz verwenden, werden die folgenden Einstellungen nicht verwendet, es gibt jedoch Standardwerte für EC2-Instances:

- NTP-Server: Standardmäßig verwenden EC2-Instances den Amazon Time Sync Service, um die Zeit abrufen.
- NetBIOS-Namenserver: Bei EC2-Instances, die Windows ausführen, ist der NetBIOS-Computername ein Anzeigename, der der Instance zur Identifizierung im Netzwerk zugewiesen wird. Der NetBIOS-Namenserver verwaltet für Netzwerke, in denen NetBIOS als Benennungsdienst genutzt wird, eine Liste von Zuordnungen zwischen NetBIOS-Computernamen und Netzwerkadressen.
- NetBIOS-Knotentyp: Bei EC2-Instances, die Windows ausführen, handelt es sich hierbei um die Methode, mit deren Hilfe sie NetBIOS-Namen in IP-Adressen auflösen.

Wenn Sie den Standardoptionssatz verwenden, verwendet der Amazon-DHCP-Server die Netzwerkeinstellungen im Standardoptionssatz. Wenn Sie Instances in Ihrer VPC starten, tun sie Folgendes, wie im Diagramm dargestellt: (1) Sie interagieren mit dem DHCP-Server, (2) sie interagieren mit dem Amazon-DNS-Server und (3) sie stellen über den Router für Ihre VPC eine Verbindung zu anderen Geräten im Netzwerk her. Die Instances können jedoch jederzeit mit dem Amazon-DHCP-Server interagieren, um die temporär zugeteilte IP-Adresse und die zusätzlichen Netzwerkeinstellungen zu erhalten.



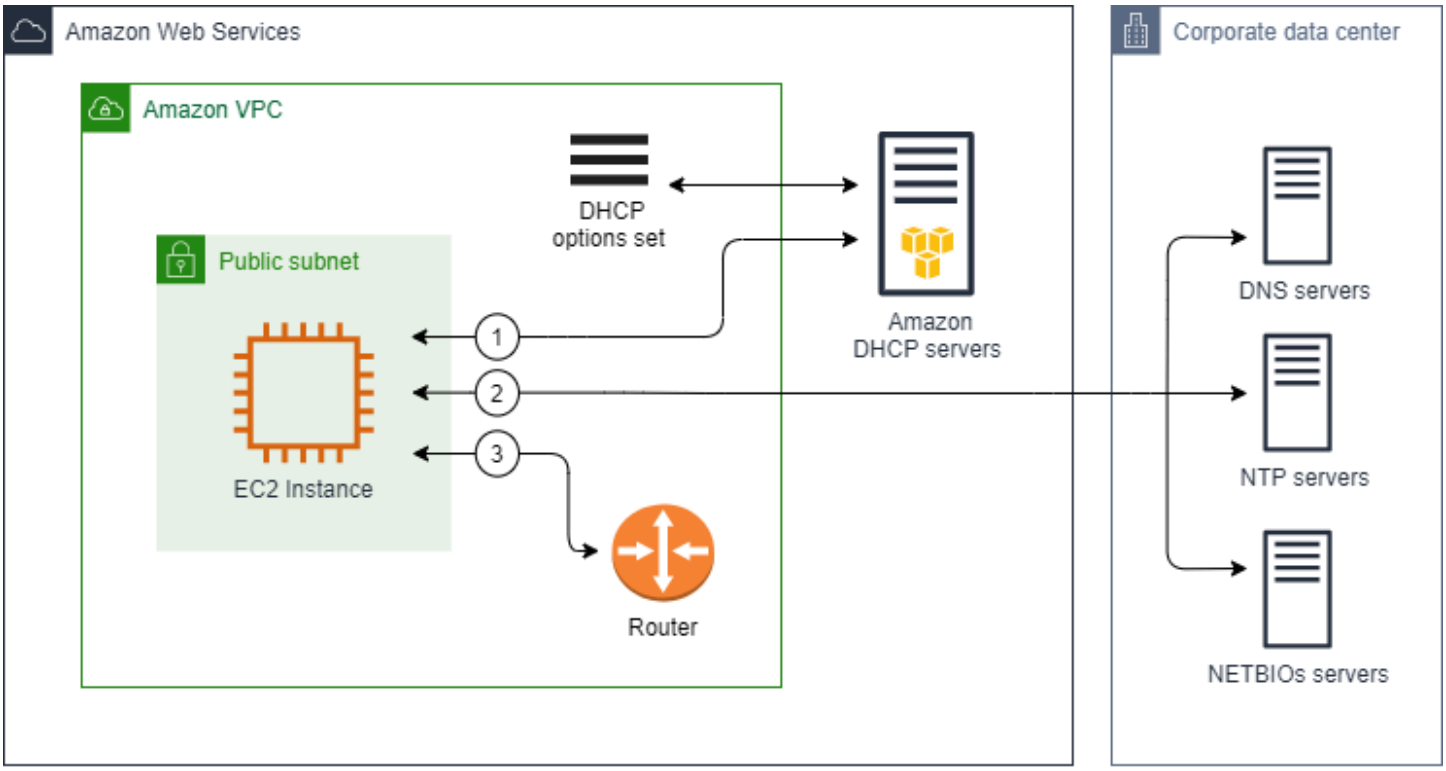
Benutzerdefinierter DHCP-Optionssatz

Sie können einen benutzerdefinierten DHCP-Optionssatz mit den folgenden Einstellungen erstellen und ihn dann einer VPC zuweisen:

- Domain-Namenserver: Die DNS-Server, die die Netzwerkschnittstellen zur Auflösung von Domain-Namen verwenden.
- Domain-Name: Der Domain-Name, den ein Client beim Auflösen von Hostnamen über das Domain Name System (DNS) verwendet.
- NTP-Server: Die NTP-Server, die die Zeit für die Instances bereitstellen.
- NetBIOS-Namenserver: Bei EC2-Instances, die Windows ausführen, ist der NetBIOS-Computername ein Anzeigename, der der Instance zur Identifizierung im Netzwerk zugewiesen wird. Ein NetBIOS-Namenserver verwaltet für Netzwerke, in denen NetBIOS als Benennungsdienst genutzt wird, eine Liste von Zuordnungen zwischen NetBIOS-Computernamen und Netzwerkadressen.
- NetBIOS-Knotentyp: Bei EC2-Instances, die Windows ausführen, handelt es sich hierbei um die Methode, mit deren Hilfe sie NetBIOS-Namen in IP-Adressen auflösen.
- Bevorzugte IPv6-Lease-Zeit (optional): Ein Wert (in Sekunden, Minuten, Stunden oder Jahren), der angibt, wie oft eine laufende Instance, der ein IPv6 zugewiesen ist, eine DHCPv6-Lease-

Verlängerung durchläuft. Zulässige Werte liegen zwischen 140 und 4294967295 Sekunden (ungefähr 138 Jahre). Wenn kein Wert eingegeben wird, beträgt die Standard-Leasingzeit 140 Sekunden. Wenn Sie die langfristige Adressierung für EC2-Instances verwenden, können Sie die Leasingdauer verlängern und häufige Anfragen zur Leasingverlängerung vermeiden. Die Leasingverlängerung erfolgt in der Regel, wenn die Hälfte der Leasingdauer abgelaufen ist.

Wenn Sie einen benutzerdefinierten Optionssatz verwenden, führen Instances, die in Ihrer VPC gestartet werden, die folgenden Aktionen aus, wie im Diagramm dargestellt: (1) Sie verwenden die Netzwerkeinstellungen im benutzerdefinierten DHCP-Optionssatz, (2) sie interagieren mit den DNS-, NTP- und NetBIOS-Servern, die im benutzerdefinierten DHCP-Optionssatz angegeben sind, und (3) sie stellen über den Router für Ihre VPC eine Verbindung zu anderen Geräten im Netzwerk her.



Verwandte Aufgaben

- Erstellen eines DHCP-Optionssatzes
- Ändern Sie den Optionssatz, der einer VPC zugeordnet ist

Arbeiten mit DHCP-Optionslisten

Gehen Sie wie folgt vor, um DHCP-Optionssätze anzuzeigen und mit ihnen zu arbeiten. Weitere Informationen zur Funktionsweise der DHCP-Optionssätze finden Sie unter the section called “DHCP-Optionssatzkonzepte”.

Aufgaben

- Ihre DHCP-Optionssätze anzeigen
- Erstellen eines DHCP-Optionssatzes
- Ändern Sie den Optionssatz, der einer VPC zugeordnet ist
- Löschen eines DHCP-Optionssatzes

Ihre DHCP-Optionssätze anzeigen

Sie können Ihre DHCP-Optionssätze wie folgt anzeigen. Bei einem standardmäßigen DHCP-Optionssatz sind die einzigen Einstellungen mit Werten Domain-Name und Domain-Namenserver.

So zeigen Sie Ihre DHCP-Optionssätze mit der Konsole an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich DHCP option sets (DHCP-Optionslisten) aus.
3. Wählen Sie die ID eines DHCP-Optionssatzes aus, um dessen Detailseite zu öffnen.

So zeigen Sie Ihre DHCP-Optionssätze mit der Befehlszeile an

Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Arbeiten mit Amazon VPC.

- describe-dhcp-options (AWS CLI)
- Get-EC2DhcpOption (AWS Tools for Windows PowerShell)

Erstellen eines DHCP-Optionssatzes

Ein benutzerdefinierter DHCP-Optionssatz ermöglicht es Ihnen, Ihre VPC u. a. mit einem eigenen DNS-Server und einem eigenen Domänennamen anzupassen. Sie können so viele zusätzliche DHCP-Optionssätze erstellen, wie Sie möchten. Sie können einer VPC jedoch immer nur einen DHCP-Optionssatz zuweisen.

> **Note**
>
> Nach dem Erstellen eines DHCP-Optionssatzes sind daran keine Änderungen mehr möglich. Um die DHCP-Optionen für Ihre VPC zu aktualisieren, müssen Sie einen neuen DHCP-Optionssatz erstellen und diesen dann Ihrer VPC zuweisen.

So erstellen Sie einen DHCP-Optionssatz mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich DHCP option sets (DHCP-Optionslisten) aus.
3. Wählen Sie Create DHCP Options Set (DHCP-Optionsliste erstellen).
4. Geben Sie für Markierungseinstellungen optional einen Namen für den DHCP-Optionssatz ein. Wenn Sie einen Wert eingeben, wird automatisch ein Namens-Tag für den DHCP-Optionsssatz erstellt.
5. Geben Sie für DHCP-Optionen die benötigten Konfigurationseinstellungen an.

   - Domain name (Domänenname) (optional): Geben Sie den Domänenname ein, den ein Client beim Auflösen von Hostnamen über das Domänennamensystem verwenden sollte. Wenn Sie kein AmazonProvided DNS verwenden, müssen Ihre benutzerdefinierten Domainnamenserver den Hostnamen entsprechend auflösen. Wenn Sie eine private gehostete Zone von Amazon Route 53 verwenden, können Sie AmazonProvided DNS verwenden. Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC.

     Einige Linux-Betriebssysteme akzeptieren mehrere Domänennamen, die durch Leerzeichen getrennt sind. Windows und andere Linux-Betriebssysteme behandeln den Wert jedoch als eine einzelne Domäne, was zu unerwartetem Verhalten führt. Wenn Ihr DHCP-Optionssatz mit einer VPC verknüpft ist, deren Instances Betriebssysteme ausführen, die den Wert als einzelne Domäne behandeln, geben Sie nur einen Domänennamen an.
   - Domain name servers (Domänennamenserver) (optional): Geben Sie den DNS-Server ein, mit deren Hilfe die IP-Adresse eines Hosts anhand seines Namens aufgelöst wird.

     Sie können entweder **`AmazonProvidedDNS`** oder benutzerdefinierte Domänennamenserver eingeben. Wenn Sie beides verwenden, kann es zu unerwartetem Verhalten kommen. Sie können die IP-Adressen von bis zu vier IPv4-Domänennamenservern (oder bis zu drei IPv4-Domänennamenservern und **`AmazonProvidedDNS`**) und von bis zu vier IPv6-Domänennamenservern eingeben, jeweils getrennt durch Kommata. Obwohl Sie bis zu

acht Domänennamenserver angeben können, können einige Betriebssysteme niedrigere Grenzwerte festlegen. Weitere Informationen zu AmazonProvidedDNS und dem Amazon DNS-Server finden Sie unterAmazon DNS-Server.

> **Important**
>
> Wenn Ihre VPC über ein Internet-Gateway verfügt, stellen Sie sicher, dass Sie Ihren eigenen DNS-Server oder einen Amazon DNS-Server (AmazonProvidedDNS) für den Wert Domain Name Servers angeben. Andernfalls können die Instances in der VPC nicht auf DNS zugreifen, wodurch der Internetzugang deaktiviert wird.

- NTP servers (NTP-Server) (optional): Geben Sie die IP-Adressen von bis zu acht NTP-Servern (Network Time Protocol) ein (vier IPv4-Adressen und vier IPv6-Adressen).

  NTP-Server stellen die Zeit in Ihrem Netzwerk bereit. Sie können den Amazon Time Sync Service unter der IPv4-Adresse `169.254.169.123` angeben oder unter der IPv6-Adresse `fd00:ec2::123` angeben. Instanzen kommunizieren standardmäßig mit dem Amazon Time Sync Service. Beachten Sie, dass auf die IPv6-Adresse nur auf EC2-Instances zugegriffen werden kann, die auf dem Nitro-System aufgebaut sind.

  Weitere Informationen zur Option „NTP servers“ (NTP-Server) finden Sie unter RFC 2132. Weitere Informationen zum Amazon Time Sync Service finden Sie unter Zeit für Ihre Instance festlegen im Amazon EC2 EC2-Benutzerhandbuch.
- NetBIOS name servers (NetBIOS-Namenserver) (optional): Geben Sie die IP-Adressen von bis zu vier NetBIOS-Namenservern ein.

  Bei EC2-Instances, die ein Windows Betriebssystem ausführen, ist der NetBIOS-Computername ein Anzeigename, der der Instance zur Identifizierung im Netzwerk zugewiesen wird. Der NetBIOS-Namenserver verwaltet für Netzwerke, in denen NetBIOS als Benennungsdienst genutzt wird, eine Liste von Zuordnungen zwischen NetBIOS-Computernamen und Netzwerkadressen.
- NetBIOS node type (NetBIOS-Knotentyp) (optional): Geben Sie **1**, **2**, **4**, oder **8** ein. Wir empfehlen, dass Sie einen **2** (point-to-point oder P-Node) angeben. Broadcast und Multicast werden derzeit nicht unterstützt. Weitere Informationen über diese Knotentypen finden Sie in Abschnitt 8.7 von RFC 2132 und Abschnitt 10 von RFC1001.

Bei EC2-Instances, die ein Windows Betriebssystem ausführen, handelt es sich hierbei um die Methode, mit deren Hilfe sie NetBIOS-Namen in IP-Adressen auflösen. Im Standardoptionssatz gib es keinen Wert für den NetBIOS-Knotentyp.

- IPv6 Preferred Lease Time (optional): Ein Wert (in Sekunden, Minuten, Stunden oder Jahren), der angibt, wie oft eine laufende Instance, der ein IPv6 zugewiesen ist, eine DHCPv6-Lease-Verlängerung durchläuft. Zulässige Werte liegen zwischen 140 und 2147483647 Sekunden (ungefähr 68 Jahre). Wenn kein Wert eingegeben wird, beträgt die Standard-Leasingzeit 140 Sekunden. Wenn Sie die langfristige Adressierung für EC2-Instances verwenden, können Sie die Leasingdauer verlängern und häufige Anfragen zur Leasingverlängerung vermeiden. Die Leasingverlängerung erfolgt in der Regel, wenn die Hälfte der Leasingdauer abgelaufen ist.

6. Fügen Sie Tags (Tags) hinzu.
7. Wählen Sie Create DHCP Options Set (DHCP-Optionsliste erstellen). Notieren Sie sich den Namen oder die ID des neuen DHCP-Optionssatzes.
8. Um Ihre VPC so zu konfigurieren, dass der neue Optionssatz verwendet wird, lesen Sie Ändern Sie den Optionssatz, der einer VPC zugeordnet ist.

So erstellen Sie einen DHCP-Optionssatz für Ihre VPC über die Befehlszeile

Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Arbeiten mit Amazon VPC.

- create-dhcp-options (AWS CLI)
- New-EC2DhcpOption (AWS Tools for Windows PowerShell)

Ändern Sie den Optionssatz, der einer VPC zugeordnet ist

Nachdem Sie einen DHCP-Optionssatz erstellt haben, können Sie ihn einer oder mehreren VPCs zuweisen. Sie können einer VPC jedoch immer nur einen DHCP-Optionssatz zuweisen. Wenn Sie einer VPC keinen DHCP-Optionssatz zuordnen, wird dadurch die Domain-Namenauflösung in der VPC deaktiviert.

Wenn Sie der VPC einen neuen DHCP-Optionssatz zuweisen, verwenden alle vorhandenen Instances sowie alle neuen Instances, die Sie in dieser VPC starten, die neuen Optionen. Sie müssen Ihre Instances nicht neu starten. Instances übernehmen die Änderungen automatisch innerhalb weniger Stunden, je nachdem, wie oft sie ihre DHCP-Leases erneuern. Wenn Sie möchten, können Sie die Lease mithilfe des Betriebssystems der Instance ausdrücklich erneuern.

So ändern Sie den der VPC zugewiesenen DHCP-Optionssatz mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Aktivieren Sie das Kontrollkästchen für die VPC und wählen Sie dann Actions (Aktionen), Edit VPC settings (VPC-Einstellungen bearbeiten).
4. Wählen Sie für DHCP options set (DHCP-Optionssatz) einen neuen DHCP-Optionssatz aus. Wählen Sie alternativ die Option Kein DHCP-Optionssatz, um die Domain-Namenauflösung für die VPC zu deaktivieren.
5. Wählen Sie Speichern.

So ändern Sie den der VPC zugewiesenen DHCP-Optionssatz mithilfe der Befehlszeile

Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Arbeiten mit Amazon VPC.

- associate-dhcp-options (AWS CLI)
- Register-EC2DhcpOption (AWS Tools for Windows PowerShell)

Löschen eines DHCP-Optionssatzes

Wenn Sie einen DHCP-Optionssatz nicht mehr benötigen, können Sie ihn mit dem folgenden Verfahren löschen. Sie können einen DHCP-Optionssatz nicht löschen, wenn er verwendet wird. Für jede VPC, die dem zu löschenden DHCP-Optionssatz zugeordnet ist, müssen Sie der VPC einen anderen DHCP-Optionssatz zuweisen oder die VPC so konfigurieren, dass kein DHCP-Optionssatz verwendet wird. Weitere Informationen finden Sie unter the section called “Ändern Sie den Optionssatz, der einer VPC zugeordnet ist”.

So löschen Sie einen DHCP-Optionssatz mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich DHCP option sets (DHCP-Optionslisten) aus.
3. Wählen Sie das Optionsfeld für den DHCP-Optionssatz und wählen Sie dann Aktionen, DHCP-Optionssatz löschen.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann DHCP-Optionssatz löschen.

So löschen Sie einen DHCP-Optionssatz mithilfe der Befehlszeile

Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Arbeiten mit Amazon VPC.

- delete-dhcp-options (AWS CLI)
- Remove-EC2DhcpOption (AWS Tools for Windows PowerShell)

DNS-Attribute für Ihre VPC

Domain Name System (DNS) ist ein Standard, nach dem Namen, die im Internet verwendet werden, entsprechend der zugehörigen IP-Adressen aufgelöst werden. Ein DNS-Hostname ist ein eindeutiger, absoluter Name für einen Computer. Er besteht aus einem Hostnamen und einem Domainnamen. DNS-Server lösen DNS-Hostnamen zu den entsprechenden IP-Adressen auf.

Öffentliche IPv4-Adressen ermöglichen die Kommunikation über das Internet, private IPv4-Adressen sind dagegen für die Kommunikation von Instances innerhalb eines Netzwerks zuständig. Weitere Informationen finden Sie unter IP-Adressierung für Ihre VPCs und Subnetze.

Amazon stellt einen DNS-Server (den Amazon Route 53 Resolver) für Ihre VPC zur Verfügung. Wenn Sie einen eigenen DNS-Server verwenden möchten, erstellen Sie stattdessen eine neue DHCP-Optionsgruppe für Ihre VPC. Weitere Informationen finden Sie unter DHCP-Optionssätze in Amazon VPC.

Inhalt

Amazon DNS-Server

Der Route 53 Resolver (auch „Amazon DNS-Server“ oder „AmazonProvidedDNS“ genannt) ist ein DNS-Resolver-Service, der in jede Availability Zone in einer AWS Region integriert ist. Der Route 53 Resolver befindet sich unter `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) und im primären privaten IPV4-CIDR-Bereich, der Ihrer VPC plus zwei bereitgestellt wird. Wenn Sie beispielsweise über eine VPC mit einem IPv4-CIDR von `10.0.0.0/16` und einem IPv6-CIDR von `fd00:ec2::253` verfügen, können Sie den Route 53 Resolver unter `169.254.169.253` (IPv4), `fd00:ec2::253` (IPv6) oder `10.0.0.2` (IPv4) erreichen. Ressourcen innerhalb einer VPC verwenden eine lokale Linkadresse für DNS-Abfragen. Diese Abfragen werden privat an den Route 53 Resolver übertragen und sind im Netzwerk nicht sichtbar. In einem reinen IPv6-Subnetz ist die link-lokale IPv4-Adresse (169.254.169.253) immer noch erreichbar, solange „DNS“ der Nameserver im DHCP-Optionssatz ist. AmazonProvided

Wenn Sie eine Instance in eine VPC starten, stellen wir der Instance einen privaten DNS-Hostnamen bereit. Wenn die Instance mit einer öffentlichen IPv4-Adresse konfiguriert ist und die VPC-DNS-Attribute aktiviert sind, stellen wir auch einen öffentlichen DNS-Hostnamen bereit.

Das Format des privaten DNS-Hostnamens hängt davon ab, wie Sie die EC2-Instance beim Start konfigurieren. Weitere Informationen zu den Typen privater DNS-Hostnamen finden Sie unter EC2 instance naming (EC2-Instance-Benennung).

Der Amazon DNS-Server in Ihrer VPC wird dazu verwendet, die DNS-Domain-Namen, die Sie in einer privaten gehosteten Zone in Route 53 angeben, aufzulösen. Weitere Informationen über private gehostete Zonen finden Sie unter Arbeiten mit privat gehosteten Zonen im Amazon-Route-53-Entwicklerhandbuch.

Regeln und Überlegungen

Bei der Verwendung des Amazon DNS-Servers gelten folgende Regeln und Überlegungen.

- Sie können den Datenverkehr von und zu dem Amazon DNS-Server nicht mit Netzwerk-ACLs oder Sicherheitsgruppen filtern.
- Services, die das Hadoop-Framework verwenden, wie beispielsweise Amazon EMR, machen es erforderlich, dass Instances ihre eigenen vollständig qualifizierten Domain-Namen (FQDNs) auflösen. In diesen Fällen kann die DNS-Auflösung fehlschlagen, wenn für die `domain-name-servers`-Option ein benutzerdefinierter Wert angegeben wird. Um eine ordnungsgemäße DNS-Auflösung sicherzustellen, sollten Sie das Hinzufügen einer bedingten Weiterleitung

auf Ihrem DNS-Server erwägen. Auf diese Weise können Abfragen für die Domain *region-name*.compute.internal an den Amazon DNS-Server weitergeleitet werden. Weitere Informationen finden Sie unter Einrichten einer VPC zum Hosten von Clustern im Amazon EMR-Managementhandbuch.

- Der Amazon Route 53 Resolver unterstützt nur rekursive DNS-Abfragen.

DNS-Hostnamen

Beim Start einer Instance erhält sie immer eine private IPv4-Adresse und einen privaten DNS-Hostnamen, der ihrer privaten IPv4-Adresse entspricht. Wenn Ihre Instance über eine öffentliche IPv4-Adresse verfügt, bestimmen die DNS-Attribute für ihre VPC, ob sie einen öffentlichen DNS-Hostnamen erhält, der der öffentlichen IPv4-Adresse entspricht. Weitere Informationen finden Sie unter DNS-Attribute in Ihrer VPC.

Wenn der von Amazon bereitgestellte DNS-Server aktiviert ist, werden DNS-Hostnamen wie folgt zugewiesen und aufgelöst.

Privater IP-DNS-Name (nur IPv4)

Sie können den Hostnamen für den privaten IP-DNS-Namen (nur IPv4) zur Kommunikation zwischen Instances im selben VPC verwenden. Sie können die privaten IP-DNS-Namen (nur IPv4) Hostnamen anderer Instances in anderen VPCs auflösen, solange sich die Instances in derselben AWS Region befinden und der Hostname der anderen Instance im privaten Adressraumbereich liegt, der durch RFC 1918: `10.0.0.0 - 10.255.255.255 (10/8 prefix)172.16.0.0 - 172.31.255.255 (172.16/12 prefix)`, und definiert ist`192.168.0.0 - 192.168.255.255 (192.168/16 prefix)`.

DNS-Name für private Ressourcen

Der RBN-basierte DNS-Name, der in die für diese Instance ausgewählten A- und AAAA-DNS-Datensätze aufgelöst werden kann. Dieser DNS-Hostname ist in den Instancedetails für Instances in Dual-Stack- und IPv6-only Subnetzen sichtbar. Weitere Informationen zu RBN finden Sie unter EC2 instance hostname types (EC2-Instance-Hostnamentypen).

Öffentliche IPv4-DNS

Ein öffentlicher (externer) IPv4-DNS-Hostname erhält das Format `ec2-`*`public-ipv4-address`*`.compute-1.amazonaws.com` für die Region `us-east-1` und das Format `ec2-`*`public-ipv4-address.region`*`.compute.amazonaws.com` für andere Regionen. Der Amazon DNS-

Server löst den öffentlichen DNS-Hostnamen zur öffentlichen IPv4-Adresse der Instance außerhalb des Netzwerks der Instance bzw. der privaten IPv4-Adresse der Instance innerhalb des Netzwerks der Instance auf. Weitere Informationen finden Sie unter Öffentliche IPv4-Adressen und externe DNS-Hostnamen im Amazon EC2 EC2-Benutzerhandbuch.

DNS-Attribute in Ihrer VPC

Die folgenden VPC-Attribute bestimmen die DNS-Unterstützung für Ihre VPC. Wenn beide Attribute aktiviert sind, erhält eine in der VPC gestartete Instance einen öffentlichen DNS-Hostnamen, wenn ihr bei der Erstellung eine öffentliche IPv4-Adresse oder eine elastische IP-Adresse zugewiesen wird. Wenn Sie beide Attribute für eine VPC aktivieren, bei der sie zuvor nicht beide aktiviert haben, erhalten Instances, die in dieser VPC ausgeführt werden, öffentliche DNS-Hostnamen, wenn sie über eine öffentliche IPv4-Adresse oder eine elastische IP-Adresse verfügen.

Um zu überprüfen, ob diese Attribute für Ihre VPC aktiviert sind, siehe Anzeigen und Aktualisieren von DNS-Attributen für Ihre VPC.

Attribut	Beschreibung
`enableDnsHostnames`	Bestimmt, ob die VPC das Zuweisen öffentlicher DNS-Hostn amen zu Instances mit öffentlichen IP-Adressen unterstützt. Der Standardwert für dieses Attribut ist `false`, es sei denn, die VPC ist eine Standard-VPC. Beachten Sie die unten stehenden Regeln und Überlegungen für dieses Attribut.
`enableDnsSupport`	Bestimmt, ob die VPC die DNS-Auflösung über den von Amazon bereitgestellten DNS-Server unterstützt. Wenn dieses Attribut `true` ist, sind Abfragen an den von Amazon bereitgestellten DNS-Server erfolgreich. Weitere Informationen finden Sie unter Amazon DNS-Server. Der Standardwert für dieses Attribut ist `true`. Beachten Sie die unten stehenden Regeln und Überlegungen für dieses Attribut.

Regeln und Überlegungen

- Wenn beide Attribute `true` sind, geschieht Folgendes:

  - Instances mit öffentlichen IP-Adressen erhalten entsprechende öffentliche DNS-Hostnamen.
  - Der Amazon Route 53 Resolver Server kann von Amazon bereitgestellte private DNS-Hostnamen auflösen.
- Wenn mindestens eines der Attribute auf `false` festgelegt ist, geschieht Folgendes:
  - Instances mit öffentlichen IP-Adressen erhalten keine entsprechenden öffentlichen DNS-Hostnamen.
  - Die von Amazon bereitgestellten privaten DNS-Hostnamen Amazon Route 53 Resolver können nicht aufgelöst werden.
  - Instances erhalten benutzerdefinierte private DNS-Hostnamen, wenn die DHCP-Optionsliste einen benutzerdefinierten Domain-Namen enthält. Wenn Sie den Amazon Route 53 Resolver -Server nicht verwenden, müssen Ihre benutzerdefinierten Domain-Namenserver den Hostnamen entsprechend auflösen.
- Bei Verwendung von DNS-Domain-Namen, die in einer privat gehosteten Zone in Amazon Route 53 definiert wurden, oder bei Verwendung des privaten DNS mit Schnittstellen-VPC-Endpunkten (AWS PrivateLink) müssen die Attribute `enableDnsHostnames` und `enableDnsSupport` `true` sein.
- Amazon Route 53 Resolver Sie können private DNS-Hostnamen in private IPv4-Adressen für alle Adressräume auflösen, auch dann, wenn der IPv4-Adressbereich Ihrer VPC außerhalb der in RFC 1918 angegebenen privaten IPv4-Adressbereiche liegt. Falls Sie Ihre VPC jedoch vor Oktober 2016 erstellt haben, löst Amazon Route 53 Resolver private DNS-Hostnamen nicht auf, wenn der IPv4-Adressbereich Ihrer VPC außerhalb dieser Bereiche liegt. Wenn Sie Unterstützung dafür aktivieren möchten, wenden Sie sich an AWS Support.
- Wenn Sie VPC-Peering verwenden, müssen Sie beide Attribute für beide VPCs aktivieren und müssen die DNS-Auflösung für die Peering-Verbindung aktivieren. Weitere Informationen finden Sie unter Aktivieren einer DNS-Auflösung für eine VPC-Peering-Verbindung.

DNS-Kontingente

Jede EC2-Instance kann 1 024 Pakete pro Sekunde pro Netzwerkschnittstelle an Route 53 Resolver senden (insbesondere die .2-Adresse, z. B. 10.0.0.2 und 169.254.169.253). Dieses Kontingent kann nicht erhöht werden. Die Zahl der DNS-Abfragen, die pro Sekunde vom Route 53 Resolver unterstützt werden, ist vom Typ der Abfrage, von der Größe der Antwort und dem verwendeten Protokoll abhängig. Weitere Informationen und Empfehlungen für eine skalierbare DNS-Architektur finden Sie im technischen Handbuch AWS -Hybrid-DNS mit Active Directory.

Wenn Sie das Kontingent erreichen, lehnt der Route 53 Resolver den Datenverkehr ab. Einige der Ursachen für das Erreichen des Kontingents können ein DNS-Drosselungsproblem oder Abfragen von Instance-Metadaten sein, die die Netzwerkschnittstelle von Route 53 Resolver verwenden. Informationen zur Lösung von Problemen bei der Drosselung von VPC DNS finden Sie unter Wie kann ich herausfinden, ob meine DNS-Anfragen an den von Amazon bereitgestellten DNS-Server aufgrund VPC DNS-Einschränkung fehlschlagen. Informationen zum Abrufen von Instance-Metadaten finden Sie unter Instance-Metadaten abrufen im Amazon EC2 EC2-Benutzerhandbuch.

Anzeigen von DNS-Hostnamen für EC2-Instances

Sie können die DNS-Hostnamen für laufende Instances oder Netzwerkschnittstellen über die Amazon EC2-Konsole oder die Befehlszeile anzeigen.

Die Felder Public DNS (IPv4) und Private DNS sind verfügbar, wenn die DNS-Optionen für die VPC aktiviert sind, die der Instance zugeordnet ist. Weitere Informationen finden Sie unter the section called “DNS-Attribute in Ihrer VPC”.

Instance

So zeigen Sie DNS-Hostnamen für Instances über die 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 Ihre Instance aus der Liste aus.
4. Die Felder Public DNS (IPv4) und Private DNS im Detailbereich enthalten gegebenenfalls die DNS-Hostnamen.

So zeigen Sie DNS-Hostnamen für Instances über die Befehlszeile an

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Arbeiten mit Amazon VPC.

- describe-instances (AWS CLI)
- Get-EC2Instance (AWS Tools for Windows PowerShell)

Netzwerkschnittstelle

So zeigen Sie den privaten DNS-Hostnamen für eine Netzwerkschnittstelle über die Konsole an

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie im Navigationsbereich Network Interfaces (Netzwerk-Instances) aus.
3. Wählen Sie die Netzwerkschnittstelle aus der Liste aus.
4. Das Feld Private DNS (IPv4) im Detailbereich enthält den privaten DNS-Hostnamen.

So zeigen Sie DNS-Hostnamen für Netzwerkschnittstellen über die Befehlszeile an

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Arbeiten mit Amazon VPC.

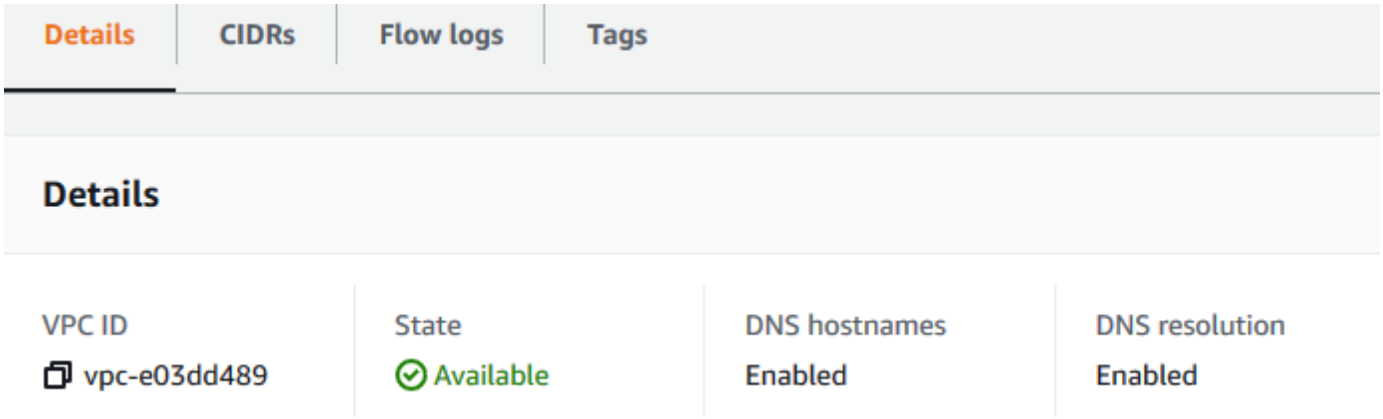
- describe-network-interfaces (AWS CLI)
- Get-EC2NetworkInterface (AWS Tools for Windows PowerShell)

Anzeigen und Aktualisieren von DNS-Attributen für Ihre VPC

Sie können die DNS-Support-Attribute für Ihre VPC über die Amazon VPC-Konsole anzeigen und aktualisieren.

So beschreiben und aktualisieren Sie den DNS-Support für eine VPC über die Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Aktivieren Sie das Kontrollkästchen für die VPC.
4. Lesen Sie die Informationen in Details. In diesem Beispiel werden sowohl DNS-Hostnamen und DNS-Auflösung aktiviert.



5. Um diese Einstellungen zu aktualisieren, wählen Sie Actions (Aktionen) und dann Edit VPC settings (VPC-Einstellungen bearbeiten) aus. Markieren oder deaktivieren Sie Enable (Aktivieren) für das entsprechende DNS-Attribut und wählen Sie Save changes (Änderungen speichern).

So beschreiben Sie den DNS-Support für eine VPC über die Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Arbeiten mit Amazon VPC.

- describe-vpc-attribute (AWS CLI)
- Get-EC2VpcAttribute (AWS Tools for Windows PowerShell)

So aktualisieren Sie den DNS-Support für eine VPC über die Befehlszeile

Verwenden Sie einen der folgenden Befehle. Weitere Informationen zu diesen Befehlszeilenschnittstellen erhalten Sie unter Arbeiten mit Amazon VPC.

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Private gehostete Zonen

Um mit benutzerdefinierten DNS-Domänennamen auf die Ressourcen in Ihrer VPC zuzugreifen, z. B. `example.com` anstatt private IPv4-Adressen oder AWS bereitgestellte private DNS-Hostnamen zu verwenden, können Sie eine private gehostete Zone in Route 53 erstellen. Eine privat gehostete Zone ist ein Container mit Informationen darüber, wie Sie Datenverkehr zu einer Domain und

ihren Subdomains innerhalb einer oder mehrerer VPCs weiterleiten möchten, ohne die Ressource über das Internet zugreifbar zu machen. Erstellen Sie dann Route 53-Ressourcendatensätze, um festzulegen, wie Route 53 auf Abfragen Ihrer Domain und Ihrer Subdomains reagiert. Wenn Sie beispielsweise möchten, dass Browseranfragen für beispiel.de an einen Webserver innerhalb Ihrer VPC weitergeleitet werden, erstellen Sie einen Datensatz A in Ihrer privat gehosteten Zone und geben die IP-Adresse dieses Webservers an. Weitere Informationen zum Erstellen einer privaten gehosteten Zone finden Sie unter Arbeiten mit privat gehosteten Zonen im Amazon-Route-53-Entwicklerhandbuch.

Um über benutzerdefinierte DNS-Domainnamen auf Ressourcen zuzugreifen, müssen Sie auf einer Instance innerhalb der VPC angemeldet sein. Sie können mit dem Befehl `ping`, z. B. `ping mywebserver.example.com`, auf der Instance testen, ob die Ressource in der privat gehosteten Zone über den benutzerdefinierten DNS-Namen zugreifbar ist. Damit der Befehl `ping` funktioniert, müssen die Sicherheitsgruppenregeln der Instance eingehenden ICMP-Datenverkehr zulassen.

Andere transitive Beziehungen außerhalb der VPC werden von privat gehosteten Zonen jedoch nicht unterstützt. Sie können zum Beispiel nicht über benutzerdefinierte private DNS-Namen über eine VPN-Verbindung von der anderen Seite auf Ihre Ressourcen zugreifen.

> **Important**
>
> Wenn Sie benutzerdefinierte DNS-Domain-Namen verwenden, die in einer privaten gehosteten Zone in Amazon Route 53 definiert sind, müssen Sie die Attribute `enableDnsHostnames` und `enableDnsSupport` auf `true` setzen.

Network Address Usage für Ihre VPC

Network Address Usage (NAU, Netzwerkadressennutzung) ist eine Metrik, die auf Ressourcen in Ihrem virtuellen Netzwerk angewendet wird und Sie bei der Planung und Überwachung der Größe Ihrer VPC unterstützt. Jede NAU-Einheit trägt zu einer Gesamtsumme bei, die der Größe Ihrer VPC entspricht.

Es ist wichtig, die Gesamtzahl der Einheiten zu verstehen, aus denen die NAU Ihrer VPC besteht, da die folgenden VPC-Kontingente die Größe einer VPC einschränken:

- Network Address Usage – Die maximale Anzahl von NAU-Einheiten, die eine einzelne VPC haben kann. Jede VPC kann standardmäßig bis zu 64 000 NAU-Einheiten haben. Sie können eine Kontingenterhöhung bis 256 000 NAU-Einheiten beantragen.

- Über Peering verbundene Network Address Usage – Die maxmiale Anzahl von NAU-Einheiten für eine VPC und alle ihre durch Peering verbundenen VPCs. Wenn eine VPC mit anderen VPCs in derselben Region verbunden ist, können die kombinierten VPCs standardmäßig über bis zu 128 000 NAU-Einheiten verfügen. Sie können eine Kontingenterhöhung bis 512 000 NAU-Einheiten beantragen. VPCs, die über verschiedene Regionen hinweg durch Peering verbunden werden, tragen nicht zu diesem Limit bei.

Sie können NAU auf folgende Arten verwenden:

- Bevor Sie Ihr virtuelles Netzwerk erstellen, berechnen Sie die NAU-Einheiten, um zu entscheiden, ob Sie die Workloads auf mehrere VPCs verteilen sollten.
- Nachdem Sie Ihre VPC erstellt haben, verwenden Sie Amazon, CloudWatch um die NAU-Nutzung der VPC zu überwachen, sodass sie die NAU-Kontingentgrenzen nicht überschreitet. Weitere Informationen finden Sie unter the section called “CloudWatch-Metriken”.

Wie NAU berechnet wird

Wenn Sie verstehen, wie NAU berechnet wird, kann es Ihnen helfen, die Skalierung Ihrer VPCs zu planen.

In der folgenden Tabelle wird erläutert, aus welchen Ressourcen die NAU-Anzahl in einer VPC besteht und wie viele NAU-Einheiten jede Ressource verwendet. Einige AWS Ressourcen werden als einzelne NAU-Einheiten dargestellt und einige Ressourcen werden als mehrere NAU-Einheiten dargestellt. Sie können die Tabelle verwenden, um zu erfahren, wie die NAU berechnet wird.

Ressource	NAU-Einheiten
Jede private oder öffentliche IPv4- und jede IPv6-Adresse, die einer Netzwerkschnittstelle für eine EC2-Instance in der VPC zugewiesen ist	1
An Instances angefügte, zusätzliche EC2-Netzwerkschnittstellen	1
Der Netzwerkschnittstelle zugewiesenes Präfix	1
Network Load Balancer pro AZ	6
Gateway Load Balancer für AZ	6

Ressource	NAU-Einheiten
VPC-Endpunkt pro AZ	6
Transit-Gateway-Anhang	6
Lambda-Funktion	6
NAT-Gateway	6
EFS-Mount-Ziel	6

NAU-Beispiele

In den folgenden Beispielen wird gezeigt, wie Sie NAU berechnen können.

Beispiel 1 – Zwei VPCs, die über VPC-Peering verbunden sind

Durch Peering verbundene VPCs in der gleichen Region tragen zu einem kombinierten NAU-Kontingent bei.

- VPC 1
  - 50 Network Load Balancer in 2 Subnetzen in separaten Availability Zones – 600 NAU-Einheiten
  - 5 000 Instances (jeweils mit einer IPv4- und IPv6-Adresse) in einem Subnetz und 5 000 Instances (jeweils mit einer IPv4- und IPv6-Adresse) in einem anderen Subnetz – 20 000 Einheiten
  - 100 Lambda-Funktionen – 600 NAU-Einheiten
- VPC 2
  - 50 Network Load Balancer in 2 Subnetzen in separaten Availability Zones – 600 NAU-Einheiten
  - 5 000 Instances (jeweils mit einer IPv4- und IPv6-Adresse) in einem Subnetz und 5 000 Instances (jeweils mit einer IPv4- und IPv6-Adresse) in einem anderen Subnetz – 20 000 Einheiten
  - 100 Lambda-Funktionen – 600 NAU-Einheiten
- Gesamtzahl der Peering-NAU: 42 400 Einheiten
- Standard-Peering-NAU-Kontingent: 128 000 Einheiten

Beispiel 2 – Zwei VPCs, die über ein Transit-Gateway verbunden sind

VPCs, die über ein Transit-Gateway verbunden sind, tragen nicht zu einem kombinierten NAU-Kontingent bei, wie dies bei durch Peering verbundene VPCs der Fall ist.

- VPC 1
  - 50 Network Load Balancer in 2 Subnetzen in separaten Availability Zones – 600 NAU-Einheiten
  - 5 000 Instances (jeweils mit einer IPv4- und IPv6-Adresse) in einem Subnetz und 5 000 Instances (jeweils mit einer IPv4- und IPv6-Adresse) in einem anderen Subnetz – 20 000 Einheiten
  - 100 Lambda-Funktionen – 600 NAU-Einheiten
- VPC 2
  - 50 Network Load Balancer in 2 Subnetzen in separaten Availability Zones – 600 NAU-Einheiten
  - 5 000 Instances (jeweils mit einer IPv4- und IPv6-Adresse) in einem Subnetz und 5 000 Instances (jeweils mit einer IPv4- und IPv6-Adresse) in einem anderen Subnetz – 20 000 Einheiten
  - 100 Lambda-Funktionen – 600 NAU-Einheiten
- Gesamtzahl der NAU pro VPC: 21 200 Einheiten
- tandard-NAU-Kontingent pro VPC: 64 000 Einheiten

Freigeben Ihrer VPC für andere Konten

Die gemeinsame Nutzung von VPC ermöglicht es mehreren AWS-Konten , ihre Anwendungsressourcen wie Amazon EC2 EC2-Instances, Amazon Relational Database Service (RDS) -Datenbanken, Amazon Redshift Redshift-Cluster und AWS Lambda Funktionen in gemeinsam genutzten, zentral verwalteten Virtual Private Clouds (VPCs) zu erstellen. In diesem Modell teilt sich das Konto, dem die VPC gehört (Eigentümer), ein oder mehrere Subnetze mit anderen Konten (Teilnehmern), die derselben Organisation angehören. AWS Organizations Wenn ein Subnetz freigegeben wurde, können die Teilnehmer ihre Anwendungsressourcen in den für sie freigegebenen Subnetzen anzeigen, erstellen, ändern oder löschen. Teilnehmer können keine Ressourcen anzeigen, ändern oder löschen, die anderen Teilnehmern oder dem VPC-Eigentümer gehören.

Sie können Ihre VPCs gemeinsam nutzen, um das implizite Routing innerhalb eines VPCs für Anwendungen zu verwenden, die einen hohen Grad an Interaktivität erfordern und sich innerhalb

derselben Vertrauensbereiche befinden. Dies reduziert die Anzahl der VPCs, die Sie erstellen und verwalten, während Sie separate Konten für die Fakturierung und Zugriffskontrolle verwenden. Sie können Netzwerktopologien vereinfachen, indem Sie gemeinsam genutzte Amazon-VPCs mithilfe von Konnektivitätsfunktionen wie AWS PrivateLink Transit-Gateways und VPC-Peering miteinander verbinden. Weitere Informationen zu den Vorteilen der VPC-Freigabe finden Sie unter VPC-Freigabe: Ein neuer Ansatz für mehrere Konten und für die VPC-Verwaltung.

Inhalt

Voraussetzungen für freigegebene VPCs

- Die Konten für den VPC-Besitzer und -Teilnehmer müssen von AWS Organizations verwaltet werden.
- Sie müssen die gemeinsame Nutzung von Ressourcen in der AWS RAM Konsole über das Verwaltungskonto Ihrer Organisation aktivieren. Weitere Informationen finden Sie AWS Organizations im AWS RAM Benutzerhandbuch unter Aktivieren der gemeinsamen Nutzung von Ressourcen innerhalb.
- Sie müssen eine Ressourcenfreigabe erstellen. Sie können bei der Erstellung der Ressourcenfreigabe angeben, welche Subnetze gemeinsam genutzt werden sollen, oder Sie können die Subnetze der Ressourcenfreigabe später hinzufügen, indem Sie das Verfahren im nächsten Abschnitt verwenden. Weitere Informationen finden Sie unter Erstellen einer Ressourcenfreigabe im AWS RAM -Benutzerhandbuch.

Freigeben eines Subnetzes

Sie können Subnetze, die nicht dem Standard entsprechen, wie folgt mit anderen Konten innerhalb Ihrer Organisation gemeinsam nutzen.

Ein Subnetz mit der Konsole freigeben

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Wählen Sie Ihr Subnetz und anschließend Actions (Aktionen), Share subnet (Subnetz freigeben) aus.
4. Wählen Sie Ihre Ressourcenfreigabe und anschließend Share subnet (Subnetz freigeben) aus.

Um ein Subnetz gemeinsam zu nutzen, verwenden Sie AWS CLI

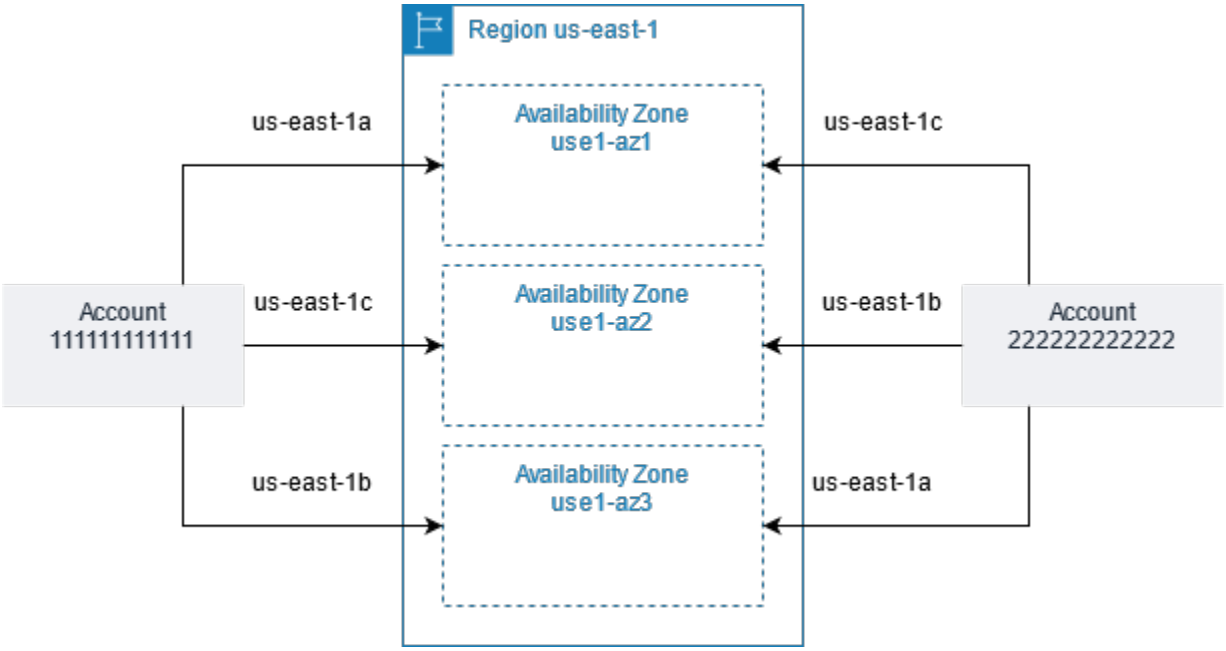
Verwenden Sie die associate-resource-shareBefehle create-resource-shareund.

Zuweisung von Subnetzen über Availability Zones hinweg

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzeln Namen für jedes -Konto zu. 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 die Availability Zones kontenübergreifend für die VPC-Freigabe zu koordinieren, müssen Sie eine AZ-ID verwenden, die eine eindeutige und konsistente Kennung für eine Availability Zone ist. Beispielsweise ist `use1-az1` die AZ-ID einer der Availability Zones in der Region `us-east-1`. Verwenden Sie AZ-IDs, um den Standort von Ressourcen in einem Konto im Verhältnis zu einem anderen Konto zu bestimmen. Sie können die AZ-ID für jedes Subnetz in der Amazon VPC-Konsole anzeigen.

Das folgende Diagramm veranschaulicht zwei Konten mit unterschiedlichen Zuordnungen von Availability Zone-Code zur AZ-ID.



Freigeben eines freigegebenen Subnetzes rückgängig machen

Der Eigentümer kann die Freigabe eines Subnetzes für Teilnehmer jederzeit aufheben. Nachdem der Eigentümer die Freigabe eines Subnetzes aufgehoben hat, gelten die folgenden Regeln:

- Bestehende Teilnehmerressourcen werden weiterhin im nicht gemeinsam genutzten Subnetz ausgeführt. AWS Managed Services (z. B. Elastic Load Balancing) mit automatisierten/verwalteten Workflows (wie Auto Scaling oder Node Replacement) benötigen für einige Ressourcen möglicherweise kontinuierlichen Zugriff auf das gemeinsam genutzte Subnetz.
- Teilnehmer können keine neuen Ressourcen mehr im nicht länger freigegebenen Subnetz erstellen.
- Teilnehmer können ihre Ressourcen im Subnetz ändern, beschreiben und löschen.
- Wenn Teilnehmer noch über Ressourcen im nicht länger freigegebenen Subnetz verfügen, kann der Eigentümer das nicht länger freigegebene Subnetz oder dessen VPC nicht löschen. Der Eigentümer kann das nicht länger freigegebene Subnetz oder dessen VPC erst löschen, nachdem die Teilnehmer alle Ressourcen im nicht länger freigegebenen Subnetz gelöscht haben.

Die Freigabe eines Subnetzes unter Verwendung der Konsole aufheben

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.

3. Wählen Sie Ihr Subnetz und anschließend Actions (Aktionen), Share subnet (Subnetz freigeben) aus.
4. Wählen Sie Actions (Aktionen) und Stop sharing (Freigabe aufheben) aus.

Um die gemeinsame Nutzung eines Subnetzes aufzuheben, verwenden Sie AWS CLI

Verwenden Sie den disassociate-resource-share-Befehl.

Identifizieren des Eigentümers eines freigegebenen Subnetzes

Teilnehmer können die für sie freigegebenen Subnetze mit der Amazon VPC-Konsole oder dem Befehlszeilen-Tool anzeigen.

So identifizieren Sie den Eigentümer eines Subnetzes mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. Die Spalte Owner (Eigentümer) zeigt den Eigentümer des Subnetzes an.

Um einen Subnetzbesitzer mit dem zu identifizieren AWS CLI

Verwenden Sie die Befehle describe-subnets und describe-vpcs, in deren Ausgabe die ID des Besitzers enthalten ist.

Verwalten Sie VPC-Ressourcen

Eigentümer und Teilnehmer sind für die VPC-Ressourcen verantwortlich, die sie besitzen.

Besitzer-Ressourcen

VPC-Besitzer sind dafür verantwortlich, die Ressourcen zu erstellen, zu verwalten und zu löschen, die mit einer gemeinsam genutzten VPC verknüpft sind. Dazu gehören Subnetze, Routing-Tabellen, Netzwerk-ACLs, Peering-Verbindungen, Gateway-Endpunkte, Interface-Endpunkte, Amazon Route 53 Resolver -Endpunkte, Internet-Gateways, NAT-Gateways, Virtual Private Gateways und Transit Gateway-Anhänge.

Teilnehmer-Ressourcen

Teilnehmer können eine begrenzte Anzahl von VPC-Ressourcen in einer freigegebenen VPC erstellen. Teilnehmer können beispielsweise Netzwerkschnittstellen und Sicherheitsgruppen und

VPC-Ablaufprotokolle für die Netzwerkschnittstellen, deren Eigentümer sie sind, erstellen. Die VPC-Ressourcen, die ein Teilnehmer erstellt, werden auf die VPC-Kontingente im Teilnehmerkonto angerechnet, nicht auf das Eigentümerkonto. Weitere Informationen finden Sie unter VPC-Freigabe.

Fakturierung und Messung für den Eigentümer und Teilnehmer

- In einer gemeinsam genutzten VPC zahlt jeder Teilnehmer für seine Anwendungsressourcen, einschließlich Amazon EC2 EC2-Instances, Amazon Relational Database Service Service-Datenbanken, Amazon Redshift Redshift-Cluster und Funktionen. AWS Lambda Die Teilnehmer zahlen auch die Datenübertragungsgebühren im Zusammenhang mit der Datenübertragung zwischen den Availability Zones sowie der Datenübertragung über VPC-Peering-Verbindungen, über Internet-Gateways und über Gateways hinweg. AWS Direct Connect
- VPC-Besitzer zahlen Stundengebühren (falls zutreffend), Datenverarbeitungs- und Datenübertragungsgebühren für NAT-Gateways, virtuelle private Gateways, Transit-Gateways und VPC-Endpunkte. AWS PrivateLink Darüber hinaus werden öffentliche IPv4-Adressen, die in gemeinsam genutzten VPCs verwendet werden, den VPC-Besitzern in Rechnung gestellt. Weitere Informationen zu den Preisen für öffentliche IPv4-Adressen finden Sie auf der Amazon VPC-Preisseite auf der Seite mit den Preisen für öffentliche IPv4-Adressen.
- Datenübertragungen innerhalb derselben Availability Zone (durch die eindeutige AZ-ID angegeben) sind kostenlos – unabhängig davon, wer der Besitzer des Kontos der kommunizierenden Ressourcen ist.

Verantwortlichkeiten und Berechtigungen für Besitzer und Teilnehmer

Die folgenden Verantwortlichkeiten und Berechtigungen gelten für VPC-Ressourcen, wenn Sie mit gemeinsam genutzten VPC-Subnetzen arbeiten:

Flow-Protokolle

- Teilnehmer können in einem gemeinsam genutzten VPC-Subnetz, das ihnen nicht gehört, keine Flow-Protokolle erstellen, löschen oder beschreiben.
- Teilnehmer können in einem gemeinsam genutzten VPC-Subnetz, das ihnen gehört, Flow-Protokolle erstellen, löschen oder beschreiben.
- VPC-Besitzer können von einem Teilnehmer erstellte Flow-Logs nicht beschreiben oder löschen.

Internet-Gateways und Internet-Gateways nur für ausgehenden Datenverkehr

- Teilnehmer können in einem gemeinsam genutzten VPC-Subnetz keine Internet-Gateways und Internet-Gateways nur für ausgehenden Verkehr erstellen, anfügen oder löschen. Die Teilnehmer können Internet-Gateways in einem gemeinsam genutzten VPC-Subnetz beschreiben. Die Teilnehmer können in einem gemeinsam genutzten VPC-Subnetz keine Internet-Gateways beschreiben, die nur für ausgehenden Datenverkehr bestimmt sind.

NAT gateways (NAT-Gateways)

- Teilnehmer können NAT-Gateways in einem gemeinsam genutzten VPC-Subnetz nicht erstellen, löschen oder beschreiben.

Netzwerk-Zugriffskontrolllisten (NACLs)

- Teilnehmer können NACLs in einem gemeinsam genutzten VPC-Subnetz nicht erstellen, löschen oder ersetzen. Teilnehmer können NACLs beschreiben, die von VPC-Besitzern in einem gemeinsam genutzten VPC-Subnetz erstellt wurden.

Netzwerkschnittstellen

- Teilnehmer können Netzwerkschnittstellen in einem gemeinsam genutzten VPC-Subnetz erstellen. Teilnehmer können nicht auf andere Weise mit Netzwerkschnittstellen arbeiten, die von VPC-Besitzern in einem gemeinsam genutzten VPC-Subnetz erstellt wurden, z. B. Anhängen, Trennen oder Ändern der Netzwerkschnittstellen. Teilnehmer können Netzwerkschnittstellen in einer gemeinsam genutzten VPC, die sie erstellt haben, ändern oder löschen. So können Teilnehmer beispielsweise IP-Adressen mit den von ihnen erstellten Netzwerkschnittstellen verknüpfen bzw. die Verknüpfung aufheben.
- VPC-Besitzer können Netzwerkschnittstellen beschreiben, die Teilnehmern eines gemeinsam genutzten VPC-Subnetzes gehören. VPC-Besitzer können nicht auf andere Weise mit Netzwerkschnittstellen arbeiten, die Teilnehmern gehören, z. B. durch Anhängen, Trennen oder Ändern der Netzwerkschnittstellen, die Teilnehmern in einem gemeinsam genutzten VPC-Subnetz gehören.

Routing-Tabellen

- Teilnehmer können in einem gemeinsam genutzten VPC-Subnetz nicht mit Routing-Tabellen arbeiten (z. B. Routing-Tabellen erstellen, löschen oder verknüpfen). Teilnehmer können Routing-Tabellen in einem gemeinsam genutzten VPC-Subnetz beschreiben.

Sicherheitsgruppen

- Die Teilnehmer können mit Sicherheitsgruppen, die sie besitzen, in einem gemeinsam genutzten VPC-Subnetz arbeiten (sie erstellen, löschen, beschreiben, ändern oder Eingangs- und Ausgangsregeln für sie erstellen). Die Teilnehmer können in keiner Weise mit Sicherheitsgruppen arbeiten, die von VPC-Besitzern erstellt wurden.
- Teilnehmer können in den Sicherheitsgruppen, deren Eigentümer sie sind, Regeln erstellen, die auf Sicherheitsgruppen verweisen, die anderen Teilnehmern oder dem VPC-Besitzer gehören, wie folgt: Kontonummer/ security-group-id
- Teilnehmer können keine Instances mit Sicherheitsgruppen starten, die anderen Teilnehmern oder dem VPC-Besitzer gehören. Teilnehmer können keine Instances mit der Standard-Sicherheitsgruppe für die VPC starten, da diese dem Besitzer gehört.
- VPC-Besitzer können Sicherheitsgruppen beschreiben, die von Teilnehmern in einem gemeinsam genutzten VPC-Subnetz erstellt wurden. VPC-Besitzer können nicht auf andere Weise mit Sicherheitsgruppen arbeiten, die von Teilnehmern erstellt wurden. VPC-Besitzer können beispielsweise keine Instances mithilfe von Sicherheitsgruppen starten, die von Teilnehmern erstellt wurden.

Subnetze

- Teilnehmer können gemeinsam genutzte Subnetze oder ihre zugehörigen Attribute nicht ändern. Das kann nur der VPC-Besitzer. Teilnehmer können Subnetze in einem gemeinsam genutzten VPC-Subnetz beschreiben.
- VPC-Besitzer können Subnetze nur mit anderen Konten oder Organisationseinheiten teilen, die sich in derselben Organisation von Organizations aus AWS befinden. VPC-Besitzer können keine Subnetze in Standard-VPCs freigeben.

Transit Gateways

- Nur ein VPC-Besitzer kann ein Transit-Gateway an das gemeinsam genutzte VPC-Subnetz anfügen. Teilnehmer können das nicht.

VPCs

- Teilnehmer können VPCs oder ihre zugehörigen Attribute nicht ändern. Das kann nur der VPC-Besitzer. Die Teilnehmer können VPCs, ihre Attribute und die DHCP-Optionssätze beschreiben.
- VPC-Tags und Tags für die Ressourcen innerhalb der freigegebenen VPC werden nicht für die Teilnehmer freigegeben.

AWS Ressourcen und gemeinsam genutzte VPC-Subnetze

Die folgenden AWS-Services Support-Ressourcen in gemeinsam genutzten VPC-Subnetzen. Weitere Informationen darüber, wie der Service freigegebene VPC-Subnetze unterstützt, finden Sie unter den Links zur entsprechenden Servicedokumentation.

- Amazon Aurora
- AWS CodeBuild
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Kubernetes Service
- Elastic Load Balancing
  - Application Load Balancer
  - Gateway Load Balancers
  - Network Load Balancers
- Amazon EMR
- AWS Glue
- AWS Lambda
- AWS Network Manager
  - AWS Cloud-WAN
  - Network Access Analyzer

  - Reachability Analyzer
- AWS PrivateLink†
- Amazon Relational Database Service (RDS)
- Amazon-Redshift
- Amazon Route 53
- AWS Transit Gateway
- AWS Verified Access
- Amazon VPC
  - Peering
  - Datenverkehrsspiegelung
- Amazon VPC Lattice

† Sie können eine Verbindung zu allen AWS Diensten herstellen, die die PrivateLink Verwendung eines VPC-Endpunkts in einer gemeinsam genutzten VPC unterstützen. Eine Liste der Dienste, die unterstützt werden PrivateLink, finden Sie AWS PrivateLink im Handbuch unter AWS Services, die sich integrieren lassen.AWS PrivateLink

VPC-Freigabekontingente

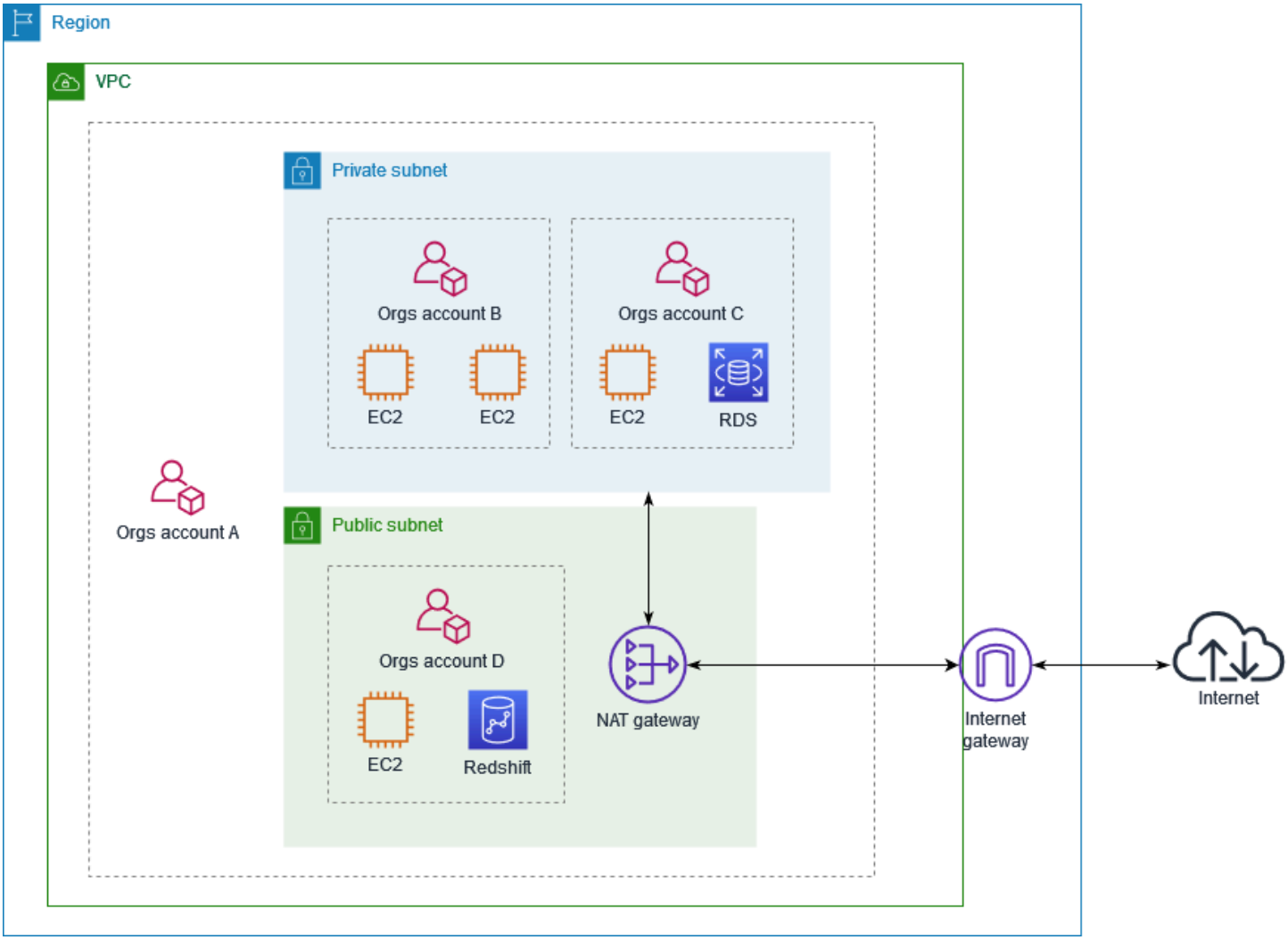
Es gibt Quoten für die VPC-Freigabe. Weitere Informationen finden Sie unter VPC-Freigabe.

Beispiel für das Freigeben öffentlicher und privater Subnetze

Betrachten Sie folgendes Szenario, in dem ein Konto (Konto A) die Infrastruktur, einschließlich der VPCs, Subnetze, Routing-Tabellen, Gateways und CIDR-Bereiche, verwalten soll und andere Mitgliedskonten für ihre Anwendungen die Subnetze verwenden sollen. Konto D enthält Anwendungen, die eine Verbindung zum Internet herstellen müssen. Konto B und Konto C verfügen über Anwendungen, die nicht mit dem Internet verbunden sein müssen.

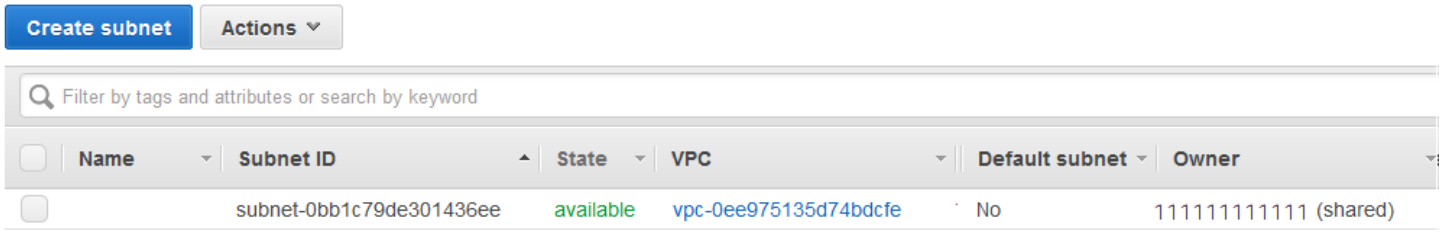
Konto A verwendet AWS Resource Access Manager, um eine Ressourcenfreigabe für die Subnetze zu erstellen, und gibt das öffentliche Subnetz für Konto D und das private Subnetz für Konto B und Konto C frei. Konto B, Konto C und Konto D können Ressourcen in den Subnetzen erstellen. In jedem Konto können nur Ressourcen in den jeweils freigegebenen Subnetzen angezeigt und erstellt werden. Jedes Konto kann die Ressourcen steuern, die es in diesen Subnetzen erstellt (z. B. EC2-Instances und Sicherheitsgruppen).

Für freigegebene Subnetze ist keine zusätzliche Konfiguration erforderlich. Die Routing-Tabellen für freigegebene Subnetze unterscheiden sich daher nicht von Routing-Tabellen für nicht freigegebene Subnetze.



Konto A (111111111111) gibt das öffentliche Subnetz für Konto D (444444444444) frei. Konto D wird das folgende Subnetz angezeigt und in der Spalte Besitzer sind zwei Anzeichen dafür erkennbar, dass das Subnetz freigegeben ist.

- Die Eigentümerkonto-ID ist Konto A (111111111111), nicht Konto D (444444444444).
- Das Wort „shared“ (Freigegeben) erscheint neben der Konto-ID des Eigentümers.



Erweitern einer VPC auf eine lokale Zone, eine Wavelength-Zone oder einen Outpost

Sie können VPC-Ressourcen wie Subnetze an mehreren Standorten weltweit hosten. Diese Standorte bestehen aus Regionen, Availability Zones, Local Zones und 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 bieten native AWS-Services, Infrastruktur und Betriebsmodelle für praktisch jedes Rechenzentrum, jeden Co-Location-Bereich oder jede On-Premises-Einrichtung.
- Mit Wavelength Zones können Developer Anwendungen mit äußerst niedriger Latenz für 5G-Geräte und Endbenutzer erstellen. Wavelength stellt standardmäßige AWS-Datenverarbeitungs- und -Speicherservices am Edge der 5G-Netze von Telekommunikationsanbietern bereit.

AWS betreibt hochmoderne, hoch verfügbare 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.

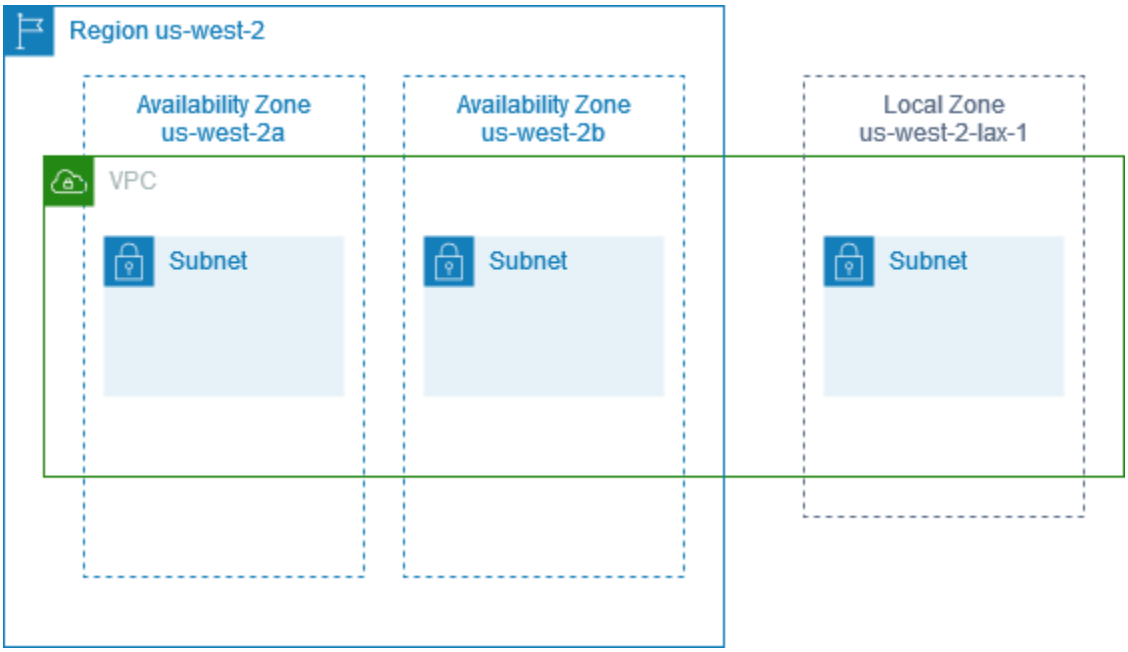
Subnetze in AWS Local Zones

Mit AWS Local Zones können Sie Ressourcen näher an Ihre Endbenutzer platzieren und sich nahtlos mit dem gesamten Serviceangebot der Region AWS mit vertrauten APIs und Toolsets verbinden. Wenn Sie ein Subnetz in einer Local Zone erstellen, erweitern Sie Ihre VPC auf diese Local Zone.

Um eine Local Zone zu verwenden, gehen Sie wie folgt vor:

- Melden Sie sich für die Local Zone an.
- Erstellen Sie ein Subnetz in der Local Zone.
- Starten Sie die Ressourcen im Subnetz der Local Zone, damit Ihre Anwendungen näher an Ihren Benutzern liegen:

Das folgende Diagramm zeigt eine VPC in der Region USA West (Oregon) (`us-west-2`), die sich über Availability Zones und eine Local Zone erstreckt.



Wenn Sie eine VPC erstellen, können Sie der VPC einen Satz von Amazon bereitgestellten öffentlichen IP-Adressen zuweisen. Sie können auch eine Netzwerkgrenzgruppe für die Adressen festlegen, die die Adressen auf die Gruppe beschränkt. Wenn Sie eine Netzwerkgrenzgruppe festlegen, können die IP-Adressen nicht zwischen Netzwerkgrenzgruppen wechseln. Der Netzwerkverkehr der Local Zone wird direkt ins Internet oder zu Points-of-Presence (PoPs) geleitet, ohne die übergeordnete Region der Local Zone zu durchqueren, und ermöglicht so den Zugang zu Datenverarbeitung mit niedriger Latenz. Die vollständige Liste der lokalen Zonen und ihrer übergeordneten Regionen finden Sie unter Available Local Zones im AWS Benutzerhandbuch für lokale Zonen.

Die folgenden Regeln gelten für Local Zones:

- Die Local-Zone-Subnetze folgen denselben Routingregeln, einschließlich Routing-Tabellen, Sicherheitsgruppen und Netzwerk-ACLs, wie das Availability-Zone-Subnetz.
- Der ausgehende Internetverkehr verlässt eine lokale Zone aus der lokalen Zone.
- Sie müssen öffentliche IP-Adressen für die Verwendung in einer Local Zone bereitstellen. Wenn Sie Adressen zuweisen, können Sie den Ort angeben, von dem aus die IP-Adresse angekündigt wird. Wir bezeichnen dies als Netzwerkgrenzgruppe, und Sie können diesen Parameter festlegen, um die Adresse auf diesen Ort zu beschränken. Nachdem Sie die IP-Adressen bereitgestellt haben, können Sie sie nicht zwischen der Local Zone und der übergeordneten Region verschieben (z. B. von `us-west-2-lax-1a` nach `us-west-2`).
- Wenn die lokale Zone IPv6 unterstützt, können Sie von Amazon bereitgestellte IPv6-IP-Adressen anfordern und sie mit der Netzwerkgrenzgruppe für eine neue oder bestehende VPC verknüpfen. Eine Liste der lokalen Zonen, die IPv6 unterstützen, finden Sie unter Überlegungen im AWS Benutzerhandbuch für lokale Zonen
- Sie können keine VPC-Endpunkte in Subnetzen der lokalen Zone erstellen.

Weitere Informationen zum Arbeiten mit Local Zones finden Sie im Benutzerhandbuch zu AWS Local Zones.

Überlegungen für Internet-Gateways

Berücksichtigen Sie folgende Informationen, wenn Sie Internet-Gateways (in der übergeordneten Region) in Local Zones verwenden:

- Sie können Internet-Gateways in Local Zones mit Elastic-IP-Adressen oder automatisch zugewiesenen öffentlichen IP-Adressen von Amazon verwenden. Die von Ihnen verknüpften Elastic-IP-Adressen müssen die Netzwerkgrenzgruppe der Local Zone enthalten. Weitere Informationen finden Sie unter the section called “Elastic-IP-Adressen”.

  Sie können keine Elastic-IP-Adresse zuordnen, die für die Region festgelegt ist.
- Elastic-IP-Adressen, die in Local Zones verwendet werden, haben die gleichen Kontingente wie Elastic IP-Adressen in einer Region. Weitere Informationen finden Sie unter the section called “Elastic-IP-Adressen”.
- Sie können Internet-Gateways in Routing-Tabellen verwenden, die mit Ressourcen der lokalen Zone verknüpft sind. Weitere Informationen finden Sie unter the section called “Routing zu einem Internet-Gateway”.

Zugreifen auf Local Zones mit einem Direct Connect Gateway

Betrachten Sie das Szenario, in dem ein On-Premises-Rechenzentrum auf Ressourcen zugreifen soll, die sich in einer lokalen Zone befinden. Sie verwenden ein Virtual Private Gateway für die VPC, die mit der Local Zone verknüpft ist, um eine Verbindung mit einem Direct Connect-Gateway herzustellen. Das Direct Connect-Gateway verbindet sich mit einem AWS Direct Connect-Standort in einer Region. Das On-Premises-Rechenzentrum hat eine AWS Direct Connect-Verbindung zum AWS Direct Connect-Standort.

> **Note**
>
> Datenverkehr innerhalb der USA, der über Direct Connect an ein Subnetz in einer lokalen Zone gerichtet ist, wird nicht durch die übergeordnete Region der lokalen Zone geleitet. Stattdessen nimmt der Verkehr den kürzesten Weg zur lokalen Zone. Dies verringert die Latenz und trägt dazu bei, dass Ihre Anwendungen schneller reagieren.

Sie konfigurieren die folgenden Ressourcen für diese Konfiguration:

- Ein Virtual Private Gateway für die VPC, das dem Subnetz der lokalen Zone zugeordnet ist. Sie können die VPC für das Subnetz auf der Seite mit den Subnetzdetails in der Amazon Virtual Private Cloud Console anzeigen oder describe-subnets verwenden.

  Informationen zum Erstellen eines Virtual Private Gateway finden Sie unter Erstellen eines Ziel-Gateways im AWS Site-to-Site VPN-Benutzerhandbuch.
- Eine Direct Connect-Verbindung. Für die beste Latenzleistung empfiehlt AWS, den Direct-Connect-Standort zu verwenden, der der Local Zone, auf die Sie Ihr Subnetz erweitern, am nächsten liegt.

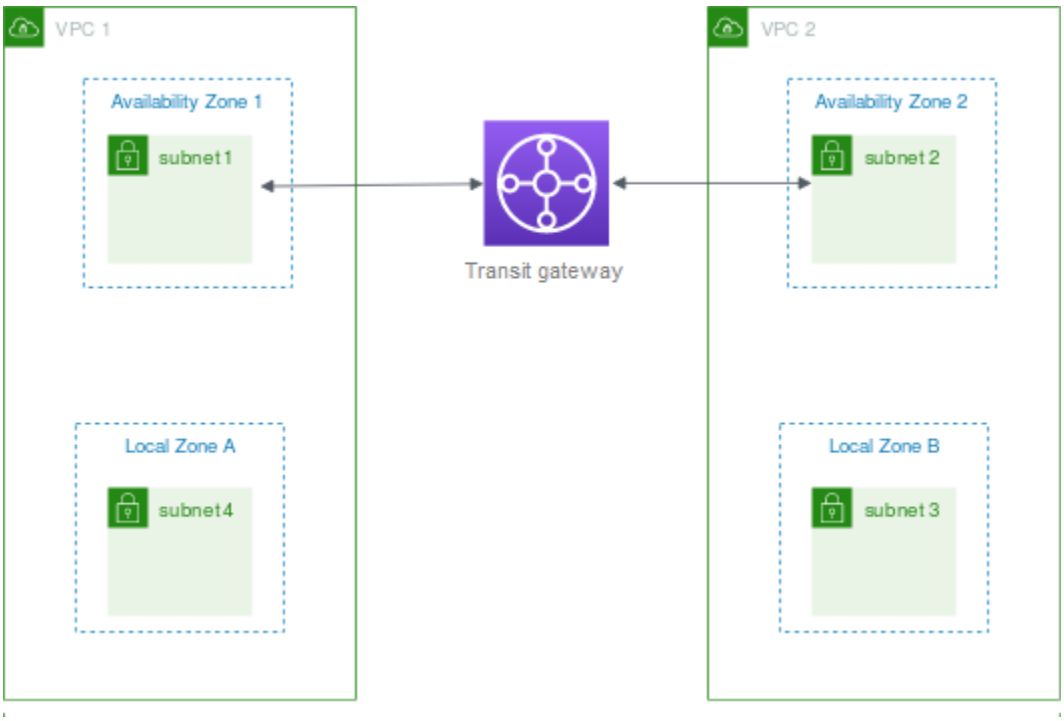
  Informationen zum Bestellen einer Verbindung finden Sie unter Querverbindungen im AWS Direct Connect-Benutzerhandbuch.
- Ein Direct Connect-Gateway Informationen zum Erstellen eines Direct Connect-Gateways finden Sie unter Erstellen eines Direct Connect Gateway im AWS Direct Connect-Benutzerhandbuch.
- Eine Virtual Private Gateway-Verbindung, um die VPC mit dem Direct Connect-Gateway zu verbinden. Informationen zum Erstellen einer Virtual Private Gateway-Verbindung finden Sie unter Zuordnen und Aufheben der Zuordnung von Virtual Private Gateways im AWS Direct Connect-Benutzerhandbuch.
- Eine private virtuelle Schnittstelle für die Verbindung vom AWS Direct Connect-Standort mit dem On-Premises-Rechenzentrum. Informationen zum Erstellen eines Direct Connect-Gateways finden

Sie unter Erstellen einer privaten virtuellen Schnittstelle für das Direct Connect-Gateway im AWS Direct Connect-Benutzerhandbuch.

Verbinden von Subnetzen der Local Zone mit einem Transit-Gateway

Sie können keinen Transit-Gateway-Anhang für ein Subnetz in einer Local Zone erstellen. Das folgende Diagramm zeigt, wie Sie Ihr Netzwerk so konfigurieren, dass Subnetze in der Local Zone eine Verbindung mit einem Transit-Gateway über die übergeordnete Availability Zone herstellen. Erstellen Sie Subnetze in den Local Zones und Subnetzen in den übergeordneten Availability Zones. Verbinden Sie die Subnetze in den übergeordneten Availability Zones mit dem Transit Gateway und erstellen Sie dann in der Routing-Tabelle für jede VPC eine Route, die den für die andere VPC-CIDR bestimmten Datenverkehr an die Netzwerkschnittstelle für den Transit-Gateway-Anhang weiterleitet.

> **Note**
>
> Datenverkehr, der für ein Subnetz in einer lokalen Zone bestimmt ist und von einem Transit-Gateway stammt, durchläuft zunächst die übergeordnete Region.



Erstellen Sie die folgenden Ressourcen für dieses Szenario:

- Ein Subnetz in jeder übergeordneten Availability Zone. Weitere Informationen finden Sie unter the section called “Erstellen eines Subnetzes”.
- Ein Transit-Gateway. Weitere Informationen finden Sie unter Transit Gateways erstellen in Amazon-VPC-Transit-Gateways.
- Ein Transit-Gateway-Anhang für jede VPC, die die übergeordnete Availability Zone verwendet. Weitere Informationen finden Sie unter Transit-Gateways-Anhang an eine VPC erstellen in Amazon-VPC-Transit-Gateways.
- Eine Transit-Gateway-Routing-Tabelle, die der Transit-Gateway-Verbindung zugeordnet ist. Weitere Informationen finden Sie unter Transit-Gateway-Routing-Tabellen in Amazon-VPC-Transit-Gateways.
- Für jede VPC einen Eintrag in der VPC-Routing-Tabelle mit dem anderen VPC-CIDR als Ziel und der ID der Netzwerkschnittstelle für den Transit-Gateway-Anhang als Ziel. Suchen Sie nach der Netzwerkschnittstelle für den Transit-Gateway-Anhang in den Beschreibungen der Netzwerkschnittstellen nach der ID des Transit-Gateway-Anhangs. Weitere Informationen finden Sie unter the section called “Routing für ein Transit-Gateway”.

Es folgt ein Beispiel für eine Routing-Tabelle für VPC 1.

Ziel	Ziel
VPC 1 CIDR	*Lokal*
VPC 2 CIDR	*vpc1-attachment-network-interface-id*

Es folgt ein Beispiel für eine Routing-Tabelle für VPC 2.

Ziel	Ziel
VPC 2 CIDR	*Lokal*
VPC 1 CIDR	*vpc2-attachment-network-interface-id*

Es folgt ein Beispiel für die Routing-Tabelle des Transit-Gateways. Die CIDR-Blöcke für jede VPC werden an die Transit-Gateway-Routing-Tabelle übertragen.

CIDR	Attachment	Routing-Typ
VPC 1 CIDR	*Anhang für VPC 1*	verbreitet
VPC 2 CIDR	*Anhang für VPC 2*	verbreitet

Subnetze in AWS Wavelength

AWS Wavelength Mit 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. Entwickler können eine Virtual Private Cloud (VPC) auf eine oder mehrere Wavelength-Zonen ausweiten und dann AWS-Ressourcen wie Amazon-EC2-Instances verwenden, um Anwendungen auszuführen, die eine extrem niedrige Latenz und eine Verbindung zu AWS-Services in der Region erfordern.

Um Wavelength Zones verwenden zu können, müssen Sie sich zunächst für die Zone anmelden. Erstellen Sie als Nächstes ein Subnetz in der Wavelength Zone. Sie können Amazon EC2-Instances, Amazon EBS-Volumes und Amazon VPC-Subnetze und Carrier Gateways in Wavelength Zones erstellen. Sie können auch Services nutzen, die EC2, EBS und VPC orchestrieren oder mit diesen zusammenarbeiten, wie Amazon EC2 Auto Scaling, Amazon EKS-Cluster, Amazon ECS-Cluster, Amazon EC2 Systems Manager, Amazon CloudWatch, AWS CloudTrail und AWS CloudFormation. Die Services in Wavelength sind Teil einer VPC, die über eine zuverlässige Verbindung mit hoher Bandbreite mit einer AWS-Region verbunden ist, um einen einfachen Zugang zu Services wie Amazon DynamoDB und Amazon RDS zu ermöglichen.

Die folgenden Regeln gelten für Wavelength Zones:

- Eine VPC erweitert sich zu einer Wavelength Zone, wenn Sie ein Subnetz in der VPC erstellen und es mit der Wavelength Zone verknüpfen.
- Standardmäßig erbt jedes Subnetz, das Sie in einer VPC erstellen, die sich über eine Wavelength Zone erstreckt, die Haupt-Routing-Tabelle der VPC, einschließlich der lokalen Route.
- Wenn Sie eine EC2-Instance in einem Subnetz in einer Wavelength Zone starten, weisen Sie ihr eine Carrier-IP-Adresse zu. Das Carrier-Gateway verwendet die Adresse für den Datenverkehr

von der Schnittstelle zum Internet oder zu mobilen Geräten. Das Carrier-Gateway verwendet NAT, um die Adresse zu übersetzen, und sendet dann den Datenverkehr an das Ziel. Der Verkehr vom Telekommunikations-Carrier-Netzwerk läuft über das Carrier-Gateway.

- Sie können das Ziel einer VPC-Routing-Tabelle oder einer Subnetz-Routing-Tabelle in einer Wavelength Zone auf ein Carrier-Gateway festlegen, das eingehenden Datenverkehr von einem Carrier-Netzwerk an einem bestimmten Standort und ausgehenden Datenverkehr zum Carrier-Netzwerk und zum Internet zulässt. Weitere Informationen zu Weiterleitungsoptionen in einer Wavelength Zone finden Sie unter Weiterleitung im AWS Wavelength Entwicklerhandbuch.
- Subnetze in Wavelength-Zonen verfügen über dieselben Netzwerkkomponenten wie Subnetze in Availability Zones, einschließlich IPv4-Adressen, DHCP-Optionssätze und Netzwerk-ACLs.
- Sie können keinen Transit-Gateway-Anhang zu einem Subnetz in einer Wavelength-Zone erstellen. Erstellen Sie stattdessen den Anhang über ein Subnetz in der übergeordneten Availability Zone, und leiten Sie dann den Datenverkehr über das Transit Gateway an die gewünschten Ziele weiter. Ein Beispiel hierfür finden Sie im nächsten Abschnitt.

Überlegungen zu mehreren Wavelength Zones

EC2-Instances, die sich in verschiedenen Wavelength Zones in derselben VPC befinden, dürfen nicht miteinander kommunizieren. Wenn Sie eine Kommunikation von Wavelength Zone zu Wavelength Zone benötigen, empfiehlt AWS, mehrere VPCs zu verwenden – eine für jede Wavelength Zone. Sie können ein Transit-Gateway verwenden, um die VPCs miteinander zu verbinden. Diese Konfiguration ermöglicht die Kommunikation zwischen Instances in den Wavelength Zones.

Der Datenverkehr von Wavelength Zone zu Wavelength Zone läuft über die AWS-Region. Weitere Informationen finden Sie unter AWS Transit Gateway.

Das folgende Diagramm zeigt, wie Sie Ihr Netzwerk so konfigurieren, dass Instances in zwei verschiedenen Wavelength Zones miteinander kommunizieren können. Sie verfügen über zwei Wavelength Zones (Wavelength Zone A und Wavelength Zone B). Sie müssen die folgenden Ressourcen erstellen, um die Kommunikation zu ermöglichen:

- Für jede Wavelength Zone ein Subnetz in einer Availability Zone, das die übergeordnete Availability Zone für die Wavelength Zone ist. In diesem Beispiel erstellen Sie Subnetz 1 und Subnetz 2. Informationen zum Erstellen von Subnetzen finden Sie unter the section called “Erstellen eines Subnetzes”. Verwenden Sie zum Suchen der übergeordneten Zone describe-availability-zones.

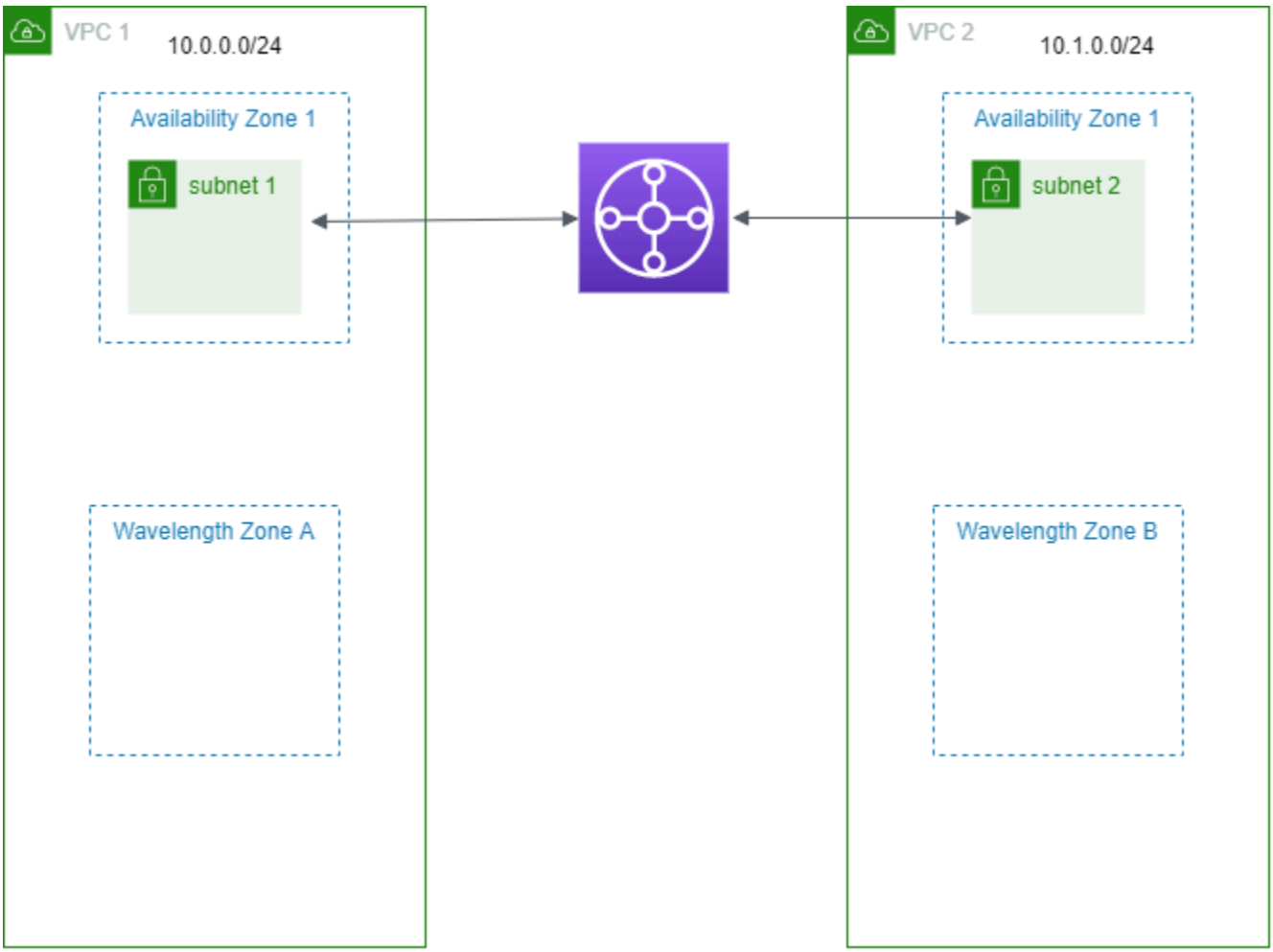
- Ein Transit-Gateway. Das Transit-Gateway verbindet die VPCs. Weitere Informationen zum Erstellen eines Transit Gateways finden Sie unter Erstellen eines Transit-Gateways im Amazon VPC Transit Gateways-Handbuch.
- Für jede VPC eine VPC-Anfügung an den Transit Gateway in der übergeordneten Availability Zone der Wavelength-Zone. Weitere Informationen finden Sie unter Transit-Gateway-Anhang an eine VPC erstellen im Amazon-VPC-Transit-Gateways-Handbuch.
- Einträge für jede VPC in der Routingtabelle des Transit-Gateways. Informationen zum Erstellen von Transit Gateway-Routen finden Sie unter Transit Gateway-Routing-Tabellen im Amazon VPC Transit Gateways-Handbuch.
- Für jede VPC ein Eintrag in der VPC-Routing-Tabelle, der das andere VPC-CIDR als Ziel enthält, und die Gateway-ID als Ziel. Weitere Informationen finden Sie unter the section called “Routing für ein Transit-Gateway”.

  In dem Beispiel hat die Routingtabelle für VPC 1 den folgenden Eintrag:

Zielbereich	Ziel
10.1.0.0/24	tgw-22222222222222222

  Die Routingtabelle für VPC 2 hat den folgenden Eintrag:

Zielbereich	Ziel
10.0.0.0/24	tgw-22222222222222222



Subnetze in AWS Outposts

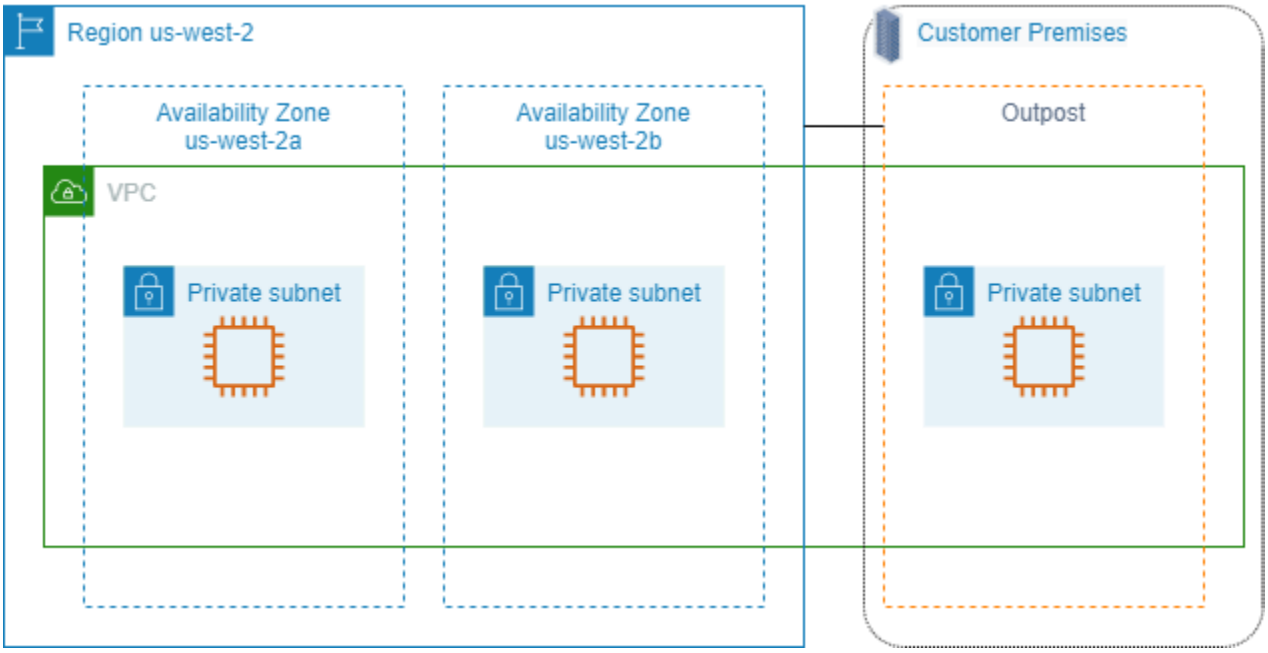
AWS Outposts bietet Ihnen die gleiche AWS-Hardwareinfrastruktur, Services, APIs und Tools zum Erstellen und Ausführen Ihrer Anwendungen On-Premises und in der Cloud. AWS Outposts ist ideal für Workloads geeignet, die einen Zugriff mit niedriger Latenz auf On-Premises-Anwendungen oder -Systeme benötigen, sowie für Workloads, die Daten lokal speichern und verarbeiten müssen. Mehr über AWS Outposts erfahren Sie unter AWS Outposts.

Eine VPC umfasst alle Availability Zones einer AWS-Region. Nachdem Sie Ihren Outpost mit seiner übergeordneten Region verbunden haben, können Sie jede VPC in der Region auf Ihren Outpost ausdehnen, indem Sie ein Subnetz für den Outpost in dieser VPC erstellen.

Es gelten die folgenden Regeln für AWS Outposts:

- Die Subnetze müssen sich an einem Outpost-Standort befinden.

- Sie erstellen ein Subnetz für einen Outpost, indem Sie den Amazon-Ressourcennamen (ARN) des Outposts angeben, wenn Sie das Subnetz erstellen.
- Outposts-Rack – Ein lokales Gateway verarbeitet die Netzwerkkonnektivität zwischen Ihrer VPC und On-Premises-Netzwerken. Weitere Informationen finden Sie unter Lokale Gateways im AWS Outposts-Benutzerhandbuch für das Outposts-Rack.
- Outposts-Server – Eine lokale Netzwerkschnittstelle verarbeitet die Netzwerkkonnektivität zwischen Ihrer VPC und On-Premises-Netzwerken. Weitere Informationen finden Sie unter Lokale Netzwerkschnittstellen im AWS Outposts-Benutzerhandbuch für Outposts-Server.
- Standardmäßig ist jedes Subnetz, das Sie in einer VPC erstellen, einschließlich Subnetze für Ihre Outposts, implizit eine Haupt-Routing-Tabelle für die VPC zugeordnet. Alternativ können Sie eine benutzerdefinierte Routing-Tabelle explizit mit den Subnetzen in Ihrer VPC On-Premises-Netzwerk bestimmt ist, festlegen.



Löschen der VPC

Wenn Sie eine VPC nicht mehr benötigen, können Sie sie löschen.

Anforderung

Bevor Sie eine VPC löschen können, müssen Sie zunächst alle Ressourcen beenden oder löschen, die eine Vom Anforderer verwaltete Netzwerkschnittstelle in der VPC erstellt haben. Sie müssen

beispielsweise Ihre EC2-Instances beenden und Ihre Load Balancer, NAT-Gateways, Transit-Gateway-VPC-Anhänge und Schnittstellen-VPC-Endpunkte löschen.

Inhalt

Löschen einer VPC mithilfe der Konsole

Falls Sie eine VPC mit der Amazon-VPC-Konsole löschen, löschen wir auch die folgenden VPC-Komponenten für Sie:

- DHCP-Optionen
- Internet-Gateways nur für ausgehenden Datenverkehr
- Gateway-Endpunkte
- Internet-Gateways
- Netzwerk-ACLs
- Routing-Tabellen
- Sicherheitsgruppen
- Subnetze

Ihre VPC mit Hilfe der Konsole löschen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Beenden aller Instances in der VPC. Weitere Informationen finden Sie unter Terminate Your Instance im Amazon EC2 EC2-Benutzerhandbuch.
3. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
4. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
5. Wählen Sie die VPC aus, die Sie löschen möchten, und klicken Sie auf Actions und danach auf Delete VPC.
6. Wenn es Ressourcen gibt, die Sie löschen oder beenden müssen, bevor wir die VPC löschen können, zeigen wir sie an. Löschen Sie oder beenden Sie diese Ressourcen und versuchen Sie es erneut. Andernfalls zeigen wir zusätzlich zur VPC die Ressourcen an, die wir löschen werden. Überprüfen Sie die Liste und fahren Sie mit dem nächsten Schritt fort.

7. (Optional) Wenn Sie eine Site-to-Site-VPN-Verbindung haben, können Sie die Option auswählen, um sie zu löschen. Wenn Sie planen, das Kunden-Gateway mit einer anderen VPC zu verwenden, empfehlen wir Ihnen, die Site-to-Site VPN-Verbindung und die Gateways beizubehalten. Andernfalls müssen Sie Ihr Kunden-Gateway-Gerät erneut konfigurieren, nachdem Sie eine neue Site-to-Site VPN-Verbindung hergestellt haben.
8. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.

Eine VPC mithilfe einer Befehlszeile löschen

Bevor Sie eine VPC mithilfe der Befehlszeile löschen können, müssen Sie alle Ressourcen beenden oder löschen, die eine vom Anforderer verwaltete Netzwerkschnittstelle in der VPC erstellt haben. Außerdem müssen Sie alle von Ihnen erstellten VPC-Ressourcen wie Subnetze, Sicherheitsgruppen, Netzwerk-ACLs, Routing-Tabellen, Internet-Gateways und Internet-Gateways für ausgehenden Verkehr löschen oder trennen. Die Standardsicherheitsgruppe, die Standard-Routing-Tabelle oder die Standard-Netzwerk-ACL müssen Sie nicht löschen.

Das folgende Verfahren zeigt die Befehle, mit denen Sie allgemeine VPC-Ressourcen und anschließend die VPC löschen. Sie müssen diese Komponenten in folgender Reihenfolge erstellen. Wenn Sie zusätzliche VPC-Ressourcen erstellt haben, müssen Sie auch den entsprechenden Löschbefehl verwenden. Erst dann können Sie die VPC löschen.

So löschen Sie eine VPC mit dem AWS CLI

1. Löschen Sie die Sicherheitsgruppe mit dem Befehl delete-security-group.

```
aws ec2 delete-security-group --group-id sg-id
```

2. Löschen Sie jede Netzwerk-ACL mit dem Befehl delete-network-acl.

```
aws ec2 delete-network-acl --network-acl-id acl-id
```

3. Löschen Sie jedes Subnetz mit dem Befehl delete-subnet.

```
aws ec2 delete-subnet --subnet-id subnet-id
```

4. Löschen Sie jede benutzerdefinierte Routing-Tabelle mit dem Befehl delete-route-table.

```
aws ec2 delete-route-table --route-table-id rtb-id
```

5. Trennen Sie das Internet-Gateway mit dem Befehl detach-internet-gateway von der VPC.

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-id --vpc-id vpc-id
```

6. Löschen Sie das Internet-Gateway mit dem Befehl delete-internet-gateway.

```
aws ec2 delete-internet-gateway --internet-gateway-id igw-id
```

7. [Dual-Stack-VPC] Löschen Sie das Internet-Gateway für ausgehenden Verkehr mit dem Befehl delete-egress-only-internet-gateway.

```
aws ec2 delete-egress-only-internet-gateway --egress-only-internet-gateway-id eigw-id
```

8. Löschen Sie die VPC mit dem Befehl delete-vpc.

```
aws ec2 delete-vpc --vpc-id vpc-id
```

Subnetze für Ihre VPC

Ein Subnetz ist ein Bereich an IP-Adressen in Ihrer VPC. Sie können AWS Ressourcen wie EC2-Instances in bestimmten Subnetzen erstellen.

Inhalt

Subnetze-Grundlagen

Jedes Subnetz muss sich vollständig innerhalb einer Availability Zone befinden und darf nicht mehrere Zonen umfassen. Indem Sie AWS Ressourcen in separaten Availability Zones starten, können Sie Ihre Anwendungen vor dem Ausfall einer einzelnen Availability Zone schützen.

Inhalt

Subnetz-IP-Adressbereiche

Wenn Sie ein Subnetz erstellen, geben Sie je nach Konfiguration der VPC seine IP-Adressen an:

- Nur IPv4 – Das Subnetz besitzt einen IPv4-CIDR-Block, besitzt jedoch keinen IPv6-CIDR-Block. Ressourcen in einem reinen IPv4-Subnetz müssen über IPv4 kommunizieren.

- Dual-Stack – Das Subnetz besitzt sowohl einen IPv4-CIDR-Block als auch einen IPv6-CIDR-Block. Die VPC muss sowohl einen IPv4-CIDR-Block als auch einen IPv6-CIDR-Block haben. Ressourcen in einem Dual-Stack-Subnetz können über IPv4 und IPv6 kommunizieren.
- Nur IPv6 – Das Subnetz besitzt einen IPv6-CIDR-Block, besitzt jedoch keinen IPv4-CIDR-Block. Die VPC muss einen IPv6-CIDR-Block aufweisen. Ressourcen in einem reinen IPv6-Subnetz müssen über IPv6 kommunizieren.

> **Note**
>
> Ressourcen in reinen IPv6-Subnetzen werden verbindungslokale IPv4-Adressen aus dem CIDR-Block `169.254.0.0/16` zugewiesen. Diese Adressen werden für die Kommunikation mit VPC-Diensten wie dem Instance Metadata Service (IMDS) verwendet.

Weitere Informationen finden Sie unter IP-Adressierung für Ihre VPCs und Subnetze.

Subnetz-Typen

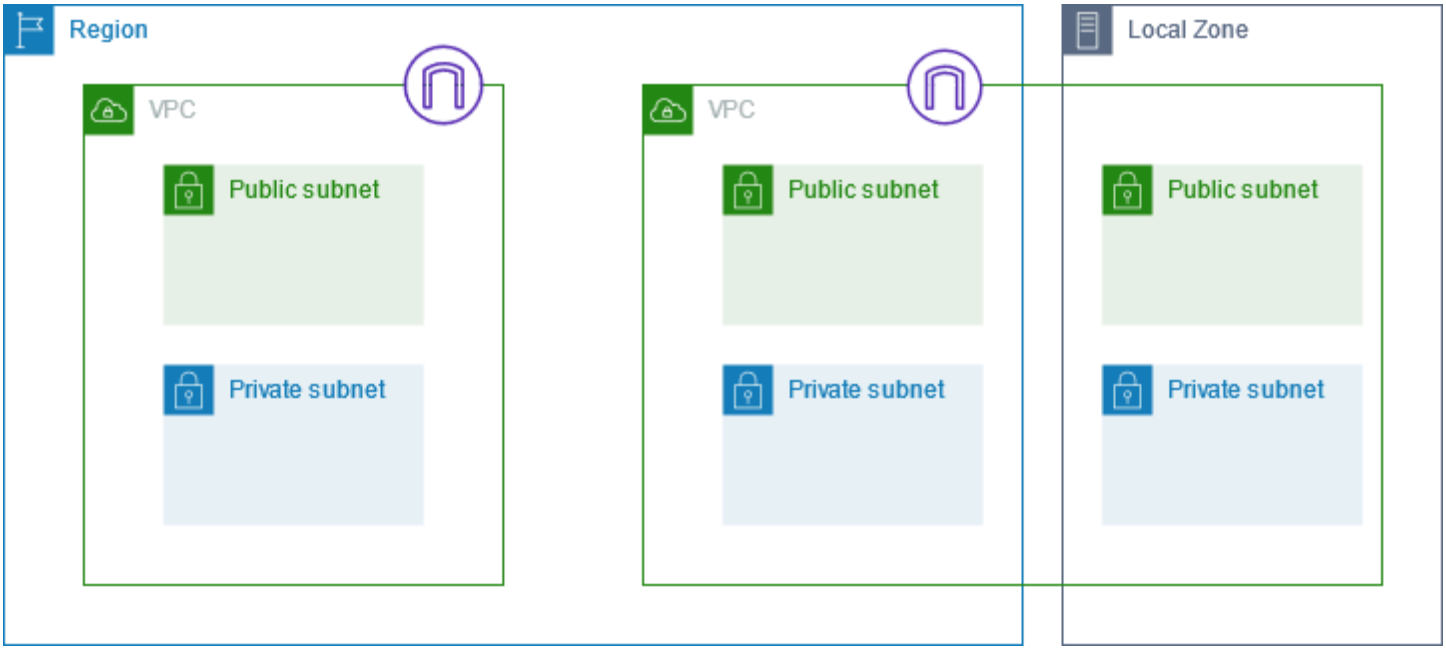
Der Subnetztyp hängt davon ab, wie Sie das Routing für Ihre Subnetze konfigurieren. Beispielsweise:

- Öffentliches Subnetz – Das Subnetz hat eine direkte Route zu einem Internet-Gateway. Ressourcen in einem öffentlichen Subnetz können auf das öffentliche Internet zugreifen.
- Privates Subnetz – Das Subnetz hat keine Weiterleitung an das Internet-Gateway. Ressourcen in einem privaten Subnetz benötigen ein NAT-Gerät, um auf das öffentliche Internet zuzugreifen.
- Reines VPN-Subnetz – Das Subnetz hat eine Weiterleitung zu einer Site-to-Site-VPN-Verbindung über ein virtuelles privates Gateway. Das Subnetz verfügt über keine Route zu einem Internet-Gateway.
- Isoliertes Subnetz – Das Subnetz weist keine Routen zu Zielen außerhalb der VPC auf. Ressourcen in einem isolierten Subnetz können nur auf andere Ressourcen in derselben VPC zugreifen bzw. sind nur für diese zugänglich.

Subnetzdiagramm

Das folgende Diagramm zeigt zwei VPCs in einer Region. Jede VPC verfügt über öffentliche und private Subnetze sowie über ein Internet-Gateway. Sie können optional Subnetze in einer lokalen Zone hinzufügen, wie im Diagramm gezeigt. Eine lokale Zone ist eine AWS Infrastrukturbereitstellung, die Rechen-, Speicher- und Datenbankdienste näher an Ihren

Endbenutzern platziert. Wenn Sie eine Local Zone verwenden, können Ihre Endbenutzer Anwendungen ausführen, die Latenzzeiten im einstelligen Millisekundenbereich erfordern. Weitere Informationen finden Sie unter AWS Local Zones.



Subnetz-Routing

Jedem Subnetz muss eine Routing-Tabelle zugeordnet werden, die die zulässigen Routen für den ausgehenden Datenverkehr des Subnetzes angibt. Jedem Subnetz, das Sie erstellen, wird automatisch eine Haupt-Routing-Tabelle für die VPC zugeordnet. Sie können die Zuordnung und die Inhalte der Haupt-Routing-Tabelle ändern. Weitere Informationen finden Sie unter Konfigurieren von Routing-Tabellen.

Subnetz-Einstellungen

Alle Subnetze verfügen über ein anpassbares Attribut, über das festlegt wird, ob eine in einem Subnetz erstellte Netzwerkschnittstelle einer öffentliche IPv4-Adresse, und falls zutreffend, einer IPv6-Adresse zugeordnet ist. Dazu zählt auch die primäre Netzwerkschnittstelle (eth0), die beim Start einer Instance in diesem Subnetz für diese Instance erstellt wurde. Unabhängig vom Subnetzattribut können Sie diese Einstellung während des Starts einer bestimmten Instance immer noch überschreiben.

Nach Erstellung eines Subnetzes können Sie die folgenden Einstellungen für das Subnetz ändern:

- IP-Einstellungen automatisch zuweisen: Ermöglicht es Ihnen, die Einstellungen für die automatische Zuweisung von IP-Einstellungen so zu konfigurieren, dass automatisch eine

öffentliche IPv4- oder IPv6-Adresse für eine neue Netzwerkschnittstelle in diesem Subnetz angefordert wird.

- Einstellungen für ressourcenbasierte Namen (RBN): Ermöglicht es Ihnen, den Hostnamentyp für EC2-Instances in diesem Subnetz anzugeben und zu konfigurieren, wie DNS A- und AAAA-Datensatzabfragen behandelt werden. Weitere Informationen finden Sie unter Hostnamentypen für Amazon EC2 EC2-Instances im Amazon EC2 EC2-Benutzerhandbuch.

Subnetzsicherheit

Um Ihre AWS Ressourcen zu schützen, empfehlen wir Ihnen, private Subnetze zu verwenden. Verwenden Sie einen Bastion-Host oder ein NAT-Gerät, um Internetzugriff auf Ressourcen, wie EC2-Instances, in einem privaten Subnetz bereitzustellen.

AWS bietet Funktionen, mit denen Sie die Sicherheit der Ressourcen in Ihrer VPC erhöhen können. Sicherheitsgruppen ermöglichen den eingehenden und ausgehenden Datenverkehr für zugehörige Ressourcen, wie z. B. EC2-Instances. Netzwerk-ACLs erlauben oder verhindern den ein- und ausgehenden Datenverkehr auf Subnetzebene. In den meisten Fällen können Sicherheitsgruppen Ihre Anforderungen erfüllen. Sie können jedoch Netzwerk-ACLs verwenden, wenn Sie eine zusätzliche Sicherheitsebene benötigen. Weitere Informationen finden Sie unter the section called “Vergleichen von Sicherheitsgruppen und Netzwerk-ACLs”.

Jedes Subnetz in Ihrer VPC muss bewusst mit einer Netzwerk-ACL verknüpft werden. Jedem Subnetz, das Sie erstellen, wird automatisch die standardmäßige Netzwerk-ACL der VPC zugeordnet. Die Standard-Netzwerk-ACL lässt den gesamten ein- und ausgehenden Datenverkehr zu. Sie können die Standard-Netzwerk-ACL aktualisieren oder benutzerdefinierte Netzwerk-ACLs erstellen und sie Ihren Subnetzen zuordnen. Weitere Informationen finden Sie unter Datenverkehr in Subnetzen mit Netzwerk-ACLs steuern.

Sie können auf Ihrer VPC oder Ihrem Subnetz ein Flow-Protokoll erstellen, um den Datenverkehr, der zu und von den Netzwerkschnittstellen in Ihrer VPC oder Ihrem Subnetz fließt, zu erfassen. Sie können Flow-Protokolle auch für individuelle Netzwerkschnittstellen erstellen. Weitere Informationen finden Sie unter Protokollieren von IP-Datenverkehr mit VPC Flow Logs.

Erstellen eines Subnetzes

Gehen Sie wie folgt vor, um Subnetze für Ihre virtuelle Virtual Private Cloud (VPC) zu erstellen. Abhängig von der benötigten Konnektivität müssen Sie möglicherweise außerdem Gateways und Routing-Tabellen hinzufügen.

Überlegungen

- Sie müssen einen IPv4 CIDR-Block für das Subnetz aus dem Bereich Ihrer VPC angeben. Wenn der VPC ein IPv6-CIDR-Block zugeordnet ist, können Sie einem Subnetz optional einen IPv6-CIDR-Block zuweisen. Weitere Informationen finden Sie unter IP-Adressierung für Ihre VPCs und Subnetze.
- Beachten Sie beim Erstellen eines reinen IPv6-Subnetzes Folgendes. Eine EC2-Instance, die in einem reinen IPv6-Subnetz gestartet wird, erhält eine IPv6-Adresse, aber keine IPv4-Adresse. Instances, die in einem reinen IPv6-Subnetz gestartet werden, müssen auf dem Nitro-System basieren.
- Um das Subnetz in einer lokalen Zone oder einer Wavelength-Zone zu erstellen, müssen Sie die Zone aktivieren. Weitere Informationen finden Sie unter Regionen und Zones im Amazon-EC2-Benutzerhandbuch.

So fügen Sie Ihrer VPC ein Subnetz hinzu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Wählen Sie Subnetz erstellen.
4. Wählen Sie unter VPC ID die VPC für das Subnetz aus.
5. (Optional) Geben Sie unter Subnet name (Subnetzname) einen Namen für das Subnetz ein. Auf diese Weise wird ein Tag mit dem Schlüssel `Name` und dem von Ihnen angegebenen Wert erstellt.
6. Für Availability Zone können Sie eine Zone für Ihr Subnetz auswählen oder die Standardeinstellung Keine Präferenz beibehalten, sodass Sie eine Zone für Sie AWS auswählen können.
7. Wählen Sie für IPv4-CIDR-Block die Option Manuelle Eingabe aus, um einen IPv4-CIDR-Block für Ihr Subnetz einzugeben (z. B. `10.0.1.0/24`), oder wählen Sie Kein IPv4-CIDR aus. Wenn Sie Amazon VPC IP Address Manager (IPAM) zur Planung, Nachverfolgung und Überwachung von IP-Adressen für Ihre AWS Workloads verwenden, haben Sie beim Erstellen

eines Subnetzes die Möglichkeit, IPAM (IPAM-zugewiesen) einen CIDR-Block zuzuweisen. Weitere Informationen zur Planung des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen im Amazon-VPC-IPAM-Benutzerhandbuch.

8. Wählen Sie für den IPv6-CIDR-Block die Option Manuelle Eingabe aus, um das IPv6-CIDR der VPC auszuwählen, in dem Sie ein Subnetz erstellen möchten. Diese Option ist nur verfügbar, wenn der VPC ein IPv6-CIDR-Block zugeordnet ist. Wenn Sie den Amazon VPC IP Address Manager (IPAM) verwenden, um IP-Adressen für Ihre AWS -Workloads zu planen, zu verfolgen und zu überwachen, haben Sie beim Erstellen eines Subnetzes die Möglichkeit, vom IPAM einen CIDR-Block zuzuweisen (IPAM-zugewiesen). Weitere Informationen zur Planung des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen finden Sie unter Tutorial: Planen des VPC-IP-Adressraums für Subnetz-IP-Zuweisungen im Amazon-VPC-IPAM-Benutzerhandbuch.
9. Wählen Sie einen IPv6-VPC-CIDR-Block.
10. Wählen Sie für den IPv6-Subnetz-CIDR-Block einen CIDR für das Subnetz aus, der dem VPC-CIDR entspricht oder spezifischer ist. Wenn der VPC-Pool-CIDR beispielsweise /50 ist, können Sie für das Subnetz eine Netzmaskenlänge zwischen /50 und /64 wählen. Mögliche IPv6-Netzmaskenlängen liegen zwischen /44 und /64 in Schritten von /4.
11. Wählen Sie Subnetz erstellen.

Um Ihrer VPC ein Subnetz hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie den Befehl create-subnet.

Nächste Schritte

Nach Erstellung eines Subnetzes können Sie es wie folgt konfigurieren:

- Konfigurieren Sie das Routing. Anschließend können Sie eine benutzerdefinierte Routing-Tabelle und Route erstellen, die den Datenverkehr an ein Gateway senden, das der VPC zugeordnet ist, z. B. ein Internet-Gateway. Weitere Informationen finden Sie unter Konfigurieren von Routing-Tabellen.
- Ändern Sie die Subnetz-IP-Adressen. Weitere Informationen finden Sie unter the section called “Konfigurieren Sie Ihre Subnetze”.
- Ändern Sie das IP-Adressierungsverhalten. Sie können festlegen, ob Instances, die in diesem Subnetz gestartet werden, eine öffentliche IPv4- und/oder eine IPv6-Adresse erhalten. Weitere Informationen finden Sie unter Subnetz-Einstellungen.

- Ändern Sie die Einstellungen für den ressourcenbasierten Namen (RBN). Weitere Informationen finden Sie unter Amazon EC2 instance hostname types (Hostnamentypen für Amazon-EC2-Instances).
- Erstellen oder ändern Sie Ihre Netzwerk-ACLs. Weitere Informationen finden Sie unter Datenverkehr in Subnetzen mit Netzwerk-ACLs steuern.
- Geben Sie das Subnetz für andere Konten frei. Weitere Informationen finden Sie unter ???.

Konfigurieren Sie Ihre Subnetze

Verwenden Sie die folgenden Verfahren, um Ihre Subnetze für Ihre Virtual Private Cloud (VPC) zu konfigurieren.

Aufgaben

- Anzeigen Ihrer Subnetze
- Hinzufügen eines IP6-CIDR-Blocks zu Ihrem Subnetz
- Entfernen Sie einen IPv6-CIDR-Block aus Ihrem Subnetz
- Ändern des öffentlichen IPv4-Adressierungsattributs Ihres Subnetzes
- Ändern des IPv6-Adressierungsattributs Ihres Subnetzes

Anzeigen Ihrer Subnetze

Führen Sie die Schritte im folgenden Abschnitt aus, um die Details zu Ihrem Subnetz anzuzeigen.

So können Sie sich die Subnetz-Details mithilfe der Konsole anzeigen lassen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Aktivieren Sie das Kontrollkästchen für das Subnetz oder wählen Sie die Subnetz-ID aus, um die Detailseite zu öffnen.

Um ein Subnetz mit dem zu beschreiben AWS CLI

Verwenden Sie den Befehl describe-subnets.

So zeigen Sie Ihre Subnetze über alle Regionen an

Öffnen Sie die Amazon EC2 Global View-Konsole unter https://console.aws.amazon.com/ec2globalview/home. Weitere Informationen finden Sie unter Ressourcen mithilfe von Amazon EC2 Global View auflisten und filtern im Amazon EC2 EC2-Benutzerhandbuch.

Hinzufügen eines IP6-CIDR-Blocks zu Ihrem Subnetz

Sie können einen IPv6 CIDR-Block in Ihrer VPC mit einem vorhandenen Subnetz verknüpfen. Das Subnetz darf keinem vorhandenen IPv6 CIDR-Block zugewiesen sein.

Hinzufügen eines IP6-CIDR-Blocks zu einem Subnetz

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Wählen Sie das Subnetz und dann Actions (Aktionen) und Edit IPv6 CIDRs (IPv6-CIDRs bearbeiten) aus.
4. Wählen Sie Add IPv6 CIDR aus.
5. Wählen Sie einen VPC-CIDR-Block, geben Sie einen Subnetz-CIDR-Block ein und wählen Sie eine Netzmaskenlänge, die der Netzmaskenlänge der VPC-CIDR entspricht oder diese spezifischer ist. Wenn der VPC-Pool-CIDR beispielsweise /50 ist, können Sie für das Subnetz eine Netzmaskenlänge zwischen /50 und /64 wählen. Mögliche IPv6-Netzmaskenlängen liegen zwischen /44 und /64 in Schritten von /4.
6. Wählen Sie Speichern.

Um einen IPv6-CIDR-Block einem Subnetz zuzuordnen, verwenden Sie AWS CLI

Verwenden Sie den Befehl associate-subnet-cidr-block.

Entfernen Sie einen IPv6-CIDR-Block aus Ihrem Subnetz

Wenn Sie IPv6 in Ihrem Subnetz nicht mehr unterstützen möchten, das Subnetz aber weiterhin für die Erstellung von IPv4-Ressourcen und für die Kommunikation mit ihnen verwenden möchten, können Sie den IPv6-CIDR-Blocks entfernen.

Bevor Sie einen IPv6-CIDR-Block entfernen können, müssen Sie zunächst die Zuordnung aller IPv6-Adressen aufheben, die Instances in Ihrem Subnetz zugeordnet sind.

Wie Sie einen IPv6-CIDR-Block aus Ihrem Subnetz entfernen

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

2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Wählen Sie das Subnetz und dann Actions (Aktionen) und Edit IPv6 CIDRs (IPv6-CIDRs bearbeiten) aus.
4. Suchen Sie nach dem IPv6-CIDR-Block und wählen Sie Remove (Entfernen) aus.
5. Wählen Sie Speichern.

Um die Zuordnung eines IPv6-CIDR-Blocks zu einem Subnetz zu trennen, verwenden Sie AWS CLI

Verwenden Sie den Befehl disassociate-subnet-cidr-block.

Ändern des öffentlichen IPv4-Adressierungsattributs Ihres Subnetzes

Standardmäßig ist das öffentliche IPv4-Adressierungsattribut für nicht standardmäßige Subnetze auf `false` eingestellt. Für standardmäßige Subnetze ist dieses Attribut auf `true` eingestellt. Eine Ausnahme stellt dabei ein nicht standardmäßiges Subnetz dar, das durch den Amazon EC2-Startassistenten der Instance erstellt wird. Hierbei legt der Assistent das Attribut auf fes `true`. Sie können dieses Attribut mit der Amazon VPC-Konsole ändern.

Ändern des öffentlichen IPv4-Adressierungsverhaltens Ihres Subnetzes

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Wählen Sie Ihr Subnetz und anschließend Actions (Aktionen), Edit subnet settings (Subnetz-Einstellungen bearbeiten) aus.
4. Wird das Kontrollkästchen Enable auto-assign public IPv4 address aktiviert, werden allen Instances, die im ausgewählten Subnetz gestartet werden, öffentliche IPv4-Adressen zugewiesen. Aktivieren oder deaktivieren Sie das Kontrollkästchen je nach Bedarf und klicken Sie anschließend auf Speichern.

Um ein Subnetzattribut mit dem zu ändern AWS CLI

Verwenden Sie den Befehl modify-subnet-attribute.

Ändern des IPv6-Adressierungsattributs Ihres Subnetzes

Standardmäßig ist das IPv6-Adressierungsattribut aller Subnetze auf eingestell `false`. Sie können dieses Attribut mit der Amazon VPC-Konsole ändern. Wenn Sie das IPv6-Adressierungsattribut Ihres

Subnetzes aktivieren, erhalten die im Subnetz erstellten Netzwerkschnittstellen eine IPv6-Adresse aus dem Subnetzbereich. Instances, die im Subnetz gestartet werden, erhalten eine IPv6-Adresse auf der primären Netzwerkschnittstelle.

Ihr Subnetz muss über einen zugeordneten IPv6 CIDR-Block verfügen.

> **Note**
>
> Wenn Sie das IPv6-Adressierungsfeature Ihres Subnetzes aktivieren, erhält Ihre Schnittstelle oder Ihre Instance nur dann eine IPv6-Adresse, wenn sie mithilfe der Amazon-EC2-API-Version `2016-11-15` oder höher erstellt wurde. Die Amazon EC2-Konsole verwendet die neueste API-Version.

Ändern des öffentlichen IPv6-Adressierungsverhaltens Ihres Subnetzes

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Wählen Sie Ihr Subnetz und anschließend Actions (Aktionen), Edit subnet settings (Subnetz-Einstellungen bearbeiten) aus.
4. Wird das Kontrollkästchen Enable auto-assign IPv6 address aktiviert, werden allen Netzwerkschnittstellen, die im ausgewählten Subnetz gestartet werden, IPv6-Adressen zugewiesen. Aktivieren oder deaktivieren Sie das Kontrollkästchen je nach Bedarf und klicken Sie anschließend auf Speichern.

Um ein Subnetzattribut zu ändern, verwenden Sie den AWS CLI

Verwenden Sie den Befehl modify-subnet-attribute.

Subnetz-CIDR-Reservierungen

Eine Subnetz-CIDR-Reservierung ist ein Bereich von IPv4- oder IPv6-Adressen, die Sie so reserviert haben, dass sie Ihren Netzwerkschnittstellen nicht zugewiesen AWS werden können. Dadurch können Sie IPv4- oder IPv6-CIDR-Blöcken (auch „Präfixe“ genannt) für die Verwendung mit Ihren Netzwerkschnittstellen reservieren.

Wenn Sie eine Subnetz-CIDR-Reservierung erstellen, geben Sie an, wie Sie die reservierten IP-Adressen verwenden werden. Verfügbar sind die nachfolgend aufgeführten Optionen:

- Präfix — AWS weist Netzwerkschnittstellen Adressen aus dem reservierten IP-Adressbereich zu. Weitere Informationen finden Sie unter Zuweisen von Präfixen zu Amazon EC2 EC2-Netzwerkschnittstellen im Amazon EC2 EC2-Benutzerhandbuch.
- Explizit – Sie weisen manuell IP-Adressen Netzwerkschnittstellen zu.

Die folgenden Regeln gelten für Subnetz-CIDR-Reservierungen:

- Wenn Sie eine Subnetz-CIDR-Reservierung erstellen, kann der IP-Adressbereich Adressen enthalten, die bereits verwendet werden. Durch das Erstellen einer Subnetzreservierung wird die Zuweisung von IP-Adressen, die bereits verwendet werden, nicht aufgehoben.
- Sie können mehrere CIDR-Bereiche pro Subnetz reservieren. Wenn Sie mehrere CIDR-Bereiche innerhalb derselben VPC reservieren, können sich die CIDR-Bereiche nicht überlappen.
- Wenn Sie mehr als einen Bereich in einem Subnetz für die Präfix-Delegierung reservieren und die Präfix-Delegierung für die automatische Zuweisung konfiguriert ist, wählen wir die IP-Adressen, die den Netzwerkschnittstellen zugewiesen werden, nach dem Zufallsprinzip aus.
- Wenn Sie eine Subnetzreservierung löschen, können Sie die ungenutzten IP-Adressen Ihren AWS Netzwerkschnittstellen zuweisen. Durch das Löschen einer Subnetzreservierung wird die Zuweisung der verwendeten IP-Adressen nicht aufgehoben.

Weitere Informationen zur CIDR-Notation (Classless Inter-Domain Routing) finden Sie unter IP-Adressierung.

Arbeiten mit Subnetz-CIDR-Reservierungen mithilfe der Konsole

Sie können Subnetz-CIDR-Reservierungen wie folgt erstellen und verwalten.

So bearbeiten Sie Subnetz-CIDR-Reservierungen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
3. Wählen Sie das Subnetz aus.
4. Wählen Sie die Registerkarte CIDR-Reservierungen, um Informationen zu vorhandenen CIDR-Reservierungen für Subnetze abzurufen.
5. Um CIDR-Reservierungen für Subnetze hinzuzufügen oder zu entfernen, wählen Sie Aktionen und CIDR-Reservierungen bearbeiten und gehen Sie dann wie folgt vor:

- Um eine IPv4-CIDR-Reservierung hinzuzufügen, wählen Sie IPv4, Add IPv4 CIDR reservation (IPv4-CIDR-Reservierung hinzufügen) aus. Wählen Sie den Reservierungstyp, geben Sie den CIDR-Bereich ein und wählen Sie Add (Hinzufügen) aus.
- Um eine IPv6-CIDR-Reservierung hinzuzufügen, wählen Sie IPv6, IPv6-CIDR-Reservierung hinzufügen aus. Wählen Sie den Reservierungstyp, geben Sie den CIDR-Bereich ein und wählen Sie Add (Hinzufügen) aus.
- Um eine CIDR-Reservierung zu entfernen, wählen Sie Entfernen für die entsprechend CIDR-Reservierung für Subnetze.

Arbeiten Sie mit CIDR-Reservierungen für Subnetze mithilfe der AWS CLI

Sie können den verwenden, AWS CLI um CIDR-Reservierungen für Subnetze zu erstellen und zu verwalten.

Aufgaben

- Erstellen einer Subnetz-CIDR-Reservierung
- Subnetz-CIDR-Reservierungen anzeigen
- Subnetz-CIDR-Reservierungen löschen

Erstellen einer Subnetz-CIDR-Reservierung

Sie können create-subnet-cidr-reservation verwenden, um eine Subnetz-CIDR-Reservierung zu erstellen.

```
aws ec2 create-subnet-cidr-reservation --subnet-id subnet-03c51e2eEXAMPLE --
reservation-type prefix --cidr 2600:1f13:925:d240:3a1b::/80
```

Es folgt eine Beispielausgabe.

```
{
    "SubnetCidrReservation": {
        "SubnetCidrReservationId": "scr-044f977c4eEXAMPLE",
        "SubnetId": "subnet-03c51e2ef5EXAMPLE",
        "Cidr": "2600:1f13:925:d240:3a1b::/80",
        "ReservationType": "prefix",
        "OwnerId": "123456789012"
    }
```

```
}
```

Subnetz-CIDR-Reservierungen anzeigen

Sie können get-subnet-cidr-reservations verwenden, um die Details einer Subnetz-CIDR-Reservierung anzuzeigen.

```
aws ec2 get-subnet-cidr-reservations --subnet-id subnet-05eef9fb78EXAMPLE
```

Subnetz-CIDR-Reservierungen löschen

Sie können delete-subnet-cidr-reservation verwenden, um eine Subnetz-CIDR-Reservierung zu löschen.

```
aws ec2 delete-subnet-cidr-reservation --subnet-cidr-reservation-
id scr-044f977c4eEXAMPLE
```

Konfigurieren von Routing-Tabellen

Eine Routing-Tabelle enthält Regeln, sogenannte Routen, die festlegen, wohin der Netzwerkverkehr von Ihrem Subnetz oder Gateway gelenkt wird.

Inhalt

Routing-Tabellen-Konzepte

Im Folgenden sind die wichtigsten Konzepte für Routing-Tabellen aufgeführt.

- Haupt-Routing-Tabelle – Die Routing-Tabelle, die automatisch mit Ihrer VPC geliefert wird. Diese steuert das Routing für alle Subnetze, denen nicht ausdrücklich eine andere Routing-Tabelle zugeordnet ist.
- Benutzerdefinierte Routing-Tabelle – Eine Routing-Tabelle, die Sie für Ihre VPC erstellen.
- Ziel – Der Bereich von IP-Adressen, zu dem der Datenverkehr gelangen soll (Ziel-CIDR). Zum Beispiel ein externes Unternehmensnetzwerk mit einem `172.16.0.0/12`-CIDR.
- Ziel – Das Gateway, die Netzwerkschnittstelle oder die Verbindung, über die der Zieldatenverkehr gesendet werden soll, z. B. ein Internet-Gateway.
- Routing-Tabellenzuordnung – Die Zuordnung zwischen einer Routing-Tabelle und einem Subnetz, einem Internet-Gateway oder einem Virtual Private Gateway.
- Subnetz-Routing-Tabelle – Eine Routing-Tabelle, die einem Subnetz zugeordnet ist.
- Lokale Route – Eine Standardroute für die Kommunikation innerhalb der VPC.
- Verteilung – Wenn Sie ein Virtual Private Gateway an Ihre VPC angefügt und die Routing-Verteilung aktiviert haben, fügen wir Ihren Subnetz-Routing-Tabellen automatisch Routen für Ihre VPN-Verbindung hinzu. Das bedeutet, dass Sie VPN-Routen nicht manuell hinzufügen oder entfernen müssen. Weitere Informationen finden Sie unter Site-to-Site-VPN-Routing-Optionen im Site-to-Site-VPN-Benutzerhandbuch.
- Gateway-Routing-Tabelle – Eine Routing-Tabelle, die einem Internet-Gateway oder einem Virtual Private Gateway zugeordnet ist.
- Edge-Zuordnung – Eine Routing-Tabelle, mit der Sie eingehenden VPC-Datenverkehr an eine Appliance weiterleiten. Sie ordnen eine Routing-Tabelle dem Internet-Gateway oder dem Virtual Private Gateway zu und geben die Netzwerkschnittstelle Ihrer Appliance als Ziel für den VPC-Datenverkehr an.
- Transit Gateway-Routing-Tabelle – Eine Routing-Tabelle, die einem Transit Gateway zugeordnet ist. Weitere Informationen finden Sie unter Transit-Gateway-Routing-Tabellen in Amazon-VPC-Transit-Gateways.
- Lokale Gateway-Routing-Tabelle – Eine Routing-Tabelle, die einem lokalen Gateway von Outposts zugeordnet ist. Weitere Informationen finden Sie unter Lokale Gateways im AWS Outposts - Benutzerhandbuch.

Subnetz-Routingtabellen

Ihre VPC verfügt über einen impliziten Router und Sie verwenden Routing-Tabellen, um zu steuern, wohin der Netzwerkdatenverkehr geleitet wird. Jedem Subnetz in Ihrer VPC muss eine Routing-

Tabelle zugeordnet werden. Diese Tabelle steuert das Routing für das Subnetz. Sie können ein Subnetz einer bestimmten Routing-Tabelle explizit zuordnen. Andernfalls wird das Subnetz implizit der Haupt-Routing-Tabelle zugeordnet. Ein Subnetz kann jeweils nur mit einer Routing-Tabelle verknüpft sein, aber Sie können einer Routing-Tabelle mehrere Subnetze zuordnen.

Inhalt

Routen

Jede Route in einer Tabelle gibt einen Zielbereich und ein Ziel an. Wenn Ihr Subnetz beispielsweise über ein Internet-Gateway auf das Internet zugreifen kann, fügen Sie der Subnetz-Routing-Tabelle die folgende Route hinzu. Der Zielbereich für die Route ist `0.0.0.0/0`, das für alle IPv4-Adressen steht. Das Ziel ist das Internet-Gateway, das an Ihre VPC angeschlossen ist.

Bestimmungsort	Ziel
0.0.0.0/0	*igw-id*

CIDR-Blöcke für IPv4 und IPv6 werden separat behandelt. Eine Route mit dem Zielbereich-CIDR `0.0.0.0/0` schließt daher nicht automatisch auch alle IPv6-Adressen ein. Sie müssen für die IPv6-Adressen eine eigene Route mit dem Zielbereich-CIDR `::/0` erstellen.

Wenn Sie in Ihren AWS Ressourcen häufig auf denselben Satz von CIDR-Blöcken verweisen, können Sie eine vom Kunden verwaltete Präfixliste erstellen, um sie zu gruppieren. Anschließend können Sie die Präfixliste als Ziel in Ihrem Routing-Tabelleneintrag angeben.

Jede Routing-Tabelle enthält eine lokale Route für die Kommunikation innerhalb der VPC. Diese Route wird standardmäßig allen Routing-Tabellen hinzugefügt. Wenn Ihr VPC mehrere IPv4-CIDR-Blöcke hat, enthalten Ihre Routing-Tabellen eine lokale Route für jeden IPv4-CIDR-Block. Wenn Sie der VPC einen IPv6-CIDR-Block zugeordnet haben, enthalten Ihre Routing-Tabellen eine lokale Route für den IPv6 CIDR-Block. Sie können das Ziel jeder lokalen Route nach Bedarf ersetzen oder wiederherstellen.

Regeln und Überlegungen

- Sie können Ihren Routing-Tabellen eine Route hinzufügen, die spezifischer als die lokale Route ist. Das Ziel muss mit dem gesamten IPv4- oder IPv6-CIDR-Block eines Subnetzes in Ihrer VPC übereinstimmen. Das Ziel muss ein NAT-Gateway, eine Netzwerkschnittstelle oder ein Gateway Load Balancer-Endpunkt sein.
- Wenn Ihre Routing-Tabelle mehrere Routen enthält, verwenden wir die spezifischste mit dem Datenverkehr übereinstimmende Route in der Routing-Tabelle, um Datenverkehr weiterzuleiten (Übereinstimmung mit dem längsten Präfix).
- Sie können keine Routen zu IPv4-Adressen hinzufügen, die dem folgenden Bereich genau entsprechen oder eine Teilmenge davon darstellen: 169.254.168.0/22. Dieser Bereich befindet sich innerhalb des Link-Local-Adressraums und ist für Dienste reserviert. AWS Amazon EC2 nutzt Adressen in diesem Bereich beispielsweise für Services, die nur über EC2-Instances zugänglich sind, z. B. den Instance Metadata Service (IMDS) und den Amazon-DNS-Server. Sie können einen CIDR-Block verwenden, der größer ist als der Bereich 169.254.168.0/22 und diesen überlappt. Allerdings werden Pakete, die für Adressen im Bereich 169.254.168.0/22 bestimmt sind, nicht weitergeleitet.
- Sie können keine Routen zu IPv6-Adressen hinzufügen, die dem folgenden Bereich genau entsprechen oder eine Teilmenge davon darstellen: fd00:ec2::/32. Dieser Bereich liegt innerhalb des ULA (Unique Local Address) -Bereichs und ist für die Nutzung durch AWS Dienste reserviert. Amazon EC2 nutzt Adressen in diesem Bereich beispielsweise für Services, die nur über EC2-Instances zugänglich sind, z. B. den Instance Metadata Service (IMDS) und den Amazon-DNS-Server. Sie können einen CIDR-Block verwenden, der größer ist als der Bereich fd00:ec2::/32 und diesen überlappt. Allerdings werden Pakete, die für Adressen im Bereich fd00:ec2::/32 bestimmt sind, nicht weitergeleitet.
- Sie können Middlebox-Appliances zu den Routing-Pfaden für Ihre VPC hinzufügen. Weitere Informationen finden Sie unter the section called “Routing für eine Middlebox-Appliance”.

Beispiel

Nehmen Sie im folgenden Beispiel an, dass die VPC sowohl einen IPv4-CIDR-Block als auch einen IPv6-CIDR-Block hat. IPv4- und IPv6-Datenverkehr wird getrennt behandelt, wie in der folgenden Routing-Tabelle dargestellt.

Bestimmungsort	Ziel
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Local
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567
::/0	eigw-aabbccddee1122334

- IPv4-Datenverkehr, der innerhalb der VPC (10.0.0.0/16) geroutet werden soll, wird von der Route Local abgedeckt.
- IPv6-Datenverkehr, der innerhalb der VPC (2001:db8:1234:1a00::/56) geroutet werden soll, wird von der Route Local abgedeckt.
- Die Route für 172.31.0.0/16 sendet Datenverkehr an eine Peering-Verbindung.
- Die Route für den gesamten IPv4-Datenverkehr (0.0.0.0/0) sendet Datenverkehr an ein Internet-Gateway. Daher wird der gesamte IPv4-Datenverkehr, mit Ausnahme des Datenverkehrs innerhalb der VPC und der Peering-Verbindung, an das Internet-Gateway weitergeleitet.
- Die Route für den gesamten IPv6-Verkehr (::/0) sendet nur ausgehenden Datenverkehr an ein Internet-Gateway. Daher wird der gesamte IPv6-Datenverkehr, mit Ausnahme des Datenverkehrs innerhalb der VPC, an das Internet-Gateway mit ausgehendem Datenverkehr weitergeleitet.

Haupt-Routing-Tabelle

Nachdem Sie eine VPC erstellt haben, besitzt diese automatisch eine Haupt-Routing-Tabelle. Wenn einem Subnetz keine explizite Routing-Tabelle zugeordnet ist, wird standardmäßig die Haupt-Routing-Tabelle verwendet. Auf der Seite Route Tables (Routing-Tabellen) der Amazon-VPC-Konsole sehen Sie anhand des Eintrags Yes (Ja) in der Spalte Main (Haupttabelle), welche Tabelle die Haupt-Routing-Tabelle der VPC ist.

Wenn Sie eine nicht standardmäßige VPC erstellen, enthält die Haupt-Routing-Tabelle standardmäßig nur eine lokale Route. Wenn Sie Erstellen einer VPC und ein NAT-Gateway auswählen, fügt Amazon VPC automatisch Routen zur Haupt-Routing-Tabelle für die Gateways hinzu.

Die folgenden Regeln gelten für die Haupt-Routingtabelle:

- Sie können Routen in der Haupt-Routing-Tabelle hinzufügen, verändern oder daraus entfernen.
- Die Haupt-Routing-Tabelle kann nicht gelöscht werden.
- Sie können keine Gateway-Routing-Tabelle als Haupt-Routing-Tabelle festlegen.
- Sie können die Haupt-Routing-Tabelle ersetzen, indem Sie eine benutzerdefinierte Routing-Tabelle einem Subnetz zuordnen.
- Sie können einem Subnetz explizit die Haupt-Routing-Tabelle zuordnen, auch wenn diese bereits implizit zugeordnet ist.

  Möglicherweise möchten Sie dies tun, wenn Sie ändern, welche Tabelle die Haupt-Routing-Tabelle ist. Wenn Sie die Haupt-Routing-Tabelle ändern, wird auch die Standardtabelle für neu hinzugefügte Subnetze sowie Subnetze ohne explizit zugeordnete Routing-Tabelle geändert. Weitere Informationen finden Sie unter So ersetzen Sie die Routing-Haupttabelle.

Benutzerdefinierte Routing-Tabellen

Jede Routing-Tabelle enthält standardmäßig eine lokale Route für die Kommunikation innerhalb der VPC. Wenn Sie Erstellen einer VPC und ein öffentliches Subnetz wählen, erstellt Amazon VPC eine benutzerdefinierte Routing-Tabelle und fügt eine Route hinzu, die auf das Internet-Gateway verweist. Eine Möglichkeit, Ihre VPC zu schützen, besteht darin, die Haupt-Routing-Tabelle in ihrem ursprünglichen Standardzustand zu belassen. Ordnen Sie dann jedes neue Subnetz, das Sie erstellen, explizit einer der von Ihnen erstellten benutzerdefinierten Routing-Tabellen zu. So wird sichergestellt, dass Sie die Weiterleitung des Datenverkehrs der einzelnen Subnetze explizit steuern können.

Sie können Routen in der benutzerdefinierten Routing-Tabelle hinzufügen, ändern oder daraus entfernen. Sie können eine benutzerdefinierte Routing-Tabelle nur löschen, wenn sie keine Zuordnungen hat.

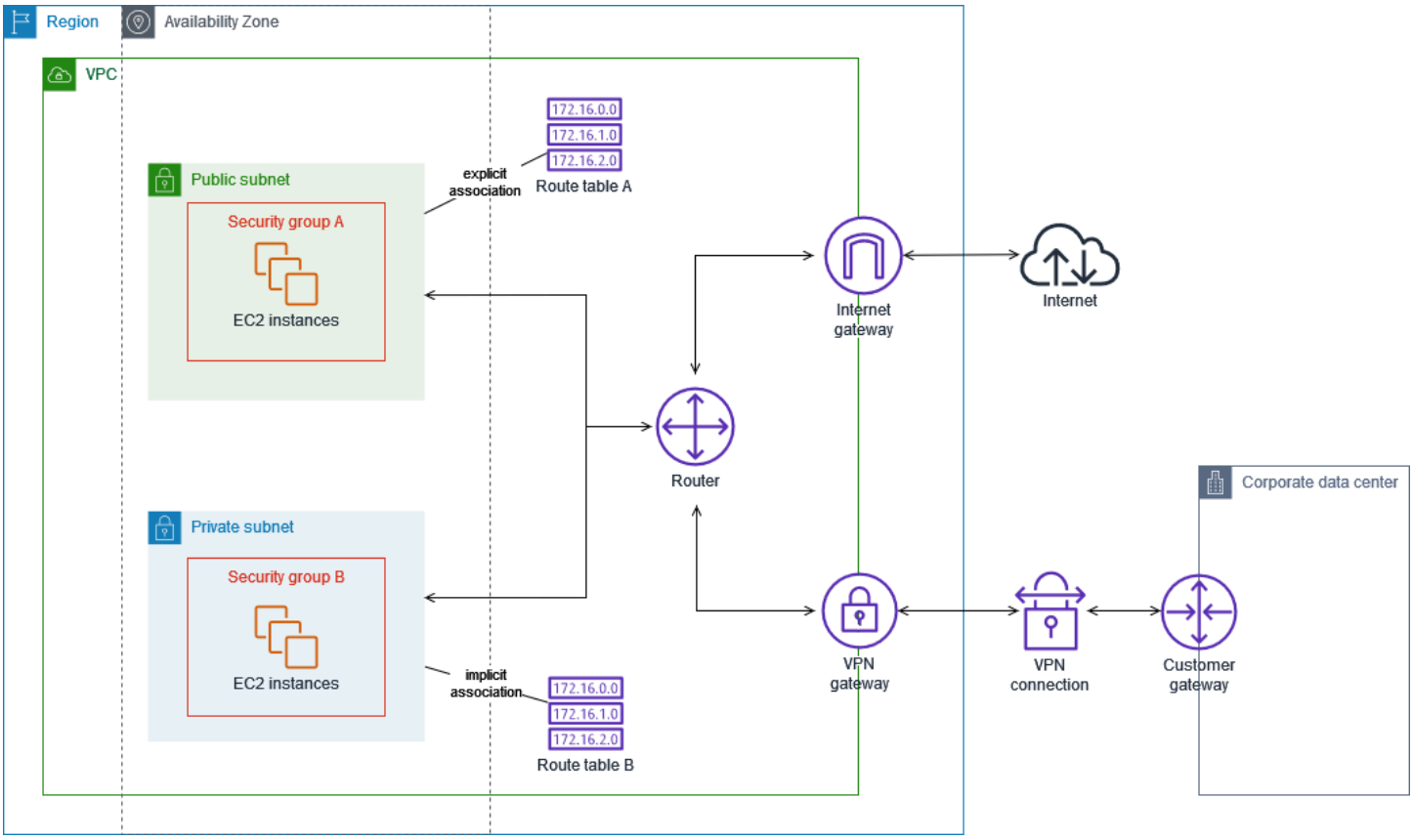
Zuordnung der Subnetz-Routing-Tabelle

Jedes Subnetz in Ihrer VPC muss mit einer Routing-Tabelle verknüpft sein. Ein Subnetz kann explizit mit einer benutzerdefinierten Routing-Tabelle oder implizit oder explizit mit der Haupt-Routing-Tabelle verknüpft werden. Weitere Hinweise zum Anzeigen der Subnetz- und Routing-Tabellenzuordnungen finden Sie unter Bestimmen, welche Subnetze und/oder Gateways explizit zugeordnet sind.

Subnetze, die sich in VPCs befinden, die mit Outposts verknüpft sind, können einen zusätzlichen Zieltyp eines lokalen Gateways haben. Dies ist der einzige Routing-Unterschied zu Nicht-Outposts-Subnetzen.

Beispiel 1: Implizite und explizite Subnetzzuordnung

Die folgende Abbildung zeigt das Routing für eine VPC mit einem Internet-Gateway und einem Virtual Private Gateway sowie einem öffentlichen Subnetz und einem reinen VPN-Subnetz.



Routing-Tabelle A ist eine benutzerdefinierte Routing-Tabelle, die dem öffentlichen Subnetz explizit zugeordnet ist. Darin enthalten ist eine Route, die den gesamten Datenverkehr an das Internet-Gateway sendet, was das Subnetz zu einem öffentlichen Subnetz macht.

Bestimmungsort	Ziel
VPC-CIDR	Local
0.0.0.0/0	*igw-id*

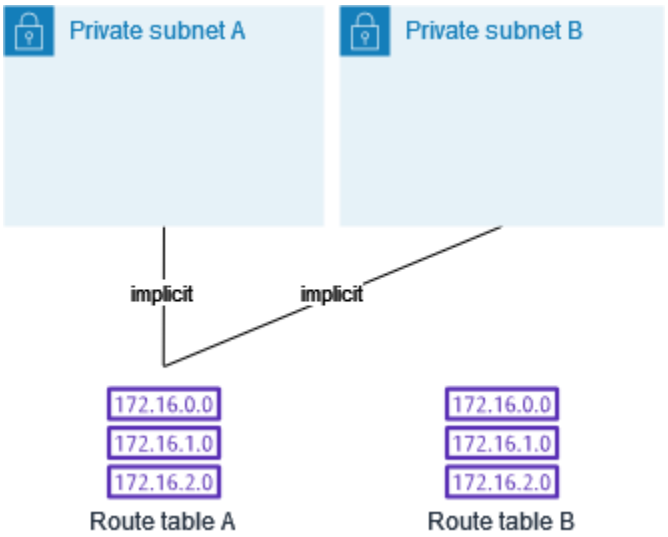
Routing-Tabelle B ist die Haupt-Routing-Tabelle. Es besteht implizit eine Zuordnung zum dem privaten Subnetz. Darin enthalten ist eine Route, die den gesamten Datenverkehr an das virtuelle private Gateway sendet, aber keine Route zum Internet-Gateway, was das Subnetz zu einem reinen VPN-Subnetz macht. Wenn Sie in dieser VPC ein weiteres Subnetz erstellen und keine benutzerdefinierte Routing-Tabelle zuordnen, wird das Subnetz auch implizit dieser Routing-Tabelle zugeordnet, da es sich um die Haupt-Routing-Tabelle handelt.

Bestimmungsort	Ziel
VPC-CIDR	Local
0.0.0.0/0	*vgw-id*

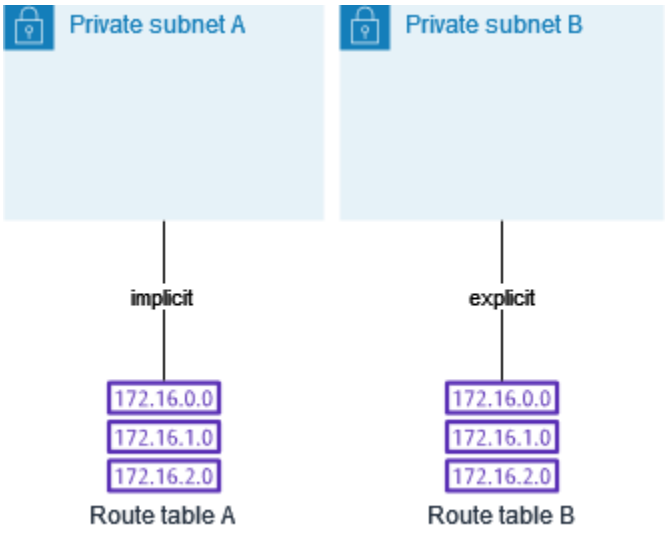
Beispiel 2: Ersetzen der Haupt-Routing-Tabelle

Möglicherweise möchten Sie Änderungen an der Haupt-Routing-Tabelle vornehmen. Um Störungen des Datenverkehrs zu vermeiden, empfehlen wir, zuerst die Routenänderungen mithilfe einer benutzerdefinierten Routing-Tabelle zu testen. Wenn Sie mit dem Ergebnis des Tests zufrieden sind, können Sie die Haupt-Routing-Tabelle durch die neue benutzerdefinierte Tabelle ersetzen.

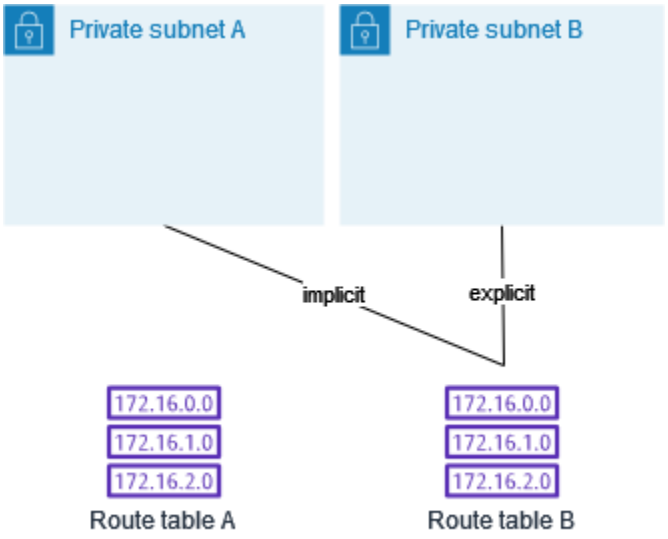
Das folgende Diagramm zeigt zwei Subnetze und zwei Routing-Tabellen. Subnetz A ist implizit der Routing-Tabelle A, der Haupt-Routing-Tabelle, zugeordnet. Subnetz B ist implizit der Routing-Tabelle A zugeordnet. Die Routing-Tabelle B, eine benutzerdefinierte Routing-Tabelle, ist keinem der Subnetze zugeordnet.



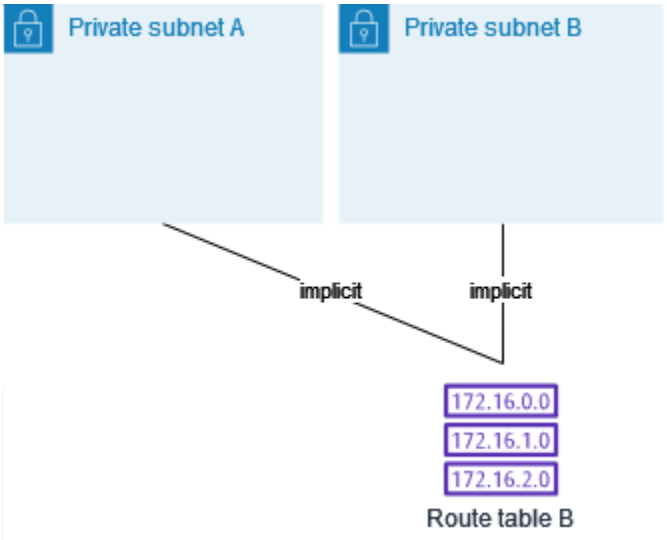
Um die Haupt-Routing-Tabelle zu ersetzen, erstellen Sie zunächst eine explizite Zuordnung zwischen Subnetz B und Routing-Tabelle B. Testen Sie die Routing-Tabelle B.



Nachdem Sie die Routing-Tabelle B getestet haben, machen Sie sie zur Haupt-Routing-Tabelle. Subnetz B hat immer noch eine explizite Zuordnung zur Routing-Tabelle B. Subnetz A hat jedoch jetzt eine implizite Zuordnung zur Routing-Tabelle B, da die Routing-Tabelle B die neue Haupt-Routing-Tabelle ist. Die Routing-Tabelle A ist keinem der Subnetze mehr zugeordnet.



(Optional) Wenn Sie das Subnetz B von der Routing-Tabelle B trennen, besteht weiterhin eine implizite Verbindung zwischen Subnetz B und Routing-Tabelle B. Wenn Sie die Routing-Tabelle A nicht mehr benötigen, können Sie sie löschen.



Gateway-Routing-Tabellen

Sie können eine Routing-Tabelle einem Internet-Gateway oder einem Virtual Private Gateway zuordnen. Wenn eine Routing-Tabelle einem Gateway zugeordnet ist, wird sie als Gateway-Routing-Tabellebezeichnet. Sie können eine Gateway-Routing-Tabelle erstellen, um den Routing-Pfad des Datenverkehrs in Ihre VPC genau zu steuern. Beispielsweise können Sie den Datenverkehr, der über ein Internet-Gateway in Ihre VPC gelangt, abfangen, indem Sie diesen Datenverkehr an eine Middlebox-Appliance (wie etwa eine Sicherheitseinheit) in Ihrer VPC umleiten.

Inhalt

Route von Gateway-Routing-Tabellen

Eine Gateway-Routing-Tabelle, die einem Internet-Gateway zugeordnet ist, unterstützt Routen mit den folgenden Zielen:

- Die standardmäßige lokale Route
- Gateway-Load-Balancer-Endpunkt
- Eine Netzwerkschnittstelle für eine Middlebox-Appliance

Eine einem Virtual Private Gateway zugeordnete Gateway-Routing-Tabelle unterstützt Routen mit den folgenden Zielen:

- Die standardmäßige lokale Route
- Gateway-Load-Balancer-Endpunkt
- Eine Netzwerkschnittstelle für eine Middlebox-Appliance

Wenn das Ziel ein Gateway Load Balancer-Endpunkt oder eine Netzwerkschnittstelle ist, sind folgende Ziele zulässig:

- Der gesamte IPv4- oder IPv6-CIDR-Block Ihrer VPC. In diesem Fall ersetzen Sie das Ziel der lokalen Standardroute.
- Der gesamte IPv4- oder IPv6-CIDR-Block eines Subnetzes in Ihrer VPC. Dies ist eine spezifischere Route als die lokale Standardroute.

Wenn Sie das Ziel der lokalen Route in einer Gateway-Routing-Tabelle zu einer Netzwerkschnittstelle in Ihrer VPC ändern, können Sie es später auf das `local`-Standardziel wiederherstellen. Weitere Informationen finden Sie unter Ersetzen oder Wiederherstellen des Ziels für eine lokale Route.

Beispiel

In der folgenden Gateway-Routing-Tabelle wird der für ein Subnetz mit dem `172.31.0.0/20`-CIDR-Block bestimmte Datenverkehr an eine bestimmte Netzwerkschnittstelle weitergeleitet. Datenverkehr, der für alle anderen Subnetze in der VPC bestimmt ist, verwendet die lokale Route.

Ziel	Ziel
172.31.0.0/16	Local
172.31.0.0/20	*eni-id*

Beispiel

In der folgenden Gateway-Routing-Tabelle wird das Ziel für die lokale Route durch eine Netzwerkschnittstellen-ID ersetzt. Datenverkehr, der für alle Subnetze innerhalb der VPC bestimmt ist, wird an die Netzwerkschnittstelle weitergeleitet.

Ziel	Ziel
172.31.0.0/16	*eni-id*

Regeln und Überlegungen

Sie können eine Routing-Tabelle einem Gateway nicht zuordnen, wenn eine der folgenden Punkte zutrifft:

- Die Routingtabelle enthält vorhandene Routen mit anderen Zielen als einer Netzwerkschnittstelle, einem Gateway Load Balancer-Endpunkt oder der lokalen Standardroute.
- Die Routing-Tabelle enthält vorhandene Routen zu CIDR-Blöcken außerhalb der Bereiche in Ihrer VPC.
- Die Routenverbreitung ist für die Routing-Tabelle aktiviert.

Darüber hinaus gelten die folgenden Regeln und Überlegungen:

- Sie können keine Routen zu CIDR-Blocks außerhalb der Bereiche in Ihrer VPC hinzufügen, einschließlich Bereiche, die größer sind als die einzelnen VPC-CIDR-Blöcke.
- Sie können nur `local`, einen Gateway Load Balancer-Endpunkt oder eine Netzwerkschnittstelle als Ziel angeben. Sie können keine anderen Zieltypen angeben, auch keine einzelnen Host-IP-Adressen. Weitere Informationen finden Sie unter the section called “Beispiele für Routing-Optionen”.
- Sie können keine Präfixliste als Ziel angeben.
- Sie können keine Gateway-Routing-Tabelle verwenden, um Datenverkehr außerhalb Ihrer VPC zu steuern oder abzufangen, z. B. den Datenverkehr über ein angeschlossenes Transit-Gateway. Sie können Datenverkehr, der in Ihre VPC eintritt, abfangen und nur an ein anderes Ziel in derselben VPC umleiten.
- Damit der Datenverkehr Ihre Middlebox-Appliance erreicht, muss die Zielnetzwerkschnittstelle an eine ausgeführte Instance angeschlossen sein. Für Datenverkehr, der durch ein Internet-Gateway fließt, muss die Zielnetzwerkschnittstelle auch über eine öffentliche IP-Adresse verfügen.
- Beachten Sie bei der Konfiguration der Middlebox-Appliance die Überlegungen zu Appliances.

- Wenn Sie Datenverkehr über eine Middlebox-Appliance weiterleiten, muss der Rückdatenverkehr aus dem Zielsubnetz über dieselbe Appliance geleitet werden. Asymmetrisches Routing wird nicht unterstützt.
- Routing-Tabellenregeln gelten für den gesamten Datenverkehr, der ein Subnetz verlässt. Datenverkehr, der ein Subnetz verlässt, wird als Datenverkehr definiert, der an die MAC-Adresse des Gatewayrouters dieses Subnetzes bestimmt ist. Der Datenverkehr, der für die MAC-Adresse einer anderen Netzwerkschnittstelle im Subnetz bestimmt ist, verwendet anstelle von Netzwerk (Schicht 3) das Datenlink-Routing (Ebene 2), sodass die Regeln nicht für diesen Datenverkehr gelten.
- Nicht alle Local Zones unterstützen die Edge-Verknüpfung mit virtuellen privaten Gateways. Weitere Informationen zu verfügbaren Zonen finden Sie unter Überlegungen im AWS - Benutzerhandbuch für Local Zones.

Routenpriorität

Im Allgemeinen leiten wir Datenverkehr über die spezifischste, mit dem Datenverkehr übereinstimmende, Route weiter. Dies wird als die längste Präfix-Übereinstimmung bezeichnet. Wenn Ihre Routing-Tabelle sich überschneidende oder übereinstimmende Routen enthält, gelten weitere Regeln.

Inhalt

Übereinstimmung mit längstem Präfix

Routen zu IPv4- und IPv6-Adressen oder CIDR-Blöcken sind voneinander unabhängig. Wir verwenden die spezifischste Route, die entweder dem IPv4-Datenverkehr oder dem IPv6-Datenverkehr entspricht, um zu bestimmen, wie der Datenverkehr weitergeleitet wird.

Die folgende Beispiel-Subnetz-Routing-Tabelle enthält eine Route für IPv4-Internetdatenverkehr (`0.0.0.0/0`), die diesen an ein Internet-Gateway leitet, sowie eine Route für IPv4-Datenverkehr (`172.31.0.0/16`), die auf eine Peering-Verbindung verweist (`pcx-11223344556677889`). Sämtlicher Datenverkehr aus dem Subnetz zum IP-Adressbereich `172.31.0.0/16` wird über die Peering-Verbindung geleitet, da diese Route spezifischer ist als die Route für das Internet-Gateway.

Sämtlicher Datenverkehr für Ziele innerhalb der VPC (`10.0.0.0/16`) wird durch die Route `local` abgedeckt und somit innerhalb der VPC weitergeleitet. Jeder andere Datenverkehr aus dem Subnetz wird über das Internet-Gateway geleitet.

Ziel	Ziel
10.0.0.0/16	Lokal
172.31.0.0/16	pcx-11223344556677889
0.0.0.0/0	igw-12345678901234567

Routenpriorität und propagierte Routen

Wenn Sie ein Virtual Private Gateway an Ihre VPC angefügt und die Routing-Verteilung in der Subnetz-Routing-Tabelle aktiviert haben, werden Routen, die die Site-to-Site VPN-Verbindung repräsentieren, in der Routing-Tabelle als automatisch propagierte Routen angezeigt.

Wenn sich das Ziel einer propagierte Route mit einer statische Route überlappt, hat die statische Route Priorität.

Wenn das Ziel einer propagierten Route identisch mit dem Ziel einer statischen Route ist, hat die statische Route Priorität, wenn das Ziel eines der folgenden ist:

- Internet-Gateway
- NAT-Gateway
- Netzwerkschnittstelle
- Instance-ID
- Gateway-VPC-Endpunkt
- Transit-Gateway
- VPC-Peering-Verbindung
- Gateway Load Balancer-Endpunkt

Weitere Informationen finden Sie unter Routing-Tabellen und VPN-Routenpriorität im AWS Site-to-Site VPN Benutzerhandbuch.

Die folgende Beispiel-Routing-Tabelle enthält eine statische Route zu einem Internet-Gateway und eine propagierte Route zu einem Virtual Private Gateway. Beide Routen haben den Zielbereich `172.31.0.0/24`. Da eine statische Route zu einem Internet-Gateway Vorrang hat, wird der gesamte Datenverkehr, der für `172.31.0.0/24` bestimmt ist, an das Internet-Gateway weitergeleitet.

Bestimmungsort	Ziel	Propagiert
10.0.0.0/16	Lokal	Nein
172.31.0.0/24	vgw-11223344556677889	Ja
172.31.0.0/24	igw-12345678901234567	Nein

Routenpriorität und Präfixlisten

Wenn Ihre Routing-Tabelle auf eine Präfixliste verweist, gelten die folgenden Regeln:

- Wenn Ihre Routing-Tabelle eine statische Route mit einem Ziel-CIDR-Block enthält, die eine statische Route mit einer Präfixliste überlappt, hat die statische Route mit dem CIDR-Block Priorität.
- Wenn Ihre Routing-Tabelle eine verbreitete Route enthält, die sich mit einer Route übereinstimmt, die auf eine Präfixliste verweist, hat die Route, die auf die Präfixliste verweist, Priorität. Bitte beachten Sie, dass bei sich überschneidenden Routen die spezifischeren Routen immer Vorrang haben, unabhängig davon, ob es sich um verbreitete Routen, statische Routen oder Routen handelt, die auf Präfixlisten verweisen.
- Wenn Ihre Routing-Tabelle auf mehrere Präfixlisten verweist, die sich überlappende CIDR-Blöcke zu verschiedenen Zielen haben, wählen wir zufällig aus, welche Route Priorität hat. Danach hat dieselbe Route immer Priorität.

Kontingente für Routing-Tabellen

Die Anzahl der Routing-Tabellen, die Sie pro VPC erstellen können, unterliegt einem Kontingent. Es gibt auch ein Kontingent für die Anzahl der Routen, die Sie pro Routing-Tabelle hinzufügen können. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.

Beheben Sie Probleme mit der Erreichbarkeit

Reachability Analyzer ist ein Tool zur statischen Konfigurationsanalyse. Verwenden Sie Reachability Analyzer, um die Netzwerkerreichbarkeit zwischen zwei Ressourcen in Ihrer VPC zu analysieren und zu debuggen. Reachability Analyzer erzeugt hop-by-hop Details zum virtuellen Pfad zwischen diesen Ressourcen, wenn sie erreichbar sind, und identifiziert andernfalls die blockierende Komponente. Es kann beispielsweise fehlende oder falsch konfigurierte Routentabellenrouten identifizieren.

Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

Beispiele für Routing-Optionen

In den folgenden Themen wird das Routing für bestimmte Gateways oder Verbindungen in Ihrer VPC erläutert.

Inhalt

Routing zu einem Internet-Gateway

Sie können ein Subnetz zu einem öffentlichen Subnetz machen, indem Sie eine Route in der Subnetz-Routing-Tabelle zu einem Internet-Gateway hinzufügen. Erstellen Sie dazu ein Internet-Gateway und fügen Sie es an Ihre VPC an. Fügen Sie dann eine Route mit dem Zielbereich `0.0.0.0/0` für IPv4-Datenverkehr oder `::/0` für IPv6-Datenverkehr und der Internet-Gateway-ID (`igw-xxxxxxxxxxxxxxxxx`) als Ziel hinzu.

Ziel	Ziel
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Weitere Informationen finden Sie unter Herstellen einer Internetverbindung über ein Internet-Gateway.

Routing zu einem NAT-Gerät

Damit Instances in einem privaten Subnetz eine Verbindung zum Internet herstellen können, können Sie ein NAT-Gateway erstellen oder eine NAT-Instance in einem öffentlichen Subnetz starten. Fügen Sie dann eine Route für die Routing-Tabelle des privaten Subnetzes hinzu, die IPv4-Internetverkehr (`0.0.0.0/0`) an das NAT-Gerät weiterleitet.

Ziel	Ziel
0.0.0.0/0	*nat-gateway-id*

Sie können auch spezifischere Routen zu anderen Zielen erstellen, um unnötige Datenverarbeitungsgebühren für die Verwendung eines NAT-Gateways zu vermeiden oder bestimmte Datenverkehrsdaten privat zu leiten. Im folgenden Beispiel wird der Amazon-S3-Datenverkehr (pl-xxxxxxxx, eine Präfixliste, die die IP-Adressbereiche für Amazon S3 in einer bestimmten Region enthält) an einen Gateway-VPC-Endpunkt und der 10.25.0.0/16-Datenverkehr an eine VPC-Peering-Verbindung weitergeleitet. Diese IP-Adressbereiche sind spezifischer als 0.0.0.0/0. Wenn Instances Datenverkehr an Amazon S3 oder an die Peer-VPC senden, wird der Datenverkehr an den Gateway-VPC-Endpunkt oder die VPC-Peering-Verbindung gesendet. Der gesamte andere Datenverkehr wird an das NAT-Gateway gesendet.

Ziel	Ziel
0.0.0.0/0	*nat-gateway-id*
pl-*xxxxxxxx*	*vpce-id*

Ziel	Ziel
10.25.0.0/16	*pcx-id*

Weitere Informationen finden Sie unter NAT-Geräte.

Routing zu einem Virtual Private Gateway

Sie können eine AWS Site-to-Site VPN Verbindung verwenden, um Instances in Ihrer VPC die Kommunikation mit Ihrem eigenen Netzwerk zu ermöglichen. Erstellen Sie dazu ein Virtual Private Gateway und fügen Sie es an Ihre VPC an. Fügen Sie dann eine Route in der Subnetz-Routing-Tabelle mit dem Zielbereich Ihres Netzwerks und einem Ziel des Virtual Private Gateways () hi (`vgw-xxxxxxxxxxxxxxxxx`).

Ziel	Ziel
10.0.0.0/16	*vgw-id*

Sie können dann Ihre Site-to-Site VPN-Verbindung erstellen und konfigurieren. Weitere Informationen finden Sie unter Was ist AWS Site-to-Site VPN? und Routing-Tabellen und VPN-Routenpriorität im AWS Site-to-Site VPN -Benutzerhandbuch.

Eine Site-to-Site VPN-Verbindung auf einem Virtual Private Gateway unterstützt keinen IPv6-Datenverkehr. Wir unterstützen jedoch IPv6-Datenverkehr zu einer AWS Direct Connect -Verbindung über ein Virtual Private Gateway. Weitere Informationen finden Sie im AWS Direct Connect - Benutzerhandbuch.

Routing zu einem AWS Outposts lokalen Gateway

In diesem Abschnitt werden Routingtabellenkonfigurationen für das Routing zu einem AWS Outposts lokalen Gateway beschrieben.

Inhalt

- Datenverkehr zwischen Outpost-Subnetzen und Ihrem On-Premises-Netzwerk ermöglichen
- Datenverkehr zwischen Subnetzen in derselben VPC über Outposts hinweg ermöglichen

Datenverkehr zwischen Outpost-Subnetzen und Ihrem On-Premises-Netzwerk ermöglichen

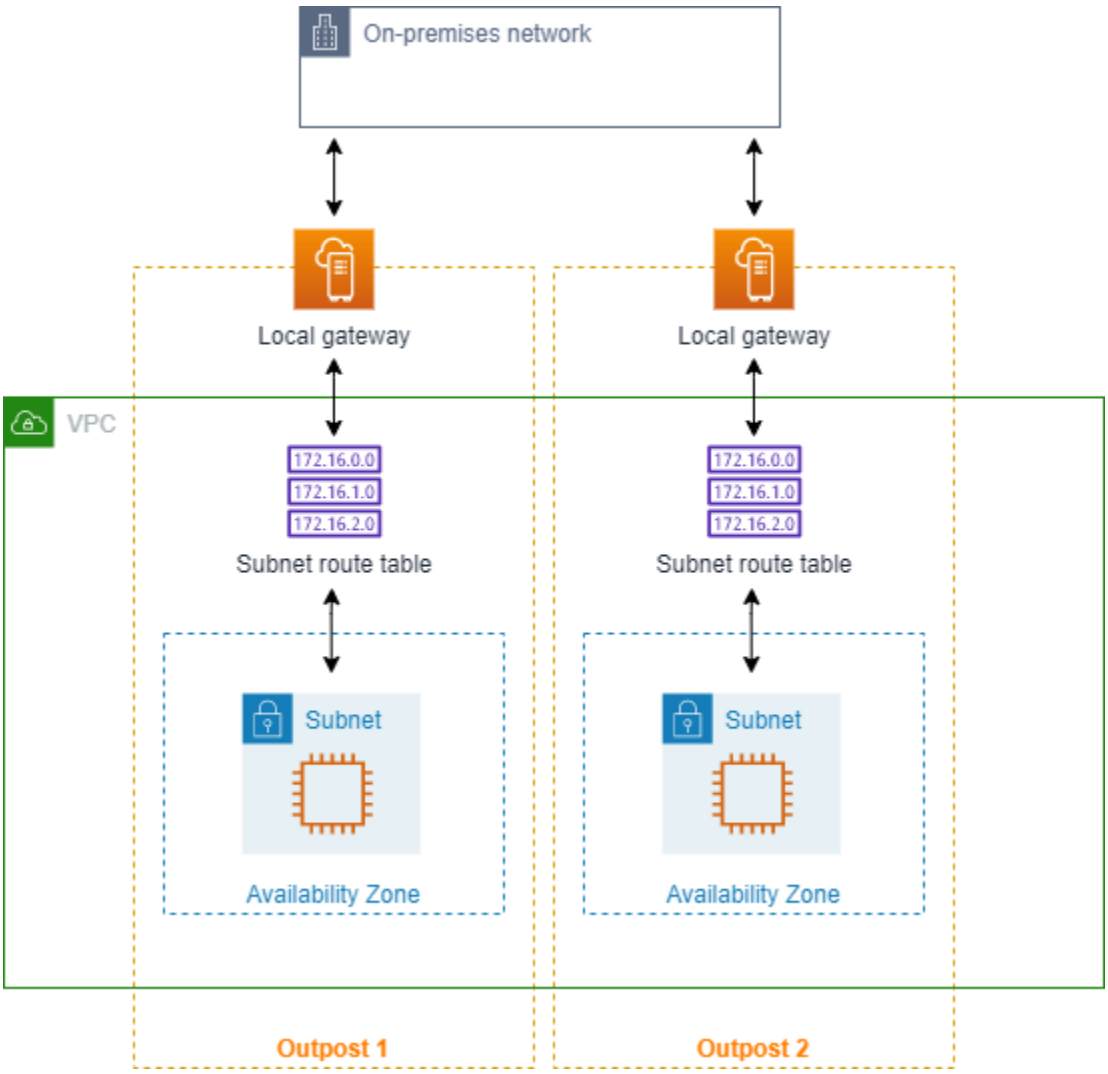
Subnetze, die sich in VPCs befinden, mit denen verknüpft sind, AWS Outposts können einen zusätzlichen Zieltyp haben, nämlich ein lokales Gateway. Betrachten Sie den Fall, in dem der lokale Gateway-Routenverkehr mit der Zieladresse 192.168.10.0/24 an das Kundennetzwerk gesendet werden soll. Fügen Sie dazu die folgende Route mit dem Zielnetzwerk und einem Ziel des lokalen Gateways () hi (`lgw-xxxx`).

Ziel	Ziel
192.168.10.0/24	*lgw-id*

Datenverkehr zwischen Subnetzen in derselben VPC über Outposts hinweg ermöglichen

Sie können die Kommunikation zwischen Subnetzen, die sich in derselben VPC befinden, über verschiedene Outposts hinweg mithilfe von lokalen Outpost-Gateways und Ihrem On-Premises-Netzwerk herstellen.

Mit diesem Feature können Sie für Ihre On-Premise-Anwendungen, die in Outposts-Racks ausgeführt werden, ähnliche Architekturen wie Multi-Availability Zone (AZ)-Architekturen erstellen. Stellen Sie dazu Verbindungen zwischen Outposts-Racks her, die sich in verschiedenen AZs befinden.



Um dieses Feature zu aktivieren, fügen Sie Ihrer Routing-Tabelle des Outpost-Rack-Subnetzes eine Route hinzu, die spezifischer ist als die lokale Route in dieser Routing-Tabelle und den Zieltyp eines lokalen Gateways aufweist. Das Ziel der Route muss mit dem gesamten IPv4-Block des Subnetzes in Ihrer VPC übereinstimmen, das sich in einem anderen Outpost befindet. Wiederholen Sie diese Konfiguration für alle Outpost-Subnetze, die kommunizieren müssen.

Important

- Zur Nutzung dieses Features müssen Sie das direkte VPC-Routing verwenden. Sie können Ihre eigenen kundeneigenen IP-Adressen nicht verwenden.
- Ihr On-Premises-Netzwerk, an das die lokalen Gateways der Outposts angeschlossen sind, muss über das erforderliche Routing verfügen, damit die Subnetze aufeinander zugreifen können.

- Wenn Sie Sicherheitsgruppen für Ressourcen in den Subnetzen verwenden möchten, müssen Sie Regeln verwenden, die IP-Adressbereiche als Quelle oder Ziel in den Outpost-Subnetzen enthalten. Sie können keine Sicherheitsgruppen-IDs verwenden.
- Bestehende Outposts-Racks erfordern möglicherweise ein Update, um die Unterstützung der Intra-VPC-Kommunikation über mehrere Outposts hinweg zu ermöglichen. Wenn dieses Feature bei Ihnen nicht funktioniert, wenden Sie sich an den AWS -Support.

Example Beispiel

Für eine VPC mit einem CIDR von 10.0.0.0/16, einem Subnetz Outpost 1 mit einem CIDR von 10.0.1.0/24 und einem Subnetz Outpost 2 mit einem CIDR von 10.0.2.0/24 würde der Eintrag für die Routing-Tabelle des Subnetzes Outpost 1 wie folgt lauten:

Bestimmungsort	Ziel
10.0.0.0/16	Local
10.0.2.0/24	*lgw-1-id*

Der Eintrag für die Routing-Tabelle des Subnetzes Outpost 2 würde wie folgt lauten:

Bestimmungsort	Ziel
10.0.0.0/16	Local
10.0.1.0/24	*lgw-2-id*

Routing an eine VPC-Peering-Verbindung

Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs. Diese ermöglicht die Weiterleitung des Datenverkehrs zwischen den VPCs mithilfe von privaten IPv4-Adressen. Instances in jeder der VPCs können so miteinander kommunizieren, als befänden sie sich im selben Netzwerk.

Um das Routing von Datenverkehr zwischen VPCs in einer VPC-Peering-Verbindung zu aktivieren, müssen Sie eine Route zu einer oder mehreren Ihrer Subnetz-Routing-Tabellen hinzufügen, die auf

die VPC-Peering-Verbindung verweist. Auf diese Weise können Sie auf den CIDR-Block der anderen VPC in der Peering-Verbindung ganz oder teilweise zugreifen. Ebenso muss der Eigentümer der anderen VPC seiner Subnetz-Routing-Tabelle eine Route hinzufügen, damit der Datenverkehr zu Ihrer VPC zurückgeleitet wird.

Angenommen Sie haben eine VPC-Peering-Verbindung (`pcx-11223344556677889`) zwischen zwei VPCs mit den folgenden Informationen:

- VPC A: CIDR-Block ist 10.0.0.0/16
- VPC B: CIDR-Block ist 172.31.0.0/16

Damit Datenverkehr zwischen den VPCs sowie Zugriff auf den gesamten IPv4-CIDR-Block beider VPCs möglich ist, wird die Routing-Tabelle von VPC A wie folgt konfiguriert.

Ziel	Ziel
10.0.0.0/16	Local
172.31.0.0/16	pcx-11223344556677889

Die Routing-Tabelle von VPC B wird folgendermaßen konfiguriert.

Ziel	Ziel
172.31.0.0/16	Local
10.0.0.0/16	pcx-11223344556677889

Ihre VPC-Peering-Verbindung kann auch IPv6-Kommunikation zwischen Instances innerhalb der VPCs unterstützen, sofern IPv6-Kommunikation für die VPCs und Instances aktiviert ist. Damit IPv6-Datenverkehr zwischen VPCs geleitet werden kann, müssen Sie der Routing-Tabelle eine Route hinzufügen, die auf die VPC-Peering-Verbindung verweist, um ganz oder teilweise auf den IPv6-CIDR-Block der Peer-VPC zuzugreifen.

Ausgehend von derselben, oben genannten VPC-Peering-Verbindung (`pcx-11223344556677889`) nehmen wir an, dass die VPCs folgende Informationen haben:

- VPC A: IPv6-CIDR-Block ist `2001:db8:1234:1a00::/56`
- VPC B: IPv6-CIDR-Block ist `2001:db8:5678:2b00::/56`

Um IPv6-Kommunikation über die VPC-Peering-Verbindung zu ermöglichen, fügen Sie der Subnetz-Routing-Tabelle für VPC A folgende Route hinzu:

Ziel	Ziel
10.0.0.0/16	Local
172.31.0.0/16	pcx-11223344556677889
2001:db8:5678:2b00::/56	pcx-11223344556677889

Fügen Sie der Routing-Tabelle für VPC B die folgende Route hinzu:

Ziel	Ziel
172.31.0.0/16	Local
10.0.0.0/16	pcx-11223344556677889
2001:db8:1234:1a00::/56	pcx-11223344556677889

Weitere Informationen zu VPC-Peering-Verbindungen erhalten Sie im Amazon VPC Peering-Handbuch.

Routing zu einem Gateway-VPC-Endpunkt

Ein Gateway-VPC-Endpunkt ermöglicht es Ihnen, eine private Verbindung zwischen Ihrer VPC und einem anderen AWS Service herzustellen. Wenn Sie einen Gateway-Endpunkt erstellen, geben Sie die Subnetz-Routing-Tabellen in Ihrer VPC an, die vom Gateway-Endpunkt verwendet werden. Den Routing-Tabellen wird automatisch eine Route mit der Präfixlisten-ID des Services (`pl-`*`xxxxxxxx`*) als Zielbereich und der Endpunkt-ID (`vpce-`*`xxxxxxxxxxxxxxxxx`*) als Ziel hinzugefügt. Sie können die Endpunktroute nicht explizit löschen oder ändern. Es ist jedoch möglich, die von dem Endpunkt verwendeten Routing-Tabellen zu ändern.

Weitere Informationen zur Weiterleitung für Endpunkte sowie zu den Auswirkungen auf Routen zu AWS -Services finden Sie unter Routing für Gateway-Endpunkte.

Routing zu einem Egress-Only-Internet-Gateway

Sie können ein Egress-Only-Internet-Gateway für Ihre VPC erstellen, um es Instances in einem privaten Subnetz zu ermöglichen, ausgehenden Datenverkehr an das Internet zu senden, ohne dass vom Internet aus eine Verbindung zu den Instances möglich ist. Ein Egress-Only-Internet-Gateway steht nur für den IPv6-Datenverkehr zur Verfügung. Um Routing für ein Egress-Only-Internet-Gateway zu konfigurieren, müssen Sie eine Route in der Routing-Tabelle des privaten Subnetzes hinzufügen, das IPv6-Internetdatenverkehr (`::/0`) an das Egress-Only-Internet-Gateway leitet.

Ziel	Ziel
::/0	*eigw-id*

Weitere Informationen finden Sie unter Aktivieren von ausgehendem IPv6-Datenverkehr mit einem Internet-Gateway, das nur ausgehenden Verkehr zulässt.

Routing für ein Transit-Gateway

Wenn Sie einem Transit-Gateway eine VPC anfügen, müssen Sie der Subnetz-Routing-Tabelle eine Route hinzufügen, damit der Datenverkehr über das Transit-Gateway weitergeleitet wird.

Betrachten Sie das folgende Szenario, in dem drei VPCs einem Transit-Gateway angefügt sind. In diesem Szenario sind alle Anfügungen der standardmäßigen Transit Gateway-Routing-Tabelle zugeordnet und werden auf die standardmäßige Transit Gateway-Routing-Tabelle übertragen. Daher können alle Anfügungen Pakete untereinander weiterleiten und das Transit-Gateway dient als einfacher Layer 3-IP-Hub.

Angenommen Sie haben 2 VPCs mit den folgenden Informationen:

- VPC A: 10.1.0.0/16, Anfügungs-ID tgw-attach-11111111111111111
- VPC B: 10.2.0.0/16, Anfügungs-ID tgw-attach-22222222222222222

Damit Datenverkehr zwischen den VPCs sowie der Zugriff auf das Transit-Gateway möglich ist, wird die Routing-Tabelle von VPC A wie folgt konfiguriert.

Ziel	Ziel
10.1.0.0/16	Lokal
10.0.0.0/8	*tgw-id*

Folgendes ist ein Beispiel für die Transit-Gateway-Routing-Tabellen-Einträge für die VPC-Anfügungen.

Ziel	Ziel
10.1.0.0/16	tgw-attach-11111111111111111
10.2.0.0/16	tgw-attach-22222222222222222

Weitere Informationen zu Transit-Gateway-Routing-Tabellen finden Sie unter Weiterleitung in Amazon VPC Transit Gateways.

Routing für eine Middlebox-Appliance

Sie können Middlebox-Appliances zu den Routing-Pfaden für Ihre VPC hinzufügen. Folgende Anwendungsfälle sind möglich:

- Fangen Sie Datenverkehr ab, der über ein Internet-Gateway oder ein Virtual Private Gateway in Ihre VPC gelangt, indem Sie ihn an eine Middlebox-Appliance in Ihrer VPC leiten. Sie können den Middlebox-Routing-Assistenten verwenden, um AWS automatisch die entsprechenden Routing-Tabellen für Ihr Gateway, Ihre Middlebox und Ihr Zielsubnetz konfigurieren zu lassen. Weitere Informationen finden Sie unter the section called “Middlebox-Routing-Assistent”.
- Direkte Datenverkehr zwischen zwei Subnetzen zu einer Middlebox-Appliance. Sie können dies tun, indem Sie eine Route für eine Subnetz-Routing-Tabelle erstellen, die mit dem Subnetz-CIDR des anderen Subnetzes übereinstimmt und einen Gateway-Load-Balancer-Endpunkt, NAT-Gateway, Network-Firewall-Endpunkt oder die Netzwerkschnittstelle einer Appliance als Ziel angibt. Um den gesamten Datenverkehr vom Subnetz zu einem anderen Subnetz umzuleiten, ersetzen Sie alternativ das Ziel der lokalen Route durch einen Gateway-Load-Balancer-Endpunkt, ein NAT-Gateway oder eine Netzwerkschnittstelle.

Sie können die Appliance entsprechend Ihren Anforderungen konfigurieren. Sie können beispielsweise eine Sicherheits-Appliance konfigurieren, die den gesamten Datenverkehr untersucht, oder eine WAN-Beschleunigungs-Appliance. Die Appliance wird als Amazon EC2-Instance in einem Subnetz in Ihrer VPC bereitgestellt und durch eine Elastic Network-Schnittstelle (Netzwerkschnittstelle) in Ihrem Subnetz dargestellt.

Wenn Sie die Routing-Weitergabe für die Routing-Tabelle des Ziel-Subnetzes aktivieren, beachten Sie die Routing-Priorität. Wir priorisieren die spezifischste Route. Wenn die Routen übereinstimmen, geben wir statischen Routen den Vorrang vor verbreiteten Routen. Überprüfen Sie Ihre Routen, um sicherzustellen, dass der Verkehr korrekt weitergeleitet wird und dass es keine unbeabsichtigten Folgen hat, wenn Sie Route Propagation aktivieren oder deaktivieren (Route Propagation ist beispielsweise für eine AWS Direct Connect Verbindung erforderlich, die Jumbo Frames unterstützt).

Um eingehenden VPC-Datenverkehr an eine Appliance weiterzuleiten, ordnen Sie eine Routing-Tabelle dem Internet-Gateway oder dem Virtual Private Gateway zu und geben die Netzwerkschnittstelle Ihrer Appliance als Ziel für den VPC-Datenverkehr an. Weitere Informationen finden Sie unter Gateway-Routing-Tabellen. Sie können auch ausgehenden Datenverkehr aus dem Subnetz an eine Middlebox-Appliance in einem anderen Subnetz weiterleiten.

Beispiele für Middlebox-Routing finden Sie unter Middlebox-Szenarien.

Inhalt

Überlegungen zu Appliances

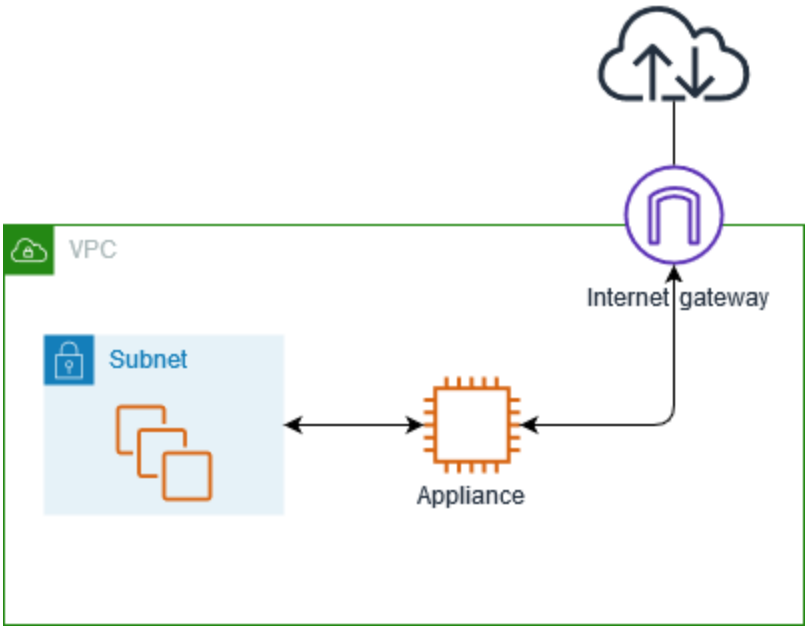
Sie können eine Drittanbieter-Appliance aus AWS Marketplace auswählen oder eine eigene Appliance konfigurieren. Beachten Sie beim Erstellen oder Konfigurieren einer Appliance Folgendes:

- Die Appliance muss in einem separaten Subnetz für den Quell- oder Zielbereichsdatenverkehr konfiguriert sein.
- Sie müssen die Quell-/Zielprüfung in der Appliance deaktivieren. Weitere Informationen finden Sie unter Ändern der Quell- oder Zielüberprüfung im Amazon EC2 EC2-Benutzerhandbuch.
- Sie können keinen Datenverkehr zwischen Hosts im selben Subnetz über eine Appliance weiterleiten.

- Die Appliance muss keine Netzwerkadressübersetzung (Network Address Translation, NAT) durchführen.
- Sie können Ihren Routing-Tabellen eine Route hinzufügen, die spezifischer als die lokale Route ist. Sie können spezifischere Routen verwenden, um Datenverkehr zwischen Subnetzen innerhalb einer VPC (Ost-West-Verkehr) zu einer Middlebox-Appliance umzuleiten. Das Ziel der Route muss mit dem gesamten IPv4- oder IPv6-CIDR-Block eines Subnetzes in Ihrer VPC übereinstimmen.
- Um IPv6-Datenverkehr abzufangen, müssen Sie sicherstellen, dass VPC, Subnetz und Appliance IPv6 unterstützen. Virtual Private Gateways unterstützen keinen IPv6-Datenverkehr.

Routing des Datenverkehrs zwischen einem Gateway und einer Appliance

Um eingehenden VPC-Datenverkehr an eine Appliance weiterzuleiten, ordnen Sie eine Routing-Tabelle dem Internet-Gateway oder dem Virtual Private Gateway zu und geben die Netzwerkschnittstelle Ihrer Appliance als Ziel für den VPC-Datenverkehr an. Im folgenden Beispiel verfügt die VPC über ein Internet-Gateway, eine Appliance und ein Subnetz mit Instances. Der Datenverkehr aus dem Internet wird über eine Appliance geleitet.



Ordnen Sie diese Routing-Tabelle Ihrem Internet-Gateway oder Ihrem Virtual Private Gateway zu. Der erste Eintrag ist die lokale Route. Der zweite Eintrag sendet IPv4-Datenverkehr, der für das Subnetz bestimmt ist, an die Netzwerkschnittstelle der Appliance. Diese Route ist spezifischer als die lokale Route.

Bestimmungsort	Ziel
VPC-CIDR	Local
Subnetz-CIDR	*Appliance-Netzwerkschnittstellen-ID*

Alternativ können Sie das Ziel für die lokale Route durch die Netzwerkschnittstelle der Appliance ersetzen. Sie können dies tun, um sicherzustellen, dass der gesamte Datenverkehr automatisch an die Appliance geleitet wird, einschließlich des Datenverkehrs, der für Subnetze bestimmt ist, die Sie der VPC in Zukunft hinzufügen.

Bestimmungsort	Ziel
VPC-CIDR	*Appliance-Netzwerkschnittstellen-ID*

Um Datenverkehr von Ihrem Subnetz an eine Appliance in einem anderen Subnetz weiterzuleiten, fügen Sie der Subnetz-Routing-Tabelle eine Route hinzu, die Datenverkehr an die Netzwerkschnittstelle der Appliance weiterleitet. Der Zielbereich muss weniger spezifisch sein als der Zielbereich für die lokale Route. Geben Sie beispielsweise für den für das Internet bestimmten Datenverkehr `0.0.0.0/0` (alle IPv4-Adressen) als Zielbereich an.

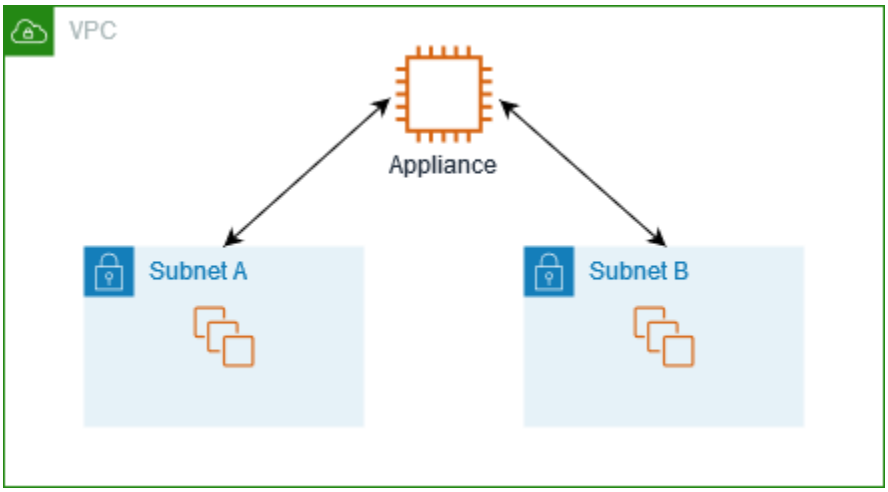
Ziel	Ziel
VPC-CIDR	Local
0.0.0.0/0	*Appliance-Netzwerkschnittstellen-ID*

Fügen Sie dann in der Routing-Tabelle, die dem Subnetz der Appliance zugeordnet ist, eine Route hinzu, die den Datenverkehr zurück an das Internet-Gateway oder Virtual Private Gateway sendet.

Bestimmungsort	Ziel
VPC-CIDR	Local
0.0.0.0/0	*igw-id*

Routing-Intersubnetzdatenverkehr an eine Appliance

Sie können Datenverkehr, der für ein bestimmtes Subnetz bestimmt ist, an die Netzwerkschnittstelle einer Appliance weiterleiten. Im folgenden Beispiel enthält die VPC zwei Subnetze und eine Appliance. Der Verkehr zwischen den Subnetzen wird über eine Appliance geleitet.



Sicherheitsgruppen

Wenn Sie Datenverkehr zwischen Instances in verschiedenen Subnetzen über eine Middlebox-Appliance leiten, müssen 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.

Routing

Im Folgenden finden Sie eine Routing-Tabelle für Subnetz A. Dieser erste Eintrag befähigt Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten Datenverkehr vom Subnetz A zum Subnetz B an die Netzwerkschnittstelle der Appliance weiter.

Bestimmungsort	Ziel
VPC-CIDR	Local
Subnetz-B-CIDR	*Appliance-Netzwerkschnittstellen-ID*

Im Folgenden finden Sie eine Routing-Tabelle für Subnetz B. Dieser erste Eintrag befähigt Instances in dieser VPC, miteinander zu kommunizieren. Der zweite Eintrag leitet den gesamten Datenverkehr vom Subnetz B zum Subnetz A an die Netzwerkschnittstelle der Appliance weiter.

Bestimmungsort	Ziel
VPC-CIDR	Local
Subnetz-A-CIDR	*Appliance-Netzwerkschnittstellen-ID*

Alternativ können Sie das Ziel für die lokale Route durch die Netzwerkschnittstelle der Appliance ersetzen. Sie können dies tun, um sicherzustellen, dass der gesamte Datenverkehr automatisch an die Appliance geleitet wird, einschließlich des Datenverkehrs, der für Subnetze bestimmt ist, die Sie der VPC in Zukunft hinzufügen.

Bestimmungsort	Ziel
VPC-CIDR	*Appliance-Netzwerkschnittstellen-ID*

Routing unter Verwendung einer Präfixliste

Wenn Sie in Ihren AWS Ressourcen häufig auf denselben Satz von CIDR-Blöcken verweisen, können Sie eine vom Kunden verwaltete Präfixliste erstellen, um sie zu gruppieren. Anschließend können Sie die Präfixliste als Ziel in Ihrem Routing-Tabelleneintrag angeben. Sie können später Einträge für die Präfixliste hinzufügen oder entfernen, ohne die Routing-Tabellen aktualisieren zu müssen.

Beispielsweise verfügen Sie über ein Transit-Gateway mit mehreren VPC-Anhängen. Die VPCs müssen in der Lage sein, mit zwei bestimmten VPC-Anhängen zu kommunizieren, die die folgenden CIDR-Blöcke haben:

- 10.0.0.0/16
- 10.2.0.0/16

Sie erstellen eine Präfixliste mit beiden Einträgen. In den Subnetz-Routing-Tabellen erstellen Sie eine Route und geben die Präfixliste als Destination und das Transit-Gateway als Ziel an.

Ziel	Ziel
172.31.0.0/16	Local
pl-123abc123abc123ab	*tgw-id*

Die maximale Anzahl von Einträgen für die Präfixlisten entspricht der Anzahl von Einträgen in der Routing-Tabelle.

Routing zu einem Gateway Load Balancer-Endpunkt

Ein Gateway Load Balancer ermöglicht es Ihnen, den Datenverkehr an eine Flotte virtueller Appliances wie Firewalls zu verteilen. Sie können den Load Balancer als Service konfigurieren, indem Sie eine VPC-Endpunktdienstkonfiguration erstellen. Sie erstellen dann in Ihrer VPC einen Gateway Load Balancer-Endpunkt, um Ihre VPC mit dem Service zu verbinden.

Um Ihren Datenverkehr an den Gateway Load Balancer weiterzuleiten (z. B. zur Sicherheitsinspektion), geben Sie den Gateway Load Balancer-Endpunkt als Ziel in Ihren Routingtabellen an.

Ein Beispiel für Sicherheitsgeräte hinter einem Gateway Load Balancer finden Sie unter the section called “Überprüfen des Datenverkehrs mithilfe von Sicherheitsanwendungen”.

Um den Gateway Load Balancer-Endpunkt in der Routingtabelle anzugeben, verwenden Sie die ID des VPC-Endpunkts. Um beispielsweise Datenverkehr für 10.0.1.0/24 an einen Gateway-Load-Balancer-Endpunkt weiterzuleiten, fügen Sie die folgende Route hinzu.

Bestimmungsort	Ziel
10.0.1.0/24	*vpc-endpoint-id*

Weitere Informationen finden Sie unter Gateway Load Balancer.

Arbeiten mit Routing-Tabellen

In diesem Abschnitt wird beschrieben, wie Sie mit Routing-Tabellen arbeiten.

Inhalt

Festlegen der Routing-Tabelle für ein Subnetz

Den Details des Subnetzes in der Amazon VPC-Konsole können Sie entnehmen, welcher Routing-Tabelle ein Subnetz zugeordnet ist.

So bestimmen Sie die Routing-Tabelle für ein Subnetz

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.

3. Wählen Sie das Subnetz aus.
4. Klicken Sie auf die Registerkarte Route Table (Routing-Tabelle), um die Routing-Tabellen-ID und ihre Routen anzuzeigen. Informationen dazu, wie Sie bestimmen, ob die Zuordnung zur Haupt-Routing-Tabelle führt und ob diese Zuordnung explizit ist, finden Sie unter Bestimmen, welche Subnetze und/oder Gateways explizit zugeordnet sind.

Bestimmen, welche Subnetze und/oder Gateways explizit zugeordnet sind

Sie können feststellen, wie viele und welche Subnetze oder Gateways einer Routing-Tabelle explizit zugeordnet sind.

Die Haupt-Routing-Tabelle kann sowohl explizite als auch implizite Subnetz-Zuordnungen haben. Benutzerdefinierte Routing-Tabellen dagegen verfügen nur über explizite Zuordnungen.

Subnetze, die nicht explizit einer anderen Routing-Tabelle zugeordnet sind, sind implizit der Haupt-Routing-Tabelle zugeordnet. Sie können ein Subnetz explizit mit der Haupt-Routing-Tabelle verknüpfen. Ein Beispiel dafür, warum Sie dies tun könnten, finden Sie unter So ersetzen Sie die Routing-Haupttabelle.

So ermitteln Sie, welche Subnetze explizit über die Konsole zugeordnet sind:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Schauen Sie in die Spalte Explicit subnet association (Explizite Subnetzzurdonung), um die explizit zugeordneten Subnetze zu bestimmen, und in die Spalte Main (Haupttabelle), um zu bestimmen, ob dies die Haupt-Routing-Tabelle ist.
4. Wählen Sie die Routing-Tabelle aus und wählen Sie die Registerkarte Subnet associations (Subnetzzuordnungen) aus.
5. Die Subnetze unter Explicit subnet association (Explizite Subnetzzuordnung) sind explizit der Routing-Tabelle zugeordnet. Die Subnetze unter Subnets without explicit associations (Subnetze ohne explizite Zuordnungen) gehören derselben VPC an wie die Routing-Tabelle, sind jedoch keiner Routing-Tabelle zugeordnet. Daher sind sie implizit der Haupt-Routing-Tabelle für die VPC zugeordnet.

So ermitteln Sie mit der Konsole, welche Gateways explizit verknüpft sind:

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

2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routing-Tabelle aus und wählen Sie die Registerkarte Edge associations (Edge-Zuordnungen) aus.

So beschreiben Sie eine oder mehrere Routing-Tabellen und zeigen ihre Zuordnungen über die Befehlszeile an:

- describe-route-tables (AWS CLI)
- Get-EC2RouteTable (AWS Tools for Windows PowerShell)

Erstellen einer benutzerdefinierten Routing-Tabelle

Sie können eine benutzerdefinierte Routing-Tabelle für Ihre VPC auf der Amazon VPC-Konsole erstellen.

Erstellen einer benutzerdefinierten Routing-Tabelle mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).
4. (Optional) Geben Sie bei Name einen Namen für Ihre Routing-Tabelle ein.
5. Wählen Sie unter VPC Ihre VPC aus.
6. (Optional) Sie fügen ein Tag hinzu, indem Sie Add new tag (Neuen Tag hinzufügen) auswählen und den Tag-Schlüssel und -Wert eingeben.
7. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).

So erstellen Sie eine benutzerdefinierte Routing-Tabelle mithilfe der Befehlszeile:

- create-route-table (AWS CLI)
- New-EC2RouteTable (AWS Tools for Windows PowerShell)

Hinzufügen und Entfernen von Routen aus einer Routing-Tabelle

Sie können Routen in Ihren Routing-Tabellen hinzufügen, verändern oder daraus entfernen. Sie können nur selbst erstellte Routen verändern.

Weitere Informationen zum Arbeiten mit statischen Routen für eine Site-to-Site VPN-Verbindung finden Sie unter Bearbeiten statischer Routen für eine Site-to-Site VPN-Verbindung im AWS Site-to-Site VPN -Benutzerhandbuch.

So aktualisieren Sie die Routen für eine Routing-Tabelle mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie Actions (Aktionen) und dann Edit routes (Routen bearbeiten).
4. Um eine Route hinzuzufügen, wählen Sie Add route (Route hinzufügen). Geben Sie unter Destination (Zielbereich) den Ziel-CIDR-Block, eine einzelne IP-Adresse oder die ID einer Präfixliste ein.
5. Um eine Route zu ändern, ersetzen Sie unter Destination (Zielbereich) den CIDR-Block oder eine einzelne IP-Adresse. Wählen Sie unter Target (Ziel) ein Ziel aus.
6. Zum Entfernen einer Route wählen Sie Remove (Entfernen) aus.
7. Wählen Sie Änderungen speichern aus.

So aktualisieren Sie die Routen für eine Routing-Tabelle mithilfe der Befehlszeile

- create-route (AWS CLI)
- replace-route (AWS CLI)
- delete-route (AWS CLI)
- New-EC2Route (AWS Tools for Windows PowerShell)
- Set-EC2Route (AWS Tools for Windows PowerShell)
- Remove-EC2Route (AWS Tools for Windows PowerShell)

> **Note**
>
> Wenn Sie eine Route mit einem Befehlszeilen-Tool oder der API hinzufügen, wird der CIDR-Block automatisch in seine kanonische Form geändert. Wenn Sie beispielsweise `100.68.0.18/18` für den CIDR-Block angeben, erstellen wir eine Route mit einem Zielbereich-CIDR-Block von `100.68.0.0/18`.

Aktivieren oder Deaktivieren der Routing-Verbreitung

Die Routing-Verteilung ermöglicht es einem Virtual Private Gateway, Routen automatisch an Ihre Routing-Tabellen zu übertragen. Das bedeutet, dass Sie VPN-Routen nicht manuell hinzufügen oder entfernen müssen.

Um diesen Vorgang abzuschließen, müssen Sie über ein Virtual Private Gateway verfügen.

Weitere Informationen finden Sie unter Site-to-Site-VPN-Routing-Optionen im Site-to-Site-VPN-Benutzerhandbuch.

So aktivieren Sie die Routing-Verbreitung in der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie Actions (Aktionen), Edit route propagation (Routing-Verbreitung bearbeiten).
4. Aktivieren Sie das Kontrollkästchen Enable (aktivieren) neben dem Virtual Private Gateway und klicken Sie auf Save (Speichern).

So aktivieren Sie die Routing-Verbreitung unter Verwendung der Befehlszeile:

- enable-vgw-route-propagation (AWS CLI)
- Enable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Deaktivieren der Route-Propagierung mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie Actions (Aktionen), Edit route propagation (Routing-Verbreitung bearbeiten).
4. Heben Sie die Aktivierung des Kontrollkästchens Enable (Aktivieren) neben dem Virtual Private Gateway auf und klicken Sie auf Save (Speichern).

So deaktivieren Sie die Routing-Verbreitung über die Befehlszeile:

- disable-vgw-route-propagation (AWS CLI)

- Disable-EC2VgwRoutePropagation (AWS Tools for Windows PowerShell)

Zuordnen eines Subnetzes zu einer Routing-Tabelle

Damit die Routen einer Routing-Tabelle auf ein bestimmtes Subnetz angewendet werden, müssen Sie die Routing-Tabelle dem Subnetz zuordnen. Eine Routing-Tabelle kann mehreren Subnetzen zugeordnet werden. Ein Subnetz kann jedoch jeweils nur einer Routing-Tabelle zugeordnet werden. Wenn ein Subnetz nicht ausdrücklich einer Routing-Tabelle zugeordnet ist, wird es standardmäßig implizit der Haupt-Routing-Tabelle zugeordnet.

So ordnen Sie eine Routing-Tabelle mit einem Subnetz über die Konsole zu:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie auf der Registerkarte Subnet associations (Subnetzzuordnungen) die Option Edit subnet associations (Subnetzzuordnungen bearbeiten) aus.
4. Aktivieren Sie das Kontrollkästchen für das Subnetz, um es der Routing-Tabelle zuzuordnen.
5. Klicken Sie auf Save associations (Zuordnungen speichern).

So ordnen Sie eine Routing-Tabelle mit einem Subnetz über die Befehlszeile zu:

- associate-route-table (AWS CLI)
- Register-EC2RouteTable (AWS Tools for Windows PowerShell)

Bearbeiten der Routing-Tabelle für ein Subnetz

Sie können die Routing-Tabellenzuordnung für ein Subnetz ändern.

Wenn Sie die Routing-Tabelle ändern, werden Ihre vorhandenen Verbindungen im Subnetz gelöscht, es sei denn, die neue Routing-Tabelle enthält eine Route für denselben Datenverkehr zum selben Ziel.

So ändern Sie eine Zuordnung von Subnetz und Routing-Tabelle mithilfe der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets (Subnetze) und dann das Subnetz aus.

3. Wählen Sie auf der Registerkarte Route Table (Routing-Tabelle) die Option Edit route table association (Zuordnung der Routing-Tabelle bearbeiten) aus.
4. Wählen Sie für Route table ID (Routing-Tabellen-ID) die neue Routing-Tabelle aus.
5. Wählen Sie Speichern.

So ändern Sie die einem Subnetz zugeordnete Routing-Tabelle mithilfe der Befehlszeile

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

Aufheben der Zuordnung eines Subnetzes zu einer Routing-Tabelle

Sie können die Zuordnung eines Subnetzes zu einer Routing-Tabelle aufheben. Sofern Sie ein Subnetz nicht explizit eine anderen Routing-Tabelle zuordnen, ist das Subnetz implizit der Haupt-Routing-Tabelle zugeordnet.

So trennen Sie die Zuordnung eines Subnetzes zu einer Routing-Tabelle mithilfe der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie auf der Registerkarte Subnet Associations (Subnetzzuordnungen) die Option Edit subnet associations (Subnetzzuordnungen bearbeiten) aus.
4. Deaktivieren Sie das Kontrollkästchen für das Subnetz.
5. Klicken Sie auf Save associations (Zuordnungen speichern).

So trennen Sie die Zuordnung eines Subnetzes zu einer Routing-Tabelle mithilfe der Befehlszeile:

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

So ersetzen Sie die Routing-Haupttabelle

Sie können die Haupt-Routing-Tabelle für Ihre VPC ändern.

So ersetzen Sie die Haupt-Routing-Tabelle mithilfe der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die neue Haupt-Routing-Tabelle aus.
3. Wählen Sie Actions (Aktionen), Set main route table (Haupt-Routing-Tabelle festlegen) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`set`** ein und wählen Sie dann OK aus.

So ersetzen Sie die Haupt-Routing-Tabelle über die Befehlszeile:

- replace-route-table-association (AWS CLI)
- Set-EC2RouteTableAssociation (AWS Tools for Windows PowerShell)

Nachfolgend wird beschrieben, wie Sie eine explizite Zuordnung zwischen einem Subnetz und der Haupt-Routing-Tabelle aufheben. Dadurch entsteht eine implizite Zuordnung des Subnetzes zur Haupt-Routing-Tabelle. Die Vorgehensweise ist hierbei dieselbe wie beim Aufheben der Zuordnung eines Subnetzes zu einer beliebigen Routing-Tabelle.

So heben Sie die explizite Zuordnung zur Haupt-Routing-Tabelle auf

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie auf der Registerkarte Subnet Associations (Subnetzzuordnungen) die Option Edit subnet associations (Subnetzzuordnungen bearbeiten) aus.
4. Deaktivieren Sie das Kontrollkästchen für das Subnetz.
5. Klicken Sie auf Save associations (Zuordnungen speichern).

Verknüpfen eines Gateways mit einer Routing-Tabelle

Sie können ein Internet-Gateway oder ein Virtual Private Gateway mit einer Routing-Tabelle verknüpfen. Weitere Informationen finden Sie unter Gateway-Routing-Tabellen.

So verknüpfen Sie ein Gateway mit einer Routing-Tabelle über die Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie auf der Registerkarte Edge Associations (Edge-Zuordnungen) die Option Edit edge associations (Edge-Zuordnungen bearbeiten) aus.
4. Aktivieren Sie das Kontrollkästchen für das Gateway.
5. Wählen Sie Änderungen speichern aus.

Um ein Gateway mit einer Routing-Tabelle zu verknüpfen, verwenden Sie AWS CLI

Verwenden Sie den Befehl associate-route-table. Im folgenden Beispiel wird das Internet-Gateway `igw-11aa22bb33cc44dd1` der Routing-Tabelle `rtb-01234567890123456` zugeordnet.

```
aws ec2 associate-route-table --route-table-id rtb-01234567890123456 --gateway-id
 igw-11aa22bb33cc44dd1
```

Trennen der Zuordnung eines Gateways zu einer Routing-Tabelle

Sie können ein Internet-Gateway oder ein Virtual Private Gateway von einer Routing-Tabelle trennen.

So verknüpfen Sie ein Gateway mit einer Routing-Tabelle über die Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie auf der Registerkarte Edge Associations (Edge-Zuordnungen) die Option Edit edge associations (Edge-Zuordnungen bearbeiten) aus.
4. Deaktivieren Sie das Kontrollkästchen für das Gateway.
5. Wählen Sie Änderungen speichern aus.

So trennen Sie die Zuordnung eines Gateways zu einer Routing-Tabelle über die Befehlszeile:

- disassociate-route-table (AWS CLI)
- Unregister-EC2RouteTable (AWS Tools for Windows PowerShell)

Ersetzen oder Wiederherstellen des Ziels für eine lokale Route

Sie können das Ziel der lokalen Standardroute ändern. Wenn Sie das Ziel einer lokalen Route ersetzen, können Sie es später auf das `local`-Standardziel wiederherstellen. Wenn Ihre VPC mehrere CIDR-Blöcke besitzt, verfügen Ihre Routing-Tabellen über mehrere lokale Routen – eine pro CIDR-Block. Sie können das Ziel jeder lokalen Route nach Bedarf ersetzen oder wiederherstellen.

So aktualisieren Sie die lokale Route mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Klicken Sie auf der Registerkarte Routes (Routen) auf Edit routes (Routen bearbeiten).
4. Löschen Sie für die lokale Route das Feld Target (Ziel) und wählen Sie dann ein neues Ziel aus.
5. Wählen Sie Änderungen speichern aus.

So stellen Sie das Ziel für eine lokale Route mithilfe der Konsole wieder her:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie Actions (Aktionen) und dann Edit routes (Routen bearbeiten).
4. Löschen Sie für die Route das Feld Target (Ziel) und wählen Sie dann local (lokal) aus.
5. Wählen Sie Änderungen speichern aus.

Um das Ziel für eine lokale Route mit dem zu ersetzen AWS CLI

Verwenden Sie den Befehl replace-route. Im folgenden Beispiel wird das Ziel der lokalen Route mit ersetz `eni-11223344556677889`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --network-interface-id eni-11223344556677889
```

Um das Ziel für eine lokale Route wiederherzustellen, verwenden Sie AWS CLI

Im folgenden Beispiel wird das lokale Ziel für die Routing-Tabelle wiederhergestell `rtb-01234567890123456`.

```
aws ec2 replace-route --route-table-id rtb-01234567890123456 --destination-cidr-block
 10.0.0.0/16 --local-target
```

Löschen einer Routing-Tabelle

Sie können eine Routing-Tabelle nur löschen, wenn ihr keine Subnetze zugeordnet sind. Die Haupt-Routing-Tabelle kann nicht gelöscht werden.

So löschen Sie eine Routing-Tabelle mithilfe der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Route Tables (Routing-Tabellen) und wählen Sie die Routing-Tabelle aus.
3. Wählen Sie Actions (Aktionen) und Delete route table (Routing-Tabelle löschen) aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Delete (Löschen) aus.

So löschen Sie eine Routing-Tabelle mithilfe der Befehlszeile:

- delete-route-table (AWS CLI)
- Remove-EC2RouteTable (AWS Tools for Windows PowerShell)

Middlebox-Routing-Assistent

Wenn Sie die Feinkornsteuerung über den Routingpfad des Datenverkehrs in Ihrer VPC konfigurieren möchten, z. B. durch Umleiten des Datenverkehrs an eine Sicherheitseinheit, können Sie den Middlebox-Routing-Assistenten in der VPC-Konsole verwenden. Der Middlebox-Routing-Assistent hilft Ihnen, indem Sie automatisch die erforderlichen Routing-Tabellen und Routen (Hops) erstellen, um den Datenverkehr nach Bedarf umzuleiten.

Mit dem Middlebox-Routing-Assistenten können Sie das Routing für die folgenden Szenarien konfigurieren:

- Weiterleiten von Datenverkehr an eine Middlebox-Appliance, z. B. eine Amazon-EC2-Instance, die als Sicherheits-Appliance konfiguriert ist.
- Routing von Datenverkehr an einen Gateway Load Balancer. Weitere Informationen finden Sie im Benutzerhandbuch zu Gateway Load Balancer.

Weitere Informationen finden Sie unter the section called “Middlebox-Szenarien”.

Inhalt

Voraussetzungen für Middlebox-Routing-Assistent

Sehen Sie sich the section called “Überlegungen des Middlebox-Routing-Assistenten” an. Stellen Sie dann sicher, dass Sie über die folgenden Informationen verfügen, bevor Sie den Middlebox-Routing-Assistenten verwenden.

- Die VPC.
- Die Ressource, über die der Datenverkehr von der VPC stammt oder in die VPC eintritt, z. B. ein Internet-Gateway, ein Virtual Private Gateway oder eine Netzwerkschnittstelle.
- Die Middlebox-Netzwerkschnittstelle oder der Gateway-Load-Balancer-Endpunkt.
- Das Zielsubnetz für den Datenverkehr

Verwalten von Middlebox-Routen

Der Middlebox-Routing-Assistent ist im Amazon Virtual Private Cloud Console verfügbar.

Inhalt

Erstellen von Routen mit dem Middlebox-Routing-Assistenten

So erstellen Sie Routen mit dem Middlebox-Routing-Assistenten

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

2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Wählen Sie Ihre VPC und dann Aktionen, Middlebox-Routen verwalten aus.
4. Wählen Sie Create route (Route erstellen) aus.
5. Gehen Sie auf der Seite Routen angeben wie folgt vor:

   - Wählen Sie für Quelle die Quelle für Ihren Datenverkehr aus. Wenn Sie ein Virtual Private Gateway auswählen, geben Sie für Ziel-IPv4-CIDR die CIDR für den On-Premises-Datenverkehr ein, der vom Virtual Private Gateway in die VPC gelangt.
   - Wählen Sie für Middlebox die Netzwerkschnittstellen-ID aus, die Ihrer Middlebox-Appliance zugeordnet ist, oder wählen Sie bei Verwendung eines Gateway-Load-Balancer-Endpunkts die VPC-Endpunkt-ID aus.
   - Wählen Sie für Zielsubnetz das Zielsubnetz aus.
6. (Optional) Um ein weiteres Zielsubnetz hinzuzufügen, wählen Sie Zusätzliches Subnetz hinzufügen und gehen Sie dann wie folgt vor:

   - Wählen Sie für Middlebox die Netzwerkschnittstellen-ID aus, die Ihrer Middlebox-Appliance zugeordnet ist, oder wählen Sie bei Verwendung eines Gateway-Load-Balancer-Endpunkts die VPC-Endpunkt-ID aus.

     Sie müssen dieselbe Middlebox-Appliance für mehrere Subnetze verwenden.
   - Wählen Sie für Zielsubnetz das Zielsubnetz aus.
7. (Optional) Um eine weitere Quelle hinzuzufügen, wählen Sie Quelle hinzufügen und wiederholen Sie dann die vorherigen Schritte.
8. Wählen Sie Weiter aus.
9. Überprüfen Sie auf der Seite Überprüfen und erstellen die Routen, und wählen Sie dann Routen erstellen aus.

Ändern von Middlebox-Routen

Sie können die Routing-Konfiguration bearbeiten, indem Sie das Gateway, die Middlebox oder das Zielsubnetz ändern.

Wenn Sie Änderungen vornehmen, führt der Middlebox-Routing-Assistent automatisch die folgenden Vorgänge aus:

- Erstellt neue Routing-Tabellen für das Gateway, die Middlebox und das Zielsubnetz.

- Fügt die erforderlichen Routen zu den neuen Routing-Tabellen hinzu.
- Trennt die aktuellen Routing-Tabellen, die der Middlebox-Routing-Assistent mit den Ressourcen verknüpft hat.
- Verknüpft die neuen Routing-Tabellen, die der Middlebox-Routing-Assistent erstellt, mit den Ressourcen.

So ändern Sie Middlebox-Routen mit dem Middlebox-Routing-Assistenten

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Wählen Sie Ihre VPC und dann Aktionen, Middlebox-Routen verwalten aus.
4. Wählen Sie Routen bearbeiten aus.
5. Um das Gateway zu ändern, wählen Sie für Quelle das Gateway aus, über das der Datenverkehr in Ihre VPC eingeht. Wenn Sie ein Virtual Private Gateway auswählen, geben Sie für Ziel-IPv4-CIDR die Ziel-Subnetz-CIDR ein.
6. Um ein weiteres Zielsubnetz hinzuzufügen, wählen Sie Zusätzliches Subnetz hinzufügen und gehen Sie dann wie folgt vor:

   - Wählen Sie für Middlebox die Netzwerkschnittstellen-ID aus, die Ihrer Middlebox-Appliance zugeordnet ist, oder wählen Sie bei Verwendung eines Gateway-Load-Balancer-Endpunkts die VPC-Endpunkt-ID aus.

     Sie müssen dieselbe Middlebox-Appliance für mehrere Subnetze verwenden.
   - Wählen Sie für Zielsubnetz das Zielsubnetz aus.
7. Wählen Sie Weiter aus.
8. Auf der Seite Überprüfen und aktualisieren wird eine Liste von Routing-Tabellen und deren Routen angezeigt, die vom Middlebox-Routing-Assistenten erstellt werden. Überprüfen Sie die Routen, und wählen Sie dann im Bestätigungsdialogfeld Routen aktualisieren aus.

Anzeigen der Middlebox-Routing-Assistenten-Routing-Tabellen

Anzeigen der Middlebox-Routing-Assistenten-Routing-Tabellen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.

3. Wählen Sie Ihre VPC und dann Aktionen, Middlebox-Routen verwalten aus.
4. Unter Middlebox-Routing-Tabellen gibt die Zahl an, wie viele Routen der Middlebox-Routing-Assistent erstellt hat. Wählen Sie die Nummer aus, um die Routen anzuzeigen.

Wir zeigen die Routen des Middlebox-Routing-Assistenten auf einer separaten Routing-Tabellenseite an.

Löschen der Konfiguration des Middlebox-Routing-Assistenten

Wenn Sie sich entscheiden, dass Sie den Middlebox-Routing-Assistenten nicht mehr konfigurieren möchten, müssen Sie die Routing-Tabellen manuell löschen.

So löschen Sie die Konfiguration des Middlebox-Routing-Assistenten

1. Anzeigen der Middlebox-Routing-Assistenten-Routing-Tabellen. Weitere Informationen finden Sie unter the section called “Anzeigen der Middlebox-Routing-Assistenten-Routing-Tabellen”.

   Nachdem Sie den Vorgang ausgeführt haben, werden die Routing-Tabellen, die der Middlebox-Routing-Assistent erstellt hat, auf einer separaten Routing-Tabellen-Seite angezeigt.
2. Löschen Sie jede Routing-Tabelle, die angezeigt wird. Weitere Informationen finden Sie unter the section called “Löschen einer Routing-Tabelle”.

Überlegungen des Middlebox-Routing-Assistenten

Berücksichtigen Sie Folgendes, wenn Sie den Middlebox-Routing-Assistenten verwenden:

- Wenn Sie den Datenverkehr überprüfen möchten, können Sie ein Internet-Gateway oder ein Virtual Private Gateway für die Quelle verwenden.
- Wenn Sie dieselbe Middlebox in einer Multiple-Middlebox-Konfiguration innerhalb derselben VPC verwenden, stellen Sie sicher, dass sich die Middlebox für beide Subnetze in derselben Hop-Position befindet.
- Die Appliance muss in einem separaten Subnetz vom Quell- oder Zielsubnetz konfiguriert werden.
- Sie müssen die Quell-/Zielprüfung in der Appliance deaktivieren. Weitere Informationen finden Sie unter Ändern der Quell- oder Zielüberprüfung im Amazon EC2 EC2-Benutzerhandbuch.
- Die Routing-Tabellen und Routen, die vom Middlebox-Routing-Assistenten erstellt werden, zählen zu Ihren Kontingenten. Weitere Informationen finden Sie unter the section called “Routing-Tabellen”.

- Wenn Sie eine Ressource löschen, beispielsweise eine Netzwerkschnittstelle, werden die Routing-Tabellenzuordnungen mit der Ressource entfernt. Wenn es sich bei der Ressource um ein Ziel handelt, wird das Routenziel auf Blackhole gesetzt. Die Routing-Tabellen werden nicht gelöscht.
- Das Middlebox-Subnetz und das Zielsubnetz müssen einer nicht standardmäßigen Routing-Tabelle zugeordnet werden.

> **Note**
>
> Es wird empfohlen, den Middlebox-Routing-Assistenten zu verwenden, um Routing-Tabellen zu ändern oder zu löschen, die Sie mit dem Middlebox-Routing-Assistenten erstellt haben.

Middlebox-Szenarien

Die folgenden Beispiele beschreiben Szenarien für den Middlebox-Routing-Assistenten.

Inhalt

Überprüfen des Datenverkehrs, der für ein Subnetz bestimmt ist

Stellen Sie sich das Szenario vor, in dem Datenverkehr über ein Internet-Gateway in die VPC eingeht und Sie den gesamten Datenverkehr, der für ein Subnetz, z. B. Subnetz B, bestimmt ist, mithilfe einer auf einer EC2-Instance installierten Firewall-Appliance überprüfen möchten. Die Firewall-Appliance sollte auf einer EC2-Instance in einem separaten Subnetz von Subnetz B in Ihrer VPC installiert und konfiguriert werden, z. B. Subnetz C. Sie können dann den Middlebox-Routing-Assistenten verwenden, um Routen für den Datenverkehr zwischen Subnetz B und dem Internet-Gateway zu konfigurieren.

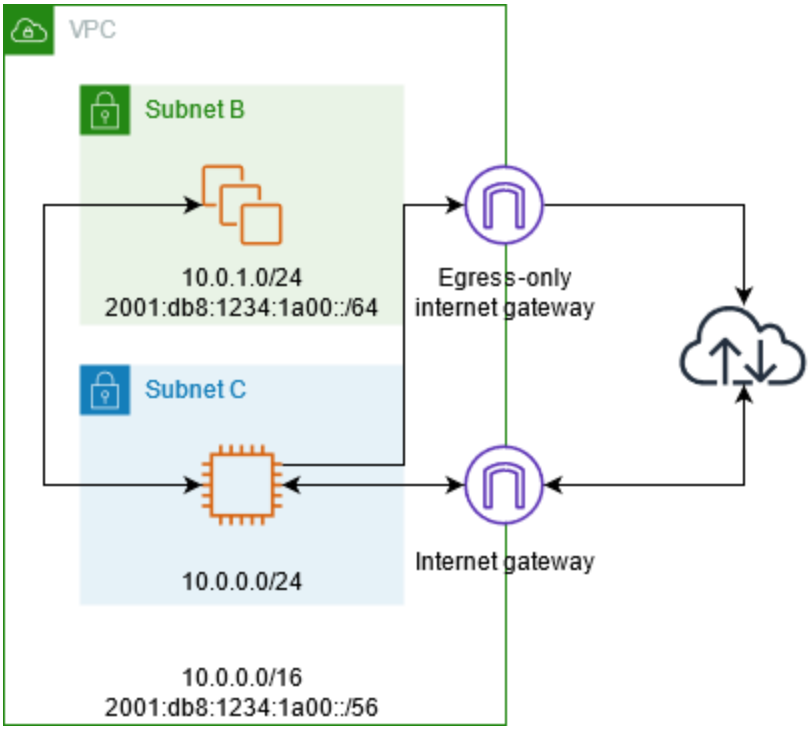
Der Middlebox-Routing-Assistent führt automatisch die folgenden Vorgänge aus:

- Erstellt die folgenden Routing-Tabellen:
  - So fügen Sie eine Routing-Tabelle für das Internet-Gateway hinzu
  - Eine Routing-Tabelle für das Zielsubnetz

  - Eine Routing-Tabelle für das Middlebox-Subnetz
- Fügt den neuen Routing-Tabellen die erforderlichen Routen hinzu, wie in den folgenden Abschnitten beschrieben.
- Trennt die Zuordnung der aktuellen Routing-Tabellen, die dem Internet-Gateway, dem Subnetz B und dem Subnetz C zugeordnet sind.
- Verknüpft Routing-Tabelle A mit dem Internet-Gateway (die Quelle im Middlebox-Routing-Assistenten), Routing-Tabelle C mit Subnetz C (die Middlebox im Middlebox-Routing-Assistent) und Routing-Tabelle B mit Subnetz B (das Ziel im Middlebox-Routing-Assistenten).
- Erstellt ein Tag, das angibt, dass es vom Middlebox-Routing-Assistenten erstellt wurde, und ein Tag, das das Erstellungsdatum angibt.

Der Middlebox-Routing-Assistent ändert Ihre vorhandenen Routing-Tabellen nicht. Es erstellt neue Routing-Tabellen und ordnet sie dann Ihren Gateway- und Subnetzressourcen zu. Wenn Ihre Ressourcen bereits explizit vorhandenen Routing-Tabellen zugeordnet sind, werden die vorhandenen Routing-Tabellen zuerst getrennt, und dann werden die neuen Routing-Tabellen Ihren Ressourcen zugeordnet. Ihre vorhandenen Routen-Tabellen werden nicht gelöscht.

Wenn Sie den Middlebox-Routing-Assistenten nicht verwenden, müssen Sie die Routing-Tabellen manuell konfigurieren und dann den Subnetzen und dem Internet-Gateway zuweisen.



Routing-Tabelle für das Internet-Gateway

Die Routing-Tabelle für das Internet-Gateway enthält die folgenden Routen.

Ziel	Ziel	Zweck
10.0.0.0/16	Local	Lokale Route für IPv4
10.0.1.0/24	*appliance-eni*	IPv4-Datenverkehr, der für Subnetz B bestimmt ist, an die Middlebox weiterleiten
2001:db8:1234:1a00::/56	Local	Lokale Route für IPv6
2001:db8:1234:1a00::/64	*appliance-eni*	IPv6-Datenverkehr für Subnetz B an die Middlebox weiterleiten

Es besteht eine Edge-Verknüpfung zwischen dem Internet-Gateway und der VPC.

Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“
- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Routing-Tabelle des Ziel-Subnetzes

Fügen Sie der Routing-Tabelle für das Zielsubnetz die folgenden Routen hinzu (Subnetz B im Beispieldiagramm).

Ziel	Ziel	Zweck
10.0.0.0/16	Local	Lokale Route für IPv4
0.0.0.0/0	*appliance-eni*	Weiterleiten des IPv4-Datenverkehrs für das Internet an die Middlebox

Ziel	Ziel	Zweck
2001:db8:1234:1a00::/56	Local	Lokale Route für IPv6
::/0	*appliance-eni*	Weiterleiten des IPv6-Datenverkehrs für das Internet an die Middlebox

Es gibt eine Subnetzzuordnung mit Subnetz B.

Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“
- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Routing-Tabelle für das Middlebox-Subnetz

Fügen Sie der Routing-Tabelle für das Zielsubnetz die folgenden Routen hinzu (Subnetz C im Beispieldiagramm).

Ziel	Ziel	Zweck
10.0.0.0/16	Local	Lokale Route für IPv4
0.0.0.0/0	*igw-id*	IPv4-Datenverkehr an das Internet-Gateway weiterleiten
2001:db8:1234:1a00::/56	Local	Lokale Route für IPv6
::/0	*eigw-id*	Route für IPv6-Datenverkehr zum nur ausgehenden Internet-Gateway

Es gibt eine Subnetzzuordnung mit dem Zielsubnetz

Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“
- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Überprüfen des Datenverkehrs mithilfe von Appliances in einer Sicherheits-VPC

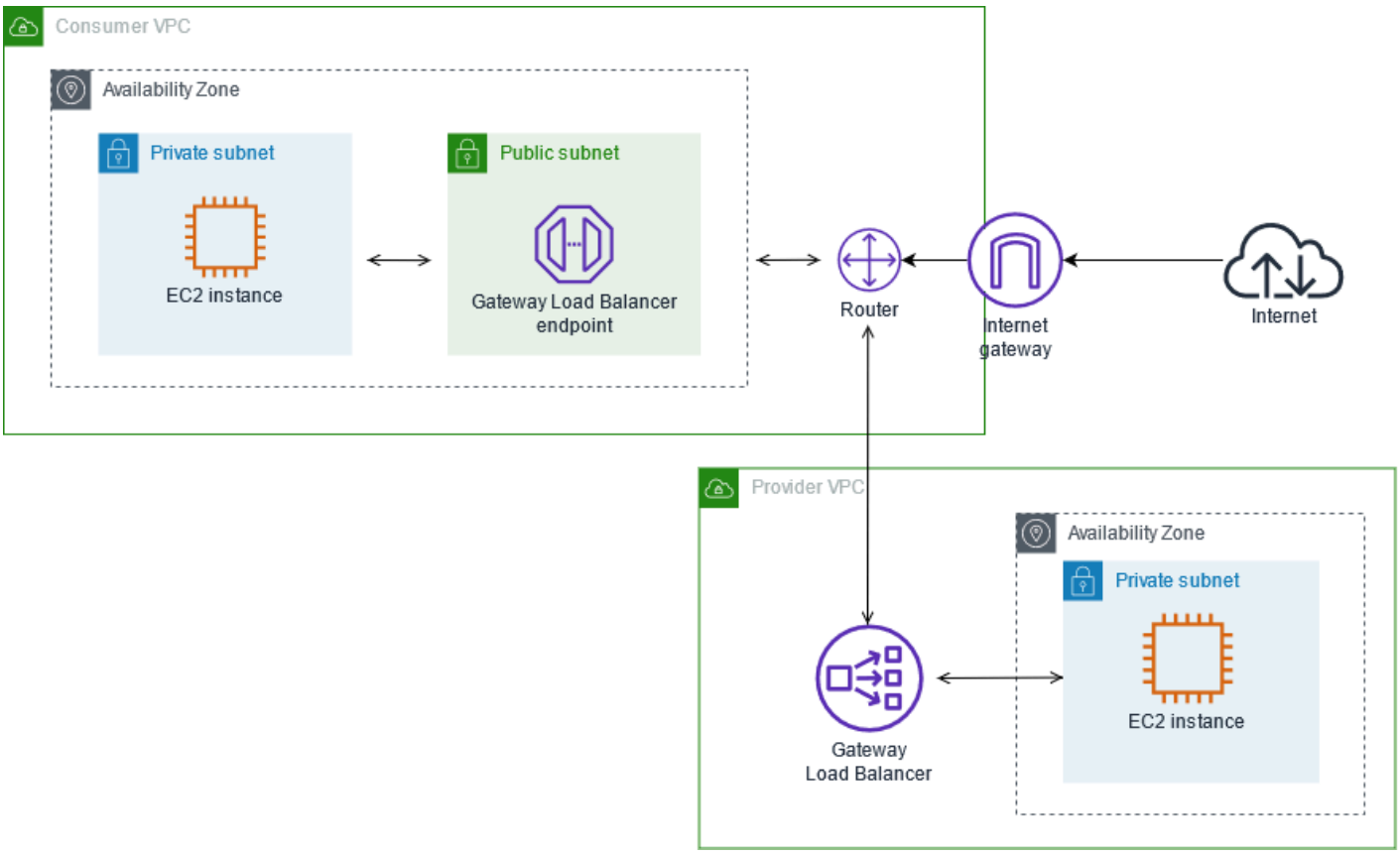
Im folgenden Beispiel möchten Sie den Datenverkehr untersuchen, der vom Internet-Gateway aus in eine VPC gelangt und für ein Subnetz bestimmt ist. Verwenden Sie dazu eine Flotte von Sicherheits-Appliances, die hinter einem Gateway Load Balancer in der Sicherheits-VPC konfiguriert sind. Der Besitzer der Service-Verbraucher-VPC erstellt einen Gateway-Load-Balancer-Endpunkt in einem Subnetz in seiner VPC (dargestellt durch eine Endpunkt-Netzwerkschnittstelle). Der gesamte Datenverkehr, der über das Internet-Gateway in die VPC gelangt, wird zunächst zur Überprüfung n den Gateway-Load-Balancer-Endpunkt weitergeleitet, bevor er an das Anwendungssubnetz weitergeleitet wird. Ebenso wird der gesamte Datenverkehr, der das Anwendungssubnetz verlässt, zunächst zur Überprüfung an den Gateway-Load-Balancer-Endpunkt geleitet, bevor er an das Internet weitergeleitet wird.

Der Middlebox-Routing-Assistent führt automatisch die folgenden Vorgänge aus:

- Erstellt die Routing-Tabellen.
- Fügt die erforderlichen Routen zu den neuen Routing-Tabellen hinzu.
- Löst die Zuordnung der aktuellen Routing-Tabellen auf, die den Subnetzen zugeordnet sind.
- Ordnet die Routing-Tabellen, die der Middlebox-Routing-Assistent erstellt, den Subnetzen zu.
- Erstellt ein Tag, das angibt, dass es vom Middlebox-Routing-Assistenten erstellt wurde, und ein Tag, das das Erstellungsdatum angibt.

Der Middlebox-Routing-Assistent ändert Ihre vorhandenen Routing-Tabellen nicht. Es erstellt neue Routing-Tabellen und ordnet sie dann Ihren Gateway- und Subnetzressourcen zu. Wenn Ihre Ressourcen bereits explizit vorhandenen Routing-Tabellen zugeordnet sind, werden die vorhandenen Routing-Tabellen zuerst getrennt, und dann werden die neuen Routing-Tabellen Ihren Ressourcen zugeordnet. Ihre vorhandenen Routen-Tabellen werden nicht gelöscht.

Wenn Sie den Middlebox-Routing-Assistenten nicht verwenden, müssen Sie die Routing-Tabellen manuell konfigurieren und dann den Subnetzen und dem Internet-Gateway zuweisen.



Routing-Tabelle für das Internet-Gateway

Die Routing-Tabelle für den Internet-Gateway enthält die folgenden Routen.

Ziel	Ziel	Zweck
VPC-CIDR des Verbraucher	Local	Lokale Route
CIDR des Anwendungs-Subnetzes	*endpunkt-ID*	Leitet den für das Anwendungssubnetz bestimmten Datenverkehr an den Gateway-Load-Balancer-Endpunkt weiter.

Es gibt eine Edge-Verknüpfung mit dem Gateway.

Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“

- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Routing-Tabelle des Anwendungssubnetzes

Die Routing-Tabelle für das Anwendungssubnetz enthält die folgenden Routen.

Ziel	Ziel	Zweck
VPC-CIDR des Verbraucher	Local	Lokale Route
0.0.0.0/0	*endpunkt-ID*	Leiten Sie den Datenverkehr von den Anwendungsservers an den Gateway-Load-Balancer-Endpunkt, bevor er an das Internet weitergeleitet wird.

Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“
- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Routing-Tabelle für das Anbietersubnetz

Die Routing-Tabelle für das Anbietersubnetz enthält die folgenden Routen.

Ziel	Ziel	Zweck
VPC-CIDR des Anbieters	Local	Lokale Route. Stellt sicher, dass der aus dem Internet stammende Datenverkehr an die Anwendungsserver weitergeleitet wird.
0.0.0.0/0	*igw-id*	Leitet den gesamten Datenverkehr an das Internet-Gateway

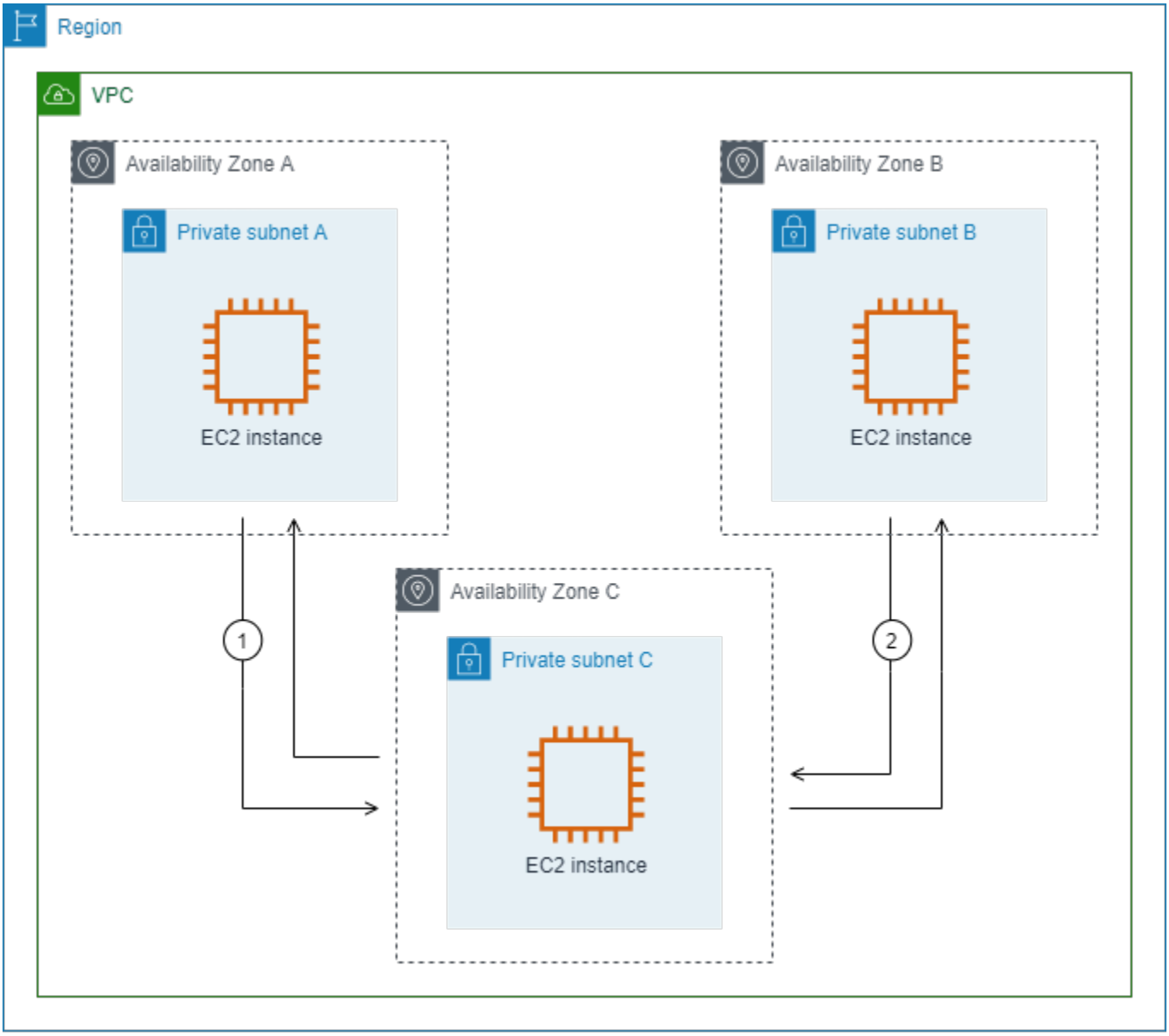
Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“
- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Überprüfen des Datenverkehrs zwischen Subnetzen

Stellen Sie sich das Szenario vor, in dem Sie über mehrere Subnetze in einer VPC verfügen und den Datenverkehr zwischen ihnen durch eine Firewall-Appliance überprüfen möchten. Konfigurieren und installieren Sie die Firewall-Appliance auf einer EC2-Instance in einem separaten Subnetz in Ihrer VPC.

Das folgende Diagramm zeigt eine Firewall-Appliance, die auf einer EC2-Instance in dem Subnetz C installiert ist. Die Appliance prüft den gesamten Datenverkehr, der vom Subnetz A in das Subnetz B (siehe 1) und vom Subnetz B in das Subnetz A (siehe 2) fließt.



Sie verwenden die Haupt-Routing-Tabelle für die VPC und das Subnetz der Middlebox. Subnetze A und B verfügen jeweils über eine benutzerdefinierte Routing-Tabelle.

Der Middlebox-Routing-Assistent führt automatisch die folgenden Vorgänge aus:

- Erstellt die Routing-Tabellen.
- Fügt die erforderlichen Routen zu den neuen Routing-Tabellen hinzu.
- Löst die Zuordnung der aktuellen Routing-Tabellen auf, die den Subnetzen zugeordnet sind.
- Ordnet die Routing-Tabellen, die der Middlebox-Routing-Assistent erstellt, den Subnetzen zu.

- Erstellt ein Tag, das angibt, dass es vom Middlebox-Routing-Assistenten erstellt wurde, und ein Tag, das das Erstellungsdatum angibt.

Der Middlebox-Routing-Assistent ändert Ihre vorhandenen Routing-Tabellen nicht. Es erstellt neue Routing-Tabellen und ordnet sie dann Ihren Gateway- und Subnetzressourcen zu. Wenn Ihre Ressourcen bereits explizit vorhandenen Routing-Tabellen zugeordnet sind, werden die vorhandenen Routing-Tabellen zuerst getrennt, und dann werden die neuen Routing-Tabellen Ihren Ressourcen zugeordnet. Ihre vorhandenen Routen-Tabellen werden nicht gelöscht.

Wenn Sie den Middlebox-Routing-Assistenten nicht verwenden, müssen Sie die Routing-Tabellen manuell konfigurieren und dann den Subnetzen und dem Internet-Gateway zuweisen.

Benutzerdefinierte Routing-Tabelle für Subnetz A

Die Routing-Tabelle für Subnetz A enthält die folgenden Routen.

Ziel	Ziel	Zweck
VPC-CIDR	Local	Lokale Route
Subnetz-B-CIDR	*appliance-eni*	Datenverkehr für Subnetz B an die Middlebox weiterleiten

Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“
- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Benutzerdefinierte Routing-Tabelle für Subnetz B

Die Routing-Tabelle für Subnetz B enthält die folgenden Routen.

Ziel	Ziel	Zweck
VPC-CIDR	Local	Lokale Route

Ziel	Ziel	Zweck
Subnetz-A-CIDR	*appliance-eni*	Datenverkehr für Subnetz A an die Middlebox weiterleiten

Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“
- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Haupt-Routing-Tabelle

Das Subnetz C verwendet die Haupt-Routing-Tabelle. Die Haupt-Routing-Tabelle enthält die folgenden Route.

Ziel	Ziel	Zweck
VPC-CIDR	Local	Lokale Route

Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- Der Schlüssel ist „Origin“ (Ursprung) und der Wert ist „Middlebox Wizard“
- Der Schlüssel ist „date_created“ und der Wert ist die Erstellungszeit (z. B. „2021-02-18T22:25:49.137Z“)

Löschen eines Subnetzes

Sie können ein Subnetz löschen, falls Sie es nicht mehr benötigen. Wenn es Netzwerkschnittstellen enthält, können Sie ein Subnetz jedoch nicht löschen. Sie müssen in einem Subnetz zum Beispiel alle Instances beenden, bevor Sie es löschen können.

Wie Sie ein Subnetz mit Hilfe der Konsole löschen

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Dazu müssen Sie zunächst alle Instances im Subnetz beenden. Weitere Informationen finden Sie unter Beenden Ihrer Instance im Amazon-EC2-Benutzerhandbuch.
3. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
4. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus.
5. Wählen Sie das Subnetz und dann Actions (Aktionen) und Delete subnet (Subnetz löschen) aus.
6. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Delete (Löschen) aus.

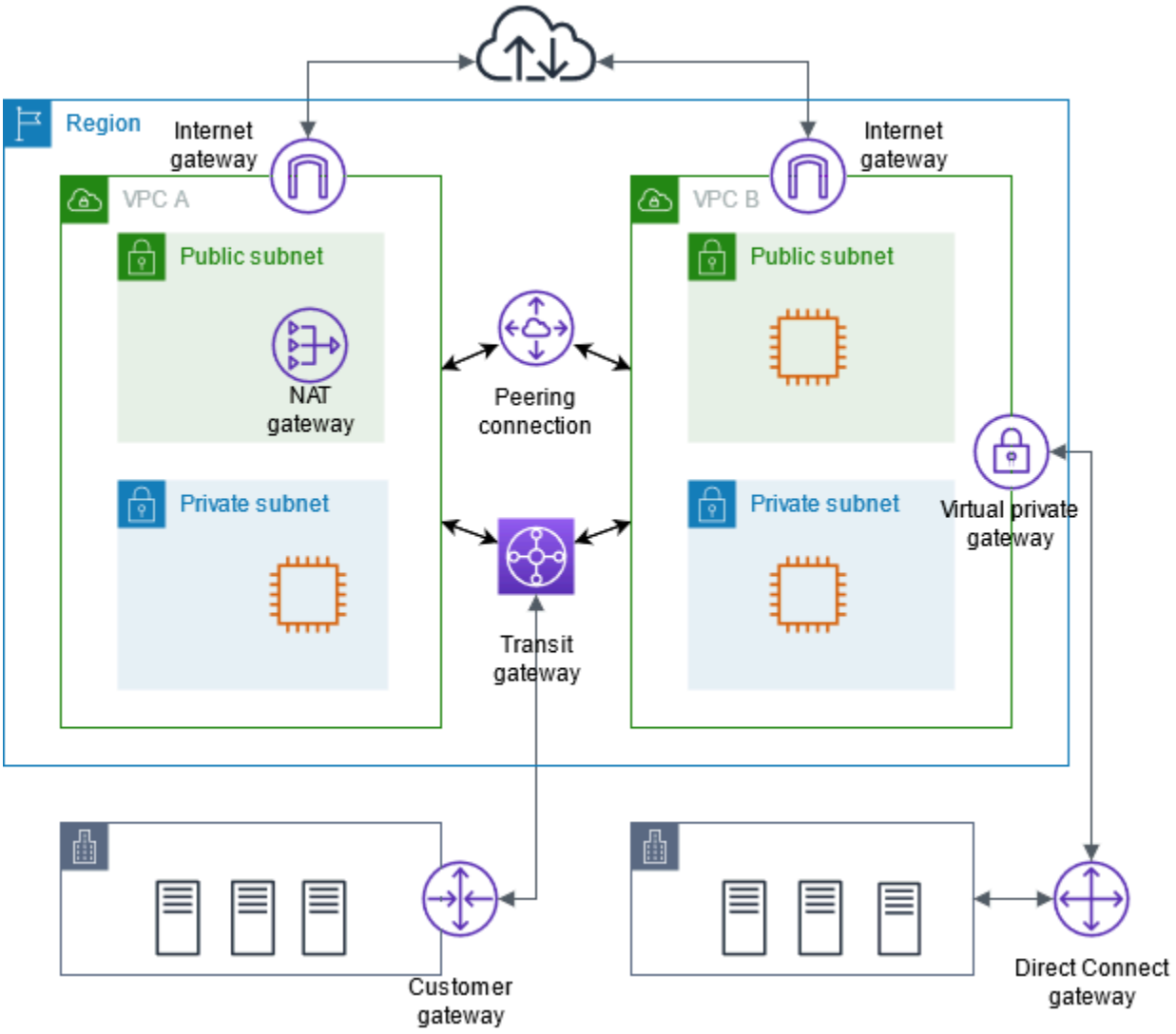
So löschen Sie ein Subnetz mit der AWS CLI

Verwenden Sie den Befehl delete-subnet.

Verbinden Ihrer VPC mit anderen Netzwerken

Ihre Virtual Private Cloud (VPC) können Sie mit anderen Netzwerken verbinden. Zum Beispiel mit anderen VPCs, mit dem Internet oder mit Ihre On-Premises Netzwerk.

Das folgende Diagramm veranschaulicht einige dieser Verbindungsoptionen. VPC A ist über ein Internet-Gateway mit dem Internet verbunden. Die EC2-Instance im privaten Subnetz von VPC A kann über das NAT-Gateway im öffentlichen Subnetz von VPC A eine Internetverbindung herstellen. VPC B ist über ein Internet-Gateway mit dem Internet verbunden. Die EC2-Instance im öffentlichen Subnetz von VPC B kann über das Internet-Gateway eine Internetverbindung herstellen. VPC A und VPC B sind über eine VPC-Peering-Verbindung und ein Transit-Gateway miteinander verbunden. Das Transit-Gateway ist per VPN an ein Rechenzentrum angeschlossen. VPC B hat eine AWS Direct Connect Verbindung zu einem Rechenzentrum.



Weitere Informationen finden Sie unter Verbindungsoptionen für Amazon Virtual Private Cloud.

Inhalt

Herstellen einer Internetverbindung über ein Internet-Gateway

Ein Internet-Gateway ist eine horizontal skalierte, redundante und hochverfügbare VPC-Komponente, die die Kommunikation zwischen Ihrer VPC und dem Internet ermöglicht. Es unterstützt IPv4- und IPv6-Datenverkehr. Es verursacht keine Verfügbarkeitsrisiken oder Bandbreitenbeschränkungen für den Netzwerkverkehr.

Über ein Internet-Gateway können Ressourcen in Ihren öffentlichen Subnetzen (wie EC2-Instances) eine Internetverbindung herstellen, sofern sie über eine öffentliche IPv4-Adresse oder eine IPv6-Adresse verfügen. Desgleichen können Ressourcen im Internet über die öffentliche IPv4-Adresse oder die IPv6-Adresse eine Verbindung mit Ressourcen in Ihrem Subnetz initiieren. Mit einem Internet-Gateway können Sie beispielsweise über Ihren lokalen Computer eine Verbindung zu einer EC2-Instance AWS herstellen.

Ein Internet-Gateway bietet in Ihren VPC-Routing-Tabellen ein Ziel für über das Internet routingfähigen Datenverkehr. Für die Kommunikation über IPv4 führt das Internet-Gateway auch Network Address Translation (NAT) aus. Für die Kommunikation mit IPv6 wird NAT nicht benötigt, da IPv6-Adressen öffentlich sind. Weitere Informationen finden Sie unter IP-Adressen und NAT.

Konfiguration des Internetzugangs

Gehen Sie wie folgt vor, damit Ihre Instances Datenverkehr aus dem Internet empfangen oder senden können:

- Erstellen Sie ein Internet-Gateway und hängen Sie es Ihrer VPC an.
- Fügen Sie der Routing-Tabelle Ihres Subnetzes eine Route hinzu, die den Datenverkehr ins Internet zum Internet-Gateway leitet.
- Vergewissern Sie sich, dass Instances in Ihrem Subnetz eine öffentliche IPv4-Adresse oder eine IPv6-Adresse haben. Weitere Informationen finden Sie unter Instance-IP-Adressierung im Amazon EC2 EC2-Benutzerhandbuch.
- Vergewissern Sie sich, dass die Netzwerkzugriffskontrolllisten und Sicherheitsgruppenregeln dem gewünschten Internetdatenverkehr erlauben, zu und von Ihren Instances zu fließen.

Um Ihren Instances Internetzugang zu bieten, ohne ihnen öffentliche IP-Adressen zuzuweisen, verwenden Sie stattdessen ein NAT-Gerät. Ein NAT-Gerät ermöglicht es Instances in einem privaten Subnetz, sich mit dem Internet zu verbinden, verhindert jedoch, dass Hosts im Internet auf diese Instances zugreifen. Weitere Informationen finden Sie unter NAT-Geräte.

Öffentliche und private Subnetze

Ist ein Subnetz einer Routing-Tabelle zugewiesen, die über eine Route zu einem Internet-Gateway verfügt, wird es als öffentliches Subnetz bezeichnet. Wenn ein Subnetz einer Routing-Tabelle zugeordnet ist, die über keine Route zu einem Internet-Gateway verfügt, wird es als privates Subnetzbezeichnet.

In der öffentlichen Subnetz-Routingtabelle können Sie eine Route für das Internet-Gateway für alle Ziele festlegen, die der Routingtabelle nicht ausdrücklich bekannt sind (`0.0.0.0/0` für IPv4 oder `::/0` für IPv6). Alternativ können Sie die Route auf einen engeren Bereich von IP-Adressen beschränken, z. B. auf die öffentlichen IPv4-Adressen der öffentlichen Endpunkte Ihres Unternehmens außerhalb oder auf die Elastic IP-Adressen anderer Amazon EC2 EC2-Instances außerhalb Ihrer VPC. AWS

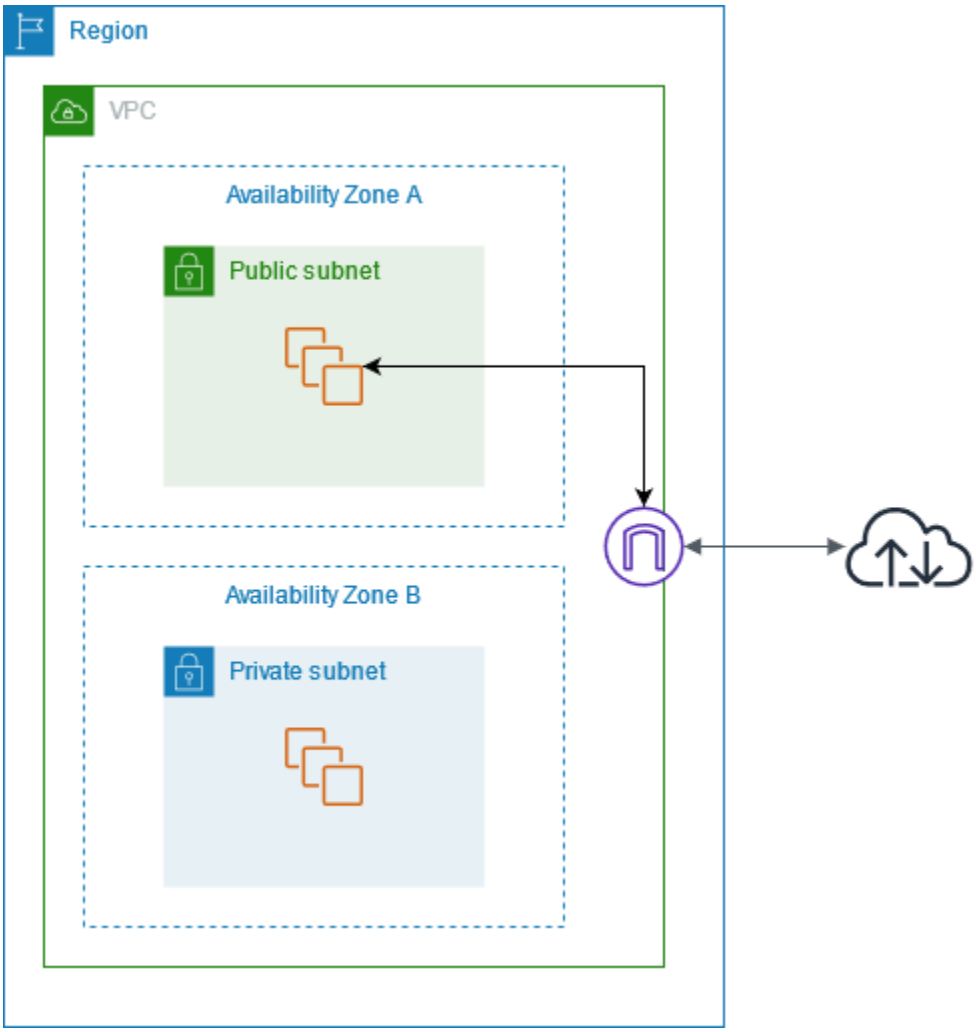
IP-Adressen und NAT

Damit die Kommunikation über das Internet für IPv4 aktiviert werden kann, muss Ihre Instance über eine öffentliche IPv4-Adresse verfügen. Sie können entweder Ihre VPC so konfigurieren, dass sie Instances öffentliche IPv4-Adressen zuweist, oder Sie können Instances Elastic-IP-Adressen zuweisen. Ihre Instance ist nur mit dem privaten (internen) IP-Adressraum kompatibel, der innerhalb der VPC und dem Subnetz definiert ist. Das Internet-Gateway stellt das one-to-one NAT logischerweise im Namen Ihrer Instance bereit. Wenn also Traffic Ihr VPC-Subnetz verlässt und ins Internet geht, wird das Antwortadressfeld auf die öffentliche IPv4-Adresse oder Elastic IP-Adresse Ihrer Instance gesetzt und nicht auf deren private IP-Adresse. Umgekehrt wird der Zielbereich des

Datenverkehrs, der für die öffentliche IPv4-Adresse oder Elastic-IP-Adresse Ihrer Instance bestimmt ist, in die private IPv4-Adresse übersetzt, bevor der Datenverkehr an die VPC übermittelt wird.

Damit die Kommunikation über das Internet für IPv6 aktiviert werden kann, muss Ihre VPC und Ihr Subnetz über einen zugehörigen IPv6 CIDR-Block verfügen und Ihrer Instance muss eine IPv6-Adresse aus dem Subnetzbereich zugeordnet sein. IPv6-Adressen sind global eindeutig und daher standardmäßig öffentlich.

Im folgenden Diagramm ist das Subnetz in Availability Zone A ein öffentliches Subnetz. Die Routing-Tabelle für dieses Subnetz hat eine Route, die den gesamten IPv4-Internet-Datenverkehr an das Internet-Gateway sendet. Die Instances im öffentlichen Subnetz müssen öffentliche IP-Adressen oder elastische IP-Adressen haben, um die Kommunikation mit dem Internet über das Internet-Gateway zu ermöglichen. Zum Vergleich ist das Subnetz in Availability Zone B ein privates Subnetz, da seine Routing-Tabelle keine Route zum Internet-Gateway hat. Da es keine Route zum Internet-Gateway gibt, können Instances im privaten Subnetz nicht mit dem Internet kommunizieren, selbst wenn sie über öffentliche IP-Adressen verfügen.



Internetzugriff für standardmäßige und nicht standardmäßige VPCs

Die folgende Tabelle bietet eine Übersicht darüber, ob Ihre VPC automatisch über die Komponenten verfügt, die für den Internetzugriff über IPv4 oder IPv6 notwendig sind.

Komponente	Standard-VPC	Nicht standardmäßige VPC
Internet-Gateway	Ja	Nein
Routing-Tabelle mit Route zum Internet-Gateway für IPv4-Datenverkehr (0.0.0.0/0)	Ja	Nein
Routing-Tabelle mit Route zum Internet-Gateway für IPv6-Datenverkehr (::/0)	Nein	Nein
Automatische Zuordnung der öffentlichen IPv4-Adresse zur Instance, die im Subnetz gestartet wird	Ja (standardmäßiges Subnetz)	Nein (nicht standardmäßiges Subnetz)
Automatische Zuordnung der öffentlichen IPv6-Adresse zur Instance, die im Subnetz gestartet wird	Nein (standardmäßiges Subnetz)	Nein (nicht standardmäßiges Subnetz)

Weitere Informationen über die VPCs finden Sie unter Standard-VPCs. Weitere Informationen zum Erstellen einer VPC finden Sie unter Erstellen einer VPC.

Arbeiten mit Internet-Gateways

Im Folgenden wird beschrieben, wie Sie den Internetzugriff von einem Subnetz in Ihrer VPC mit einem Internet-Gateway unterstützen. Um den Internetzugang zu entfernen, können Sie das Internet-Gateway von Ihrer VPC trennen und dann löschen.

Aufgaben

- Ein Internet-Gateway erstellen

- Hinzufügen eines Internet-Gateways zu einer VPC
- Trennen eines Internet-Gateways von Ihrer VPC
- Löschen eines Internet-Gateways

Ein Internet-Gateway erstellen

Gehen Sie wie folgt vor, um ein Internet-Gateway zu erstellen.

So erstellen Sie ein Internet-Gateway

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Internet Gateways (Internet-Gateways) aus.
3. Wählen Sie Create internet gateway (Internet-Gateway erstellen) aus.
4. (Optional) Geben Sie einen Namen für Ihr Internet-Gateway ein.
5. (Optional) Um ein Tag hinzuzufügen, wählen Sie Add new tag (Neuen Tag hinzufügen) aus und geben Sie den Schlüssel und den Wert für den Tag ein.
6. Wählen Sie Create internet gateway (Internet-Gateway erstellen) aus.
7. (Optional) Um das Internet-Gateway jetzt mit einer VPC zu verbinden, wählen Sie im Banner oben auf dem Bildschirm die Option An eine VPC anhängen, wählen Sie eine verfügbare VPC aus und wählen Sie dann Internet-Gateway anhängen. Andernfalls können Sie Ihr Internet-Gateway zu einem anderen Zeitpunkt an eine VPC anhängen.

Hinzufügen eines Internet-Gateways zu einer VPC

Um ein Internet-Gateway zu verwenden, müssen Sie es einer VPC anhängen.

So hängen Sie ein Internet-Gateway einer VPC an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Internet Gateways (Internet-Gateways) aus.
3. Wählen Sie das Feld neben dem Internet-Gateway aus.
4. Wählen Sie unter Aktionen die Option An VPC anfügen aus.
5. Wählen Sie eine verfügbare VPC aus.
6. Wählen Sie Internet-Gateway anfügen.

Trennen eines Internet-Gateways von Ihrer VPC

Wenn Sie für Instances, die Sie in einer VPC starten, keinen Internetzugriff mehr benötigen, können Sie ein Internet-Gateway von einer VPC trennen. Wenn die VPC über Ressourcen verfügt, die öffentlichen IP-Adressen oder Elastic-IP-Adressen zugeordnet sind, dann können Sie das Internet-Gateway nicht trennen.

So trennen Sie ein Internet-Gateway

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Internet Gateways (Internet-Gateways) aus.
3. Wählen Sie das Feld neben dem Internet-Gateway aus.
4. Wählen Sie Aktionen, Von VPC trennen.
5. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Internet-Gateway trennen.

Löschen eines Internet-Gateways

Wenn Sie ein Internet-Gateway nicht mehr benötigen, können Sie es löschen. Sie können ein Internet-Gateway, das noch immer einer VPC zugeordnet ist, nicht löschen.

So löschen Sie ein Internet-Gateway

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Internet Gateways (Internet-Gateways) aus.
3. Wählen Sie das Feld neben dem Internet-Gateway aus.
4. Wählen Sie Aktionen, Internet-Gateway löschen.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Internet-Gateway löschen aus.

Überblick über die API und Befehlszeile

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile oder eine API ausführen. Weitere Informationen über Befehlszeilenschnittstellen und eine Liste der verfügbaren API-Aktionen finden Sie unter Arbeiten mit Amazon VPC.

Ein Internet-Gateway erstellen

- create-internet-gateway (AWS CLI)
- New-EC2InternetGateway (AWS Tools for Windows PowerShell)

Hinzufügen eines Internet-Gateways zu einer VPC

- attach-internet-gateway (AWS CLI)
- Add-EC2InternetGateway (AWS Tools for Windows PowerShell)

Beschreiben eines Internet-Gateways

- describe-internet-gateways (AWS CLI)
- Get-EC2InternetGateway (AWS Tools for Windows PowerShell)

Trennen eines Internet-Gateways von einer VPC

- detach-internet-gateway (AWS CLI)
- Dismount-EC2InternetGateway (AWS Tools for Windows PowerShell)

Löschen eines Internet-Gateways

- delete-internet-gateway (AWS CLI)
- Remove-EC2InternetGateway (AWS Tools for Windows PowerShell)

Preisgestaltung

Für ein Internet-Gateway fallen keine Gebühren an. Für EC2-Instances, die Internet-Gateways verwenden, fallen jedoch Datenübertragungsgebühren an. Weitere Informationen finden Sie unter Amazon EC2 – On-Demand-Preise.

Aktivieren von ausgehendem IPv6-Datenverkehr mit einem Internet-Gateway, das nur ausgehenden Verkehr zulässt

Ein Internet-Gateway nur für ausgehenden Verkehr ist eine horizontal skalierte, redundante und hochverfügbare VPC-Komponente, die ausgehende Kommunikation über IPv6-Instances in Ihrer VPC zum Internet ermöglicht. Darüber hinaus verhindert sie, dass das Internet eine IPv6-Verbindung mit Ihren Instances initiiert.

> **Note**
>
> Ein Internet-Gateway nur für ausgehenden Verkehr steht ausschließlich für den IPv6-Datenverkehr zur Verfügung. Verwenden Sie stattdessen ein NAT-Gateway, um die ausgehende Internet-Kommunikation über IPv4 zuzulassen. Weitere Informationen finden Sie unter NAT gateways (NAT-Gateways).

Inhalt

Grundlagen des Internet-Gateways für ausgehenden Verkehr

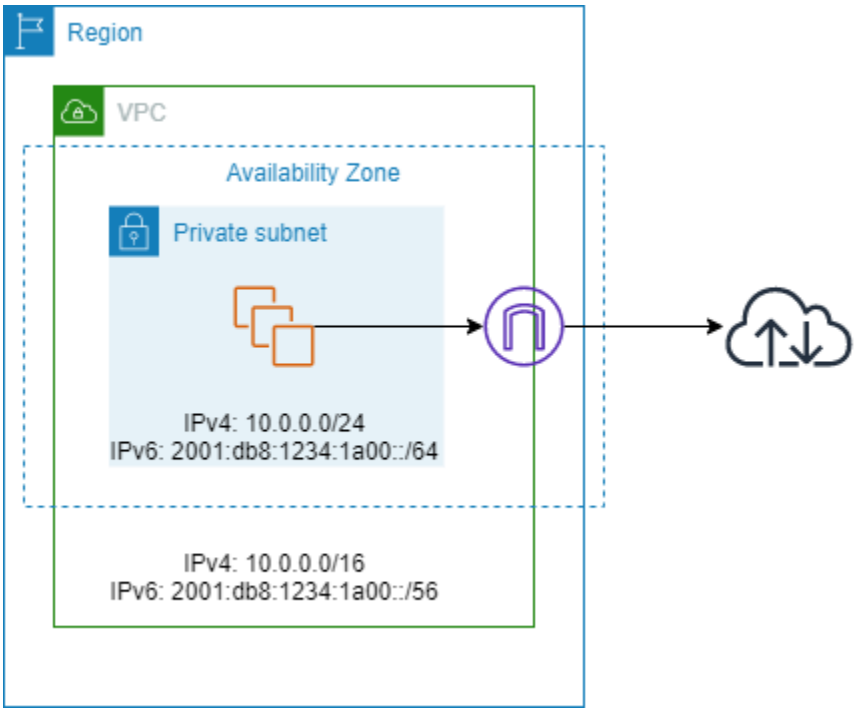
IPv6-Adressen sind global eindeutig und daher standardmäßig öffentlich. Wenn Sie Ihrer Instance den Zugriff auf das Internet ermöglichen, aber verhindern möchten, dass Internet-Ressourcen die Kommunikation mit Ihrer Instance initiieren, verwenden Sie ein Internet-Gateway nur für ausgehenden Verkehr. Erstellen Sie dazu in Ihrer VPC ein Internet-Gateway nur für ausgehenden Verkehr und fügen Sie Ihrer Routing-Tabelle eine Route hinzu, die den gesamten IPv6-Datenverkehr (`::/0`) oder einen bestimmten Bereich von IPv6-Adressen an das Internet-Gateway nur für ausgehenden Verkehr leitet. IPv6-Datenverkehr im Subnetz, der mit der Routing-Tabelle verknüpft ist, wird an das Internet-Gateway nur für ausgehenden Verkehr weitergeleitet.

Ein Internet-Gateway nur für ausgehenden Datenverkehr ist statusbehaftet: Es leitet den Datenverkehr von den Instances im Subnetz an das Internet oder andere AWS Dienste weiter und sendet dann die Antwort zurück an die Instances.

Ein Internet-Gateway nur für ausgehenden Verkehr weist folgende Merkmale auf:

- Sie können einem Internet-Gateway nur für ausgehenden Verkehr keine Sicherheitsgruppe zuordnen. Sie können die Sicherheitsgruppen für Instances im privaten Subnetz zur Steuerung des Datenverkehrs zu und von diesen Instances verwenden.
- Sie können eine Netzwerk-ACL verwenden, um den Datenverkehr zu und von dem Subnetz zu steuern, für das das Internet-Gateway nur für ausgehenden Verkehr Datenverkehr weiterleitet.

Im folgenden Diagramm verfügen sowohl die VPC als auch das Subnetz über IPv4- und IPv6-CIDR-Blöcke. Die VPC verfügt über ein Internet-Gateway, das nur ausgehenden Verkehr zulässt.



Die folgende Tabelle ist ein Beispiel für eine Routing-Tabelle, die dem Subnetz zugeordnet ist. Es gibt eine Route, über die der gesamte für das Internet bestimmte IPv6-Datenverkehr (::/0) an das nur für ausgehenden Verkehr vorgesehene Internet-Gateway gesendet wird.

Bestimmungsort	Ziel
10.0.0.0/16	Local
2001:db8:1234:1a00:/64	Local
::/0	*eigw-id*

Arbeiten mit Internet-Gateways für ausgehenden Verkehr

Die folgenden Aufgaben beschreiben, wie Sie für Ihr privates Subnetz ein Internet-Gateway nur für ausgehenden Verkehr erstellen und das Routing für das Subnetz konfigurieren.

Aufgaben

- Erstellen eines Internet-Gateways nur für ausgehenden Verkehr
- Anzeigen des Internet-Gateways für ausgehenden Datenverkehr
- Erstellen einer benutzerdefinierten Routing-Tabelle
- Löschen eines Internet-Gateways nur für ausgehenden Verkehr

Erstellen eines Internet-Gateways nur für ausgehenden Verkehr

Sie können für Ihre VPC mithilfe der Amazon VPC-Konsole ein Internet-Gateway für ausgehenden Verkehr erstellen.

So erstellen Sie ein Internet-Gateway nur für ausgehenden Verkehr

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Egress Only Internet Gateways aus.
3. Klicken Sie auf Create Egress Only Internet Gateway.
4. (Optional) Hinzufügen oder Entfernen eines Tags.

   [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).
5. Wählen Sie die VPC aus, in der Sie das Internet-Gateway für ausgehenden Verkehr erstellen möchten.
6. Wählen Sie Erstellen.

Anzeigen des Internet-Gateways für ausgehenden Datenverkehr

Sie können für Ihre VPC mithilfe der Amazon VPC-Konsole ein Internet-Gateway für ausgehenden Verkehr erstellen.

So zeigen Sie Informationen über ein Internet-Gateway nur für ausgehenden Verkehr an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Egress Only Internet Gateways aus.
3. Wählen Sie das Internet-Gateway nur für ausgehenden Verkehr aus, um dessen Informationen im Detailbereich anzuzeigen.

Erstellen einer benutzerdefinierten Routing-Tabelle

Um den für außerhalb der VPC bestimmten Datenverkehr an das Internet-Gateway nur für ausgehenden Verkehr zu senden, müssen Sie eine benutzerdefinierte Routing-Tabelle erstellen, eine Route hinzufügen, die den Datenverkehr an das Gateway sendet, und diese anschließend Ihrem Subnetz zuordnen.

So erstellen Sie eine benutzerdefinierte Routing-Tabelle und fügen eine Route zum Internet-Gateway nur für ausgehenden Verkehr hinzu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables die Option Create route table aus.
3. Im Dialogfeld Create route table können Sie Ihre Routing-Tabelle wahlweise benennen, Ihre VPC auswählen und anschließend auf Create route table klicken.
4. Wählen Sie die benutzerdefinierte Routing-Tabelle aus, die Sie gerade erstellt haben. Der Detailbereich enthält Registerkarten für die Arbeit mit Routen, Zuordnungen und Routing-Verbreitung.
5. Wählen Sie auf der Registerkarte Routes (Routen) die Option Edit routes (Routen bearbeiten) aus und geben Sie `::/0` in das Feld Destination (Ziel) ein. Wählen Sie in der Liste Target (Ziel) die ID des Internet-Gateway nur für ausgehenden Verkehr und dann Save changes (Änderungen speichern) aus.
6. Wählen Sie auf der Registerkarte Subnet associations (Subnetzzuordnungen) die Option Edit subnet associations (Subnetzzuordnungen bearbeiten) aus und aktivieren Sie für das Subnetz das Kontrollkästchen. Wählen Sie Speichern.

Alternativ können Sie einer bereits vorhandenen Routing-Tabelle, die mit Ihrem Subnetz verknüpft ist, eine Route hinzufügen. Wählen Sie die bereits vorhandene Routing-Tabelle aus und befolgen Sie die oben angegebenen Schritte 5 und 6, um eine Route zum Internet-Gateway nur für ausgehenden Verkehr hinzuzufügen.

Weitere Informationen über die Routing-Tabellen finden Sie unter Konfigurieren von Routing-Tabellen.

Löschen eines Internet-Gateways nur für ausgehenden Verkehr

Wenn Sie ein Internet-Gateway nur für ausgehenden Verkehr nicht länger benötigen, können Sie es löschen. Alle Routen in einer Routing-Tabelle, die auf ein gelöschtes Internet-Gateway nur für ausgehenden Verkehr verweisen, verbleiben im Status `blackhole`, bis Sie die Route manuell löschen oder aktualisieren.

So löschen Sie ein Internet-Gateway nur für ausgehenden Verkehr

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Egress Only Internet Gateways (Internet-Gateways nur für ausgehenden Verkehr) und dann das Internet-Gateway nur für ausgehenden Verkehr aus.
3. Wählen Sie Delete (Löschen).
4. Klicken Sie im Bestätigungsdialogfeld auf Delete Egress Only Internet Gateway.

API- und CLI-Übersicht

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile oder eine API ausführen. Weitere Informationen über Befehlszeilenschnittstellen und eine Liste der verfügbaren API-Aktionen finden Sie unter Arbeiten mit Amazon VPC.

Erstellen eines Internet-Gateways nur für ausgehenden Verkehr

- create-egress-only-internet AWS CLI-Gateway ()
- New-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

Beschreiben eines Internet-Gateways nur für ausgehenden Verkehr

- describe-egress-only-internet-Gateways ()AWS CLI

- Get-EC2EgressOnlyInternetGatewayList (AWS Tools for Windows PowerShell)

Löschen eines Internet-Gateways nur für ausgehenden Verkehr

- delete-egress-only-internet-Gateway ()AWS CLI
- Remove-EC2EgressOnlyInternetGateway (AWS Tools for Windows PowerShell)

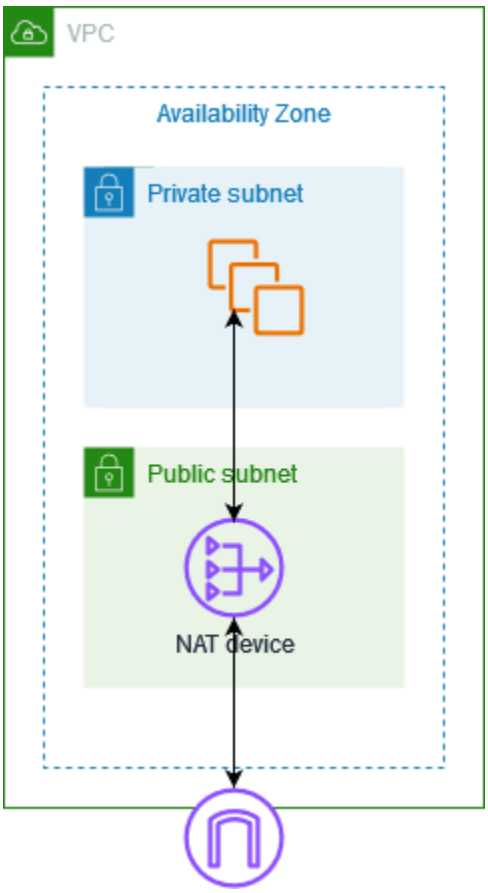
Preisgestaltung

Für ein Internet-Gateway für reinen ausgehenden Datenverkehr fallen keine Gebühren an. Für EC2-Instances, die Internet-Gateways verwenden, fallen jedoch Datenübertragungsgebühren an. Weitere Informationen finden Sie unter Amazon EC2 – On-Demand-Preise.

Herstellen einer Verbindung mit dem Internet oder anderen Netzwerken über NAT-Geräte

Sie können ein NAT-Gerät verwenden, um Ressourcen in privaten Subnetzen die Verbindung mit dem Internet, anderen VPCs oder lokalen Netzwerken zu ermöglichen. Diese Instances können mit Services außerhalb der VPC kommunizieren, aber sie können keine unerwünschten Verbindungsanforderungen empfangen.

Das folgende Diagramm zeigt beispielsweise ein NAT-Gerät in einem öffentlichen Subnetz, das es den EC2-Instances in einem privaten Subnetz ermöglicht, sich über ein Internet-Gateway mit dem Internet zu verbinden. Das NAT-Gerät ersetzt die IPv4-Quelladresse der Instances durch die Adresse des NAT-Geräts. Beim Senden von Antwortdatenverkehr an die Instances übersetzt das NAT-Gerät die Adressen zurück in die ursprünglichen IPv4-Quelladressen.



Important

- Wir verwenden in dieser Dokumentation den in der IT gängigen Begriff NAT, obwohl ein NAT-Gerät tatsächlich sowohl Adressübersetzung als auch Port-Adressübersetzung (PAT) leistet.
- Sie können ein verwaltetes NAT-Gerät verwenden, das von angeboten wird AWS, ein sogenanntes NAT-Gateway, oder Sie können Ihr eigenes NAT-Gerät auf einer EC2-Instance, einer sogenannten NAT-Instance, erstellen. Es wird empfohlen, NAT-Gateways zu verwenden, da sie eine bessere Verfügbarkeit und Bandbreite bieten und weniger Administrationsaufwand erfordern.

Inhalt

NAT gateways (NAT-Gateways)

Ein NAT-Gateway ist ein Network Address Translation (NAT)-Service. Sie können ein NAT-Gateway verwenden, damit Instances in einem privaten Subnetz eine Verbindung zu Services außerhalb Ihrer VPC herstellen können, externe Services jedoch keine Verbindung mit diesen Instances herstellen können.

Wenn Sie ein NAT-Gateway erstellen, geben Sie einen der folgenden Verbindungstypen an:

- Öffentlich – (Standard) Instances in privaten Subnetzen können über ein öffentliches NAT-Gateway eine Verbindung zum Internet herstellen, aber keine unerwünschten eingehenden Verbindungen aus dem Internet empfangen. Sie erstellen ein öffentliches NAT-Gateway in einem öffentlichen Subnetz und müssen beim Erstellen eine elastische IP-Adresse mit dem NAT-Gateway verknüpfen. Sie leiten den Datenverkehr vom NAT-Gateway zum Internet-Gateway für die VPC weiter. Alternativ können Sie ein öffentliches NAT-Gateway verwenden, um eine Verbindung zu anderen VPCs oder Ihrem On-Premises-Netzwerk herzustellen. In diesem Fall leiten Sie den Datenverkehr vom NAT-Gateway über ein Transit Gateway oder ein Virtual Private Gateway weiter.
- Privat – Instances in privaten Subnetzen können über ein privates NAT-Gateway eine Verbindung mit anderen VPCs oder Ihrem On-Premises-Netzwerk herstellen. Sie können den Datenverkehr vom NAT-Gateway über ein Transit Gateway oder ein Virtual Private Gateway weiterleiten. Sie können einem privaten NAT-Gateway keine elastische IP-Adresse zuordnen. Sie können ein Internet-Gateway mit einem privaten NAT-Gateway an eine VPC anfügen. Wenn Sie jedoch den Datenverkehr vom privaten NAT-Gateway zum Internet-Gateway weiterleiten, wird der Datenverkehr vom Internet-Gateway unterbrochen.

Sowohl private als auch öffentliche NAT-Gateways ordnen die private IPv4-Adresse der Instances der privaten IPv4-Adresse des NAT-Gateways zu. Im Fall eines öffentlichen NAT-Gateways ordnet das Internet-Gateway dann die private IPv4-Adresse des öffentlichen NAT-Gateways der Elastic-IP-Adresse zu, die dem NAT-Gateway zugeordnet ist. Beim Senden von Antwortdatenverkehr an die Instances übersetzt das NAT-Gateway die Adresse zurück in die ursprüngliche IP-Adresse.

> **Important**
>
> Sie können entweder ein öffentliches oder ein privates NAT-Gateway verwenden, um den Datenverkehr an Transit-Gateways und virtuelle private Gateways weiterzuleiten.

Wenn Sie mit einem privaten NAT-Gateway eine Verbindung zu einem Transit-Gateway oder einem virtuellen privaten Gateway herstellen, wird der Datenverkehr über die private IP-Adresse des privaten NAT-Gateways an das Ziel geleitet.
Wenn Sie die gleiche Verbindung mit einem öffentlichen NAT-Gateway herstellen, wird der Datenverkehr über die private IP-Adresse des öffentlichen NAT-Gateways an das Ziel geleitet, sofern Sie kein Internet-Gateway nutzen. Das öffentliche NAT-Gateway nutzt die EIP-Adresse nur dann als IP-Quelladresse, wenn es zusammen mit einem Internet-Gateway verwendet wird.

Inhalt

Grundlagen zu NAT-Gateways

Jedes NAT-Gateway wird in einer bestimmten Availability Zone erstellt und redundant innerhalb dieser Zone implementiert. Die Anzahl der NAT-Gateways, die Sie in einer Availability Zone erstellen können, unterliegt einem Kontingent. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.

Wenn Sie Ressourcen in mehreren Availability Zones haben, die gemeinsam ein NAT-Gateway nutzen, verlieren die Ressourcen in den anderen Availability Zones den Zugriff auf das Internet, wenn die Availability Zone des NAT-Gateways ausfällt. Um die Ausfallsicherheit zu erhöhen, richten Sie in jeder Availability Zone ein NAT-Gateway ein und konfigurieren Sie Ihr Routing so, dass die Ressourcen das NAT-Gateway in derselben Availability Zone verwenden.

Die folgenden Merkmale und Regeln gelten für NAT-Gateways:

- NAT-Gateways unterstützen die folgenden Protokolle: TCP, UDP und ICMP.
- NAT-Gateways werden für den IPv4- oder IPv6-Verkehr unterstützt. Für IPv6-Datenverkehr führt NAT-Gateway NAT64 aus. Durch die Verwendung davon in Verbindung mit DNS64 (verfügbar im Resolver Route 53) können Ihre IPv6-Workloads in einem Subnetz in Amazon VPC mit IPv4-Ressourcen kommunizieren. Diese IPv4-Services können in derselben VPC (in einem separaten Subnetz) oder einer anderen VPC, in Ihrer On-Premises-Umgebung oder im Internet verfügbar sein.
- Ein NAT-Gateway unterstützt eine Bandbreite von 5 Gbps und skaliert automatisch bis auf 100 Gbit/s. Wenn Sie mehr Bandbreite benötigen, können Sie Ihre Ressourcen auf mehrere Subnetze verteilen und pro Subnetz ein NAT-Gateway erstellen.
- Ein NAT-Gateway kann eine Million Pakete pro Sekunde verarbeiten und skaliert automatisch bis zu zehn Millionen Pakete pro Sekunde. Über diese Grenze hinaus wird ein NAT-Gateway Pakete löschen. Teilen Sie Ihre Ressourcen auf, um Paketverluste zu vermeiden, und erstellen Sie pro Subnetz ein separates NAT-Gateway.
- Jede IPv4-Adresse kann bis zu 55 000 gleichzeitige Verbindungen zu jedem eindeutigen Ziel unterstützen. Ein eindeutiges Ziel wird durch eine eindeutige Kombination aus Ziel-IP-Adresse, Zielport und Protokoll (TCP/UDP/ICMP) identifiziert. Sie können dieses Limit erhöhen, indem Sie Ihren NAT-Gateways bis zu 8 IPv4-Adressen zuweisen (1 primäre IPv4-Adresse und 7 sekundäre IPv4-Adressen). Sie können Ihrem öffentlichen NAT-Gateway standardmäßig nur 2 Elastic-IP-Adressen zuweisen. Sie können dieses Limit erhöhen, indem Sie eine Kontingentanpassung beantragen. Weitere Informationen finden Sie unter Elastic-IP-Adressen.
- Sie können die private IPv4-Adresse auswählen, die dem NAT-Gateway zugewiesen werden soll, oder diese automatisch aus dem IPv4-Adressbereich des Subnetzes zuweisen lassen. Die zugewiesene private IPv4-Adresse bleibt bestehen, bis Sie das private NAT-Gateway löschen. Sie können diese private IPv4-Adresse nicht trennen und keine zusätzlichen privaten IPv4-Adressen anfügen.
- Sie können einer Sicherheitsgruppe kein NAT-Gateway zuordnen. Sie können Ihren Instances Sicherheitsgruppen zuordnen, um den ein- und ausgehenden Datenverkehr zu steuern.
- Sie können eine Netzwerk-ACL verwenden, um den Datenverkehr zu und von dem Subnetz zu Ihrem NAT-Gateway zu steuern. NAT-Gateways verwenden die Ports 1024 bis 65535. Weitere Informationen finden Sie unter Datenverkehr in Subnetzen mit Netzwerk-ACLs steuern.
- Ein NAT-Gateway empfängt eine Netzwerkschnittstelle. Sie können die private IPv4-Adresse auswählen, die der Schnittstelle zugewiesen werden soll, oder diese automatisch aus dem IPv4-Adressbereich des Subnetzes zuweisen lassen. Sie können die Netzwerkschnittstelle des NAT-Gateways in der Amazon EC2-Konsole anzeigen. Weitere Informationen finden Sie unter Anzeige

von Details zu einer Netzwerkschnittstelle. Die Attribute dieser Netzwerkschnittstelle können nicht verändert werden.

- Sie können den Verkehr nicht über eine VPC-Peering-Verbindung an ein NAT-Gateway weiterleiten. Sie können den Datenverkehr nicht über ein NAT-Gateway weiterleiten, wenn der Datenverkehr über eine Hybridverbindung (Site-to-Site-VPN oder Direct Connect) über ein Virtual Private Gateway eingeht. Sie können den Verkehr über ein NAT-Gateway weiterleiten, wenn der Verkehr über eine Hybridverbindung (Site-to-Site-VPN oder Direct Connect) über ein Transit-Gateway eingeht.
- NAT-Gateways unterstützen Datenverkehr mit einer maximalen Übertragungseinheit (MTU) von 8500, es ist jedoch wichtig, Folgendes zu beachten:
  - Um potenziellen Paketverlust bei der Kommunikation mit Ressourcen über das Internet über ein öffentliches NAT-Gateway zu verhindern, sollte die MTU-Einstellung für Ihre EC2-Instances 1500 Byte nicht überschreiten. Weitere Informationen zum Überprüfen und Einstellen der MTU für eine Instance finden Sie unter Überprüfen und Einstellen der MTU auf Ihrer Linux-Instance im Amazon EC2 EC2-Benutzerhandbuch.
  - NAT-Gateways unterstützen Path MTU Discovery (PMTUD) über FRAG_NEEDED ICMPv4-Pakete und Packet Too Big (PTB) ICMPv6-Pakete.
  - NAT-Gateways erzwingen das Clamping der maximalen Segmentgröße (MSS) für alle Pakete. Weitere Informationen finden Sie unter RFC879

Kontrollieren Sie die Verwendung von NAT-Gateways

Standardmäßig haben -Benutzer keine Berechtigungen zur Arbeit mit NAT-Gateways. Sie können eine IAM-Rolle mit einer Benutzerrichtlinie erstellen, über die Benutzer die Berechtigungen zum Erstellen, Beschreiben und Löschen von NAT-Gateways erhalten. Weitere Informationen finden Sie unter Identity and Access Management für Amazon VPC.

Arbeiten mit NAT-Gateways

Sie können die Amazon VPC-Konsole verwenden, um Ihre NAT-Gateways zu erstellen und zu verwalten.

Aufgaben

- Erstellen eines NAT-Gateways
- Bearbeiten sekundärer IP-Adresszuweisungen
- Markieren eines NAT-Gateways

- Löschen eines NAT-Gateways

Erstellen eines NAT-Gateways

Gehen Sie wie folgt vor, um ein NAT-Gateway zu erstellen.

Verwandte Quotas

- Sie können kein öffentliches NAT-Gateway erstellen, wenn Sie die Anzahl der Ihrem Konto zugewiesenen EIPs ausgeschöpft haben. Weitere Informationen zu EIP-Kontingenten und deren Anpassung finden Sie unter Elastic-IP-Adressen.
- Sie können Ihrem privaten NAT-Gateway bis zu 8 private IPv4-Adressen zuweisen. Diese Grenze ist nicht einstellbar.
- Sie können Ihrem öffentlichen NAT-Gateway standardmäßig nur 2 Elastic-IP-Adressen zuweisen. Sie können dieses Limit erhöhen, indem Sie eine Kontingentanpassung beantragen. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

So erstellen Sie ein NAT-Gateway

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf NAT-Gateways.
3. Wählen Sie NAT-Gateway erstellen aus.
4. (Optional) Geben Sie einen Namen für das NAT-Gateway an. Dadurch wird eine Markierung mit dem Schlüssel **`Name`** erstellt und der Wert ist der von Ihnen angegebene Name.
5. Wählen Sie das öffentliche Subnetz aus, in dem das NAT-Gateway erstellt werden soll.
6. Behalten Sie für Konnektivitätstyp die Standardauswahl Öffentlich bei, um ein öffentliches NAT-Gateway zu erstellen, oder wählen Sie Privat, um ein privates NAT-Gateway zu erstellen. Weitere Informationen zum Unterschied zwischen einem öffentlichen und einem privaten NAT-Gateway finden Sie unter NAT gateways (NAT-Gateways).
7. Wenn Sie die Option Öffentlich ausgewählt haben, tun Sie das Folgende. Andernfalls gehen Sie direkt zum Schritt 8:

    1. Wählen Sie eine Elastic-IP-Zuweisungs-ID aus, um dem NAT-Gateway eine EIP zuzuweisen, oder wählen Sie Elastic-IP zuweisen, um dem öffentlichen NAT-Gateway automatisch eine EIP zuzuweisen. Sie können Ihrem öffentlichen NAT-Gateway standardmäßig nur 2 Elastic-IP-

Adressen zuweisen. Sie können dieses Limit erhöhen, indem Sie eine Kontingentanpassung beantragen. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

> **Important**
>
> Wenn Sie einem öffentlichen NAT-Gateway eine EIP zuweisen, muss die Netzwerkgrenzgruppe der EIP mit der Netzwerkgrenzgruppe der Availability Zone (AZ) übereinstimmen, in der Sie das öffentliche NAT-Gateway starten. Wenn dies nicht der Fall ist, kann das NAT-Gateway nicht gestartet werden. Sie können die Netzwerkgrenzgruppe für die AZ des Subnetzes anhand der Details des Subnetzes sehen. In ähnlicher Weise können Sie die Netzwerkgrenzgruppe eines EIP anzeigen, indem Sie sich die Details der EIP-Adresse ansehen. Weitere Informationen zu Netzwerkgrenzgruppen und EIPs finden Sie unter Zuweisen einer Elastic-IP-Adresse.

2. (Optional) Wählen Sie Zusätzliche Einstellungen aus und geben Sie unter Private IP-Adresse – optional eine private IPv4-Adresse für das NAT-Gateway ein. Wenn Sie keine Adresse eingeben, AWS wird Ihrem NAT-Gateway automatisch eine private IPv4-Adresse nach dem Zufallsprinzip aus dem Subnetz zugewiesen, in dem sich Ihr NAT-Gateway befindet.
3. Fahren Sie mit Schritt 11 fort.

8. Wenn Sie sich für Privat entschieden haben, wählen Sie Zusätzliche Einstellungen und anschließend unter Zuordnungsmethode für private IP-v4Adressen eine der folgenden Optionen aus:

   - Automatische Zuweisung: AWS Wählt die primäre private IPv4-Adresse für das NAT-Gateway aus. Für Anzahl der automatisch zugewiesenen privaten IPv4-Adressen können Sie optional die Anzahl der sekundären privaten IPv4-Adressen für das NAT-Gateway angeben. AWS wählt diese IP-Adressen nach dem Zufallsprinzip aus dem Subnetz für Ihr NAT-Gateway aus.
   - Benutzerdefiniert: Wählen Sie unter Primäre private IPv4-Adresse die private IPv4-Adresse für das NAT-Gateway aus. Für Sekundäre private IPv4-Adressen können Sie optional bis zu 7 sekundäre private IPv4-Adressen für das NAT-Gateway angeben.

9. Wenn Sie in Schritt 8 Benutzerdefiniert ausgewählt haben, überspringen Sie diesen Schritt. Wenn Sie Automatisch zuweisen ausgewählt haben, wählen Sie unter Anzahl der automatisch zugewiesenen privaten IP-Adressen die Anzahl der sekundären IPv4-Adressen aus, die Sie diesem privaten AWS NAT-Gateway zuweisen möchten. Sie können bis zu 7 IPv4-Adressen auswählen.

> **Note**
>
> Sekundäre IPv4-Adressen sind optional und sollten zugewiesen oder zugeordnet werden, wenn Ihre Workloads, die ein NAT-Gateway verwenden, 55 000 gleichzeitige Verbindungen zu einem einzigen Ziel (dieselbe Ziel-IP, derselbe Zielport und dasselbe Protokoll) überschreiten. Sekundäre IPv4-Adressen erhöhen die Anzahl der verfügbaren Ports und somit das Limit für die Anzahl der gleichzeitigen Verbindungen, die Ihre Workloads mithilfe eines NAT-Gateways herstellen können.

10. Wenn Sie in Schritt 9 Automatisch zuweisen ausgewählt haben, überspringen Sie diesen Schritt. Wenn Sie Benutzerdefiniert ausgewählt haben, gehen Sie wie folgt vor:
    1. Geben Sie unter Primäre private IPv4-Adresse eine private IPv4-Adresse ein.
    2. Geben Sie unter Sekundäre private IPv4-Adresse bis zu 7 sekundäre private IPv4-Adressen ein.
11. (Optional) Sie fügen einem NAT-Gateway ein Tag hinzu, indem Sie Add new tag (Neuen Tag hinzufügen) auswählen und den Schlüsselnamen und den Wert eingeben. Sie können bis zu 50 Tags hinzufügen.
12. Wählen Sie Erstellen eines NAT-Gateways.
13. Der anfängliche Status des NAT-Gateways ist `Pending`. Nachdem sich der Status in `Available` geändert hat, steht Ihnen das NAT-Gateway zur Verwendung bereit. Stellen Sie sicher, dass Sie Ihre Routentabellen nach Bedarf aktualisieren. Beispiele finden Sie unter the section called “Anwendungsfälle”.

Wenn der Status des NAT-Gateways auf `Failed` geändert wird, ist bei der Erstellung ein Fehler aufgetreten. Weitere Informationen finden Sie unter Fehler bei der NAT-Gateway-Erstellung.

Bearbeiten sekundärer IP-Adresszuweisungen

Jede IPv4-Adresse kann bis zu 55 000 gleichzeitige Verbindungen zu jedem eindeutigen Ziel unterstützen. Ein eindeutiges Ziel wird durch eine eindeutige Kombination aus Ziel-IP-Adresse, Zielport und Protokoll (TCP/UDP/ICMP) identifiziert. Sie können dieses Limit erhöhen, indem Sie Ihren NAT-Gateways bis zu 8 IPv4-Adressen zuweisen (1 primäre IPv4-Adresse und 7 sekundäre IPv4-Adressen). Sie können Ihrem öffentlichen NAT-Gateway standardmäßig nur 2 Elastic-IP-Adressen zuweisen. Sie können dieses Limit erhöhen, indem Sie eine Kontingentanpassung beantragen. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

Mithilfe der CloudWatchNAT-Gateway-Metriken ErrorPort Allocation und PacketsDropCount können Sie ermitteln, ob Ihr NAT-Gateway Fehler bei der Portzuweisung generiert oder Pakete verwirft. Um dieses Problem zu beheben, fügen Sie Ihrem NAT-Gateway sekundäre IPv4-Adressen hinzu.

Überlegungen

- Sie können sekundäre private IPv4-Adressen hinzufügen, wenn Sie ein privates NAT-Gateway erstellen oder nachdem Sie das NAT-Gateway erstellt haben, indem Sie das Verfahren in diesem Abschnitt verwenden. Sie können sekundäre EIP-Adressen zu öffentlichen NAT-Gateways erst hinzufügen, nachdem Sie das NAT-Gateway mithilfe des in diesem Abschnitt beschriebenen Verfahrens erstellt haben.
- Ihrem NAT-Gateway können bis zu 8 IPv4-Adressen zugeordnet werden (1 primäre IPv4-Adresse und 7 sekundäre IPv4-Adressen). Sie können Ihrem privaten NAT-Gateway bis zu 8 private IPv4-Adressen zuweisen. Sie können Ihrem öffentlichen NAT-Gateway standardmäßig nur 2 Elastic-IP-Adressen zuweisen. Sie können dieses Limit erhöhen, indem Sie eine Kontingentanpassung beantragen. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

So bearbeiten Sie sekundäre IPv4-Adresszuweisungen

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf NAT-Gateways.
3. Wählen Sie das NAT-Gateway aus, dessen sekundäre IPv4-Adresszuweisungen Sie bearbeiten möchten.
4. Wählen Sie Aktionen und dann Bearbeiten sekundärer IP-Adresszuweisungen aus.
5. Wenn Sie die sekundären IPv4-Adresszuweisungen eines privaten NAT-Gateways bearbeiten, wählen Sie unter Aktion die Option Neue IPv4-Adressen zuweisen oder Zuordnung vorhandener IPv4-Adressen aufheben aus. Wenn Sie die sekundären IPv4-Adresszuweisungen eines öffentlichen NAT-Gateways bearbeiten, wählen Sie unter Aktion die Option Neue IPv4-Adressen zuweisen oder Zuordnung vorhandener IPv4-Adressen aufheben aus.
6. Führen Sie eine der folgenden Aktionen aus:

   - Wenn Sie neue IPv4-Adressen zuweisen oder zuordnen möchten, gehen Sie wie folgt vor:
     1. Dieser Schritt ist erforderlich. Sie müssen eine private IPv4-Adresse auswählen. Wählen Sie Zuweisungsmethode für private IPv4-Adressen aus:
        - Automatische Zuweisung: Wählt AWS automatisch eine primäre private IPv4-Adresse aus und Sie entscheiden, ob Sie AWS dem NAT-Gateway bis zu 7 sekundäre private IPv4-

Adressen zuweisen möchten. AWS wählt sie automatisch aus dem Subnetz, in dem sich Ihr NAT-Gateway befindet, aus und weist sie Ihnen nach dem Zufallsprinzip zu.

- Benutzerdefiniert: Wählen Sie die primäre private IPv4-Adresse und bis zu 7 sekundäre private IPv4-Adressen aus, die dem NAT-Gateway zugewiesen werden sollen.

2. Wählen Sie unter Elastic-IP-Zuweisungs-ID eine EIP aus, die Sie als sekundäre IPv4-Adresse hinzufügen möchten. Dieser Schritt ist erforderlich. Sie müssen eine EIP zusammen mit einer privaten IPv4-Adresse auswählen. Wenn Sie Benutzerdefiniert als Zuweisungsmethode für private IP-Adressen ausgewählt haben, müssen Sie auch eine private IPv4-Adresse für jede hinzugefügte EIP eingeben.

> **Important**
>
> Wenn Sie einem öffentlichen NAT-Gateway eine sekundäre EIP zuweisen, muss die Netzwerkgrenzgruppe der EIP mit der Netzwerkgrenzgruppe der Availability Zone (AZ) übereinstimmen, in der sich das öffentliche NAT-Gateway befindet. Wenn sie nicht identisch ist, schlägt die EIP die Zuweisung fehl. Sie können die Netzwerkgrenzgruppe für die AZ des Subnetzes anhand der Details des Subnetzes sehen. In ähnlicher Weise können Sie die Netzwerkgrenzgruppe eines EIP anzeigen, indem Sie sich die Details der EIP-Adresse ansehen. Weitere Informationen zu Netzwerkgrenzgruppen und EIPs finden Sie unter Zuweisen einer Elastic-IP-Adresse.

Ihrem NAT-Gateway können bis zu 8 IP-Adressen zugeordnet werden. Wenn es sich um ein öffentliches NAT-Gateway handelt, gibt es ein standardmäßiges Kontingentlimit für EIPs pro Region. Weitere Informationen finden Sie unter Elastic-IP-Adressen.

- Wenn Sie die Zuweisung oder Zuordnung neuer IPv4-Adressen aufheben möchten, gehen Sie wie folgt vor:

1. Wählen Sie unter Vorhandene sekundäre IP-Adresse, deren Zuweisung aufgehoben werden soll die sekundären IP-Adressen für diesen Vorgang aus.
2. (optional) Geben Sie unter Verbindungsablauf-Dauer die maximale Wartezeit (in Sekunden) ein, bevor die IP-Adressen zwangsweise freigegeben werden, wenn noch Verbindungen bestehen. Wenn Sie keinen Wert eingeben, beträgt der Standardwert 350 Sekunden.

7. Wählen Sie Änderungen speichern aus.

Wenn der Status des NAT-Gateways auf `Failed` geändert wird, ist bei der Erstellung ein Fehler aufgetreten. Weitere Informationen finden Sie unter Fehler bei der NAT-Gateway-Erstellung.

Markieren eines NAT-Gateways

Sie können Ihren NAT-Gateway markieren, um ihn identifizieren oder in Übereinstimmung mit den Anforderungen Ihrer Organisation kategorisieren zu können. Informationen zur Arbeit mit Tags finden Sie unter Tagging your Amazon EC2 EC2-Ressourcen im Amazon EC2 EC2-Benutzerhandbuch.

Kostenzuordnungs-Markierungen werden für NAT-Gateways unterstützt. Daher können Sie Tags auch verwenden, um Ihre AWS Rechnung zu organisieren und Ihre eigene Kostenstruktur widerzuspiegeln. Weitere Informationen finden Sie unter Verwendung von Tags zur Kostenzuordnung im Benutzerhandbuch zu AWS Billing . Weitere Informationen zum Einrichten eines Kostenzuordnungsberichts mit Stichwörtern finden Sie unter Monatlicher Kostenzuordnungsbericht unter Informationen zur AWS Kontoabrechnung.

So markieren Sie ein NAT-Gateway

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf NAT Gateways.
3. Wählen Sie das NAT-Gateway aus, das Sie markieren möchten, und wählen Sie Aktionen. Wählen Sie dann Tags verwalten aus.
4. Wählen Sie Neues Tag hinzufügen und definieren Sie einen Schlüssel und einen Wert für das Tag. Sie können bis zu 50 Tags hinzufügen.
5. Wählen Sie Speichern.

Löschen eines NAT-Gateways

Wenn Sie ein NAT-Gateway nicht mehr benötigen, können Sie es löschen. Nach der Löschung eines NAT-Gateways wird dessen Eintrag für etwa eine Stunde in der Amazon VPC-Konsole angezeigt und anschließend automatisch entfernt. Sie können den Eintrag nicht selbst entfernen.

Durch das Löschen wird die Zuordnung der Elastic-IP-Adresse zum NAT-Gateway aufgehoben. Die Adresse wird jedoch nicht im Konto gelöscht. Wenn Sie ein NAT-Gateway löschen, erhalten die Routen des NAT-Gateways den Status `blackhole`, bis Sie die Routen löschen oder aktualisieren.

So löschen Sie ein NAT-Gateway

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

2. Klicken Sie im Navigationsbereich auf NAT Gateways.
3. Wählen Sie das Optionsfeld für das NAT-Gateway und wählen Sie dann Aktionrn, NAT-Gateway löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Löschen aus.
5. Wenn Sie die Elastic-IP-Adresse, die einem öffentlichen NAT-Gateway zugeordnet war, nicht mehr benötigen, empfehlen wir, sie freizugeben. Weitere Informationen finden Sie unter Freigeben einer Elastic-IP-Adresse.

API- und CLI-Übersicht

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile oder API ausführen. Weitere Informationen zu Befehlszeilenschnittstellen und eine Liste der verfügbaren API-Operationen finden Sie unter Arbeiten mit Amazon VPC.

Zuweisen einer privaten IPv4-Adresse an ein privates NAT-Gateway

- assign-private-nat-gateway-address (AWS CLI)
- Register-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)
- AssignPrivateNatGatewayAdresse (Amazon EC2 Query API)

Zuordnen von Elastic-IP-Adressen (EIPs) und privaten IPv4-Adressen zu einem öffentlichen NAT-Gateway

- associate-nat-gateway-address (AWS CLI)
- Register-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)
- AssociateNatGatewayAddress(Amazon EC2 EC2-Abfrage-API)

Erstellen eines NAT-Gateways

- create-nat-gateway (AWS CLI)
- New-EC2NatGateway (AWS Tools for Windows PowerShell)
- CreateNatGateway (Amazon EC2 EC2-Abfrage-API)

Löschen eines NAT-Gateways

- delete-nat-gateway (AWS CLI)
- Remove-EC2NatGateway (AWS Tools for Windows PowerShell)
- DeleteNatGateway (Amazon EC2 EC2-Abfrage-API)

Beschreiben eines NAT-Gateways

- describe-nat-gateways (AWS CLI)
- Get-EC2NatGateway (AWS Tools for Windows PowerShell)
- DescribeNatGateways (Amazon EC2 EC2-Abfrage-API)

Aufheben der Zuordnung von sekundären Elastic-IP-Adressen (EIPs) von einem öffentlichen NAT-Gateway

- disassociate-nat-gateway-address (AWS CLI)
- Unregister-EC2NatGatewayAddress (AWS Tools for Windows PowerShell)
- DisassociateNatGatewayAddress(Amazon EC2 EC2-Abfrage-API)

Markieren eines NAT-Gateways

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)
- CreateTags(Amazon EC2 EC2-Abfrage-API)

Aufheben der Zuweisung sekundärer IPv4-Adressen zu einem privaten NAT-Gateway

- unassign-private-nat-gateway-address (AWS CLI)
- Unregister-EC2PrivateNatGatewayAddress (AWS Tools for Windows PowerShell)
- UnassignPrivateNatGatewayAdresse (Amazon EC2 Query API)

Anwendungsfälle für NAT-Gateway

Im Folgenden finden Sie Beispiele für Anwendungsfälle für öffentliche und private NAT-Gateways.

Szenarien

- Zugriff auf das Internet von einem privaten Subnetz
- Zugriff auf Ihr Netzwerk mit bereits aufgeführten IP-Adressen
- Aktivieren Sie die Kommunikation zwischen sich überschneidenden Netzwerken

Zugriff auf das Internet von einem privaten Subnetz

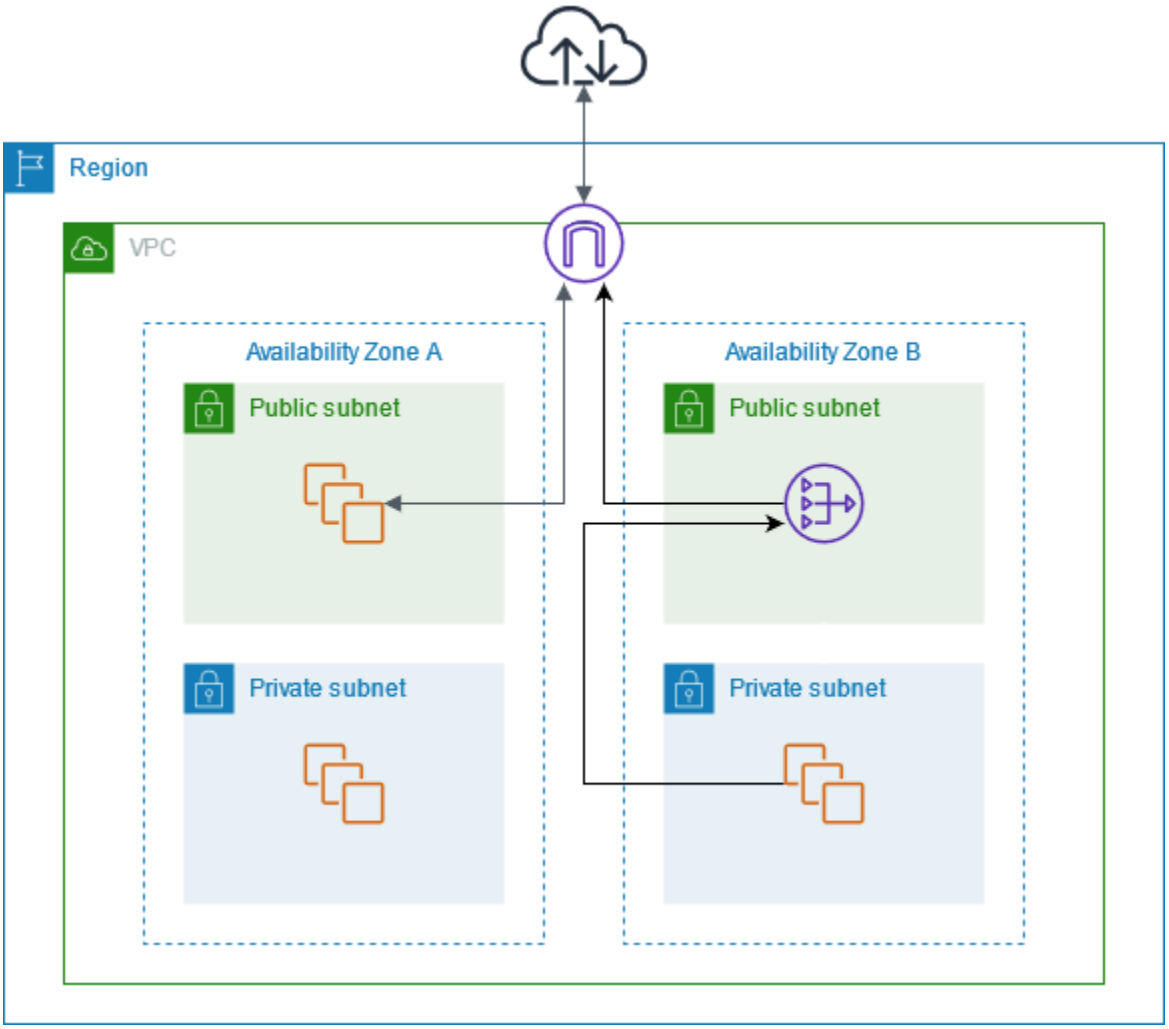
Sie können ein öffentliches NAT-Gateway verwenden, um es Instances in einem privaten Subnetz zu ermöglichen, ausgehenden Datenverkehr an das Internet zu senden, ohne dass das Internet Verbindungen zu den Instances herstellen kann.

Inhalt

- Übersicht
- Routing
- Testen des öffentlichen NAT-Gateways

Übersicht

Das folgende Diagramm veranschaulicht diesen Anwendungsfall. Es gibt zwei Availability Zones, mit zwei Subnetzen in jeder Availability Zone. Die Routing-Tabelle für jedes Subnetz bestimmt, wie der Datenverkehr weitergeleitet wird. In Availability Zone A können die Instances im öffentlichen Subnetz über eine Route zum Internet-Gateway ins Internet gelangen, während die Instances im privaten Subnetz keine Route zum Internet haben. In Availability Zone B enthält das öffentliche Subnetz ein NAT-Gateway, und die Instances im privaten Subnetz können über eine Route zum NAT-Gateway im öffentlichen Subnetz das Internet erreichen. Sowohl private als auch öffentliche NAT-Gateways ordnen die private IPv4-Adresse der Instances der privaten IPv4-Adresse des privaten NAT-Gateways zu. Im Fall eines öffentlichen NAT-Gateways ordnet das Internet-Gateway dann die private IPv4-Adresse des öffentlichen NAT-Gateways der Elastic IP-Adresse zu, die dem NAT-Gateway zugeordnet ist. Beim Senden von Antwortdatenverkehr an die Instances übersetzt das NAT-Gateway die Adresse zurück in die ursprüngliche IP-Adresse.



Beachten Sie, dass Sie, wenn die Instances im privaten Subnetz in Availability Zone A auch das Internet erreichen müssen, eine Route von diesem Subnetz zum NAT-Gateway in Availability Zone B erstellen können. Alternativ können Sie die Resilienz verbessern, indem Sie in jeder Availability Zone ein NAT-Gateway erstellen, das Ressourcen enthält, für die ein Internetzugang erforderlich ist. Ein Beispieldiagramm finden Sie unter the section called “Private Server”.

Routing

Die folgende Routing-Tabelle ist dem öffentlichen Subnetz in Availability Zone A zugeordnet. Der erste Eintrag ist die lokale Route; dieser Eintrag ermöglicht es den Instances im Subnetz mit anderen Instances in der VPC über private IP-Adressen zu kommunizieren. Der zweite Eintrag sendet den übrigen Datenverkehr des Subnetzes zum Internet-Gateway, wodurch die Instances im Subnetz auf das Internet zugreifen können.

Bestimmungsort	Ziel
VPC-CIDR	Lokal
0.0.0.0/0	*internet-gateway-id*

Die folgende Routing-Tabelle ist dem privaten Subnetz in Availability Zone A zugeordnet. Der Eintrag ist die lokale Route, die es den Instances im Subnetz ermöglicht, mit anderen Instances in der VPC mit privaten IP-Adressen zu kommunizieren. Die Instances in diesem Subnetz haben keinen Zugriff auf das Internet.

Bestimmungsort	Ziel
VPC-CIDR	local

Die folgende Routing-Tabelle ist dem öffentlichen Subnetz in Availability Zone B zugeordnet. Der erste Eintrag ist die lokale Route; dieser Eintrag ermöglicht es den Instances im Subnetz mit anderen Instances in der VPC über private IP-Adressen zu kommunizieren. Der zweite Eintrag sendet den übrigen Datenverkehr des Subnetzes zum Internet-Gateway, wodurch das NAT-Gateway im Subnetz auf das Internet zugreifen kann.

Bestimmungsort	Ziel
VPC-CIDR	Lokal
0.0.0.0/0	*internet-gateway-id*

Die folgende Routing-Tabelle ist dem privaten Subnetz in Availability Zone B zugeordnet. Der erste Eintrag ist die lokale Route; dieser Eintrag ermöglicht es den Instances im Subnetz durch private IP-Adressen mit anderen Instances in der VPC zu kommunizieren. Der zweite Eintrag sendet den übrigen Subnetz-Verkehr zum NAT-Gateway.

Bestimmungsort	Ziel
VPC-CIDR	Lokal

Bestimmungsort	Ziel
0.0.0.0/0	*nat-gateway-id*

Weitere Informationen finden Sie unter the section called “Arbeiten mit Routing-Tabellen”.

Testen des öffentlichen NAT-Gateways

Nachdem Sie ein NAT-Gateway erstellt und die Routing-Tabellen aktualisiert haben, können Sie von einer Instance in Ihrem privaten Subnetz aus einen Ping an Remote-Adressen im Internet senden, um die Verbindung zum Internet zu testen. Ein Beispiel für diese Vorgehensweise finden Sie unter Testen Sie die Internetverbindung.

Wenn Sie eine Verbindung zum Internet herstellen können, können Sie testen, ob Internetdatenverkehr über das NAT-Gateway geleitet wird:

- Sie können die Route, die der Datenverkehr von einer Instance zu Ihrem privaten Subnetz nimmt, nachvollziehen. Führen Sie dazu den Befehl `traceroute` auf einer Linux-Instance in Ihrem privaten Subnetz aus. Die Ausgabe enthält die private IP-Adresse des NAT-Gateways in einem der Hops (in der Regel der erste Hop).
- Verwenden Sie eine Drittanbieter-Website oder ein Drittanbieter-Tool, um die Quell-IP-Adresse anzuzeigen, wenn Sie sich von einer Instance in Ihrem privaten Subnetz mit dem NAT-Gateway verbinden. Die Quell-IP-Adresse sollte die elastische IP-Adresse des NAT-Gateways sein.

Sollten diese Tests fehlschlagen, finden Sie weitere Informationen unter Problembehandlung bei NAT-Gateways.

Testen Sie die Internetverbindung

Das folgende Beispiel veranschaulicht, wie Sie überprüfen, ob eine Instance in einem privaten Subnetz eine Verbindung zum Internet herstellen kann.

1. Starten Sie eine Instance in Ihrem öffentlichen Subnetz (diese dient als Bastion Host). Wählen Sie im Startassistenten ein Amazon Linux-AMI aus und weisen Sie der Instance eine öffentliche IP-Adresse zu. Die Sicherheitsgruppenregeln müssen eingehenden SSH-Datenverkehr im IP-Adressbereich Ihres lokalen Netzwerks sowie ausgehenden SSH-Datenverkehr im IP-Adressbereich Ihres privaten Subnetzes zulassen (für Testzwecke können Sie sowohl für ein- als auch ausgehenden SSH-Datenverkehr auch `0.0.0.0/0` verwenden).

2. Starten Sie eine Instance in Ihrem privaten Subnetz. Wählen Sie im Startassistenten ein Amazon Linux-AMI aus. Weisen Sie der Instance keine öffentliche IP-Adresse zu. Die Sicherheitsgruppenregeln müssen eingehenden SSH-Datenverkehr von der privaten IP-Adresse der Instance zulassen, die Sie im öffentlichen Subnetz gestartet haben, sowie den gesamten ausgehenden ICMP-Datenverkehr. Sie müssen dasselbe Schlüsselpaar auswählen, mit dem Sie die Instance im öffentlichen Subnetz gestartet haben.
3. Konfigurieren Sie das SSH-Agent-Forwarding auf Ihrem lokalen Computer und stellen Sie eine Verbindung zum Bastion Host im öffentlichen Subnetz her. Weitere Informationen finden Sie unter So konfigurieren Sie SSH-Agent-Forwarding für Linux oder macOS oder So konfigurieren Sie die Weiterleitung des SSH-Agenten für Windows.
4. Verbinden Sie sich vom Bastion Host aus mit der Instance im privaten Subnetz und testen Sie die Internetverbindung von der Instance im privaten Subnetz aus. Weitere Informationen finden Sie unter So testen Sie die Internetverbindung.

So konfigurieren Sie SSH-Agent-Forwarding für Linux oder macOS

1. Fügen Sie dem Authentifizierungsagenten von Ihrem lokalen Computer aus Ihren privaten Schlüssel hinzu.

   Verwenden Sie für Linux den folgenden Befehl.

   ```
   ssh-add -c mykeypair.pem
   ```

   Verwenden Sie für macOS den folgenden Befehl.

   ```
   ssh-add -K mykeypair.pem
   ```

2. Verbinden Sie sich mit der Option `-A` mit der Instance im öffentlichen Subnetz, um SSH-Agent-Forwarding zu aktivieren, und verwenden Sie die öffentliche Adresse der Instance, wie im nachfolgenden Beispiel gezeigt.

   ```
   ssh -A ec2-user@54.0.0.123
   ```

So konfigurieren Sie die Weiterleitung des SSH-Agenten für Windows

Sie können den in Windows verfügbaren OpenSSH-Client verwenden oder Ihren bevorzugten SSH-Client (z. B. PuTTY) installieren.

OpenSSH

Installieren Sie OpenSSH für Windows wie im folgenden Artikel beschrieben: Erste Schritte mit OpenSSH für Windows. Fügen Sie anschließend Ihren Schlüssel zum Authentifizierungsagenten hinzu. Weitere Informationen finden Sie unter Schlüsselbasierte Authentifizierung in OpenSSH für Windows.

PuTTY

1. Falls Pageant noch nicht installiert ist, laden Sie das Programm auf der PuTTY-Downloadseite herunter und installieren Sie es.
2. Konvertieren Sie Ihren privaten Schlüssel ins PPK-Format. Weitere Informationen finden Sie unter Konvertieren Ihres privaten Schlüssels mit PuTTYgen im Amazon EC2 EC2-Benutzerhandbuch.
3. Starten Sie Pageant, klicken Sie mit der rechten Maustaste auf das Pageant-Symbol in der Taskleiste (das Symbol ist möglicherweise ausgeblendet) und klicken Sie auf Add Key. Wählen Sie die .ppk-Datei, die Sie erstellt haben, geben Sie gegebenenfalls das Passwort ein, und wählen Sie Open (Öffnen).
4. Starten Sie eine PuTTY-Sitzung und verbinden Sie sich mithilfe der öffentlichen IP-Adresse der Instance mit der Instance im öffentlichen Subnetz. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit Ihrer Linux-Instance. Wählen Sie in der Kategorie Auth die Option Allow agent forwarding aus und lassen Sie das Feld Private key file for authentication frei.

So testen Sie die Internetverbindung

1. Verbinden Sie sich von der Instance im öffentlichen Subnetz aus mit der Instance im privaten Subnetz unter Verwendung von deren privater IP-Adresse, wie im nachfolgenden Beispiel gezeigt.

```
ssh ec2-user@10.0.1.123
```

2. Überprüfen Sie auf der eigenen Instance, ob Sie eine Verbindung mit dem Internet herstellen können. Senden Sie dazu den Befehl `ping` an eine ICMP-fähige Website.

```
ping ietf.org
```

```
PING ietf.org (4.31.198.44) 56(84) bytes of data.
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=1 ttl=47 time=86.0 ms
64 bytes from mail.ietf.org (4.31.198.44): icmp_seq=2 ttl=47 time=75.6 ms
...
```

Drücken Sie auf der Tastatur Strg + C, um den Befehl `ping` abzubrechen. Falls der Befehl `ping` fehlschlägt, lesen Sie hier weiter: Instances haben keinen Zugriff auf das Internet..

3. (Optional) Beenden Sie Ihre Instances, wenn Sie sie nicht mehr benötigen. Weitere Informationen finden Sie unter Beenden Ihrer Instance im Amazon-EC2-Benutzerhandbuch.

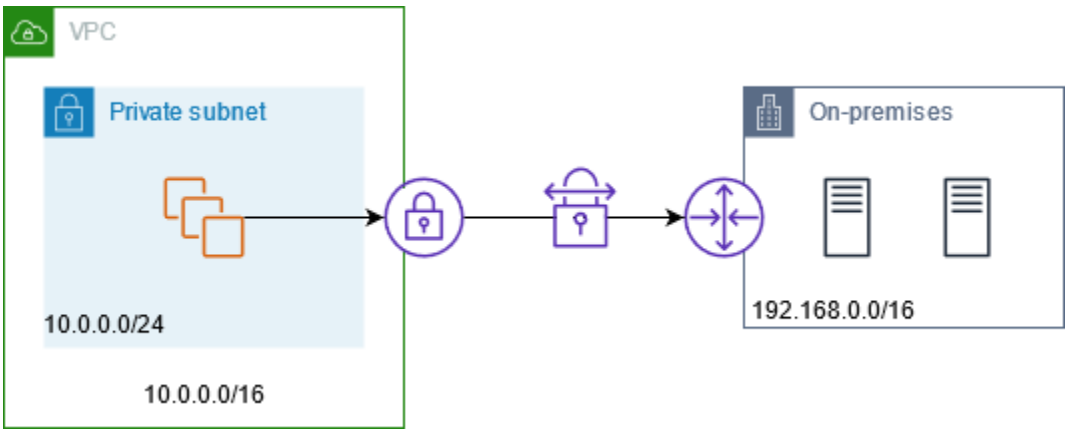
Zugriff auf Ihr Netzwerk mit bereits aufgeführten IP-Adressen

Sie können ein privates NAT-Gateway verwenden, um die Kommunikation von Ihren VPCs zu Ihrem On-Premises-Netzwerk mit einem Pool von bereits aufgeführten Adressen zu ermöglichen. Anstatt jeder Instance eine separate IP-Adresse von dem bereits aufgeführten IP-Adressbereich zuzuweisen, können Sie Datenverkehr von dem Subnetz, das für das On-Premises-Netzwerk vorgesehen ist, über ein privates NAT-Gateway mit einer IP-Adresse aus dem bereits aufgeführten IP-Adressbereich leiten.

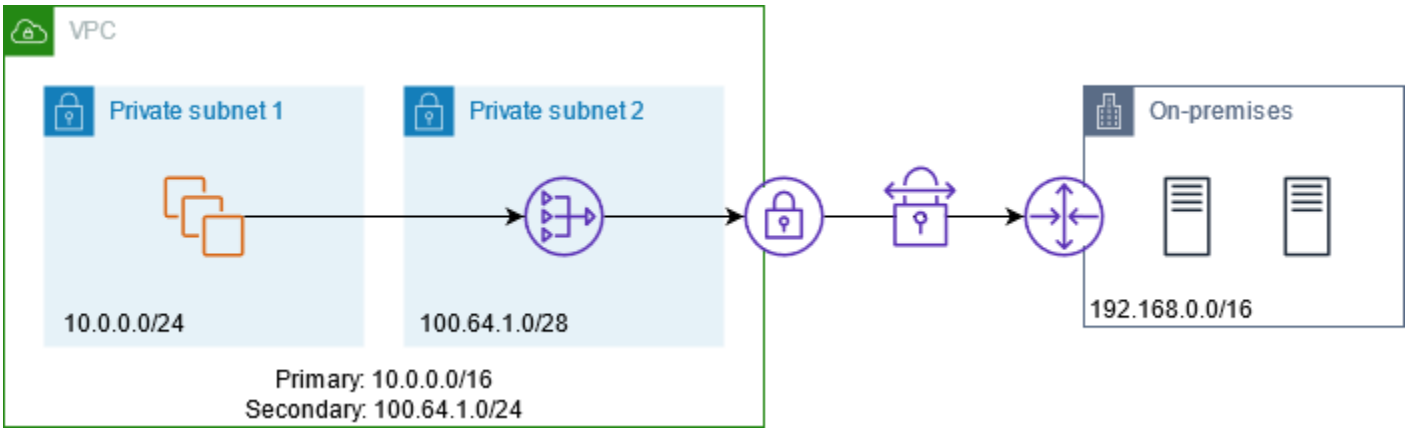
Inhalt

Übersicht

Das folgende Diagramm zeigt, wie Instances über auf lokale Ressourcen zugreifen können. AWS VPN Der Datenverkehr von den Instances wird über die VPN-Verbindung an ein Virtual Private Gateway, an das Kunden-Gateway und dann an das Ziel im On-Premises-Netzwerk weitergeleitet. Angenommen, das Ziel lässt Datenverkehr nur aus einem bestimmten IP-Adressbereich wie 100.64.1.0/28 zu. Dies würde verhindern, dass der Datenverkehr von diesen Instances das On-Premises-Netzwerk erreicht.



Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Die VPC verfügt über ihren ursprünglichen IP-Adressbereich plus den zulässigen IP-Adressbereich. Die VPC verfügt über ein Subnetz aus dem zulässigen IP-Adressbereich mit einem privaten NAT-Gateway. Der Datenverkehr von den Instances, die für das On-Premises-Netzwerk bestimmt sind, wird an das NAT-Gateway gesendet, bevor er an die VPN-Verbindung weitergeleitet wird. Das On-Premises-Netzwerk empfängt den Datenverkehr von den Instances mit der Quell-IP-Adresse des NAT-Gateways, die aus dem zulässigen IP-Adressbereich stammt.



Ressourcen

Erstellen oder aktualisieren Sie Ressourcen wie folgt:

- Ordnen Sie den zulässigen IP-Adressbereich mit der VPC zu.
- Erstellen Sie aus dem zulässigen IP-Adressbereich ein Subnetz in der VPC.
- Erstellen Sie im neuen Subnetz ein privates NAT-Gateway.
- Aktualisieren Sie die Routing-Tabelle für das Subnetz mit den Instances, um den für das On-Premises-Netzwerk bestimmten Datenverkehr an das NAT-Gateway zu senden. Fügen Sie

eine Route zur Routing-Tabelle für das Subnetz mit dem privaten NAT-Gateway hinzu, das Datenverkehr für das On-Premises-Netzwerk an das Virtual Private Gateway sendet.

Routing

Die folgende Routing-Tabelle ist dem ersten Subnetz zugeordnet. Für jeden VPC CIDR gibt es eine lokale Route. Lokale Routen ermöglichen es Ressourcen im Subnetz, mit anderen Ressourcen in der VPC über private IP-Adressen zu kommunizieren. Der dritte Eintrag sendet den für das On-Premises-Netzwerk bestimmten Datenverkehr an das private NAT-Gateway.

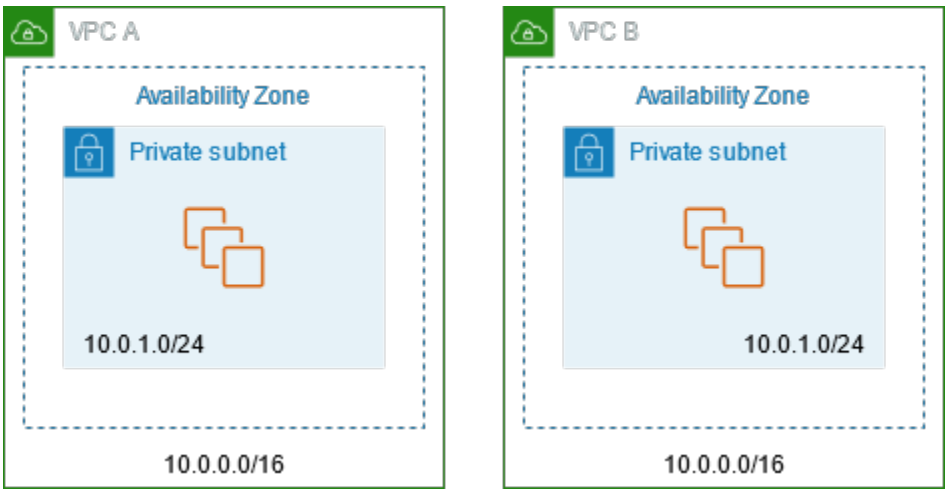
Bestimmungsort	Ziel
10.0.0.0/16	Lokal
100,64.1,0/24	local
192.168.0.0/16	*nat-gateway-id*

Die folgende Routing-Tabelle ist dem zweiten Subnetz zugeordnet. Für jeden VPC CIDR gibt es eine lokale Route. Lokale Routen ermöglichen es Ressourcen im Subnetz, mit anderen Ressourcen in der VPC über private IP-Adressen zu kommunizieren. Der dritte Eintrag sendet Datenverkehr, der für das On-Premises-Netzwerk vorgesehen ist, an das Virtual Private Gateway.

Bestimmungsort	Ziel
10.0.0.0/16	Lokal
100,64.1,0/24	local
192.168.0.0/16	*vgw-id*

Aktivieren Sie die Kommunikation zwischen sich überschneidenden Netzwerken

Sie können ein privates NAT-Gateway verwenden, um die Kommunikation zwischen Netzwerken zu ermöglichen, auch wenn sie sich überschneidende CIDR-Bereiche haben. Angenommen, die Instances in VPC A müssen auf die Dienste zugreifen, die von den Instances in VPC B bereitgestellt werden.



Inhalt

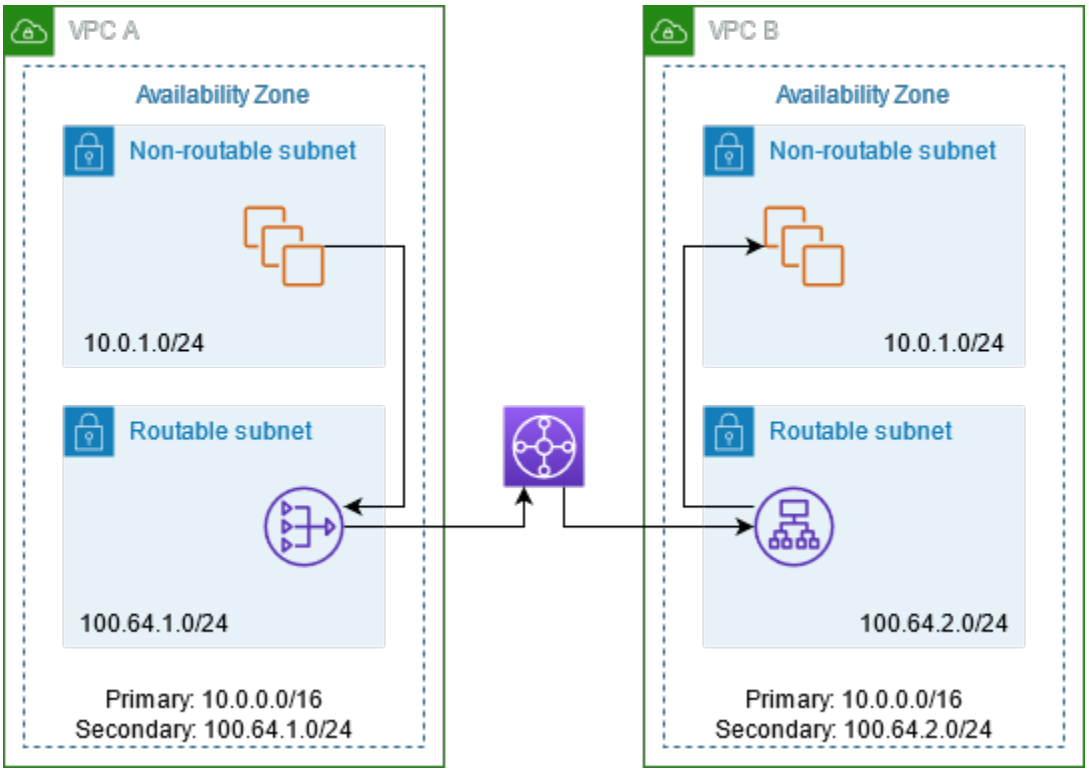
Übersicht

Die folgende Abbildung zeigt die Hauptkomponenten der Konfiguration für dieses Szenario. Zunächst bestimmt Ihr IP-Management-Team, welche Adressbereiche sich überschneiden können (nicht routbare Adressbereiche) und welche nicht (routbare Adressbereiche). Das IP-Management-Team weist auf Anfrage Adressbereiche vom Pool routierbarer Adressbereiche bis hin zu Projekten zu.

Jede VPC hat ihren ursprünglichen IP-Adressbereich, der nicht routbar ist, sowie den routbaren IP-Adressbereich, den ihr vom IP-Managementteam zugewiesen wurde. VPC A verfügt über ein Subnetz aus seinem routbaren Bereich mit einem privaten NAT-Gateway. Das private NAT-Gateway erhält seine IP-Adresse aus seinem Subnetz. VPC B verfügt über ein Subnetz aus seinem routbaren Bereich mit einem Application Load Balancer. Der Application Load Balancer erhält seine IP-Adressen aus seinen Subnetzen.

Der Datenverkehr von einer Instance im nicht routbaren Subnetz von VPC A, die für die Instances im nicht routbaren Subnetz von VPC B bestimmt ist, wird über das private NAT-Gateway gesendet und dann an das Transit-Gateway weitergeleitet. Das Transit-Gateway sendet den Datenverkehr an den Application Load Balancer, der den Datenverkehr an eine der Ziel-Instances im nicht routbaren Subnetz von VPC B weiterleitet. Der Datenverkehr vom Transit-Gateway zum Application Load Balancer hat die Quell-IP-Adresse des privaten NAT-Gateways. Daher verwendet der Antwortverkehr vom Load Balancer die Adresse des privaten NAT-Gateways als Ziel. Der Antwortverkehr wird an das

Transit-Gateway gesendet und dann an das private NAT-Gateway weitergeleitet, welches das Ziel in die Instance im nicht routbaren Subnetz von VPC A übersetzt.



Ressourcen

Erstellen oder aktualisieren Sie Ressourcen wie folgt:

- Ordnen Sie die zugewiesenen routierbaren IP-Adressbereiche ihren jeweiligen VPCs zu.
- Erstellen Sie ein Subnetz in VPC A aus seinem routfähigen IP-Adressbereich und erstellen Sie in diesem neuen Subnetz ein privates NAT-Gateway.
- Erstellen Sie ein Subnetz in VPC B aus seinem routfähigen IP-Adressbereich und erstellen Sie in diesem neuen Subnetz einen Application Load Balancer. Registrieren Sie die Instances im nicht routbaren Subnetz bei der Zielgruppe für den Load Balancer.
- Erstellen Sie einen Transit-Gateway, um die VPCs zu verbinden. Stellen Sie sicher, dass Sie die Routing-Verbreitung deaktivieren. Wenn Sie jede VPC an das Transit-Gateway anfügen, verwenden Sie den routbaren Adressbereich der VPC.
- Aktualisieren Sie die Routing-Tabelle des nicht routbaren Subnetzes in VPC A, um den gesamten Datenverkehr, der für den routbaren Adressbereich von VPC B bestimmt ist, an das private NAT-Gateway zu senden. Aktualisieren Sie die Routing-Tabelle des routbaren Subnetzes in VPC A, um den gesamten Datenverkehr, der für den routbaren Adressbereich von VPC B bestimmt ist, an das Transit-Gateway zu senden.

- Aktualisieren Sie die Routing-Tabelle des routbaren Subnetzes in VPC B, um den gesamten Datenverkehr, der für den routbaren Adressbereich von VPC A bestimmt ist, an das Transit-Gateway zu senden.

Routing

Dies ist die Routing-Tabelle für das nicht routbare Subnetz in VPC A:

Bestimmungsort	Ziel
10.0.0.0/16	Lokal
100,64.1,0/24	local
100,64,2,0/24	*nat-gateway-id*

Dies ist die Routing-Tabelle für das routbare Subnetz in VPC A:

Bestimmungsort	Ziel
10.0.0.0/16	Lokal
100,64.1,0/24	local
100,64,2,0/24	*Transit-Gateway-ID*

Dies ist die Routing-Tabelle für das nicht routbare Subnetz in VPC B:

Bestimmungsort	Ziel
10.0.0.0/16	Lokal
100,64.2,0/24	local

Dies ist die Routing-Tabelle für das routbare Subnetz in VPC B:

Bestimmungsort	Ziel
10.0.0.0/16	Lokal
100,64.2,0/24	local
100,64,1,0/24	*Transit-Gateway-ID*

Es folgt ein Beispiel für die Routing-Tabelle des Transit-Gateways.

CIDR	Attachment	Routing-Typ
100,64,1,0/24	*Anfügung für VPC A*	Statisch
100,64,2,0/24	*Anfügung für VPC B*	Statisch

DNS64 und NAT64

Ein NAT-Gateway unterstützt die Übersetzung von Netzwerkadressen von IPv6 nach IPv4, im Volksmund als NAT64 bekannt. NAT64 unterstützt Ihre AWS IPv6-Ressourcen bei der Kommunikation mit IPv4-Ressourcen in derselben VPC oder einer anderen VPC, in Ihrem lokalen Netzwerk oder über das Internet. Sie können NAT64 mit DNS64 auf Amazon Route 53 Resolver verwenden oder Ihren eigenen DNS64-Server verwenden.

Inhalt

Was ist DNS64?

Ihre IPv6-only Workloads, die in VPCs ausgeführt werden, können nur IPv6-Netzwerkpakete senden und empfangen. Ohne DNS64 liefert eine DNS-Abfrage für einen reinen IPv4-Dienst als Antwort eine IPv4-Zieladresse, und Ihr reiner IPv6-Dienst kann nicht damit kommunizieren. Um diese Kommunikationslücke zu schließen, können Sie DNS64 für ein Subnetz aktivieren. Es gilt dann für

alle Ressourcen innerhalb dieses Subnetzes. AWS Mit DNS64 sucht der Amazon Route 53 Resolver den DNS-Datensatz für den Service, den Sie abgefragt haben, und führt einen der folgenden Schritte aus:

- Wenn der Datensatz eine IPv6-Adresse enthält, gibt er den ursprünglichen Datensatz zurück und die Verbindung wird ohne Übersetzung über IPv6 hergestellt.
- Wenn mit dem Ziel im DNS-Datensatz keine IPv6-Adresse verknüpft ist, synthetisiert der Route 53 Resolver eine, indem er dem bekannten `/96`-Präfix vorangestellt wird, definiert in RFC6052 (`64:ff9b::/96`), an die IPv4-Adresse im Datensatz. Ihr IPv6-only Dienst sendet Netzwerkpakete an die synthetisierte IPv6-Adresse. Sie müssen diesen Datenverkehr dann durch das NAT-Gateway leiten, das die erforderliche Übersetzung des Datenverkehrs durchführt, damit IPv6-Dienste in Ihrem Subnetz auf IPv4-Dienste außerhalb dieses Subnetzes zugreifen können.

Sie können DNS64 in einem Subnetz mithilfe des modify-subnet-Attributs mithilfe der AWS CLI oder mit der VPC-Konsole aktivieren oder deaktivieren, indem Sie ein Subnetz auswählen und Aktionen > Subnetzeinstellungen bearbeiten wählen.

Was ist NAT64?

NAT64 ermöglicht es Ihren IPv6-only-Services in Amazon VPCs, mit IPv4-only-Services innerhalb derselben VPC (in verschiedenen Subnetzen) oder verbundenen VPCs, in Ihren On-Premises-Netzwerken oder über das Internet zu kommunizieren.

NAT64 ist automatisch auf Ihren bestehenden NAT-Gateways oder auf neuen NAT-Gateways verfügbar, die Sie erstellen. Es ist kein Feature, das Sie aktivieren oder deaktivieren können. Das Subnetz, in dem sich das NAT-Gateway befindet, muss kein Dual-Stack-Subnetz sein, damit NAT64 funktioniert.

Wenn Sie DNS64 aktiviert haben und Ihr reiner IPv6-Service Netzwerkpakete über das NAT-Gateway an eine synthetisierte IPv6-Adresse sendet, geschieht Folgendes:

- Vom `64:ff9b::/96`-Präfix erkennt das NAT-Gateway, dass das ursprüngliche Ziel IPv4 ist und übersetzt die IPv6-Pakete in IPv4, indem es Folgendes ersetzt:
  - Quelle IPv6 mit eigener privater IP, die vom Internet-Gateway in die Elastic-IP-Adresse übersetzt wird.
  - Ziel IPv6 nach IPv4 durch Entfernen des `64:ff9b::/96`-Präfix.
- Das NAT-Gateway sendet die übersetzten IPv4-Pakete über das Internet-Gateway, das virtuelle private Gateway oder das Transit-Gateway an das Ziel und initiiert eine Verbindung.

- Der IPv4-only Host sendet IPv4-Antwortpakete zurück. Sobald eine Verbindung hergestellt wurde, akzeptiert NAT-Gateway die Antwort-IPv4-Pakete der externen Hosts.
- Die Antwort-IPv4-Pakete sind für NAT-Gateway bestimmt, das die Pakete empfängt und sie entlastet, indem seine IP (Ziel-IP) durch die IPv6-Adresse des Hosts ersetzt und `64:ff9b::/96` an die Quell-IPv4-Adresse vorangestellt wird. Das Paket fließt dann in der lokalen Route zum Host.

Auf diese Weise ermöglicht das NAT-Gateway Ihren reinen IPv6-Workloads in einem Subnetz die Kommunikation mit reinen IPv4-Services außerhalb des Subnetzes.

DNS64 und NAT64 konfigurieren

Führen Sie die Schritte in diesem Abschnitt aus, um DNS64 und NAT64 so zu konfigurieren, dass die Kommunikation mit IPv4-only Diensten möglich ist.

Inhalt

Aktivieren Sie die Kommunikation mit IPv4-only Diensten im Internet mit dem AWS -CLI

Wenn Sie ein Subnetz mit IPv6-only Workloads haben, das mit IPv4-only Diensten außerhalb des Subnetzes kommunizieren muss, zeigt dieses Beispiel, wie Sie diesen IPv6-only Diensten ermöglichen, mit IPv4-only Diensten im Internet zu kommunizieren.

Sie sollten zuerst ein NAT-Gateway in einem öffentlichen Subnetz konfigurieren (getrennt vom Subnetz, das die IPv6-only Workloads enthält). Beispielsweise sollte das Subnetz, das das NAT-Gateway enthält, eine `0.0.0.0/0` Route haben, die auf das Internet-Gateway zeigt.

Führen Sie diese Schritte aus, um diesen IPv6-only Diensten die Verbindung mit IPv4-only Diensten im Internet zu ermöglichen:

1. Fügen Sie der Routing-Tabelle des Subnetzes, das die reinen IPv6-Workloads enthält, die folgenden drei Routen hinzu:

   - IPv4-Route (falls vorhanden), die auf das NAT-Gateway gerichtet ist.
   - `64:ff9b::/96`-Route, die auf das NAT-Gateway zeigt. Auf diese Weise kann der Datenverkehr von Ihren IPv6-only Workloads, die für IPv4-only Dienste bestimmt sind, über das NAT-Gateway weitergeleitet werden.

- IPv6 `::/0`-Route, die auf das Internet-Gateway nur für ausgehenden Verkehr (oder das Internet-Gateway) gerichtet ist.

Beachten Sie, dass die Ausrichtung von `::/0` auf das Internet-Gateway externen IPv6-Hosts (außerhalb der VPC) ermöglicht, eine Verbindung über IPv6 zu initiieren.

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-cidr-block
0.0.0.0/0 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
64:ff9b::/96 --nat-gateway-id nat-05dba92075d71c408
```

```
aws ec2 create-route --route-table-id rtb-34056078 --destination-ipv6-cidr-block
::/0 --egress-only-internet-gateway-id eigw-c0a643a9
```

2. Aktivieren Sie die DNS64-Funktion im Subnetz, das die IPv6-only Workloads enthält.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Jetzt können Ressourcen in Ihrem privaten Subnetz statusbehaftete Verbindungen mit IPv4- und IPv6-Diensten im Internet herstellen. Konfigurieren Sie Ihre Sicherheitsgruppe und NACLs entsprechend, um ausgehenden und eingehenden Datenverkehr zum `64:ff9b::/96`-Datenverkehr zuzulassen.

Aktivieren Sie die Kommunikation mit IPv4-only-Services in Ihrer On-Premises-Umgebung

Mit Amazon Route 53 Resolver können Sie DNS-Abfragen von Ihrer VPC an ein On-Premises-Netzwerk weiterleiten und umgekehrt. Sie können dies wie folgt tun:

- Sie erstellen einen ausgehenden Endpunkt des Route 53 Resolvers in einer VPC und weisen diesem die IPv4-Adressen zu, von denen Route 53 Resolver Abfragen weiterleiten soll. Für Ihren On-Premises-DNS-Resolver sind dies die IP-Adressen, von denen die DNS-Abfragen stammen, und sollten daher IPv4-Adressen stammen.

- Sie erstellen eine oder mehrere Regeln, welche die Domainnamen der DNS-Abfragen angeben, die Route 53 Resolver an Ihre On-Premises-Resolver weiterleiten soll. Sie legen auch die IPv4-Adressen der On-Premises-Resolver fest.
- Nachdem Sie nun einen ausgehenden Endpunkt von Route 53 Resolver eingerichtet haben, müssen Sie DNS64 im Subnetz aktivieren, das Ihre IPv6-only Workloads enthält, und alle Daten, die für Ihr On-Premises-Netzwerk bestimmt sind, über ein NAT-Gateway weiterleiten.

So funktioniert DNS64 für IPv4-only-Ziele in On-Premises-Netzwerken:

1. Sie weisen dem ausgehenden Endpunkt von Route 53 Resolver in Ihrer VPC eine IPv4-Adresse zu.
2. Die DNS-Abfrage Ihres IPv6-Dienstes geht an Route 53 Resolver über IPv6. Route 53 Resolver gleicht die Abfrage mit der Weiterleitungsregel ab und ruft eine IPv4-Adresse für Ihren On-Premises-Resolver ab.
3. Route 53 Resolver konvertiert das Abfragepaket von IPv6 in IPv4 und leitet es an den ausgehenden Endpunkt weiter. Jede IP-Adresse des Endpunkts stellt eine ENI dar, welche die Anfrage an die On-Premises-IPv4-Adresse Ihres DNS-Resolvers weiterleitet.
4. Der On-Premises-Resolver sendet das Antwortpaket über IPv4 zurück über den ausgehenden Endpunkt an Route 53 Resolver.
5. Unter der Annahme, dass die Abfrage aus einem DNS64-fähigen Subnetz erstellt wurde, führt Route 53 Resolver zwei Dinge aus:

    a. Überprüft den Inhalt des Antwortpakets. Wenn der Datensatz eine IPv6-Adresse enthält, lässt dieser den Inhalt so, wie er ist, aber wenn er einen IPv4-only Datensatz enthält. Dieser synthetisiert auch einen IPv6-Datensatz, indem `64:ff9b::/96` der IPv4-Adresse vorangestellt wird.

    b. Packt den Inhalt neu und sendet diesen über IPv6 an den Dienst in Ihrer VPC.

Überwachen von NAT-Gateways mit Amazon CloudWatch

Sie können Ihr NAT-Gateway mit überwachen CloudWatch, das Informationen von Ihrem NAT-Gateway sammelt und lesbare Metriken nahezu in Echtzeit erstellt. Diese Informationen können Sie für die Überwachung Ihres NAT-Gateways und die Fehlersuche verwenden. NAT-Gateway-Metrikdaten werden in 1-minütigen Intervallen bereitgestellt und die Statistik wird für einen Zeitraum von 15 Monaten aufgezeichnet.

Weitere Informationen zu Amazon CloudWatchfinden Sie im Amazon- CloudWatch Benutzerhandbuch. Weitere Informationen zu Preisen finden Sie unter Amazon- CloudWatch Preise.

Metriken und Dimensionen des NAT-Gateway

Für Ihre NAT-Gateways stehen folgende Metriken zur Verfügung: Die Beschreibungsspalte enthält eine Beschreibung der einzelnen Metriken sowie die Einheiten und Statistiken.

Metrik	Beschreibung
`ActiveConnectionCount`	Anzahl der Pakete, die durch den TCP-Gatew ay an die Clients in Ihrer NAT gesendet wurden. Ein Wert gleich 0 deutet darauf hin, dass es keine aktiven Verbindungen durch den NAT-Gateway gibt. Einheiten: Anzahl Statistiken: Die nützlichste Statistik ist `Max`.
`BytesInFromDestination`	Anzahl der Bytes, die von dem NAT-Gateway vom Ziel empfangen wurden. Wenn der Wert für `BytesOutToSource` kleiner als der Wert für `BytesInFr omDestination` ist, kommt es ggf. bei der Verarbeitung des NAT-Gateways zu einem Datenverlust, oder der Datenverkehr wird vom NAT-Gateway aktiv blockiert. Einheiten: Byte Statistiken: Die nützlichste Statistik ist `Sum`.
`BytesInFromSource`	Anzahl der Bytes, die von dem NAT-Gateway von Clients in Ihrer VPC empfangen wurden.

Metrik	Beschreibung
	Wenn der Wert für `BytesOutToDestination` kleiner als der Wert für `BytesInFromSource` ist, erfolgt möglicherweise ein Datenverlust während der Verarbeitung des NAT-Gateways. Einheiten: Byte Statistiken: Die nützlichste Statistik ist `Sum`.
`BytesOutToDestination`	Anzahl der Bytes, die durch den NAT-Gateway an das Ziel gesendet wurden. Ein Wert größer 0 deutet darauf hin, dass Verkehr zum Internet von Clients verläuft, die hinter dem NAT-Gateway liegen. Wenn der Wert für `BytesOutToDestination` kleiner als der Wert für `BytesInFromSource` ist, erfolgt möglicherweise ein Datenverlust während der Verarbeitung des NAT-Gateways. Einheit: Byte Statistiken: Die nützlichste Statistik ist `Sum`.

Metrik	Beschreibung
`BytesOutToSource`	Anzahl der Bytes, die durch den NAT-Gateway an die Clients in Ihrer VPC gesendet wurden. Ein Wert größer 0 deutet darauf hin, dass Verkehr vom Internet an Clients verläuft, die hinter dem NAT-Gateway liegen. Wenn der Wert für `BytesOutToSource` kleiner als der Wert für `BytesInFromDestination` ist, kommt es ggf. bei der Verarbeitung des NAT-Gateways zu einem Datenverlust, oder der Datenverkehr wird vom NAT-Gateway aktiv blockiert. Einheiten: Byte Statistiken: Die nützlichste Statistik ist `Sum`.
`ConnectionAttemptCount`	Die Anzahl der Verbindungsversuche durch den NAT-Gateway. Wenn der Wert für `ConnectionEstablishedCount` kleiner als der Wert für `ConnectionAttemptCount` ist, deutet dies darauf hin, dass clients hinter dem NAT-Gateway versucht haben, neue Verbindungen einzurichten, für die es keine Antwort gab. Einheit: Anzahl Statistiken: Die nützlichste Statistik ist `Sum`.

Metrik	Beschreibung
ConnectionEstablishedCount	Die Anzahl der durch den NAT-Gateway eingerichteten Verbindungen. Wenn der Wert für ConnectionEstablishedCount kleiner als der Wert für ConnectionAttemptCount ist, deutet dies darauf hin, dass clients hinter dem NAT-Gateway versucht haben, neue Verbindungen einzurichten, für die es keine Antwort gab. Einheit: Anzahl Statistiken: Die nützlichste Statistik ist Sum.
ErrorPortAllocation	Die Anzahl, wie oft der NAT-Gateway einen Quell-Port nicht zuordnen konnte. Ein Wert größer 0 deutet darauf hin, dass zu viele gleichzeitige Verbindungen durch den NAT-Gateway offen sind. Einheiten: Anzahl Statistiken: Die nützlichste Statistik ist Sum.

Metrik	Beschreibung
`IdleTimeoutCount`	Die Anzahl von Verbindungen, die aus dem aktiven Zustand in den Leerlaufzustand („Idle“) übergegangen sind. Eine aktive Verbindung wechselt in den Leerlaufzustand, wenn sie nicht korrekt geschlossen wurde und in den letzten 350 Sekunden keine Aktivitäten aufgetreten sind. Ein Wert größer 0 deutet darauf hin, dass es Verbindungen gibt, die in einen Leerlaufs tatus übergegangen sind. Wenn der Wert für `IdleTimeoutCount` zunimmt, kann dies darauf hindeuten, dass Clients hinter dem NAT-Gateway ältere Verbindungen wiederver wenden. Einheit: Anzahl Statistiken: Die nützlichste Statistik ist `Sum`.

Metrik	Beschreibung
PacketsDropCount	Anzahl der Pakete, die vom NAT-Gateway verworfen wurden. Verwenden Sie diese Formel, um die Anzahl der verworfenen Pakete als Prozentsatz des gesamten Paketverkehrs zu berechnen : PacketsDropCount/(PacketsIn FromSource+PacketsInFromDes tination)*100 . Wenn dieser Wert 0,01 Prozent des gesamten Datenverkehrs auf dem NAT-Gateway überschreitet, liegt möglicher weise ein Problem mit dem Amazon-VPC-Service vor. Verwenden Sie das AWS Servicest atus-Dashboard, um Probleme mit dem Service zu identifizieren, die dazu führen können, dass NAT-Gateways Pakete löschen. Einheiten: Anzahl Statistiken: Die nützlichste Statistik ist Sum.
PacketsInFromDestination	Anzahl der Pakete, die von dem NAT-Gateway vom Ziel empfangen wurden. Wenn der Wert für PacketsOutToSource kleiner als der Wert für PacketsIn FromDestination ist, kommt es ggf. bei der Verarbeitung des NAT-Gateways zu einem Datenverlust, oder der Datenverkehr wird vom NAT-Gateway aktiv blockiert. Einheit: Anzahl Statistiken: Die nützlichste Statistik ist Sum.

Metrik	Beschreibung
PacketsInFromSource	Anzahl der Pakete, die von dem NAT-Gateway von Clients in Ihrer VPC empfangen wurden. Wenn der Wert für PacketsOutToDestination kleiner als der Wert für PacketsInFromSource ist, erfolgt möglicherweise ein Datenverlust während der Verarbeitung des NAT-Gateways. Einheit: Anzahl Statistiken: Die nützlichste Statistik ist Sum.
PacketsOutToDestination	Anzahl der Pakete, die durch den NAT-Gateway an das Ziel gesendet wurden. Ein Wert größer 0 deutet darauf hin, dass Verkehr zum Internet von Clients verläuft, die hinter dem NAT-Gateway liegen. Wenn der Wert für PacketsOutToDestination kleiner als der Wert für PacketsInFromSource ist, erfolgt möglicherweise ein Datenverlust während der Verarbeitung des NAT-Gateways. Einheit: Anzahl Statistiken: Die nützlichste Statistik ist Sum.

Metrik	Beschreibung
PacketsOutToSource	Anzahl der Pakete, die durch den NAT-Gateway an die Clients in Ihrer VPC gesendet wurden. Ein Wert größer 0 deutet darauf hin, dass Verkehr vom Internet an Clients verläuft, die hinter dem NAT-Gateway liegen. Wenn der Wert für PacketsOutToSource kleiner als der Wert für PacketsInFromDestination ist, kommt es ggf. bei der Verarbeitung des NAT-Gateways zu einem Datenverlust, oder der Datenverkehr wird vom NAT-Gateway aktiv blockiert. Einheit: Anzahl Statistiken: Die nützlichste Statistik ist Sum.
PeakBytesPerSecond	Diese Metrik gibt den höchsten Durchschnitt von 10-Sekunden-Bytes pro Sekunde in einer bestimmten Minute an. Einheiten: Anzahl Statistiken: Die nützlichste Statistik ist Maximum.
PeakPacketsPerSecond	Diese Metrik berechnet 60 Sekunden lang alle 10 Sekunden die durchschnittliche Paketrate (pro Sekunde verarbeitete Pakete) und meldet dann das Maximum der sechs Raten (die höchste durchschnittliche Paketrate). Einheiten: Anzahl Statistiken: Die nützlichste Statistik ist Maximum.

Verwenden Sie die nachstehende Dimension, um die Metrikdaten zu filtern.

Dimension	Beschreibung
`NatGatewayId`	Filtern Sie die Metrikdaten nach der NAT-Gateway-ID.

Anzeigen von NAT-Gateway- CloudWatch Metriken

NAT-Gateway-Metriken werden CloudWatch in Intervallen von 1 Minute an gesendet. Metriken werden zuerst nach dem Service-Namespace und dann nach den möglichen Kombinationen von Dimensionen in jedem Namespace gruppiert. Sie können die folgenden Vorgehensweisen nutzen, um die Metriken für Ihre NAT-Gateways anzuzeigen.

So zeigen Sie Metriken mit der CloudWatch Konsole an

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Metrics (Metriken) All metrics (Alle Metriken) aus.
3. Wählen Sie den NATGateway-Metrik-Namespace aus.
4. Wählen Sie die Metrikdimension.

So zeigen Sie Metriken mit der an AWS CLI

Führen Sie bei der Eingabeaufforderung den folgenden Befehl aus, um die Metriken aufzulisten, die für den NAT-Gateway-Service zur Verfügung stehen:

```
aws cloudwatch list-metrics --namespace "AWS/NATGateway"
```

Erstellen von CloudWatch Alarmen zur Überwachung eines NAT-Gateways

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum. Er sendet eine Benachrichtigung an ein Amazon SNS-Thema basierend auf dem Wert der Metrik im Hinblick auf einen Schwellenwert über verschiedene Zeiträume.

Sie können beispielsweise einen Alarm einrichten, der das Datenverkehrsvolumen überwachen, das in einen bzw. aus dem NAT-Gateway kommt. Der folgende Alarm überwacht das Volumen des ausgehenden Datenverkehrs von Clients in Ihrer VPC durch den NAT-Gateway in das Internet. Er

sendet eine Benachrichtigung, wenn die Anzahl der Bytes innerhalb eines Zeitraums von 15 Minuten einen Schwellenwert von 5.000.000 erreicht.

Einen Alarm für ausgehenden Datenverkehr durch den NAT-Gateway erstellen

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Alarms (Alarme) und All alarms (Alle Alarme) aus.
3. Wählen Sie Create alarm (Alarm erstellen) aus.
4. Wählen Sie Select metric (Metrik auswählen) aus.
5. Wählen Sie den NATGateway-Metrik-Namespace und dann eine Metrikdimension aus. Wenn Sie zu den Metriken gelangen, aktivieren Sie das Kontrollkästchen neben der BytesOutToDestination Metrik für das NAT-Gateway und wählen Sie dann Metrik auswählen aus.
6. Konfigurieren Sie den Alarm wie folgt, und wählen Sie dann Weiter:
   - Wählen Sie für Statistic (Statistik) Sum (Summe) aus.
   - Wählen Sie als Period (Zeitraum) 15 Minuten aus.
   - Wählen Sie für Whenever (Jederzeit) Greater/Equal (Größer/Gleich) aus und geben Sie `5000000` für den Schwellenwert ein.
7. Wählen Sie für Notification (Benachrichtigung) ein vorhandenes SNS-Thema aus oder wählen Sie Create new topic (Neues Thema erstellen), um ein neues zu erstellen. Wählen Sie Weiter aus.
8. Geben Sie einen Namen und eine Beschreibung für den Alarm ein und wählen Sie Next (Weiter).
9. Wenn Sie mit der Konfiguration des Alarms fertig sind, wählen Sie Create alarm (Alarm erstellen).

Als weiteres Beispiel können Sie einen Alarm erstellen, der Fehler bei der Portzuweisung überwacht und eine Benachrichtigung sendet, wenn der Wert in drei aufeinanderfolgenden 5-Minuten-Zeiträumen größer als Null (0) ist.

Einen Alarm für die Überwachung von Port-Zuordnungsfehlern erstellen

1. Öffnen Sie die - CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Alarms (Alarme) und All alarms (Alle Alarme) aus.
3. Wählen Sie Create alarm (Alarm erstellen) aus.
4. Wählen Sie Select metric (Metrik auswählen) aus.

5. Wählen Sie den NATGateway-Metrik-Namespace und dann eine Metrikdimension aus. Wenn Sie zu den Metriken gelangen, aktivieren Sie das Kontrollkästchen neben der ErrorPortAllocation Metrik für das NAT-Gateway und wählen Sie dann Metrik auswählen aus.
6. Konfigurieren Sie den Alarm wie folgt, und wählen Sie dann Weiter:
   - Wählen Sie für Statistic (Statistik) Maximum aus.
   - Wählen Sie als Period (Zeitraum) 5 minutes (5 Minuten) aus.
   - Wählen Sie für Whenever (Jederzeit) Greater (Größer) aus und geben Sie 0 für den Schwellenwert ein.
   - Geben Sie unter Additional configuration (Zusätzliche Konfiguration) für die zu alarmierenden Datenpunkte 3 ein.
7. Wählen Sie für Notification (Benachrichtigung) ein vorhandenes SNS-Thema aus oder wählen Sie Create new topic (Neues Thema erstellen), um ein neues zu erstellen. Wählen Sie Weiter aus.
8. Geben Sie einen Namen und eine Beschreibung für den Alarm ein und wählen Sie Next (Weiter).
9. Wenn Sie mit der Konfiguration des Alarms fertig sind, wählen Sie Create alarm (Alarm erstellen).

Weitere Informationen finden Sie unter Verwenden von Amazon- CloudWatch Alarmen im Amazon-CloudWatch Benutzerhandbuch.

Problembehandlung bei NAT-Gateways

Die folgenden Themen helfen Ihnen bei der Lösung häufiger Probleme, die beim Erstellen oder Verwenden von NAT-Gateways auftreten können.

Problembereiche

- Fehler bei der NAT-Gateway-Erstellung
- NAT-Gateway-Kontingent
- Kontingent für Elastic-IP-Adressen
- Die Availability Zone wird nicht unterstützt.
- Das NAT-Gateway wird nicht mehr angezeigt
- Das NAT-Gateway reagiert nicht auf einen Ping-Befehl.
- Instances haben keinen Zugriff auf das Internet.
- Die TCP-Verbindung mit einem Ziel schlägt fehl.

- Traceroute-Ausgabe zeigt die private IP-Adresse des NAT-Gateways nicht an.
- Die Internetverbindung wird nach 350 Sekunden getrennt.
- IPsec-Verbindung kann nicht hergestellt werden.
- Es können keine weiteren Verbindungen hergestellt werden

Fehler bei der NAT-Gateway-Erstellung

Problem

Sie erstellen ein NAT-Gateway und der Status wird angezeig `Failed`.

> **Note**
>
> Ein ausgefallenes NAT-Gateway wird automatisch gelöscht, normalerweise in etwa einer Stunde.

Ursache

Beim Erstellen des NAT-Gateway ist ein Fehler aufgetreten. Die zurückgegebene Statusmeldung enthält den Grund für den Fehler.

Lösung

Zum Anzeigen der Fehlermeldung öffnen Sie die Amazon VPC-Konsole und wählen NAT Gateways (NAT-Gateways) aus. Wählen Sie das Optionsfeld für Ihr NAT-Gateway aus und suchen Sie dann auf der Registerkarte Details nach der Statusmeldung.

Die folgende Tabelle enthält die möglichen Ursachen für diesen Fehler, wie sie in der Amazon VPC-Konsole angezeigt werden. Nachdem Sie die angegebenen Korrekturmaßnahmen durchgegangen sind, können Sie versuchen, das NAT-Gateway erneut zu erstellen.

Angezeigter Fehler	Ursache	Lösung
Subnetz hat unzureichende freie Adressen zum Erstellen dieses NAT-Gateways.	Das angegebene Subnetz verfügt nicht über freie private IP-Adressen. Für das NAT-Gateway ist eine Netzwerks chnittstelle mit einer privaten	Prüfen Sie auf der Seite Subnets (Subnetze) der Amazon VPC-Konsole, wie viele IP-Adressen in Ihrem Subnetz verfügbar sind.

Angezeigter Fehler	Ursache	Lösung
	IP-Adresse aus dem IP-Adressbereich des Subnetzes erforderlich.	Sie können die verfügbaren IP-Adressen im Feld Available IPs (Verfügbare IPs) im Detailbereich für Ihr Subnetz anzeigen. Um freie IP-Adressen in Ihrem Subnetz zu generieren, können Sie nicht verwendete Netzwerkschnittstellen löschen oder nicht mehr benötigte Instances beenden.
Dem Netzwerk vpc-xxxxxxxx ist kein Internet-Gateway zugeordnet.	Ein NAT-Gateway muss in einer VPC mit einem Internet-Gateway erstellt werden.	Erstellen Sie ein Internet-Gateway und ordnen Sie es Ihrer VPC zu. Weitere Informationen finden Sie unter Arbeiten mit Internet-Gateways.

Angezeigter Fehler	Ursache	Lösung
Die Elastic-IP-Adresse eipalloc-xxxxxxxx ist bereits zugeordnet.	Die angegebene Elastic-IP-Adresse ist bereits einer anderen Ressource zugeordnet und kann diesem NAT-Gateway nicht zugeordnet werden.	Stellen Sie fest, welche Ressource der Elastic-IP-Adresse zugeordnet ist. Wechseln Sie zur Seite Elastic IPs der Amazon VPC-Konsole und zeigen Sie die für die Instance-ID oder die Netzwerkschnittstellen-ID angegebenen Werte an. Wenn Sie die Elastic-IP-Adresse für diese Ressource nicht benötigen, heben Sie die Zuordnung auf. Oder weisen Sie Ihrem Konto eine neue Elastic-IP-Adresse zu. Weitere Informationen finden Sie unter Arbeiten mit Elastic-IP-Adressen.

NAT-Gateway-Kontingent

Wenn Sie versuchen, ein NAT-Gateway zu erstellen, wird die folgende Fehlermeldung angezeigt.

```
Performing this operation would exceed the limit of 5 NAT gateways
```

Ursache

Sie haben das Kontingent für die Anzahl von NAT-Gateways für diese Availability Zone erreicht.

Lösung

Wenn Sie das Gateway-Kontingent für NAT-Gateways erreicht haben, haben Sie folgende Möglichkeiten:

- Fordern Sie eine Erhöhung des NAT-Gateways pro Availability Zone-Kontingents mithilfe der Service-Quotas-Konsole an.

- Überprüfen Sie den Status des NAT-Gateways. Ein Status von `Pending`, `Available` oder `Deleting` wird auf Ihr Kontingent angerechnet. Wenn Sie kürzlich ein NAT-Gateway gelöscht haben, warten Sie einige Minuten, bis der Status von `Deleting` zu `Deleted` wechselt. Versuchen Sie dann erneut, ein NAT-Gateway zu erstellen.
- Wenn Sie Ihr NAT-Gateway in einer bestimmten Availability Zone nicht benötigen, versuchen Sie, ein NAT-Gateway in einer anderen Availability Zone zu erstellen, in der das Kontingent noch nicht erreicht wurde.

Weitere Informationen finden Sie unter Amazon VPC-Kontingente.

Kontingent für Elastic-IP-Adressen

Problem

Wenn Sie versuchen, eine Elastic-IP-Adresse für Ihr öffentliches NAT-Gateway zuzuordnen, wird der folgende Fehler angezeigt.

```
The maximum number of addresses has been reached.
```

Ursache

Sie haben das Kontingent für die Anzahl von Elastic-IP-Adressen für Ihr Konto für diese Region erreicht.

Lösung

Wenn Sie das Kontingent für Elastic-IP-Adressen erreicht haben, können Sie die Zuordnung einer Elastic-IP-Adresse von einer anderen Ressource aufheben. Alternativ können Sie mit der Service–Quotas-Konsole eine Erhöhung des Elastic IPs-Kontingents beantragen.

Die Availability Zone wird nicht unterstützt.

Problem

Wenn Sie versuchen, ein NAT-Gateway zu erstellen, wird die folgende Fehlermeldung angezeig: `NotAvailableInZone`.

Ursache

Möglicherweise versuchen Sie, ein NAT-Gateway in einer beschränkten Availability Zone zu erstellen, d. h. einer Zone, in der Sie nicht beliebig Erweiterungen vornehmen dürfen.

Lösung

NAT-Gateways werden in diesen Availability Zones nicht unterstützt. Erstellen Sie ein NAT-Gateway in einer anderen Availability Zone und verwenden Sie es für private Subnetze in der beschränkten Zone. Sie können Ihre Ressourcen auch in eine Availability Zone ohne Beschränkungen verschieben, um Ressourcen und NAT-Gateway in derselben Availability Zone zu betreiben.

Das NAT-Gateway wird nicht mehr angezeigt

Problem

Sie haben ein NAT-Gateway erstellt, das in der Amazon VPC-Konsole nicht mehr angezeigt wird.

Ursache

Möglicherweise ist bei der Erstellung Ihres NAT-Gateways ein Fehler aufgetreten und die Erstellung ist fehlgeschlagen. Ein NAT-Gateway mit dem Status `Failed` wird über einen kurzen Zeitraum (etwa eine Stunde) in der Amazon VPC-Konsole angezeigt. Anschließend wird es automatisch gelöscht.

Lösung

Lesen Sie die Informationen unter Fehler bei der NAT-Gateway-Erstellung und versuchen Sie erneut, ein neues NAT-Gateway zu erstellen.

Das NAT-Gateway reagiert nicht auf einen Ping-Befehl.

Problem

Wenn Sie versuchen, vom Internet (z. B. von Ihrem lokalen Computer) oder einer Instance in Ihrer VPC aus einen Ping an die Elastic-IP-Adresse oder private IP-Adresse des NAT-Gateways zu senden, erhalten Sie keine Antwort.

Ursache

NAT-Gateways leiten nur Datenverkehr von einer Instance in einem privaten Subnetz an das Internet weiter.

Lösung

Wie Sie die Funktionsweise eines NAT-Gateways testen, ist unter erläuter Testen des öffentlichen NAT-Gateways.

Instances haben keinen Zugriff auf das Internet.

Problem

Sie haben ein öffentliches NAT-Gateway erstellt und die Schritte zum Testen des Gateways ausgeführt, der Befehl `ping` schlägt jedoch fehl oder Ihre Instances im privaten Subnetz können nicht auf das Internet zugreifen.

Ursachen

Dieses Problem kann folgende Ursachen haben:

- Das NAT-Gateway ist nicht bereit für den Datenverkehr.
- Ihre Routing-Tabellen sind nicht korrekt konfiguriert.
- Ihre Sicherheitsgruppen oder Netzwerk-ACLs blockieren ein- oder ausgehenden Datenverkehr.
- Sie verwenden ein nicht unterstütztes Protokoll.

Lösung

Prüfen Sie die folgenden Informationen:

- Überprüfen Sie, ob das NAT-Gateway den Zustand `Available` aufweist. Rufen Sie auf der Amazon VPC-Konsole die Seite NAT Gateways auf und prüfen Sie die Statusinformationen auf der Detailseite. Wenn der Status des NAT-Gateways "Failed" lautet, ist möglicherweise bereits beim Erstellen ein Fehler aufgetreten. Weitere Informationen finden Sie unter Fehler bei der NAT-Gateway-Erstellung.
- Überprüfen Sie, ob die Routing-Tabellen korrekt konfiguriert sind:
  - Das NAT-Gateway muss sich in einem öffentlichen Subnetz mit einer Routing-Tabelle befinden, die Internetdatenverkehr an ein Internet-Gateway leitet.
  - Die Instance muss sich in einem privaten Subnetz mit einer Routing-Tabelle befinden, die Internetdatenverkehr an das NAT-Gateway leitet.
  - Stellen Sie sicher, dass keine anderen Einträge in der Routing-Tabelle den Internetdatenverkehr ganz oder teilweise an andere Geräte als das NAT-Gateway leiten.
- Stellen Sie sicher, dass die Sicherheitsgruppenregeln der privaten Instance ausgehenden Internetdatenverkehr erlauben. Damit der Befehl `ping` funktionieren kann, müssen die Regeln auch ausgehenden ICMP-Datenverkehr erlauben.

Das NAT-Gateway selbst erlaubt den gesamten ausgehenden Datenverkehr sowie Datenverkehr als Antwort auf ausgehende Anfragen (es ist somit zustandsbehaftet).

- Stellen Sie sicher, dass die Netzwerk-ACLs, die dem privaten Subnetz und den öffentlichen Subnetzen zugeordnet sind, keine Regeln enthalten, die eingehenden oder ausgehenden Internetdatenverkehr blockieren. Damit der Befehl `ping` funktionieren kann, müssen die Regeln auch ein- und ausgehenden ICMP-Datenverkehr erlauben.

  Sie können Flow-Protokolle aktivieren, um verloren gegangene Verbindungen aufgrund der Netzwerk-ACL- oder Sicherheitsgruppenregeln zu diagnostizieren. Weitere Informationen finden Sie unter Protokollieren von IP-Datenverkehr mit VPC Flow Logs.
- Stellen Sie beim Verwenden des Befehls `ping` sicher, dass Sie den Ping an einen ICMP-fähigen Host senden. Wenn die Website nicht ICMP-fähig ist, erhalten Sie keine Antwortpakete. Führen Sie zum Testen denselben Befehl `ping` auf der Befehlszeile auf Ihrem lokalen Computer aus.
- Überprüfen Sie, ob Ihre Instance einen Ping an andere Ressourcen wie beispielsweise andere Instances im privaten Subnetz senden kann (vorausgesetzt, die Sicherheitsgruppenregeln erlauben dies).
- Stellen Sie sicher, dass Sie für Verbindungen nur die Protokolle TCP, UDP oder ICMP verwenden.

Die TCP-Verbindung mit einem Ziel schlägt fehl.

Problem

Einige Ihrer TCP-Verbindungen von Instances in einem privaten Subnetz mit einem bestimmten Ziel über ein NAT-Gateway sind erfolgreich, andere hingegen schlagen fehl oder es tritt eine Zeitüberschreitung auf.

Ursachen

Dieses Problem kann folgende Ursachen haben:

- Der Zielendpunkt antwortet mit fragmentierten TCP-Paketen. NAT-Gateways unterstützen keine IP-Fragmentierung für TCP oder ICMP. Weitere Informationen finden Sie unter Vergleich zwischen NAT-Gateways und NAT-Instances.
- Die Option `tcp_tw_recycle` ist auf dem Remote-Server aktiviert. Dies verursacht bekanntermaßen Probleme bei mehreren Verbindungen hinter einem NAT-Gerät.

Lösungen

Überprüfen Sie, ob der Endpunkt, mit dem Sie eine Verbindung herzustellen versuchen, mit fragmentierten TCP-Paketen antwortet. Gehen Sie dazu wie folgt vor:

1. Verwenden Sie eine Instance in einem öffentlichen Subnetz mit einer öffentlichen IP-Adresse, um eine Antwort auszulösen, die ausreicht, um eine Fragmentierung am angegebenen Endpunkt auszulösen.
2. Überprüfen Sie mithilfe des `tcpdump`-Tools, ob der Endpunkt fragmentierte Pakete sendet.

   > **Important**
   >
   > Für diese Überprüfungen müssen Sie eine Instance in einem öffentlichen Subnetz verwenden. Verwenden Sie weder die Instance, bei der die Verbindung ursprünglich fehlgeschlagen ist, noch eine Instance in einem privaten Subnetz hinter einem NAT-Gateway oder einer NAT-Instance.

   Diagnose-Tools, die große ICMP-Pakete senden oder empfangen, melden Paketverluste. Der Befehl `ping -s 10000 example.com` funktioniert mit einem NAT-Gateway beispielsweise nicht.
3. Wenn der Endpunkt fragmentierte TCP-Pakete sendet, können Sie anstelle eines NAT-Gateways eine NAT-Instance verwenden.

Wenn Sie Zugriff auf den Remote-Server haben, können Sie überprüfen, ob die Option `tcp_tw_recycle` aktiviert ist, indem Sie folgende Schritte ausführen:

1. Führen Sie den folgenden Befehl auf dem Server aus:

   ```
   cat /proc/sys/net/ipv4/tcp_tw_recycle
   ```

   Wenn die Ausgabe 1 lautet, ist die Option `tcp_tw_recycle` aktiviert.
2. Wenn die Option `tcp_tw_recycle` aktiviert ist, empfehlen wir, sie zu deaktivieren. Wenn Sie Verbindungen erneut verwenden müssen, bietet die Option `tcp_tw_reuse` mehr Sicherheit.

Wenn Sie keinen Zugriff auf den Remote-Server haben, können Sie den Test ausführen, indem Sie die Option `tcp_timestamps` in einer Instance in einem privaten Subnetz vorübergehend deaktivieren. Stellen Sie dann erneut eine Verbindung mit dem Remote-Server her. Wenn die

Verbindung erfolgreich hergestellt wird, liegt der Fehler wahrscheinlich daran, dass die Option `tcp_tw_recycle` auf dem Remote-Server aktiviert ist. Wenden Sie sich möglichst an den Eigentümer des Remote-Servers, um festzustellen, ob diese Option aktiviert ist, und bitten Sie darum, sie zu deaktivieren.

Traceroute-Ausgabe zeigt die private IP-Adresse des NAT-Gateways nicht an.

Problem

Ihre Instance kann auf das Internet zugreifen, aber wenn Sie den Befehl `traceroute` ausführen, wird in der Ausgabe die private IP-Adresse des NAT-Gateways nicht angezeigt.

Ursache

Ihre Instance greift über ein anderes Gateway, z. B. über ein Internet-Gateway, auf das Internet zu.

Lösung

Überprüfen Sie in der Routing-Tabelle des Subnetzes Ihrer Instance folgende Informationen:

- Stellen Sie sicher, dass eine Route für Internetdatenverkehr zum NAT-Gateway vorhanden ist.
- Stellen Sie sicher, dass es keine spezifischere Route gibt, die Internetdatenverkehr an andere Geräte leitet, wie beispielsweise ein Virtual Private Gateway oder ein Internet-Gateway.

Die Internetverbindung wird nach 350 Sekunden getrennt.

Problem

Ihre Instances können auf das Internet zugreifen, doch die Verbindung wird nach 350 Sekunden unterbrochen.

Ursache

Wenn eine Verbindung über ein NAT-Gateway mindestens 350 Sekunden inaktiv ist, wird die Verbindung getrennt.

Wenn eine Verbindung abläuft, gibt ein NAT-Gateway ein RST-Paket an die Ressourcen hinter dem NAT-Gateway zurück, um zu versuchen, die Verbindung wiederaufzunehmen (es wird kein FIN-Paket gesendet).

Lösung

Senden Sie weiteren Datenverkehr über die Verbindung, um die Verbindung aufrechtzuerhalten. Alternativ können Sie TCP-Keepalive auf der Instance mit einem Wert kleiner als 350 Sekunden aktivieren.

IPsec-Verbindung kann nicht hergestellt werden.

Problem

Sie können keine IPsec-Verbindung mit einem Ziel herstellen.

Ursache

Das IPsec-Protokoll wird von NAT-Gateways gegenwärtig nicht unterstützt.

Lösung

Sie können NAT-Traversal (NAT-T) verwenden, um IPsec-Datenverkehr in UDP einzukapseln, ein für NAT-Gateways unterstütztes Protokoll. Testen Sie unbedingt Ihre NAT-T- und IPsec-Konfiguration, um sicherzustellen, dass Ihr IPsec-Datenverkehr nicht verloren geht.

Es können keine weiteren Verbindungen hergestellt werden

Problem

Sie haben bestehende Verbindungen mit einem Ziel über ein NAT-Gateway, können jedoch keine weiteren Verbindungen herstellen.

Ursache

Möglicherweise haben Sie das Limit für gleichzeitige Verbindungen für ein einzelnes NAT-Gateway erreicht. Weitere Informationen finden Sie unter Grundlagen zu NAT-Gateways. Wenn Ihre Instances im privaten Subnetz viele Verbindungen herstellen, kann dieses Limit erreicht werden.

Lösung

Führen Sie eine der folgenden Aktionen aus:

- Erstellen Sie pro Availability Zone ein NAT-Gateway und verteilen Sie Ihre Clients auf diese Zonen.
- Erstellen Sie zusätzliche NAT-Gateways im öffentlichen Subnetz und verteilen Sie Ihre Clients auf mehrere private Subnetze mit je einer Route zu einem anderen NAT-Gateway.
- Begrenzen Sie die Anzahl der Verbindungen, die Clients zum Zielbereich erstellen können.

- Verwenden Sie die `IdleTimeoutCount`-Metrik in CloudWatch, um die Zunahme von Leerlaufverbindungen zu überwachen. Trennen Sie inaktive Verbindungen, um Kapazitäten freizugeben.
- Erstellen Sie ein NAT-Gateway mit mehreren IP-Adressen oder fügen Sie einem vorhandenen NAT-Gateway sekundäre IP-Adressen hinzu. Jede neue IPv4-Adresse kann bis zu 55 000 gleichzeitige Verbindungen unterstützen. Weitere Informationen finden Sie unter Erstellen eines NAT-Gateways oder Bearbeiten sekundärer IP-Adresszuweisungen.

Preisgestaltung

Wenn Sie ein NAT-Gateway bereitstellen, wird Ihnen jede Stunde, die Ihr NAT-Gateway verfügbar ist, und jedes Gigabyte an Daten, das es verarbeitet, in Rechnung gestellt. Weitere Informationen dazu finden Sie unter Amazon VPC – Preise.

Die folgenden Strategien können Ihnen helfen, die Datenübertragungsgebühren für Ihr NAT-Gateway zu senken:

- Wenn Ihre AWS Ressourcen ein erhebliches Datenvolumen über Availability Zones senden oder empfangen, stellen Sie sicher, dass sich die Ressourcen in derselben Availability Zone wie das NAT-Gateway befinden. Erstellen Sie alternativ ein NAT-Gateway in jeder Availability Zone mit Ressourcen.
- Wenn der Großteil des Datenverkehrs über Ihr NAT-Gateway an AWS Dienste geht, die Schnittstellen-Endpunkte oder Gateway-Endpunkte unterstützen, sollten Sie in Erwägung ziehen, einen Schnittstellen- oder Gateway-Endpunkt für diese Dienste einzurichten. Weitere Informationen zu den potenziellen Kosteneinsparungen finden Sie unter: AWS PrivateLink -Preise.

NAT-Instances

Eine NAT-Instance bietet Network Address Translation (NAT). Sie können eine NAT-Instance verwenden, um Ressourcen in einem privaten Subnetz die Kommunikation mit Zielen außerhalb der Virtual Private Cloud (VPC) wie dem Internet oder einem On-Premises-Netzwerk zu ermöglichen. Die Ressourcen im privaten Subnetz können ausgehenden IPv4-Datenverkehr ins Internet initiieren, aber sie können keinen eingehenden Datenverkehr empfangen, der über das Internet initiiert wurde.

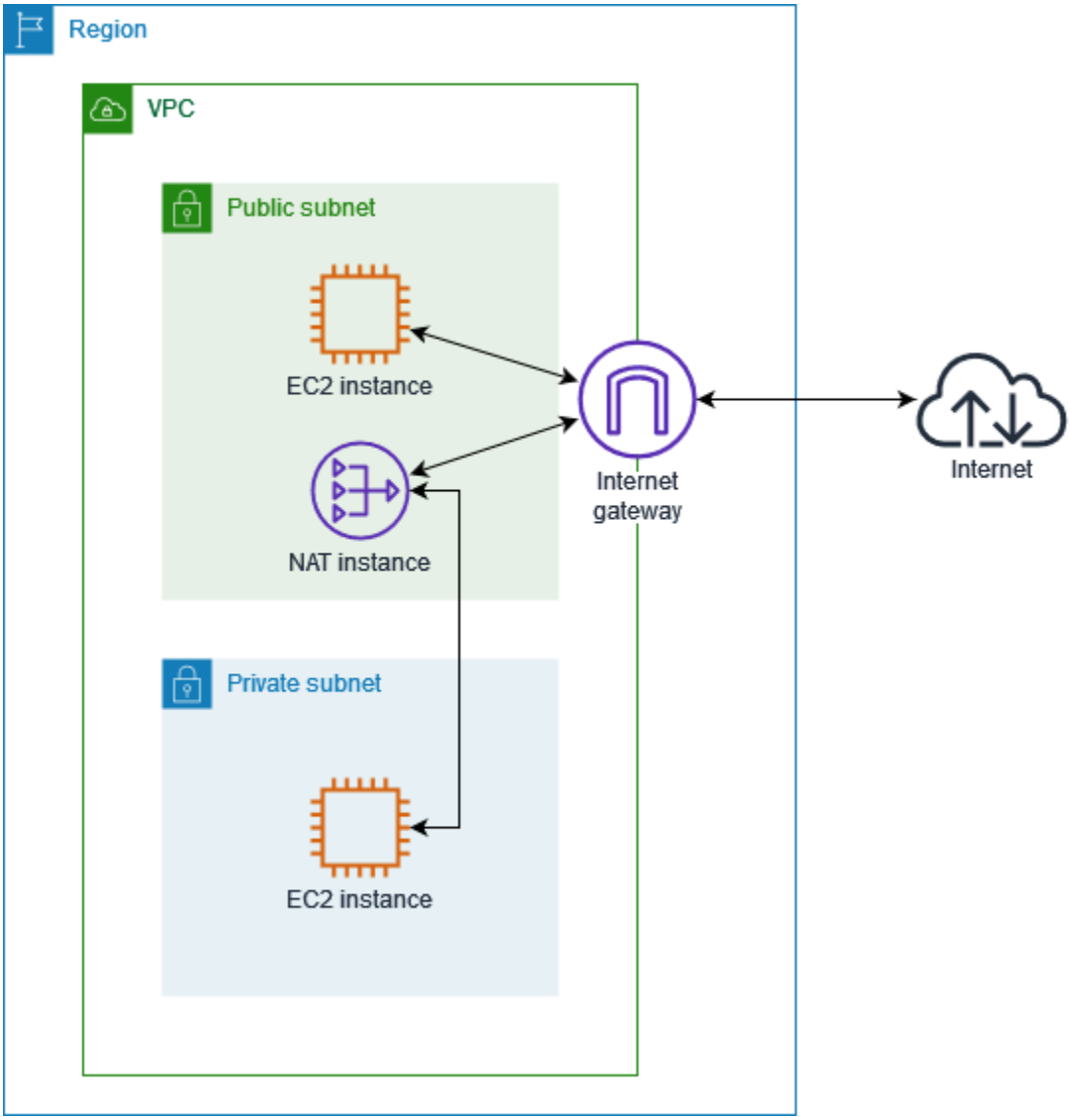
> **Important**
>
> NAT AMI basiert auf der letzten Version des Amazon Linux AMI, 2018.03, für die der Standardsupport am 31. Dezember 2020 und der Wartungssupport am 31. Dezember 2023 eingestellt wurde. Weitere Informationen finden Sie im folgenden Blogbeitrag: Amazon Linux AMI End of Life.
>
> Wenn Sie ein vorhandenes NAT-AMI verwenden, AWS empfiehlt die Migration zu einem NAT-Gateway. Die NAT-Gateways bieten bessere Verfügbarkeit, höherer Bandbreite und weniger Verwaltungsaufwand. Weitere Informationen finden Sie unter Vergleich zwischen NAT-Gateways und NAT-Instances.
>
> Wenn NAT-Instances besser zu Ihrem Anwendungsfall passen als NAT-Gateways, können Sie Ihr eigenes NAT-AMI aus einer aktuellen Version von Amazon Linux erstellen, wie unter beschrieben. the section called “Erstellen eines NAT-AMI”

Inhalt

Grundlagen zu NAT-Instances

Die folgende Abbildung stellt die Grundlagen einer NAT-Instance dar. Die Routing-Tabelle, die dem privaten Subnetz zugeordnet ist, sendet den Internetdatenverkehr von den Instances im privaten Subnetz zur NAT-Instance im öffentlichen Subnetz. Die NAT-Instance sendet anschließend den Datenverkehr zum Internet-Gateway. Der Datenverkehr ist der öffentliche IP-Adresse der NAT-Instance zugeordnet. Die NAT-Instance legt für Antworten eine hohe Portnummer fest. Wenn eine Antwort eingeht, sendet die NAT-instance diese abhängig von der Portnummer der Antwort an eine bestimmte Instance im privaten Subnetz.

Die NAT-Instance Internetzugang haben, d. h. sie muss sich in einem öffentlichen Subnetz (einem Subnetz, das eine Routing-Tabelle mit einer Route zum Internet-Gateway besitzt) befinden und über eine öffentliche oder Elastic-IP-Adresse verfügen.



Um mit NAT-Instances zu beginnen, erstellen Sie ein NAT-AMI, erstellen Sie eine Sicherheitsgruppe für die NAT-Instance und starten Sie die NAT-Instance in Ihrer VPC.

Ihr NAT-Instance-Kontingent hängt von Ihrem Instance-Kontingent für die Region ab. Weitere Informationen finden Sie unter Amazon-EC2-Service-Quotas in der Allgemeine AWS-Referenz.

Erstellen einer VPC für die NAT-Instance

Gehen Sie wie folgt vor, um eine VPC mit einem öffentlichen Subnetz und einem privaten Subnetz zu erstellen.

So erstellen Sie die 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 unter Name tag auto-generation (Automatische Generierung des Namens-Tags) einen Namen für die VPC ein.
5. Führen Sie zur Konfiguration der Subnetze folgende Schritte aus:
   a. Wählen Sie unter Number of Availability Zones (Anzahl der Availability Zones) je nach Bedarf 1 oder 2 aus.
   b. Stellen Sie unter Number of public subnets (Anzahl der öffentlichen Subnetze) sicher, dass ein öffentliches Subnetz pro Availability Zone vorhanden ist.
   c. Stellen Sie unter Number of private subnets (Anzahl der privaten Subnetze) sicher, dass ein privates Subnetz pro Availability Zone vorhanden ist.
6. Wählen Sie VPC erstellen aus.

Erstellen einer Sicherheitsgruppe für Ihre NAT-Instance

Erstellen Sie eine Sicherheitsgruppe mit den in der folgenden Tabelle beschriebenen Regeln. Diese Regeln ermöglichen es Ihrer NAT-Instance, an das Internet gerichteten Datenverkehr von Instances im privaten Subnetz sowie SSH-Datenverkehr aus Ihrem Netzwerk zu empfangen. Die NAT-Instance kann auch Datenverkehr an das Internet senden, sodass Instances im privaten Subnetz Softwareaktualisierungen empfangen können.

Im Folgenden sind die empfohlenen Regeln aufgeführt.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Kommentare
CIDR für privates Subnetz	TCP	80	Erlauben Sie eingehenden HTTP-Datenverkehr von Servern zum privaten Subnetz.

Source	Protocol (Protokoll)	Port-Bereich	Kommentare
CIDR für privates Subnetz	TCP	443	Erlauben Sie eingehenden HTTPS-Datenverkehr von Servern zum privaten Subnetz.
Öffentlicher IP-Adressbereich Ihres Netzwerks	TCP	22	Lässt eingehenden SSH-Zugriff auf die NAT-Instance von Ihrem Netzwerk zu (über das Internet-Gateway)

Ausgehend

Ziel	Protocol (Protokoll)	Port-Bereich	Kommentare
0.0.0.0/0	TCP	80	Lässt ausgehenden HTTP-Zugriff auf das Internet zu
0.0.0.0/0	TCP	443	Lässt ausgehenden HTTPS-Zugriff auf das Internet zu

So erstellen Sie die Sicherheitsgruppe

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für die Sicherheitsgruppe ein.
5. Wählen Sie für VPC die ID der VPC für Ihre NAT-Instance aus.
6. Fügen Sie unter Regeln für eingehenden Datenverkehr wie nachfolgend beschrieben die Regeln für eingehenden Datenverkehr hinzu:

    a. Wählen Sie Regel hinzufügen aus. Wählen Sie HTTP als Typ und geben Sie den IP-Adressbereich Ihres privaten Subnetzes als Quelle ein.

b. Wählen Sie Regel hinzufügen aus. Wählen Sie HTTPS als Typ und geben Sie den IP-Adressbereich Ihres privaten Subnetzes als Quelle ein.

c. Wählen Sie Regel hinzufügen aus. Wählen Sie SSH als Typ und geben Sie den IP-Adressbereich Ihres Netzwerks als Quelle ein.

7. Fügen Sie unter Regeln für ausgehenden Datenverkehr wie nachfolgend beschrieben die Regeln für ausgehenden Datenverkehr hinzu:

a. Wählen Sie Regel hinzufügen aus. Wählen Sie HTTP als Typ und geben Sie 0.0.0.0/0 als Ziel ein.

b. Wählen Sie Regel hinzufügen aus. Wählen Sie HTTPS als Typ und geben Sie 0.0.0.0/0 als Ziel ein.

8. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.

Weitere Informationen finden Sie unter Sicherheitsgruppen.

Erstellen eines NAT-AMI

Ein NAT-AMI ist so konfiguriert, dass NAT auf einer EC2-Instance ausgeführt wird. Sie müssen ein NAT-AMI erstellen und dann Ihre NAT-Instance mit Ihrem NAT-AMI starten.

Wenn Sie planen, ein anderes Betriebssystem als Amazon Linux für Ihr NAT-AMI zu verwenden, finden Sie in der Dokumentation zu diesem Betriebssystem Informationen zur Konfiguration von NAT. Stellen Sie sicher, dass Sie diese Einstellungen speichern, damit diese auch nach einem Instance-Neustart bestehen bleiben.

So erstellen Sie ein NAT-AMI für Amazon Linux

1. Starten Sie eine EC2-Instance, auf der AL2023 oder Amazon Linux 2 ausgeführt wird. Geben Sie unbedingt die Sicherheitsgruppe an, die Sie für die NAT-Instance erstellt haben.
2. Stellen Sie eine Verbindung mit Ihrer Instance her und führen Sie auf der Instance die folgenden Befehle aus, um iptables zu aktivieren.

```
sudo yum install iptables-services -y
sudo systemctl enable iptables
sudo systemctl start iptables
```

3. Gehen Sie auf der Instance wie folgt vor, um die IP-Weiterleitung so zu aktivieren, dass sie nach dem Neustart bestehen bleibt:

a. Erstellen Sie mithilfe eines Texteditors, wie nano oder vim, die folgende Konfigurationsdatei: `/etc/sysctl.d/custom-ip-forwarding.conf`

b. Fügen Sie die folgende Zeile in die Konfigurationsdatei ein.

```
net.ipv4.ip_forward=1
```

c. Speichern Sie die Konfigurationsdatei und schließen Sie den Text-Editor.

d. Führen Sie den folgenden Befehl aus, um die Konfigurationsdatei anzuwenden.

```
sudo sysctl -p /etc/sysctl.d/custom-ip-forwarding.conf
```

4. Führen Sie den folgenden Befehl auf der Instance aus und notieren Sie sich den Namen der primären Netzwerkschnittstelle. Diese Informationen sind für den nächsten Schritt erforderlich.

```
netstat -i
```

In der folgenden Beispielausgabe ist `docker0` eine von Docker erstellte Netzwerkschnittstelle, `eth0` ist die primäre Netzwerkschnittstelle und `lo` ist die Loopback-Schnittstelle.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
docker0   1500        0      0      0 0             0      0      0      0 BMU
eth0      9001  7276052      0      0 0       5364991      0      0      0 BMRU
lo       65536   538857      0      0 0        538857      0      0      0 LRU
```

In der folgenden Beispielausgabe ist die primäre Netzwerkschnittstelle `enX0`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enX0      9001     1076      0      0 0          1247      0      0      0 BMRU
lo       65536       24      0      0 0            24      0      0      0 LRU
```

In der folgenden Beispielausgabe ist die primäre Netzwerkschnittstelle `ens5`.

```
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
ens5      9001    14036      0      0 0          2116      0      0      0 BMRU
lo       65536       12      0      0 0            12      0      0      0 LRU
```

5. Führen Sie auf der Instance die folgenden Befehle aus, um NAT zu konfigurieren. Wenn es sich bei der primären Netzwerkschnittstelle nicht um `eth0` handelt, ersetzen Sie *`eth0`* durch die primäre Netzwerkschnittstelle, die Sie im vorherigen Schritt notiert haben.

```
sudo /sbin/iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
sudo /sbin/iptables -F FORWARD
sudo service iptables save
```

6. Erstellen Sie aus der EC2-Instance ein NAT-AMI. Weitere Informationen finden Sie unter Erstellen eines Linux-AMI aus einer Instance im Amazon EC2 EC2-Benutzerhandbuch.

Starten einer NAT-Instance

Gehen Sie wie folgt vor, um eine NAT-Instance mithilfe der von Ihnen erstellten VPC, Sicherheitsgruppe und NAT-AMI zu starten.

So starten Sie eine NAT-Instance

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. Geben Sie unter Name einen Namen für Ihre NAT-Instance ein.
4. Wählen Sie für Anwendungs- und Betriebssystemabbilder Ihr NAT-AMI aus (wählen Sie Weitere AMIs durchsuchen, Meine AMIs).
5. Wählen Sie für Instance-Typ einen Instance-Typ aus, der die Anforderungen Ihrer NAT-Instance an Rechenleistung, Arbeitsspeicher und Speicherplatz erfüllt.
6. Wählen Sie unter Schlüsselpaar ein vorhandenes Schlüsselpaar aus oder Erstellen Sie ein neues Schlüsselpaar.
7. Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:
   a. Wählen Sie Bearbeiten aus.
   b. Wählen Sie für VPC die erstellte VPC aus.
   c. Wählen Sie für Subnetz das für von Ihnen erstellte öffentliche Subnetz aus.
   d. Wählen Sie unter Auto-assign public IP (Öffentlche IP automatisch zuweisen) die Option Enable (Aktivieren) aus. Alternativ können Sie nach dem Start der NAT-Instance eine Elastic IP-Adresse zuweisen und sie der NAT-Instance zuweisen.

e. Wählen Sie unter Firewall die Option Vorhandene Sicherheitsgruppe auswählen aus und wählen Sie dann die Sicherheitsgruppe, die Sie erstellt haben, aus.

8. Wählen Sie Launch Instance (Instance starten) aus. Wählen Sie die Instance-ID, um die Instance-Detailseite zu öffnen. Warten Sie, bis der Instance-Status in Wird ausgeführt wechselt und die Statusprüfungen erfolgreich sind.
9. Deaktivieren Sie die Quell-/Zielprüfungen für die NAT-Instance (siehe Deaktivieren der Quell-/Zielprüfungen).
10. Aktualisieren Sie die Routing-Tabelle, um Datenverkehr an die NAT-Instance zu senden (siehe Aktualisieren der Routing-Tabelle).

Deaktivieren der Quell-/Zielprüfungen

Auf EC2-Instances werden standardmäßig Quell-/Zielprüfungen ausgeführt. Das bedeutet, die Instance muss entweder Quelle oder Ziel des gesendeten bzw. empfangenen Datenverkehrs sein. Eine NAT-Instance muss jedoch in der Lage sein, Datenverkehr zu senden bzw. zu empfangen, dessen Quelle oder Ziel sie nicht selbst ist. Daher müssen Sie für NAT-Instances die Quell-/Zielprüfung deaktivieren.

So deaktivieren Sie die Quell-/Zielprüfungen

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 NAT-Instance aus.
4. Wählen Sie Aktionen, Netzwerk, Quell-/Zielprüfung ändern).
5. Wählen Sie für die Quell-/Zielprüfung die Option Stopp aus.
6. Wählen Sie Speichern.
7. Wenn die NAT-Instance eine sekundäre Netzwerkschnittstelle hat, wählen Sie sie aus Network interfaces (Netzwerkschnittstellen) im Reiter Networking aus. Wählen Sie die Schnittstellen-ID aus, um zur Seite mit den Netzwerkschnittstellen zu gelangen. Wählen Sie Actions (Aktionen) und Change source/dest. check (Quell-/Ziel-Prüfung ändern) aus, löschen Sie Enable (Aktivieren) und wählen Sie Save (Speichern) aus.

Aktualisieren der Routing-Tabelle

Die Routing-Tabelle für das private Subnetz muss eine Route enthalten, die den Internetverkehr an die NAT-Instance leitet.

So aktualisieren Sie die Routing-Tabelle

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Route Tables (Routing-Tabellen) aus.
3. Wählen Sie die Routing-Tabelle für das private Subnetz aus.
4. Klicken Sie auf der Registerkarte Routen auf Routen bearbeiten und wählen Sie dann Route hinzufügen.
5. Geben Sie 0.0.0.0/0 als Ziel und die Instance-ID der NAT-Instance als Ziel an.
6. Wählen Sie Änderungen speichern aus.

Weitere Informationen finden Sie unter Konfigurieren von Routing-Tabellen.

Testen Ihrer NAT-Instance

Nachdem Sie eine NAT-Instance gestartet und wie oben beschrieben konfiguriert haben, können Sie testen, ob die Instance im privaten Subnetz über die NAT-Instance als Bastion Host auf das Internet zugreifen kann.

Aufgaben

- Schritt 1: Aktualisieren der Sicherheitsgruppe der NAT-Instance
- Schritt 2: Starten einer Test-Instance im privaten Subnetz
- Schritt 3: Pingen einer ICMP-fähigen Website
- Schritt 4: Bereinigen

Schritt 1: Aktualisieren der Sicherheitsgruppe der NAT-Instance

Damit Instances in Ihrem privaten Subnetz Ping-Verkehr an die NAT-Instance senden können, fügen Sie eine Regel hinzu, die ein- und ausgehenden ICMP-Verkehr zulässt. Damit die NAT-Instance als Bastion-Server fungieren kann, fügen Sie eine Regel hinzu, die ausgehenden SSH-Datenverkehr zum privaten Subnetz zulässt.

So aktualisieren Sie die Sicherheitsgruppe Ihrer NAT Instance

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Aktivieren Sie das Kontrollkästchen für die Sicherheitsgruppe, die mit Ihrer NAT-Instance verknüpft ist.
4. Wählen Sie auf der Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) die Option Edt inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) aus.
5. Wählen Sie Regel hinzufügen aus. Wählen Sie All ICMP - IPv4 (Alle ICMP - IPv4) für Type (Typ) aus. Wählen Sie für Quelle Benutzerdefiniert aus und geben Sie den IP-Adressbereich Ihres privaten Subnetzes ein. Wählen Sie Save rules (Regeln speichern) aus.
6. Wählen Sie auf der Registerkarte Regeln für ausgehenden Datenverkehr die Option Regeln für ausgehenden Datenverkehr bearbeiten aus.
7. Wählen Sie Regel hinzufügen aus. Wählen Sie SSH für Type aus. Wählen Sie für Ziel Benutzerdefiniert aus und geben Sie den IP-Adressbereich Ihres privaten Subnetzes ein.
8. Wählen Sie Regel hinzufügen aus. Wählen Sie All ICMP - IPv4 (Alle ICMP - IPv4) für Type (Typ) aus. Wählen Sie Überall – IPv4 als Ziel. Wählen Sie Save rules (Regeln speichern) aus.

Schritt 2: Starten einer Test-Instance im privaten Subnetz

Starten Sie eine Instance in Ihrem privaten Subnetz. Sie müssen den SSH-Zugriff von der NAT-Instance aus zulassen und dasselbe Schlüsselpaar verwenden, das Sie für die NAT-Instance genutzt haben.

So starten Sie eine Test-Instance im privaten Subnetz

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 Ihr privates Subnetz aus.
4. Weisen Sie dieser Instance keine öffentliche IP-Adresse zu.
5. Stellen Sie sicher, dass die Sicherheitsgruppe für diese Instance eingehenden SSH-Zugriff von Ihrer NAT-Instance oder aus dem IP-Adressbereich Ihres öffentlichen Subnetzes sowie ausgehenden ICMP-Datenverkehr zulässt.
6. Wählen Sie dasselbe Schlüsselpaar aus, das Sie für die NAT-Instance verwendet haben.

Schritt 3: Pingen einer ICMP-fähigen Website

Um zu überprüfen, ob die Test-Instance in Ihrem privaten Subnetz Ihre NAT-Instance für die Kommunikation mit dem Internet verwenden kann, führen Sie den ping-Befehl aus.

So testen Sie die Internetverbindung von Ihrer privaten Instance aus

1. Konfigurieren Sie auf Ihrem lokalen Computer die SSH-Agent-Weiterleitung, sodass Sie die NAT-Instance als Bastion-Server nutzen können.

   Linux and macOS

   ```
   ssh-add key.pem
   ```

   Windows

   Downloaden und installieren Sie Pageant, sofern es noch nicht installiert ist.

   Konvertieren Sie den privaten Schlüssel mit PuTTYgen in das PPK-Format.

   Starten Sie Pageant, klicken Sie in der Taskleiste mit der rechten Maustaste auf das Pageant-Symbol (ist möglicherweise ausgeblendet) und wählen Sie Schlüssel hinzufügen. Wählen Sie die erstellte PPK-Datei aus, geben Sie gegebenenfalls das Passwort ein und wählen Sie Öffnen.
2. Stellen Sie auf dem lokalen Computer eine Verbindung mit Ihrer NAT-Instance her.

   Linux and macOS

   ```
   ssh -A ec2-user@nat-instance-public-ip-address
   ```

   Windows

   Stellen Sie mit PuTTY eine Verbindung mit der NAT-Instance her. Unter Authentifizierung müssen Sie Agent-Weiterleitung zulassen auswählen und Private Schlüsseldatei für Authentifizierung leer lassen.
3. Führen Sie auf der NAT-Instance den ping-Befehl aus. Geben Sie dabei eine Website an, die für ICMP aktiviert ist.

   ```
   [ec2-user@ip-10-0-4-184]$ ping ietf.org
   ```

Um sich zu vergewissern, dass die NAT-Instance über Internetzugriff verfügt, überprüfen Sie, ob Sie eine Ausgabe wie die folgende erhalten haben. Drücken Sie anschließend Ctrl+C, um den ping-Befehl abzubrechen. Überprüfen Sie andernfalls, ob sich die NAT-Instance in einem öffentlichen Subnetz befindet (ihre Routing-Tabelle enthält eine Route zu einem Internet-Gateway).

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=7.88 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.09 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=7.97 ms
...
```

4. Verbinden Sie sich von der NAT-Instance aus mit der Instance im privaten Subnetz unter Verwendung deren privater IP-Adresse.

```
[ec2-user@ip-10-0-4-184]$ ssh ec2-user@private-server-private-ip-address
```

5. Überprüfen Sie auf der privaten Instance, ob Sie eine Verbindung mit dem Internet herstellen können. Führen Sie dazu den Befehl ping aus.

```
[ec2-user@ip-10-0-135-25]$ ping ietf.org
```

Um sich zu vergewissern, dass Ihre private Instance über die NAT-Instance auf das Internet zugreifen kann, überprüfen Sie, ob Sie eine Ausgabe wie die folgende erhalten haben. Drücken Sie anschließend Ctrl+C, um den ping-Befehl abzubrechen.

```
PING ietf.org (104.16.45.99) 56(84) bytes of data.
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=1 ttl=33 time=8.76 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=2 ttl=33 time=8.26 ms
64 bytes from 104.16.45.99 (104.16.45.99): icmp_seq=3 ttl=33 time=8.27 ms
...
```

Fehlerbehebung

Wenn der Befehl ping auf dem Server im privaten Subnetz fehlschlägt, gehen Sie wie folgt vor, um das Problem zu beheben:

- Stellen Sie sicher, dass Sie eine Website angepingt haben, auf der ICMP aktiviert ist. Andernfalls kann Ihr Server keine Antwortpakete empfangen. Führen Sie zum Testen denselben Befehl ping auf den Befehlszeilenterminal auf Ihrem lokalen Computer aus.
- Stellen Sie sicher, dass die Sicherheitsgruppe für Ihre NAT-Instance eingehenden ICMP-Datenverkehr aus Ihrem privaten Subnetz zulässt. Ist das nicht der Fall, kann die NAT-Instance den Befehl ping von der privaten Instance nicht empfangen.
- Stellen Sie sicher, dass Sie die Quell-/Zielprüfung für Ihre NAT-Instance deaktiviert haben. Weitere Informationen finden Sie unter Deaktivieren der Quell-/Zielprüfungen.
- Stellen Sie sicher, dass Ihre Routing-Tabellen korrekt konfiguriert sind. Weitere Informationen finden Sie unter Aktualisieren der Routing-Tabelle.

Schritt 4: Bereinigen

Wenn Sie den Testserver im privaten Subnetz nicht mehr benötigen, beenden Sie die Instance, damit sie Ihnen nicht mehr in Rechnung gestellt wird. Weitere Informationen finden Sie unter Beenden Ihrer Instance im Amazon-EC2-Benutzerhandbuch.

Wenn Sie die NAT-Instance nicht mehr benötigen, können Sie sie anhalten oder beenden, sodass sie Ihnen nicht mehr in Rechnung gestellt wird. Wenn Sie ein NAT-AMI erstellt haben, können Sie bei Bedarf jederzeit eine neue NAT-Instance erstellen.

Vergleich zwischen NAT-Gateways und NAT-Instances

Nachfolgend werden die Unterschiede zwischen NAT-Gateways und NAT-Instances übersichtlich beschrieben. Es wird empfohlen, NAT-Gateways zu verwenden, da sie eine bessere Verfügbarkeit und Bandbreite bieten und weniger Administrationsaufwand erfordern.

Attribut	NAT-Gateway	NAT-Instance
Verfügbarkeit	Hochverfügbar. NAT-Gateways werden innerhalb jeder Availability Zone redundant implementiert. Erstellen Sie ein NAT-Gateway in jeder Availability Zone, um eine zonenunabhängige Architektur sicherzustellen.	Den Failover zwischen Instances können Sie mithilfe eines Skripts verwalten.

Attribut	NAT-Gateway	NAT-Instance
Bandbreite	Bis zu 100 Gbit/s hochskalierbar.	Abhängig von der Bandbreite des Instance-Typs
Wartung	Verwaltet von AWS. Wartung ist nicht erforderlich.	Von Ihnen verwaltet, beispielsweise zur Installation von Softwareupdates oder Betriebssystem-Patches auf der Instance
Leistung	Software auf NAT-Datenverkehr optimiert	Generisches, für NAT konfiguriertes AMI
Kosten	Gebühren abhängig von der Anzahl der verwendeten NAT-Gateways, der Nutzungsdauer und dem über die NAT-Gateways gesendeten Datenvolumen	Gebühren abhängig von der Anzahl der verwendeten NAT-Instances, der Nutzungsdauer und dem Instance-Typ sowie der Instance-Größe
Typ und Größe	Einheitliches Angebot, keine Auswahl von Typ oder Größe	Auswahl des geeigneten Instance-Typs und der Instance-Größe anhand des erwarteten Workloads
Öffentliche IP-Adresse	Sie ordnen beim Erstellen eines öffentlichen NAT-Gateways eine elastische IP-Adresse zu.	Für NAT-Instances können Sie eine Elastic-IP-Adresse oder eine öffentliche IP-Adresse verwenden. Sie können die öffentliche IP-Adresse jederzeit ändern, indem Sie der Instance eine neue Elastic-IP-Adresse zuordnen.
Private IP-Adressen	Die private IP-Adresse wird beim Erstellen des Gateways automatisch aus dem IP-Adressbereich des Subnetzes zugewiesen.	Weisen Sie beim Starten der Instance eine bestimmte private IP-Adresse aus dem IP-Adressbereich des Subnetzes zu.

Attribut	NAT-Gateway	NAT-Instance
Sicherheitsgruppen	Sie können einer Sicherheitsgruppe kein NAT-Gateway zuordnen. Sie können den Ressourcen hinter dem NAT-Gateway Sicherheitsgruppen zuordnen, um den ein- und ausgehenden Datenverkehr zu steuern.	Ordnen Sie sie NAT-Instances und den Ressourcen hinter der NAT-Instance zu, um ein- und ausgehenden Datenverkehr zu steuern.
Netzwerk-ACLs	Verwenden Sie eine Netzwerk-ACL, um den Datenverkehr zu und von dem Subnetz zu steuern, in dem sich das NAT-Gateway befindet.	Verwenden Sie eine Netzwerk-ACL, um den Datenverkehr zu und von dem Subnetz zu steuern, in dem sich die NAT-Instance befindet.
Flow-Protokolle	Verwenden Sie Flow-Protokolle, um den Datenverkehr zu erfassen.	Verwenden Sie Flow-Protokolle, um den Datenverkehr zu erfassen.
Port-Weiterleitung	Nicht unterstützt	Manuelle Anpassung der Konfiguration zur Unterstützung von Port-Weiterleitung
Bastion Hosts	Nicht unterstützt	Als Bastion Host verwenden
Datenverkehr-Metriken	Anzeigen von CloudWatch -Metriken für den NAT-Gateway.	CloudWatch Metriken für die Instanz anzeigen.
Timeout-V erhalten	Wenn eine Verbindung abläuft, gibt ein NAT-Gateway ein RST-Paket an die Ressourcen hinter dem NAT-Gateway zurück, um zu versuchen, die Verbindung wiederaufzunehmen (es wird kein FIN-Paket gesendet).	Wenn eine Verbindung abläuft, sendet eine NAT-Instance ein FIN-Paket an die Ressourcen hinter der NAT-Instance, um die Verbindung zu beenden.

Attribut	NAT-Gateway	NAT-Instance
IP-Fragmentierung	Weiterleitung von IP-fragmentierten Paketen für das UDP-Protokoll wird unterstützt. Fragmentierung für das TCP- und ICMP-Protokoll wird nicht unterstützt. Fragmentierte Pakete werden für diese Protokolle verworfen.	Zusammenführung von IP-fragmentierten Paketen wird für das UDP-, TCP- und ICMP-Protokoll unterstützt.

Migrieren von einer NAT-Instance zu einem NAT-Gateway

Wenn Sie bereits eine NAT-Instance verwenden, empfehlen wir, diese durch ein NAT-Gateway zu ersetzen. Erstellen Sie dafür ein NAT-Gateway im selben Subnetz wie die NAT-Instance und ersetzen Sie die vorhandene Route in der Routing-Tabelle zur NAT-Instance durch eine Route zum NAT-Gateway. Wenn Sie dieselbe Elastic-IP-Adresse, die Sie für die NAT-Instance verwenden, für das NAT-Gateway verwenden möchten, müssen Sie die Zuordnung der Elastic-IP-Adresse zur NAT-Instance zunächst aufheben und sie beim Erstellen des NAT-Gateways dann diesem zuordnen.

Wenn Sie die Route von einer NAT-Instance auf ein NAT-Gateway ändern oder die Zuordnung der Elastic-IP-Adresse zur NAT-Instance aufheben, werden alle bestehenden Verbindungen getrennt und müssen neu hergestellt werden. Achten Sie darauf, dass keine wichtigen Aufgaben (oder Aufgaben auf der NAT-Instance) ausgeführt werden.

Zuordnen von elastischen IP-Adressen zu Ressourcen in Ihrer VPC

Die Elastic-IP-Adresse ist eine statische, öffentliche IPv4-Adresse, die für dynamisches Cloud Computing konzipiert ist. Sie können eine Elastic-IP-Adresse beliebigen Instances oder Netzwerkschnittstellen in beliebigen VPCs in Ihrem Konto zuordnen. Mit einer Elastic-IP-Adresse können Sie Ausfälle bei Instances maskieren. Weisen Sie dazu die Adresse einer anderen Instance in Ihrer VPC neu zu.

Elastic-IP-Adresskonzepte und -Regeln

Um eine Elastic-IP-Adresse verwenden zu können, weisen Sie sie zuerst für die Verwendung in Ihrem Konto zu. Anschließend können Sie sie einer Instance oder Netzwerkschnittstelle in Ihrer VPC

zuordnen. Ihre Elastic IP-Adresse bleibt Ihrem AWS Konto zugewiesen, bis Sie sie ausdrücklich freigeben.

Eine Elastic-IP-Adresse ist eine Eigenschaft einer Netzwerkschnittstelle. Sie können eine Elastic-IP-Adresse einer Instance zuweisen, indem Sie die mit der Instance verknüpfte Netzwerkschnittstelle aktualisieren. Der Vorteil der Zuordnung der Elastic-IP-Adresse zur Netzwerkschnittstelle anstatt direkt zur Instance liegt darin, dass Sie in nur einem Schritt alle Attribute der Netzwerkschnittstelle von einer Instance auf eine andere übertragen können. Weitere Informationen finden Sie unter Elastic Network Interfaces im Amazon EC2 EC2-Benutzerhandbuch.

Die folgenden Regeln gelten:

- Eine Elastic-IP-Adresse kann gleichzeitig einer einzelnen Instance oder Netzwerkschnittstelle zugeordnet werden.
- Sie können eine Elastic-IP-Adresse von einer Instance oder Netzwerkschnittstelle zu einer anderen verschieben.
- Wenn Sie eine Elastic-IP-Adresse einer eth0-Netzwerkschnittstelle einer Instance zuweisen, wird die aktuelle öffentliche IPv4-Adresse (sofern vorhanden) für den öffentlichen IP-Adress-Pool der EC2-VPC freigegeben. Wenn Sie die Zuordnung der Elastic-IP-Adresse aufheben, wird der eth0-Netzwerkschnittstelle automatisch innerhalb weniger Minuten eine neue öffentliche IPv4-Adresse zugewiesen. Dies gilt jedoch nicht, wenn Sie eine zweite Netzwerkschnittstelle mit der Instance verknüpft haben.
- Sie sind auf fünf Elastic-IP-Adressen beschränkt. Um diese Zahl nicht auszuschöpfen, können Sie ein NAT-Gerät verwenden. Weitere Informationen finden Sie unter Herstellen einer Verbindung mit dem Internet oder anderen Netzwerken über NAT-Geräte.
- Elastic-IP-Adressen für IPv6 werden nicht unterstützt.
- Sie können eine Elastic-IP-Adresse, die einer VPC zugeordnet ist, markieren. Kostenzuordnungs-Tags werden jedoch nicht unterstützt. Wenn Sie eine Elastic-IP-Adresse wiederherstellen, werden Tags jedoch nicht mit wiederhergestellt.
- Sie können über das Internet auf eine Elastic-IP-Adresse zugreifen, wenn die Sicherheitsgruppe und die Netzwerk-ACL den Datenverkehr von der Quell-IP-Adresse zulassen. Für den Antwortdatenverkehr aus der VPC zurück ins Internet ist ein Internet-Gateway erforderlich. Weitere Informationen erhalten Sie unter Sicherheitsgruppen und Netzwerk-ACLs.
- Sie können eine der folgenden Optionen für die Elastic-IP-Adressen verwenden:
  - Amazon soll die Elastic-IP-Adressen bereitstellen. Wenn Sie diese Option auswählen, 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.

- Verwenden Sie Ihre eigenen IP-Adressen. Informationen zum Mitbringen eigener IP-Adressen finden Sie unter Bring your own IP Addresses (BYOIP) im Amazon EC2 EC2-Benutzerhandbuch.

Elastische IP-Adressen sind regional. Weitere Informationen zur Verwendung von Global Accelerator zur Bereitstellung globaler IP-Adressen finden Sie unter Verwendung globaler statischer IP-Adressen anstelle von regionalen statischen IP-Adressen im AWS Global Accelerator -Entwicklerhandbuch.

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
- So ordnen Sie eine Elastic-IP-Adresse zu
- So zeigen Sie Ihre Elastic-IP-Adressen an
- Markieren einer Elastic-IP-Adresse
- Aufheben der Zuordnung einer Elastic-IP-Adresse
- Übertragen von Elastic-IP-Adressen
- Freigeben einer Elastic-IP-Adresse
- Wiederherstellen einer Elastic-IP-Adresse
- Überblick über die API und Befehlszeile

Zuweisen einer Elastic-IP-Adresse

Bevor Sie eine Elastic-IP-Adresse verwenden, müssen Sie sie für die Verwendung in Ihrer VPC zuweisen.

So weisen Sie eine Elastic IP-Adresse zu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
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 (siehe Local Zones). 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 IP addresses (Amazon-Pool von IP-Adressen) – Wenn Sie möchten, dass eine IPv4-Adresse aus dem Amazon-Pool von IP-Adressen zugewiesen werden soll.

- Mein Pool öffentlicher IPv4-Adressen — Wenn Sie eine IPv4-Adresse aus einem IP-Adresspool zuweisen möchten, den Sie Ihrem Konto hinzugefügt haben. AWS Diese Option ist deaktiviert, wenn Sie keine IP-Adresspools haben.
- Kundeneigener Pool von IPv4-Adressen – Wenn Sie eine IPv4-Adresse aus einem Pool zuweisen möchten, der von Ihrem On-Premises-Netzwerk für die Verwendung mit einem Außenposten erstellt wurde. Diese Option ist nur dann aktiviert, wenn Sie einen Außenposten haben.

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.

So ordnen Sie eine Elastic-IP-Adresse zu

Sie können eine Elastic-IP-Adresse einer laufenden Instance oder Netzwerkschnittstelle in Ihrer VPC zuordnen.

Nachdem Sie die Elastic-IP-Adresse der Instance zugeordnet haben, erhält sie einen öffentlichen DNS-Hostnamen, sofern DNS-Hostnamen aktiviert sind. Weitere Informationen finden Sie unter DNS-Attribute für Ihre VPC.

So ordnen Sie eine Elastic-IP-Adresse einer Instance oder Netzwerkschnittstelle zu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie eine Elastic-IP-Adresse aus, die einer VPC zur Verwendung zugeordnet ist (die Spalte Scope (Bereich) hat den Wert `vpc`), klicken Sie auf Actions (Aktionen) und anschließend auf Associate address (Adresse zuordnen).

4. Wählen Sie Instance oder Network interface und anschließend entweder die Instance oder die Netzwerkschnittstellen-ID aus. Wählen Sie die private IP-Adresse aus, der die Elastic-IP-Adresse zugeordnet werden soll. Wählen Sie Associate aus.

So zeigen Sie Ihre Elastic-IP-Adressen an

Sie können die Elastic-IP-Adressen anzeigen, die Ihrem Konto zugeordnet sind.

So zeigen Sie Ihre Elastic-IP-Adressen an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Um die angezeigte Liste zu filtern, geben Sie einen Teil der Elastic-IP-Adresse oder eines ihrer Attribute in das Suchfeld ein.

Markieren einer Elastic-IP-Adresse

Sie können Ihre Elastic-IP-Adresse markieren, um sie identifizieren oder in Übereinstimmung mit den Anforderungen Ihrer Organisation kategorisieren zu können.

Markieren einer Elastic IP-Adresse

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die Elastic-IP-Adresse aus und klicken Sie anschließend auf Tags.
4. Wählen Sie Add/Manage Tags (Tags verwalten) aus, geben Sie die erforderlichen Tag-Schlüssel und Werte ein und klicken Sie anschließend auf Save (Speichern).

Aufheben der Zuordnung einer Elastic-IP-Adresse

Um die Ressource zu ändern, der die Elastic-IP-Adresse zugeordnet ist, müssen Sie sie zunächst von der aktuell zugeordneten Ressource trennen.

So heben Sie die Zuordnung einer Elastic-IP-Adresse auf

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Elastic IPs.

3. Wählen Sie die Elastic-IP-Adresse und dann nacheinander Actions (Aktionen), Disassociate Elastic IP address (Elastic-IP-Adresse trennen) aus.
4. Klicken Sie im Bestätigungsdialogfeld auf Disassociate (Trennen).

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.

So aktivieren Sie die Übertragung von Elastic-IP-Adressen

1. Stellen Sie sicher, dass Sie das AWS Quellkonto verwenden.
2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
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.

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.

So deaktivieren Sie die Übertragung einer Elastic-IP-Adresse

1. Stellen Sie sicher, dass Sie das AWS Quellkonto verwenden.
2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
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.

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 Elastic IP Address Limit im Amazon EC2 EC2-Benutzerhandbuch.
- 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 Entfernen eines Reverse-DNS-Eintrags im Amazon EC2 EC2-Benutzerhandbuch.
- 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 Trennen einer Elastic IP-Adresse im Amazon EC2 EC2-Benutzerhandbuch.

Für alle anderen Ausnahmen wenden Sie sich an AWS Support.

Diese Schritte müssen von dem Übertragungskonto ausgeführt werden.

So akzeptieren Sie die Übertragung einer Elastic-IP-Adresse

1. Stellen Sie sicher, dass Sie das Übertragungskonto verwenden.
2. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
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.

Freigeben einer Elastic-IP-Adresse

Wenn Sie eine Elastic-IP-Adresse nicht mehr benötigen, empfehlen wir, diese freizugeben. Es fallen für jede zur Verwendung in einer VPC zugeordnete Elastic-IP-Adresse, die keiner Instance zugeordnet ist, Gebühren an. Die Elastic-IP-Adresse darf keiner Instance oder Netzwerkschnittstelle zugeordnet werden.

So geben Sie eine Elastic-IP-Adresse frei

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Elastic IPs.
3. Wählen Sie die Elastic-IP-Adresse aus und dann nacheinander Actions (Aktionen), Release Elastic IP addresses (Elastic-IP-Adressen freigeben) aus.

4. Klicken Sie im Bestätigungsdialogfeld auf Release.

Wiederherstellen einer Elastic-IP-Adresse

Wenn Sie eine Elastic-IP-Adresse freigeben, aber Ihre Meinung ändern, können Sie sie möglicherweise wiederherstellen. Sie können die Elastic IP-Adresse nicht wiederherstellen, wenn sie einem anderen AWS Konto zugewiesen wurde oder wenn Ihre Wiederherstellung dazu führt, dass Sie Ihr Elastic IP-Adresskontingent überschreiten.

Sie können eine Elastic-IP-Adresse mit der Amazon EC2 API oder einem Befehlszeilen-Tool wiederherstellen.

Um eine Elastic IP-Adresse wiederherzustellen, verwenden Sie AWS CLI

Verwenden Sie den Befehl allocate-address und geben Sie die IP-Adresse mit dem Parameter `--address` an.

```
aws ec2 allocate-address --domain vpc --address 203.0.113.3
```

Überblick über die API und Befehlszeile

Sie können die in diesem Abschnitt beschriebenen Aufgaben über die Befehlszeile oder eine API ausführen. Weitere Informationen über Befehlszeilenschnittstellen und eine Liste der verfügbaren API-Aktionen finden Sie unter Arbeiten mit Amazon VPC.

Akzeptieren der Übertragung einer Elastic-IP-Adresse

- accept-address-transfer (AWS CLI)
- Approve-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Zuweisen einer Elastic-IP-Adresse

- allocate-address (AWS CLI)
- New-EC2Address (AWS Tools for Windows PowerShell)

Zuordnen einer Elastic IP-Adresse zu einer Instance oder Netzwerkschnittstelle

- associate-address (AWS CLI)

- Register-EC2Address (AWS Tools for Windows PowerShell)

Beschreiben der Übertragungen von Elastic-IP-Adressen

- describe-address-transfers (AWS CLI)
- Get-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Deaktivieren der Übertragung von Elastic-IP-Adressen

- adressübertragung deaktivieren (AWS CLI)
- Disable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Aufheben der Zuordnung einer Elastic-IP-Adresse

- disassociate-address (AWS CLI)
- Unregister-EC2Address (AWS Tools for Windows PowerShell)

Aktivieren der Übertragung von Elastic-IP-Adressen

- enable-address-transfer (AWS CLI)
- Enable-EC2AddressTransfer (AWS Tools for Windows PowerShell)

Freigeben einer Elastic-IP-Adresse

- release-address (AWS CLI)
- Remove-EC2Address (AWS Tools for Windows PowerShell)

Markieren einer Elastic-IP-Adresse

- create-tags (AWS CLI)
- New-EC2Tag (AWS Tools for Windows PowerShell)

So zeigen Sie Ihre Elastic-IP-Adressen an

- describe-addresses (AWS CLI)

- Get-EC2Address (AWS Tools for Windows PowerShell)

Preisgestaltung

Um eine effiziente Nutzung von Elastic IP-Adressen zu gewährleisten, erheben wir eine geringe stündliche Gebühr. Weitere Informationen finden Sie unter Öffentliche IPv4-Adresse in Preise für Amazon VPC.

Verbinden Ihrer VPC mit anderen VPCs und Netzwerken über ein Transit-Gateway

Sie können Ihre Virtual Private Clouds (VPCs) und lokalen Netzwerke über ein Transit-Gateway verbinden, das als zentraler Hub fungiert und den Datenverkehr zwischen VPCs, VPN-Verbindungen und AWS Direct Connect-Verbindungen weiterleitet. Weitere Informationen finden Sie unter AWS Transit Gateway.

In der folgenden Tabelle werden einige gängige Anwendungsfälle für Transit-Gateways beschrieben. Außerdem enthält sie Links zu weiteren Informationen in Transit-Gateways für Amazon VPC.

Beispiel	Verwendung
Zentralisierter Router	Konfigurieren Sie Ihr Transit Gateway als zentralisierten Router, der alle Ihre VPCs, AWS Direct Connect- und AWS Site-to-Site VPN-Verbindungen miteinander verbindet. Weitere Informationen finden Sie unter Beispiel: Zentralisierter Router.
Isolierte VPCs	Konfigurieren Sie Ihr Transit-Gateway als mehrere isolierte Router. Dies gleicht der Verwendung mehrerer Transit-Gateways, bietet aber mehr Flexibilität, falls sich die Routen und Anfügungen ändern. Weitere Informationen finden Sie unter Beispiel: Isolierte VPCs.
Isolierte VPCs mit freigegeben Services	Konfigurieren Sie Ihr Transit-Gateway als mehrere isolierte Router, die einen freigegebenen Service verwenden. Dies gleicht der Verwendung mehrerer Transit-Gateways, bietet aber mehr Flexibilität, falls sich die Routen und Anfügungen ändern.

Beispiel	Verwendung
	Weitere Informationen finden Sie unter Beispiele: Isolierte VPCs mit freigegebenen Services.

Verbinden Ihrer VPC mit Remote-Netzwerken über AWS Virtual Private Network

Sie können Ihre VPC mit den folgenden VPN-Konnektivitätsoptionen mit entfernten Netzwerken und Benutzern verbinden.

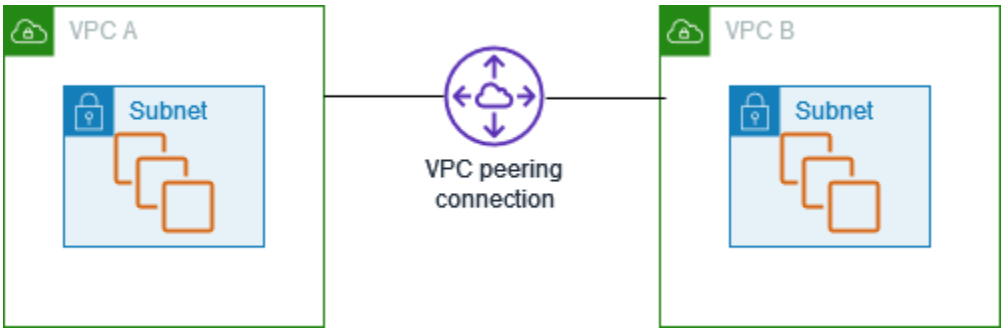
VPN-Konnektivitätsoption	Beschreibung
AWS Site-to-Site VPN	Sie können eine IPsec-VPN-Verbindung zwischen Ihrer VPC und Ihrem Remote-Netzwerk einrichten. Auf der AWS-Seite der Site-to-Site VPN-Verbindung stellt ein Virtual Private Gateway bzw. ein Transit-Gateway zwei VPN-Endpunkte (Tunnel) bereit, um ein automatisches Failover zu ermöglichen. Sie konfigurieren Ihr Kunden-Gateway-Gerät auf der Remote-Seite der Site-to-Site VPN-Verbindung. Weitere Informationen finden Sie im AWS Site-to-Site VPN-Benutzerhandbuch.
AWS Client VPN	AWS Client VPN ist ein verwalteter clientbasierter VPN-Service, der Ihnen einen sicheren Zugriff auf Ihre AWS-Ressourcen oder auf Ihr On-Premises-Netzwerk ermöglicht. Mit AWS Client VPN konfigurieren Sie einen Endpunkt, zu dem Ihre Benutzer eine Verbindung herstellen und so eine sichere TLS-VPN-Sitzung einrichten können. So können Clients über einen OpenVPN-basierten VPN-Client standortunabhängig auf Ressourcen in AWS oder in einem On-Premises-Netzwerk zugreifen. Weitere Informationen finden Sie im Administrationshandbuch zu AWS Client VPN.
AWS VPN CloudHub	Wenn Sie über mehrere Remote-Netzwerke verfügen (beispielsweise bei mehreren Zweigstellen), können Sie über Ihr Virtual Private Gateway mehrere AWS Site-to-Site VPN-Verbindungen erstellen, um die Kommunikation zwischen diesen Netzwerken zu ermöglich

VPN-Konnektivitäts option	Beschreibung
	en. Weitere Informationen finden Sie unter Sichere Kommunikation zwischen Standorten über VPN CloudHub im AWS Site-to-Site VPN-Benutzerhandbuch.
Softwarebasierte VPN-Anwendung von Drittanbieter	Sie können eine VPN-Verbindung zu Ihrem Remote-Netzwerk erstellen , indem Sie eine Amazon EC2-Instance in Ihrer VPC verwenden, auf der eine softwarebasierte VPN-Appliance eines Drittanbieters ausgeführ t wird. AWS stellt softwarebasierte VPN-Appliances von Drittanbietern weder bereit noch wartet es diese. Sie können jedoch aus einer breiten Auswahl an Produkten, die von Partnern und Open-Source-Commun ities angeboten werden, wählen. Hier finden Sie softwarebasierte VPN-Appliances von Drittanbietern: AWS Marketplace.

Zudem können mit AWS Direct Connect eine dedizierte, private Verbindung zwischen einem Remote-Netzwerk und Ihrer VPC herstellen. Sie können diese Verbindung mit einer AWS Site-to-Site VPN kombinieren, um eine durch IPsec verschlüsselte Verbindung zu erstellen. Weitere Informationen finden Sie unter Was ist AWS Direct Connect? im AWS Direct Connect-Benutzerhandbuch.

Verbinden von VPCs mit VPC-Peering

Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs, die den privaten Datenverkehr zwischen diesen beiden VPCs ermöglicht. Ressourcen in peered VPCs können so miteinander kommunizieren, als befänden sie sich im selben Netzwerk. Sie können eine VPC-Peering-Verbindung zwischen Ihren eigenen VPCs, mit einer VPC in einem anderen AWS-Konto oder mit einer VPC in einer anderen AWS-Region herstellen. Der Datenverkehr zwischen über Peering verbundenen VPCs wird niemals über das öffentliche Internet übertragen.



AWS verwendet die vorhandene Infrastruktur einer VPC zum Erstellen einer VPC-Peering-Verbindung. Eine VPC-Peering-Verbindung ist weder ein Gateway noch um eine AWS Site-to-Site VPN-Verbindung und die Verbindung basiert auch nicht auf spezieller physischer Hardware. Es gibt keine einzelne Fehlerstelle für die Kommunikation und keinen Bandbreiten-Engpass.

Weitere Informationen finden Sie im Benutzerhandbuch zu Amazon VPC Peering.

Überwachen Ihrer VPC

Mithilfe der folgenden Tools können Sie den Datenverkehr oder Netzwerkzugriff in Ihrer Virtual Private Cloud (VPC) überwachen.

VPC Flow Logs

Mit VPC Flow Logs können Sie detaillierte Informationen über den ein- und ausgehenden Datenverkehr in Ihren VPCs erfassen.

Amazon VPC IP Address Manager (IPAM)

Mit IPAM können Sie IP-Adressen für Ihre Workloads planen, verfolgen und überwachen. Weitere Informationen finden Sie unter IP Address Manager.

Datenverkehrsspiegelung

Mit dieser Funktion können Sie den Netzwerkverkehr aus einer Netzwerkschnittstelle einer Amazon-EC2-Instance kopieren und zur ausführlichen Untersuchung von Paketen an externe Sicherheits- und Überwachungs-Appliances senden. So können Sie Netzwerk- und Sicherheitsanomalien erkennen, betriebliche Erkenntnisse gewinnen, Compliance- und Sicherheitskontrollen implementieren und Probleme beheben. Weitere Informationen finden Sie unter Datenverkehrsspiegelung.

Reachability Analyzer

Mit diesem Tool können Sie die Netzwerkerreichbarkeit zwischen zwei Ressourcen in Ihrer VPC analysieren und debuggen. Nach Angabe der Quell- und Zielressource erstellt Reachability Analyzer Hop-by-Hop-Details des virtuellen Pfads zwischen ihnen, wenn sie erreichbar sind, und identifiziert die blockierende Komponente, falls sie nicht erreichbar sind. Weitere Informationen finden Sie unter Reachability Analyzer.

Network Access Analyzer

Mit Network Access Analyzer können Sie den Netzwerkzugriff auf die eigenen Ressourcen analysieren. So können Sie leichter Verbesserungen für die Sicherheit Ihres Netzwerks identifizieren und zeigen, dass das Netzwerk bestimmte Compliance-Anforderungen erfüllt. Weitere Informationen finden Sie unter Network Access Analyzer.

CloudTrail-Protokolle

Mit AWS CloudTrail können Sie detaillierte Informationen zu den Aufrufen der Amazon-VPC-API erfassen. Anhand der generierten CloudTrail-Protokolle können Sie die durchgeführten Aufrufe,

die Quell-IP-Adresse, von der der jeweilige Aufruf stammte, den Aufrufenden, den Zeitpunkt des Aufrufs usw. ermitteln. Weitere Informationen finden Sie unter Protokollierung von Aufrufen der Amazon-EC2-, Amazon-EBS- und Amazon-VPC-API mit AWS CloudTrail in der Referenz zur Amazon-EC2-API.

Protokollieren von IP-Datenverkehr mit VPC Flow Logs

VPC Flow Logs ist ein Feature, mit der Sie Informationen über den IP-Datenverkehr zu und von Netzwerkschnittstellen in Ihrer VPC erfassen können. Flow-Protokolldaten können an den folgenden Speicherorten veröffentlicht werden: Amazon CloudWatch Logs, Amazon S3 oder Amazon Data Firehose. Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie die Flow-Protokolldatensätze in der von Ihnen konfigurierten Protokollgruppe, dem Bucket oder dem Bereitstellungsstream abrufen und anzeigen.

Mit Flow-Protokollen können Sie eine Reihe von Aufgaben ausführen, z. B.:

- Diagnose übermäßig restriktiver Sicherheitsgruppenregeln
- Überwachen des Datenverkehrs, der auf Ihrer Instance eintrifft
- Ermitteln der Richtung des Datenverkehrs zu und von den Netzwerkschnittstellen

Flow-Potokolldaten werden außerhalb des Pfades des Netzwerkdatenverkehrs erfasst und wirken sich daher nicht auf den Netzwerkdurchsatz oder die Latenz aus. Sie können Flow-Protokolle erstellen oder löschen, ohne dass die Netzwerkleistung beeinträchtigt wird.

> **Note**
>
> In diesem Abschnitt geht es nur um Flow-Logs für VPCs. Informationen zu Flow-Protokollen für Transit-Gateways, die in Version 6 eingeführt wurden, finden Sie unter Protokollieren von Netzwerkverkehr mithilfe von Transit Gateway Flow Logs im Amazon VPC Transit Gateways-Benutzerhandbuch.

Inhalt

Grundlagen zu Flow-Protokollen

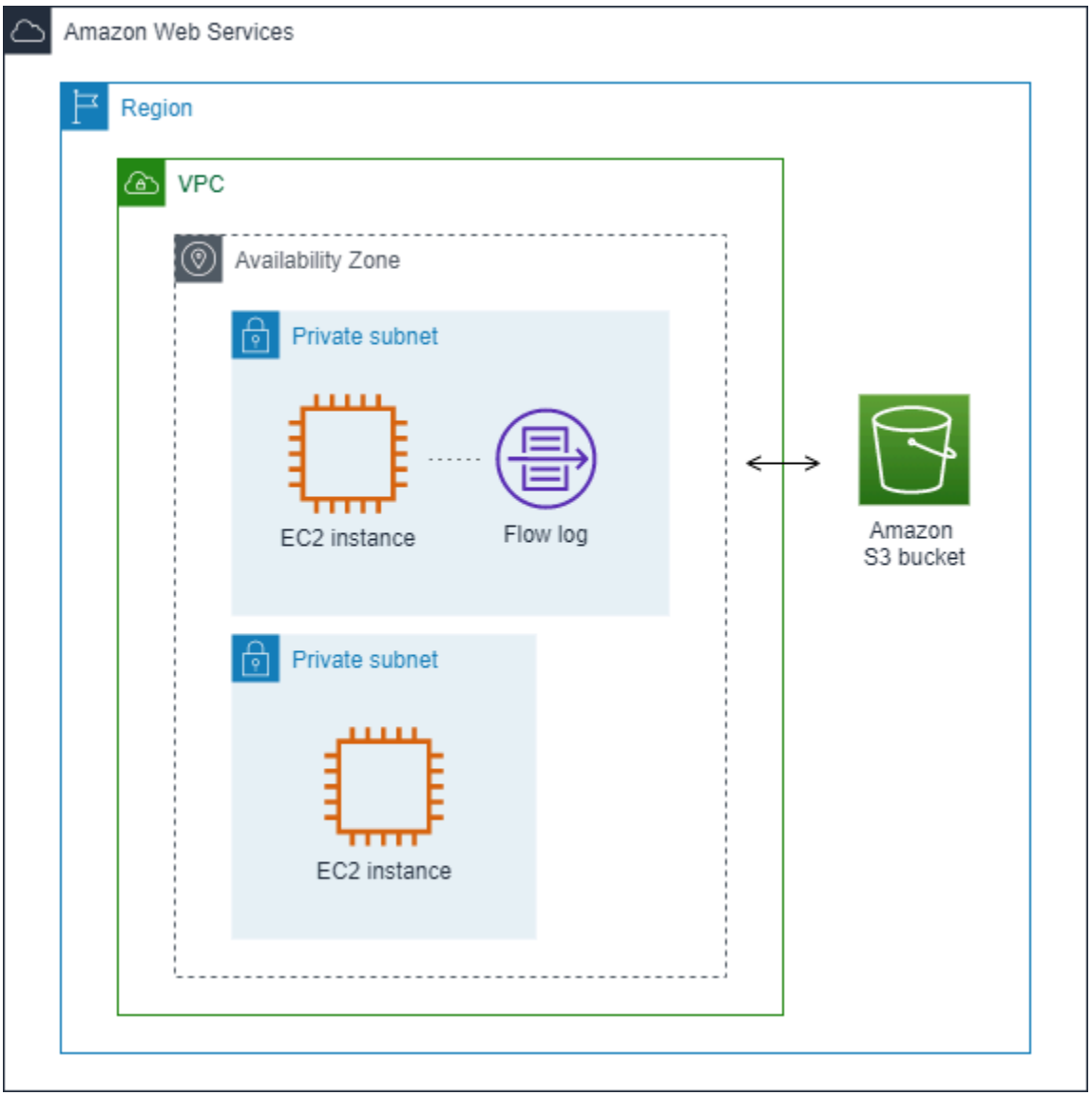
Sie können Flow-Protokolle für VPCs, Subnetze oder Netzwerkschnittstellen erstellen. Wenn Sie ein Flow-Protokoll für ein Subnetz oder eine VPC erstellen, werden alle Netzwerkschnittstellen innerhalb dieses Subnetzes oder der VPC überwacht.

Flow-Protokolldaten für eine überwachte Netzwerkschnittstelle werden als Flow-Protokolldatensätze aufgezeichnet. Hierbei handelt es sich um Protokollereignisse bestehend aus Feldern, die den Datenfluss beschreiben. Weitere Informationen finden Sie unter Flow-Protokolldatensätze.

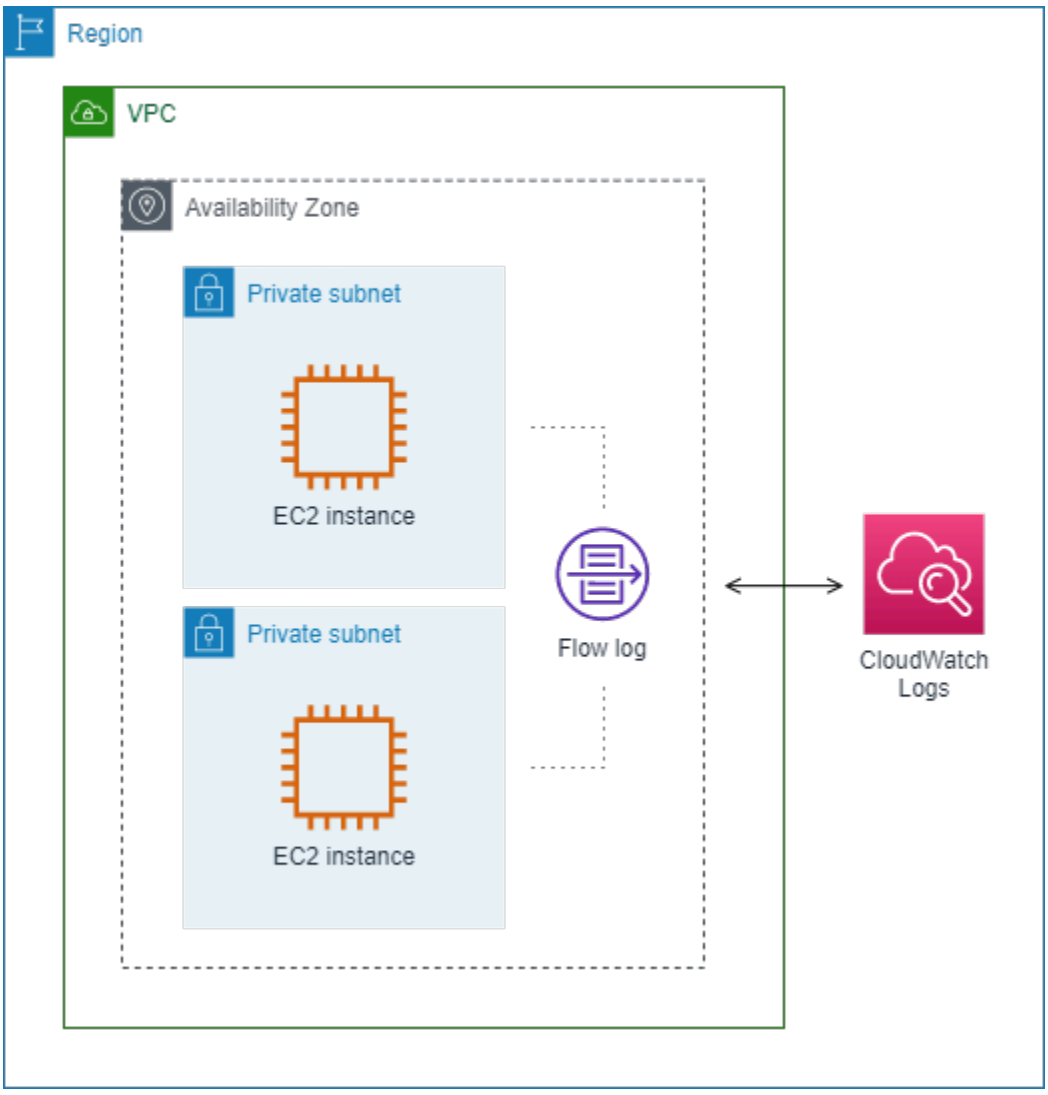
Für die Erstellung eines Flow-Protokolls geben Sie Folgendes an:

- Die Ressource, für die das Flow-Protokoll erstellt werden soll
- Den Typ des zu erfassenden Datenverkehrs (zulässiger Datenverkehr, abgelehnter Datenverkehr oder gesamter Datenverkehr)
- Die Ziele, an die die Flow-Protokolldaten veröffentlicht werden sollen.

Im folgenden Beispiel erstellen Sie ein Flow-Protokoll, das den akzeptierten Datenverkehr für die Netzwerkschnittstelle einer der EC2-Instances in einem privaten Subnetz erfasst und die Flow-Protokollsätze in einem Amazon-S3-Bucket veröffentlicht.



Im folgenden Beispiel erfasst ein Flow-Protokoll den gesamten Datenverkehr für ein Subnetz und veröffentlicht die Flow-Protokolldatensätze in Amazon CloudWatch Logs. Das Flow-Protokoll erfasst den Datenverkehr für alle Netzwerkschnittstellen im Subnetz.



Nach dem Erstellen eines Flow-Protokolls kann es einige Minuten dauern, bis Daten erfasst und an den gewünschten Zielen veröffentlicht werden. Flow-Protokolle erfassen keine Echtzeitprotokollstreams für Ihre Netzwerkschnittstellen. Weitere Informationen finden Sie unter Erstellen eines Flow-Protokolls.

Wenn Sie eine Instance in Ihrem Subnetz starten, nachdem Sie ein Flow-Log für Ihr Subnetz oder Ihre VPC erstellt haben, erstellen wir einen Log-Stream (für CloudWatch Logs) oder ein Protokolldatei-Objekt (für Amazon S3) für die neue Netzwerkschnittstelle, sobald Netzwerkverkehr für die Netzwerkschnittstelle vorhanden ist.

Sie können Flow-Protokolle für Netzwerkschnittstellen erstellen, die von anderen AWS -Services erstellt wurden, z. B.:

- Elastic Load Balancing

- Amazon RDS
- Amazon ElastiCache
- Amazon-Redshift
- Amazon WorkSpaces
- NAT-Gateways
- Transit-Gateways

Unabhängig von der Art der Netzwerkschnittstelle müssen Sie die Amazon EC2-Konsole oder die Amazon EC2-API verwenden, um ein Flow-Protokoll für eine Netzwerkschnittstelle zu erstellen.

Sie können auf Ihre Flow-Protokolle Tags anwenden. Jeder Tag besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen. Tags können Ihnen dabei helfen, Ihre Flow-Protokolle zu organisieren, z. B. nach Zweck oder Besitzer.

Wenn Sie ein Flow-Protokoll nicht mehr benötigen, können Sie es löschen. Durch das Löschen eines Flow-Protokolls wird der Flow-Protokoll-Service für die Ressource deaktiviert, so dass keine neuen Flow-Protokollsätze erstellt oder veröffentlicht werden. Durch das Löschen eines Flow-Protokolls werden keine vorhandenen Flow-Protokolldaten gelöscht. Nachdem Sie ein Flow-Protokoll gelöscht haben, können Sie die Flow-Protokolldaten direkt vom Ziel löschen, wenn Sie damit fertig sind. Weitere Informationen finden Sie unter Löschen eines Flow-Protokolls.

Flow-Protokolldatensätze

Ein Flow-Protokolldatensatz repräsentiert einen Netzwerk-Flow in Ihrer VPC. Standardmäßig erfasst jeder Datensatz einen Netzwerk-Internetprotokoll-(IP)-Datenverkehrsfluss (gekennzeichnet durch ein 5-Tupel auf der Basis der einzelnen Netzwerkschnittstellen), der innerhalb eines Aggregationsintervalls auftritt, das auch als Erfassungsfenster bezeichnet wird.

Jeder Datensatz ist ein String mit durch Leerzeichen getrennten Feldern. Der Datensatz enthält Werte für die verschiedenen Komponenten des IP-Flows, zum Beispiel Quelle, Ziel und Protokoll.

Wenn Sie ein Flow-Protokoll erstellen, können Sie das Standardformat für den Flow-Protokolldatensatz verwenden oder ein benutzerdefiniertes Format angeben.

Inhalt

- Standardformat
- Benutzerdefiniertes Format
- Verfügbare Felder

Aggregationsintervall

Das Aggregationsintervall ist der Zeitraum, in dem ein bestimmter Flow erfasst und zu einem Flow-Protokolldatensatz aggregiert wird. Standardmäßig beträgt das maximale Aggregationsintervall 10 Minuten. Wenn Sie ein Flow-Protokoll erstellen, können Sie optional ein maximales Aggregationsintervall von 1 Minute angeben. Flow-Protokolle mit einem maximalen Aggregationsintervall von 1 Minute erzeugen ein höheres Volumen an Flow-Protokoll-Datensätzen als Flow-Protokolle mit einem maximalen Aggregationsintervall von 10 Minuten.

Wenn eine Netzwerkschnittstelle einer Nitro-basierten Instance zugewiesen ist, beträgt das Aggregationsintervall immer 1 Minute oder weniger, unabhängig vom angegebenen maximalen Aggregationsintervall.

Nachdem Daten innerhalb eines Aggregationsintervalls erfasst wurden, nimmt die Verarbeitung und Veröffentlichung der Daten in CloudWatch Logs oder Amazon S3 zusätzliche Zeit in Anspruch. Der Flow Log-Service übermittelt Protokolle in der Regel in etwa 5 Minuten an CloudWatch Logs und in etwa 10 Minuten an Amazon S3. Die Protokollbereitstellung erfolgt jedoch nach bestem Bemühen, und Ihre Protokolle können über die typische Lieferzeit hinaus verzögert werden.

Standardformat

Mit dem Standardformat enthalten die Flow-Protokolldatensätze die Felder der Version 2 in der Reihenfolge, die in der Tabelle Verfügbare Felder angezeigt wird. Das Standardformat kann nicht angepasst oder geändert werden. Um zusätzliche Felder oder eine unterschiedliche Teilmenge an Feldern zu erfassen, müssen Sie stattdessen ein benutzerdefiniertes Format angeben.

Benutzerdefiniertes Format

Mit einem benutzerdefinierten Format geben Sie an, welche Felder in den Flow-Protokolldatensätzen in welcher Reihenfolge enthalten sind. Auf diese Weise können Sie spezifische Flow-Protokolle für Ihre Anforderungen erstellen und Felder auslassen, die nicht relevant sind. Ein benutzerdefiniertes Format kann dazu beitragen, dass weniger separate Prozesse erforderlich sind, um spezifische Informationen aus veröffentlichten Flow-Protokollen zu extrahieren. Sie können eine beliebige Anzahl an verfügbaren Flow-Protokollfeldern angeben, Sie müssen jedoch mindestens eins angeben.

Verfügbare Felder

Die folgende Tabelle beschreibt alle verfügbaren Felder für einen Flow-Protokolldatensatz. In der Spalte Version wird die Version des VPC-Flow-Protokolls angegeben, in der das Feld eingeführt wurde. Das Standardformat enthält alle Felder der Version 2 in der Reihenfolge, in der sie in der Tabelle angezeigt werden.

Beim Veröffentlichen von Flow-Protokoll-Daten in Amazon S3 hängt der Datentyp für die Felder vom Flow-Protokoll-Format ab. Wenn das Format reiner Text ist, sind alle Felder vom Typ STRING. Wenn das Format Parquet ist, lesen Sie die Tabelle für die Felddatentypen.

Wenn ein Feld für einen bestimmten Datensatz nicht anwendbar ist oder nicht verarbeitet werden konnte, wird für diesen Eintrag „-“ angezeigt. Metadatenfelder, die nicht direkt aus dem Paket-Header stammen, sind Best-Effort-Annäherungen, und ihre Werte können fehlen oder ungenau sein.

Feld	Beschreibung	Version
version	Die Version des VPC-Flow-Protokolls. Wenn Sie das Standardformat verwenden, lautet die Version 2. Wenn Sie ein benutzerdefiniertes Format verwenden, ist die Version die höchste Version unter den angegebenen Feldern. Wenn Sie beispielsweise nur Felder aus Version 2 angeben, lautet die Version 2. Wenn Sie eine Mischung aus Feldern aus den Versionen 2, 3 und 4 angeben, lautet die Version 4. Parquet-Datentyp: INT_32	2
account-id	Die AWS Konto-ID des Besitzers der Quellnetzwerkschnittstelle, für die der Datenverkehr aufgezeichnet wird. Wenn die Netzwerkschnittstelle von einem AWS Dienst erstellt wird, z. B. beim Erstellen eines VPC-Endpunkts oder eines Network Load Balancer, wird der Datensatz möglicherweise unknown für dieses Feld angezeigt. Parquet-Datentyp: STRING	2
interface-id	Die ID der Netzwerkschnittstelle, für die der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: SCHNUR	2

Feld	Beschreibung	Version
srcaddr	Die Quelladresse für eingehenden Datenverkehr oder die IPv4- oder IPv6-Adresse der Netzwerkschnittstelle für ausgehenden Datenverkehr an der Netzwerkschnittstelle. Die IPv4-Adresse der Netzwerkschnittstelle ist immer deren private IPv4-Adresse. Weitere Informationen finden Sie auch unter pkt-srcaddr. Parquet-Datentyp: SCHNUR	2
dstaddr	Die Zieladresse für ausgehenden Datenverkehr oder die IPv4- oder IPv6-Adresse der Netzwerkschnittstelle für eingehenden Datenverkehr an der Netzwerkschnittstelle. Die IPv4-Adresse der Netzwerkschnittstelle ist immer deren private IPv4-Adresse. Weitere Informationen finden Sie auch unter pkt-dstaddr. Parquet-Datentyp: SCHNUR	2
srcport	Der Quellport des Datenverkehrs Parquet-Datentyp: INT_32	2
dstport	Der Zielport des Datenverkehrs Parquet-Datentyp: INT_32	2
protocol	Die IANA-Protokollnummer des Datenverkehrs. Weitere Informationen finden Sie unter Zugewiesene IP-Nummern. Parquet-Datentyp: INT_32	2
packets	Die Anzahl der Pakete, die während des Flows übertragen wurden Parquet-Datentyp: INT_64	2
bytes	Die Anzahl der Bytes, die während des Flows übertragen wurden Parquet-Datentyp: INT_64	2

Feld	Beschreibung	Version
start	Die Zeit, in Unix-Sekunden, in der das erste Paket des Flows innerhalb des Aggregationsintervalls empfangen wurde. Dies kann bis zu 60 Sekunden dauern, nachdem das Paket auf der Netzwerks chnittstelle übertragen oder empfangen wurde. Parquet-Datentyp: INT_64	2
end	Die Zeit, in Unix-Sekunden, in der das letzte Paket des Flows innerhalb des Aggregationsintervalls empfangen wurde. Dies kann bis zu 60 Sekunden dauern, nachdem das Paket auf der Netzwerks chnittstelle übertragen oder empfangen wurde. Parquet-Datentyp: INT_64	2
action	Die mit dem Datenverkehr verknüpfte Aktion: • ACCEPT – Der Verkehr wurde akzeptiert. • REJECT – Der Verkehr wurde abgelehnt. Beispielsweise wurde der Datenverkehr von den Sicherheitsgruppen oder Netzwerk-ACLs nicht zugelassen, oder Pakete kamen an, nachdem die Verbindung geschlossen wurde. Parquet-Datentyp: STRING	2
log-status	Der Protokollstatus des Flow-Protokolls: • OK – Daten werden normal auf den ausgewählten Zielen protokoll iert. • NODATA – Es gab während des Aggregationsintervalls keinen Datenverkehr von oder zur Netzwerkschnittstelle. • SKIPDATA – Einige Flow-Protokolldatensätze wurden während des Aggregationsintervalls übersprungen. Dies kann an internen Kapazitätsbeschränkungen oder einem internen Fehler liegen. Parquet-Datentyp: STRING	2

Feld	Beschreibung	Version
vpc-id	Die ID der VPC mit der Netzwerkschnittstelle, für die der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: SCHNUR	3
subnet-id	Die ID des Subnetzes mit der Netzwerkschnittstelle, für die der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: SCHNUR	3
instance-id	Die ID der Instance, die mit der Netzwerkschnittstelle verbunden ist, für die der Datenverkehr aufgezeichnet wird, sofern die Instance Ihnen gehört. Gibt das Symbol '-' für eine vom Anforderer verwaltete Netzwerkschnittstelle zurück, wie beispielsweise die Netzwerkschnittstelle für ein NAT-Gateway. Parquet-Datentyp: SCHNUR	3

Feld	Beschreibung	Version
tcp-flags	Der Bitmasken-Wert für die folgenden TCP-Flags: • FIN — 1 • SYN — 2 • RST — 4 • SYN-ACK — 18 Wenn keine unterstützten Flags aufgezeichnet werden, ist der TCP-Flag-Wert 0. Da tcp-flags beispielsweise die Protokollierung von ACK- oder PSH-Flags nicht unterstützt, führen Datensätze für Datenverkehr mit diesen nicht unterstützten Flags zu einem tcp-flags-Wert von 0. Wenn jedoch ein nicht unterstütztes Flag von einem unterstützten Flag begleitet wird, geben wir den Wert des unterstützten Flags an. Wenn ACK beispielsweise Teil von SYN-ACK ist, wird 18 angegeben. Und wenn es einen Datensatz wie SYN+ECE gibt, ist der TCP-Flaggenwert 2, da SYN ein unterstützt es Flag ist und ECE nicht. Wenn die Flag-Kombination aus irgendeinem Grund ungültig ist und der Wert nicht berechnet werden kann, lautet der Wert '-'. Wenn keine Flags gesendet werden, ist der TCP-Flag-Wert 0. TCP-Flags können während des Aggregationsintervalls ODER-verknüpft werden. Für kurze Verbindungen können die Flags in derselben Zeile im Flow-Protokolldatensatz festgelegt werden, wie beispielsweise 19 für SYN-ACK und FIN und 3 für SYN und FIN. Ein Beispiel finden Sie unter TCP-Flag-Sequenz. Allgemeine Informationen zu TCP-Flags (z. B. die Bedeutung von Flags wie FIN, SYN und ACK) finden Sie unter TCP-Segmentstruktur auf Wikipedia. Parquet-Datentyp: INT_32	3

Feld	Beschreibung	Version
type	Der Typ des Datenverkehrs. Die möglichen Werte sind: IPv4 | IPv6 | EFA. Weitere Informationen finden Sie unter Elastic Fabric Adapter. Parquet-Datentyp: STRING	3
pkt-srcaddr	Die (ursprüngliche) Quell-IP-Adresse des Datenverkehrs auf Paketebene. Verwenden Sie dieses Feld mit dem Feld srcaddr, um zwischen der IP-Adresse einer Zwischenebene, durch die Datenverkehr fließt, und der ursprünglichen Quell-IP-Adresse des Datenverkehrs zu unterscheiden. Beispiel: Wenn Datenverkehr durch eine Netzwerkschnittstelle für ein NAT-Gateway fließt oder wenn die IP-Adresse eines Pods in Amazon EKS von der IP-Adresse der Netzwerkschnittstelle des Instance-Knotens abweicht, auf dem der Pod (für die Kommunikation innerhalb der VPC) ausgeführt wird. Parquet-Datentyp: SCHNUR	3
pkt-dstaddr	Die (ursprüngliche) Ziel-IP-Adresse für den Datenverkehr auf Paketebene. Verwenden Sie dieses Feld mit dem Feld dstaddr, um zwischen der IP-Adresse einer Zwischenebene, durch die Datenverkehr fließt, und der endgültigen Ziel-IP-Adresse des Datenverkehrs zu unterscheiden. Beispiel: Wenn Datenverkehr durch eine Netzwerkschnittstelle für ein NAT-Gateway fließt oder wenn die IP-Adresse eines Pods in Amazon EKS von der IP-Adresse der Netzwerkschnittstelle des Instance-Knotens abweicht, auf dem der Pod (für die Kommunikation innerhalb der VPC) ausgeführt wird. Parquet-Datentyp: SCHNUR	3
region	Die Region, die die Netzwerkschnittstelle enthält, für die der Datenverkehr aufgezeichnet wird. Parquet-Datentyp: SCHNUR	4

Feld	Beschreibung	Version
az-id	Die ID der Availability Zone, die die Netzwerkschnittstelle enthält, für die der Datenverkehr aufgezeichnet wird. Wenn der Datenverkehr von einem untergeordneten Standort stammt, zeigt der Datensatz das Symbol „-“ für dieses Feld an. Parquet-Datentyp: SCHNUR	4
sublocation-type	Der Typ des untergeordneten Standorts, der im Feld sublocation-id zurückgegeben wird. Die möglichen Werte sind: wavelength | outpost | localzone. Wenn der Datenverkehr nicht von einem untergeordneten Standort stammt, zeigt der Datensatz das Symbol „-“ für dieses Feld an. Parquet-Datentyp: SCHNUR	4
sublocation-id	Die ID des untergeordneten Standorts mit der Netzwerkschnittstelle, für die der Datenverkehr aufgezeichnet wird. Wenn der Datenverkehr nicht von einem untergeordneten Standort stammt, zeigt der Datensatz das Symbol „-“ für dieses Feld an. Parquet-Datentyp: SCHNUR	4
pkt-src-aws-service	Der Name der Teilmenge der IP-Adressbereiche für das pkt-srcaddr Feld, wenn die Quell-IP-Adresse für einen AWS Dienst bestimmt ist. Wenn pkt-srcaddr zu einem überlappenden Bereich gehört, pkt-src-aws-service wird nur einer der Dienstcodes angezeigt. AWS Die möglichen Werte sind: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | KINESIS_VIDEO_STREAMS | ROUTE53 | ROUTE53_HEALTHCHECKS | ROUTE53_HEALTHCHECKS_PUBLISHING | ROUTE53_RESOLVER | S3 | WORKSPACES_GATEWAYS. Parquet-Datentyp: SCHNUR	5

Feld	Beschreibung	Version
pkt-dst-aws-service	Der Name der Teilmenge der IP-Adressbereiche für das pkt-dstaddr Feld, wenn die Ziel-IP-Adresse für einen Dienst bestimmt ist. AWS Eine Liste möglicher Werte finden Sie im Feld pkt-src-aws-service. Parquet-Datentyp: SCHNUR	5
flow-direction	Die Richtung des Flusses in Bezug auf die Schnittstelle, an der der Verkehr erfasst wird. Die möglichen Werte sind: ingress | egress. Parquet-Datentyp: SCHNUR	5
traffic-path	Der Weg, der ausgehenden Verkehr zum Ziel führt. Um festzustellen, ob es sich bei dem Verkehr um einen ausgehenden Verkehr handelt, überprüfen Sie die Feld flow-direction. Die möglichen Werte lauten wie folgt: Wenn keiner der Werte zutrifft, wird für das Feld „-“ angezeigt. • 1 – Über eine andere Ressource in derselben VPC, einschließlich Ressourcen, die eine Netzwerkschnittstelle in der VPC erstellen • 2 – Über ein Internet-Gateway oder einen Gateway-VPC-Endpunkt • 3 – Über ein Virtual Private Gateway • 4– Über eine VPC-Peering-Verbindung innerhalb von Regionen • 5 – Über eine VPC-Peering-Verbindung zwischen Regionen • 6 – Über ein lokales Gateway • 7 – Über einen Gateway-VPC-Endpunkt (nur auf Nitro-basierte Instances) • 8 – Über ein Internet-Gateway (nur auf Nitro-basierte Instances) Parquet-Datentyp: INT_32	5

Feld	Beschreibung	Version
ecs-cluster-arn	AWS Ressourcenname (ARN) des ECS-Clusters, wenn der Datenverkehr von einer laufenden ECS-Task stammt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: aufzurufenListClusters. Parquet-Datentyp: STRING	7
ecs-Clustername	Name des ECS-Clusters, wenn der Datenverkehr von einer laufenden ECS-Task stammt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: aufzurufenListClusters. Parquet-Datentyp: STRING	7
ecs-container-instance-arn	ARN der ECS-Container-Instance, wenn der Datenverkehr von einer laufenden ECS-Task auf einer EC2-Instance stammt. Wenn es sich bei dem Kapazitätsanbieter um einen AWS Fargate solchen handelt, lautet dieses Feld '-'. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: - ListClusters und ecs: ListContainer -Instances aufzurufen. Parquet-Datentyp: STRING	7
ecs-container-instance-id	ID der ECS-Container-Instance, wenn der Datenverkehr von einer laufenden ECS-Task auf einer EC2-Instance stammt. Wenn es sich bei dem Kapazitätsanbieter um einen AWS Fargate solchen handelt, lautet dieses Feld '-'. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: - ListClusters und ecs: ListContainer -Instances aufzurufen. Parquet-Datentyp: STRING	7
ecs-container-id	Docker-Laufzeit-ID des Containers, wenn der Datenverkehr von einer laufenden ECS-Task stammt. Wenn die ECS-Aufgabe einen oder mehrere Container enthält, ist dies die Docker-Laufzeit-ID des ersten Containers. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters aufzurufen. Parquet-Datentyp: STRING	7

Feld	Beschreibung	Version
ecs-second container-id	Docker-Laufzeit-ID des Containers, wenn der Datenverkehr von einer laufenden ECS-Task stammt. Wenn die ECS-Aufgabe mehr als einen Container enthält, ist dies die Docker-Runtime-ID des zweiten Containers. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters aufzurufen. Parquet-Datentyp: STRING	7
ecs-Dienstname	Name des ECS-Dienstes, wenn der Datenverkehr von einer laufenden ECS-Task stammt und die ECS-Task von einem ECS-Service gestartet wird. Wenn die ECS-Aufgabe nicht von einem ECS-Service gestartet wird, lautet dieses Feld '-'. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters und ecs: ListServices aufzurufen. Parquet-Datentyp: STRING	7
ecs-task-definition-arn	ARN der ECS-Aufgabendefinition, wenn der Datenverkehr von einer laufenden ECS-Task stammt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters und ecs aufzurufen: ListTaskDefinitions Parquet-Datentyp: STRING	7
ecs-task-arn	ARN der ECS-Task, wenn der Datenverkehr von einer laufenden ECS-Task stammt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters und ecs: aufzurufenListTasks. Parquet-Datentyp: STRING	7
ecs-task-id	ID der ECS-Task, wenn der Datenverkehr von einer laufenden ECS-Task stammt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters und ecs: aufzurufenListTasks. Parquet-Datentyp: STRING	7

Beispiele für Flow-Protokolldatensätze

Im Folgenden finden Sie Beispiele für Flow-Protokolldatensätze, die spezifischen Datenverkehr erfassen.

Informationen zum Format des Flow-Protokolldatensatzes finden Sie unter Flow-Protokolldatensätze. Informationen zum Erstellen von Flow-Protokollen finden Sie unter Arbeiten mit Flow-Protokollen.

Inhalt

Zulässiger und abgelehnter Datenverkehr

Im Folgenden finden Sie Beispiele für Standard-Flow-Protokolldatensätze.

In diesem Beispiel ist der SSH-Verkehr (Zielport 22, TCP-Protokoll) von der IP-Adresse 172.31.16.139 zur Netzwerkschnittstelle mit privater IP-Adresse 172.31.16.21 und die ID eni-1235b8ca123456789 im Konto 123456789010 wurde zugelassen.

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 172.31.16.21 20641 22 6 20 4249
 1418530010 1418530070 ACCEPT OK
```

In diesem Beispiel wurde RDP-Datenverkehr (Zielport 3389, TCP-Protokoll) zur Netzwerkschnittstelle eni-1235b8ca123456789 im Konto 123456789010 abgelehnt.

```
2 123456789010 eni-1235b8ca123456789 172.31.9.69 172.31.9.12 49761 3389 6 20 4249
 1418530010 1418530070 REJECT OK
```

Keine Daten und übersprungene Datensätze

Im Folgenden finden Sie Beispiele für Standard-Flow-Protokolldatensätze.

In diesem Beispiel wurden während des Aggregationsintervalls keine Daten aufgezeichnet.

```
2 123456789010 eni-1235b8ca123456789 - - - - - - - 1431280876 1431280934 - NODATA
```

In diesem Beispiel wurden Datensätze während des Aggregationsintervalls übersprungen. VPC Flow Logs überspringt Datensätze, wenn es während eines Aggregationsintervalls keine Flow-Protokolldaten erfassen kann, weil sie die interne Kapazität überschreiten. Ein einzelner übersprungener Datensatz kann mehrere Datenflüsse darstellen, die während des Aggregationsintervalls nicht für die Netzwerkschnittstelle erfasst wurden.

```
2 123456789010 eni-11111111aaaaaaaaa - - - - - - - 1431280876 1431280934 - SKIPDATA
```

Sicherheitsgruppen- und Netzwerk-ACL-Regeln

Wenn Sie mithilfe von Flow-Protokollen übermäßig restriktive oder offene Sicherheitsgruppenregeln oder Netzwerk-ACL-Regeln diagnostizieren, müssen Sie dabei beachten, inwieweit eine Ressource zustandsbehaftet ist. Sicherheitsgruppen sind zustandsbehaftet, d. h. Antworten auf zulässigen Datenverkehr sind immer zulässig, auch wenn die Regeln der Sicherheitsgruppe dies nicht zulassen würden. Netzwerk-ACLs hingegen sind zustandslos und Antworten auf zulässigen Datenverkehr sind somit abhängig von den Netzwerk-ACL-Regeln.

Sie senden beispielsweise den Befehl ping von Ihrem privaten Computer (mit der IP-Adresse 203.0.113.12) an Ihre Instance (mit der privaten IP-Adresse der Netzwerkschnittstelle 172.31.16.139). Die Regeln für eingehenden Datenverkehr Ihrer Sicherheitsgruppe lassen ICMP-Datenverkehr zu, die Regeln für ausgehenden Datenverkehr lassen ICMP-Datenverkehr jedoch nicht zu. Da die Sicherheitsgruppen zustandsbehaftet sind, ist der Antwort-Ping von Ihrer Instance zulässig. Ihre Netzwerk-ACL erlaubt eingehenden, jedoch keinen ausgehenden ICMP-Datenverkehr. Da Netzwerk-ACLs zustandslos sind, verfällt der Antwortping und wird nicht an den Computer gesendet. In einem Flow-Standardprotokoll wird dies als zwei Flow-Protokolldatensätze angezeigt:

- Ein ACCEPT-Datensatz für den ursprünglichen Ping, der sowohl von der Netzwerk-ACL als auch der Sicherheitsgruppe zugelassen wird und daher zur Instance durchdringen konnte
- Ein REJECT-Datensatz für den Antwortping, der von der Netzwerk-ACL abgelehnt wurde

```
2 123456789010 eni-1235b8ca123456789 203.0.113.12 172.31.16.139 0 0 1 4 336 1432917027
 1432917142 ACCEPT OK
```

```
2 123456789010 eni-1235b8ca123456789 172.31.16.139 203.0.113.12 0 0 1 4 336 1432917094
 1432917142 REJECT OK
```

Wenn Ihre Netzwerk-ACL ausgehenden ICMP-Datenverkehr zulässt, enthält das Flow-Protokoll zwei ACCEPT-Datensätze (einen für den ursprünglichen Ping und einen für den Antwortping). Wenn Ihre Sicherheitsgruppe eingehenden ICMP-Datenverkehr ablehnt, enthält das Flow-Protokoll einen REJECT-Datensatz, da der Datenverkehr die Instance nicht erreicht hat.

IPv6-Datenverkehr

Der folgende Code ist ein Beispiel für einen Standard-Flow-Protokolldatensatz. Im Beispiel war der SSH-Verkehr (Port 22) von IPv6-Adresse 2001:db8:1234:a100:8d6e:3477:df66:f105 an die Netzwerkschnittstelle eni-1235b8ca123456789 auf Konto 123456789010 zulässig.

```
2 123456789010 eni-1235b8ca123456789 2001:db8:1234:a100:8d6e:3477:df66:f105
 2001:db8:1234:a102:3304:8879:34cf:4071 34892 22 6 54 8855 1477913708 1477913820 ACCEPT
 OK
```

TCP-Flag-Sequenz

Dieser Abschnitt enthält Beispiele für benutzerdefinierte Flow-Protokolle, die die folgenden Felder in der folgenden Reihenfolge erfassen.

```
version vpc-id subnet-id instance-id interface-id account-id type srcaddr dstaddr
 srcport dstport pkt-srcaddr pkt-dstaddr protocol bytes packets start end action tcp-
flags log-status
```

tcp-flagsDas Feld in den Beispielen in diesem Abschnitt wird durch den Wert im second-to-last Flow-Protokoll dargestellt. Mit Hilfe von TCP-Flags können Sie die Richtung des Datenverkehrs ermitteln, z. B. welcher Server die Verbindung initiiert hat.

> **Note**
>
> Weitere Informationen über die Option tcp-flags und eine Erklärung der einzelnen TCP-Flags finden Sie unter Verfügbare Felder.

In den folgenden Datensätzen (mit Beginn um 19:47:55 und Ende um 19:48:53) wurden zwei Verbindungen von einem Client auf einem Server gestartet, der auf Port 5001 ausgeführt wird. Der Server empfing zwei SYN-Flags (2) vom Client von verschiedenen Quell-Ports auf dem Client (43416 und 43418). Für jedes SYN wurde ein SYN-ACK vom Server an den Client (18) auf dem entsprechenden Port gesendet.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43416 5001
 52.213.180.42 10.0.0.62 6 568 8 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43416 10.0.0.62
 52.213.180.42 6 376 7 1566848875 1566848933 ACCEPT 18 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 100701 70 1566848875 1566848933 ACCEPT 2 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 632 12 1566848875 1566848933 ACCEPT 18 OK
```

Im zweiten Aggregationsintervall ist jetzt eine der Verbindungen beendet, die während des vorherigen Flows hergestellt wurde. Der Client hat ein FIN-Flag (1) für die Verbindung auf Port 43418 an den Server gesendet. Der Server hat ein FIN-Flag an den Client auf Port 43418 gesendet.

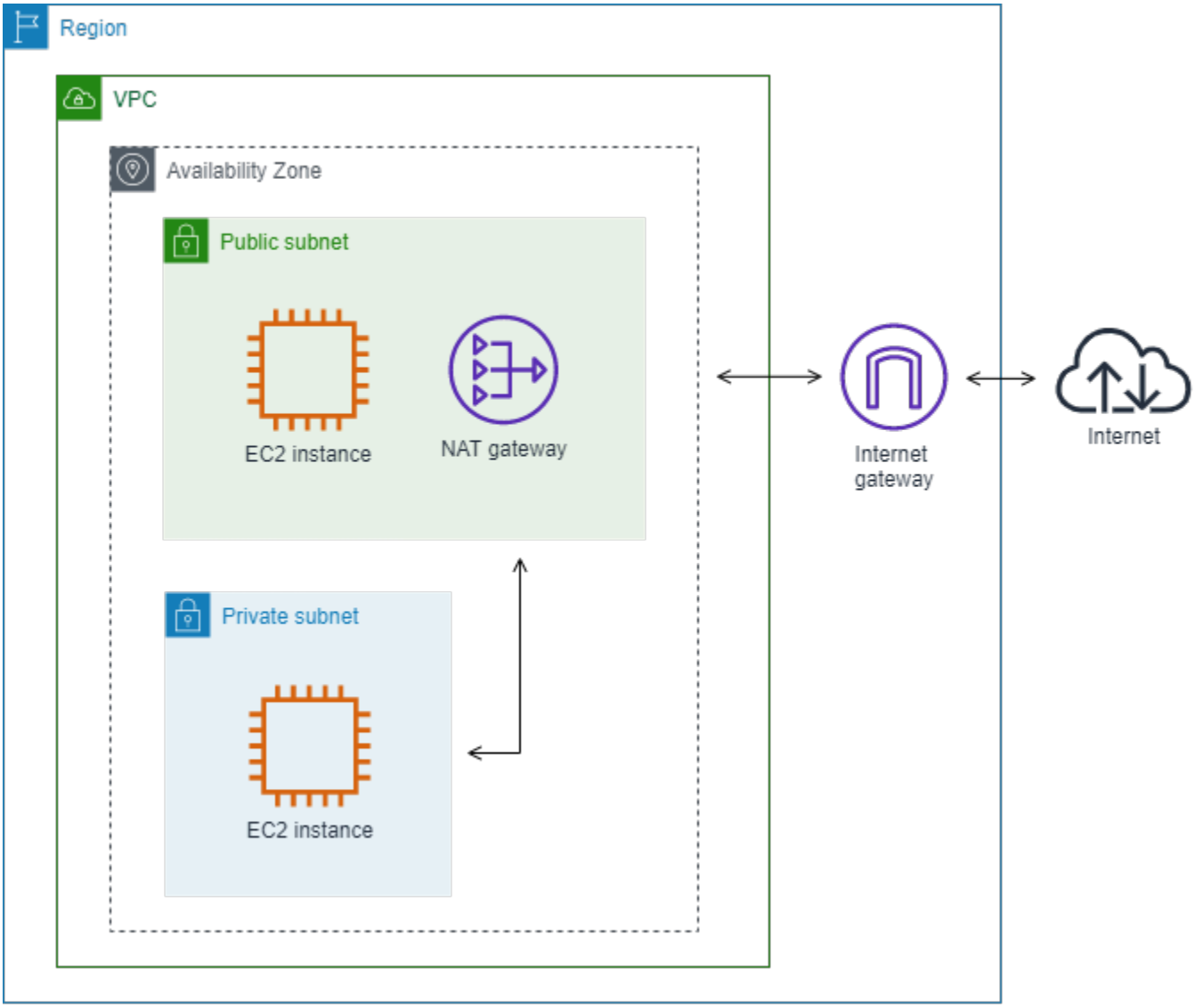
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
 52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43418 5001
 52.213.180.42 10.0.0.62 6 23294588 15774 1566848933 1566849113 ACCEPT 1 OK
```

Für kurze Verbindungen (z. B. wenige Sekunden), die innerhalb eines einzigen Aggregationsintervalls hergestellt und beendet werden, können die Flags in derselben Zeile im Flow-Protokolldatensatz für Datenverkehr in die gleiche Richtung festgelegt werden. Im folgenden Beispiel wird die Verbindung innerhalb desselben Aggregationsintervalls hergestellt und beendet. In der ersten Zeile lautet der Wert des TCP-Flags 3. Dies deutet darauf hin, dass eine SYN- und eine FIN-Meldung vom Client an den Server gesendet wurden. In der zweiten Zeile lautet der Wert des TCP-Flags 19. Dies deutet darauf hin, dass eine SYN-ACK- und eine FIN-Meldung vom Server an den Client gesendet wurden.

```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 52.213.180.42 10.0.0.62 43638 5001
 52.213.180.42 10.0.0.62 6 1260 17 1566933133 1566933193 ACCEPT 3 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
 eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43638  10.0.0.62
 52.213.180.42 6 967 14 1566933133 1566933193 ACCEPT 19 OK
```

Datenverkehr durch ein NAT-Gateway

In diesem Beispiel greift eine Instance in einem privaten Subnetz über ein NAT-Gateway in einem öffentlichen Subnetz auf das Internet zu.



Das folgende benutzerdefinierte Flow-Protokoll für die Netzwerkschnittstelle des NAT-Gateways erfasst die folgenden Felder in der folgenden Reihenfolge.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Das Flow-Protokoll zeigt den Flow des Datenverkehrs von der IP-Adresse der Instance (10.0.1.5) über die Netzwerkschnittstelle des NAT-Gateways zu einem Host im Internet (203.0.113.5). Die Netzwerkschnittstelle des NAT-Gateways ist eine vom Anforderer verwaltete Netzwerkschnittstelle. Daher zeigt der Flow-Protokolldatensatz für das Feld instance-id das Symbol '-'. Die folgende Zeile zeigt Datenverkehr von der Quell-Instance zur Netzwerkschnittstelle des NAT-Gateways. Die Werte für die Felder dstaddr und pkt-dstaddr unterscheiden sich. Das Feld dstaddr zeigt die private IP-Adresse der Netzwerkschnittstelle des NAT-Gateways an und das Feld pkt-dstaddr zeigt die endgültige Ziel-IP-Adresse des Hosts im Internet an.

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

Die nächsten beiden Zeilen zeigen den Datenverkehr von der Netzwerkschnittstelle des NAT-Gateways zum Ziel-Host im Internet sowie den Antwortdatenverkehr vom Host zur Netzwerkschnittstelle des NAT-Gateways an.

```
- eni-1235b8ca123456789 10.0.0.220 203.0.113.5 10.0.0.220 203.0.113.5
- eni-1235b8ca123456789 203.0.113.5 10.0.0.220 203.0.113.5 10.0.0.220
```

Die folgende Zeile zeigt den Antwortdatenverkehr von der Netzwerkschnittstelle des NAT-Gateways zur Quell-Instance an. Die Werte für die Felder srcaddr und pkt-srcaddr unterscheiden sich. Das Feld srcaddr zeigt die private IP-Adresse der Netzwerkschnittstelle des NAT-Gateways an und das Feld pkt-srcaddr zeigt die IP-Adresse des Hosts im Internet an.

```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

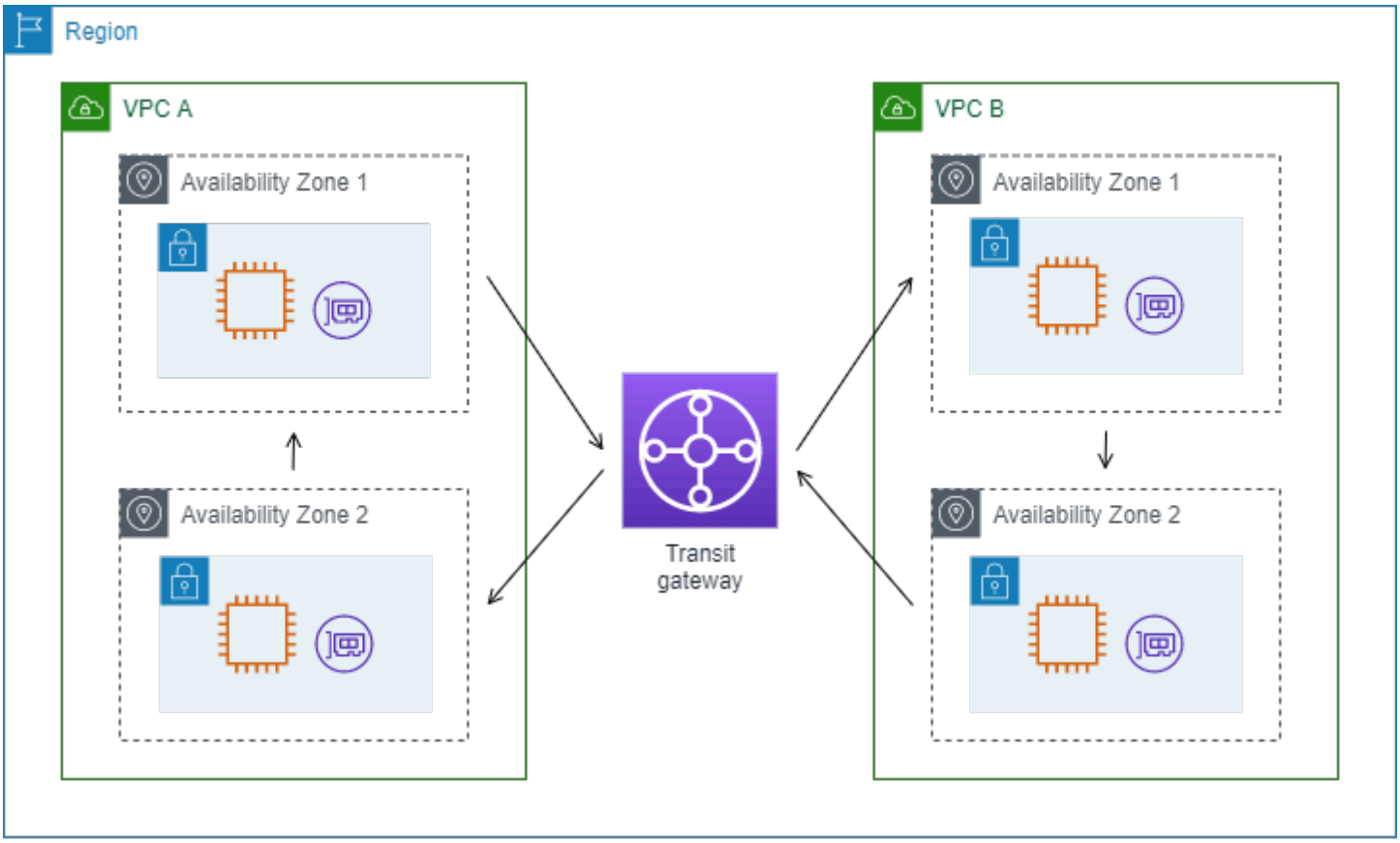
Sie erstellen ein weiteres benutzerdefiniertes Flow-Protokoll mit derselben Gruppe an Feldern wie oben. Sie erstellen das Flow-Protokoll für die Netzwerkschnittstelle für die Instance im privaten Subnetz. In diesem Fall gibt das Feld instance-id die ID der mit der Netzwerkschnittstelle verknüpften Instance zurück und die Felder dstaddr und pkt-dstaddr sowie srcaddr und pkt-srcaddr unterscheiden sich nicht. Anders als bei der Netzwerkschnittstelle für das NAT-Gateway handelt es sich bei dieser Netzwerkschnittstelle nicht um eine Netzwerkzwischenschnittstelle für Datenverkehr.

```
i-01234567890123456 eni-1111aaaa2222bbbb3 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
 #Traffic from the source instance to host on the internet
```

```
i-01234567890123456 eni-1111aaaa2222bbbb3 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
 #Response traffic from host on the internet to the source instance
```

Datenverkehr durch ein Transit-Gateway

In diesem Beispiel stellt ein Client in VPC A über ein Transit-Gateway eine Verbindung mit einem Webserver in VPC B her. Client und Server befinden sich in verschiedenen Availability Zones. Der Datenverkehr erreicht den Server in VPC B über eine elastische Netzwerkschnittstellen-ID (in diesem Beispiel ist die ID eni-11111111111111111) und verlässt VPC B über eine andere (z. B. eni-22222222222222222).



Sie erstellen ein benutzerdefiniertes Flow-Protokoll für VPC B mit dem folgenden Format.

```
version interface-id account-id vpc-id subnet-id instance-id srcaddr dstaddr srcport
 dstport protocol tcp-flags type pkt-srcaddr pkt-dstaddr action log-status
```

Die folgenden Zeilen aus den Flow-Protokolldatensätzen zeigen den Flow des Datenverkehrs an der Netzwerkschnittstelle für den Webserver. Die erste Zeile zeigt den Anfragedatenverkehr vom Client und die letzte Zeile zeigt den Antwortdatenverkehr vom Webserver.

```
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.20.33.164 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164
 10.40.2.236 ACCEPT OK
...
3 eni-33333333333333333 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb
 i-01234567890123456 10.40.2.236 10.20.33.164 80 39812 6 19 IPv4 10.40.2.236
 10.20.33.164 ACCEPT OK
```

Die folgende Zeile zeigt den Anforderungsdatenverkehr auf eni-11111111111111111, einer vom Anforderer verwalteten Netzwerkschnittstelle für das Transit-Gateway in Subnetz subnet-11111111aaaaaaaaa. Daher zeigt der Flow-Protokolldatensatz für das Feld instance-id das Symbol '-'. Das Feld srcaddr zeigt die private IP-Adresse der Netzwerkschnittstelle des Transit-Gateways an, und das Feld pkt-srcaddr zeigt die Quell-IP-Adresse des Clients in VPC A an.

```
3 eni-11111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaaa -
 10.40.1.175 10.40.2.236 39812 80 6 3 IPv4 10.20.33.164 10.40.2.236 ACCEPT OK
```

Die folgende Zeile zeigt den Antwortdatenverkehr auf eni-22222222222222222, einer vom Anforderer verwalteten Netzwerkschnittstelle für das Transit-Gateway in Subnetz subnet-22222222bbbbbbbbb an. Das Feld dstaddr zeigt die private IP-Adresse der Netzwerkschnittstelle des Transit-Gateways an, und das Feld pkt-dstaddr zeigt die IP-Adresse des Clients in VPC A an.

```
3 eni-22222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbb -
 10.40.2.236 10.40.2.31 80 39812 6 19 IPv4 10.40.2.236 10.20.33.164 ACCEPT OK
```

Servicename, Verkehrspfad und Flow-Richtung

Im Folgenden finden Sie ein Beispiel der Felder für einen benutzerdefinierten Flow-Protokolldatensatz.

```
version srcaddr dstaddr srcport dstport protocol start end type packets bytes account-
id vpc-id subnet-id instance-id interface-id region az-id sublocation-type sublocation-
id action tcp-flags pkt-srcaddr pkt-dstaddr pkt-src-aws-service pkt-dst-aws-service
 traffic-path flow-direction log-status
```

Im folgenden Beispiel ist die Version 5, da die Datensätze Felder der Version 5 enthalten. Eine EC2-Instance ruft den Amazon S3-Service auf. Flow-Protokolle werden auf der Netzwerkschnittstelle für die Instance erfasst. Der erste Datensatz hat eine Flow-Richtung von ingress und der zweite Datensatz hat eine Flow-Richtung von egress. Für den egress-Datensatz ist traffic-path 8, was darauf

hinweist, dass der Datenverkehr über ein Internet-Gateway läuft. Das Feld traffic-path wird nicht für ingress-Verkehr unterstützt. Wenn pkt-srcaddr oder pkt-dstaddr eine öffentliche IP-Adresse ist, wird der Servicename angezeigt.

```
5 52.95.128.179 10.0.0.71 80 34210 6 1616729292 1616729349 IPv4 14 15044
 123456789012 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b
 eni-1235b8ca123456789 ap-southeast-2 apse2-az3 - - ACCEPT 19 52.95.128.179 10.0.0.71
 S3 - - ingress OK
5 10.0.0.71 52.95.128.179 34210 80 6 1616729292 1616729349 IPv4 7 471 123456789012 vpc-
abcdefab012345678 subnet-aaaaaaaa012345678 i-0c50d5961bcb2d47b eni-1235b8ca123456789
 ap-southeast-2 apse2-az3 - - ACCEPT 3 10.0.0.71 52.95.128.179 - S3 8 egress OK
```

Einschränkungen von Flow-Protokollen

Machen Sie sich bei der Verwendung von Flow-Protokollen folgende Beschränkungen bewusst:

- Es ist nicht möglich, Flow-Protokolle für VPCs zu aktivieren, die per Peering mit Ihrer VPC verbunden sind, es sei denn, die Peer-VPC befindet sich in Ihrem Konto.
- Nachdem Sie ein Flow-Protokoll erstellt haben, können Sie seine Konfiguration und das Format des Flow-Protokolldatensatzes nicht mehr ändern. Sie können beispielsweise keine andere IAM-Rolle mit dem Flow-Protokoll verknüpfen und keine Felder zum Flow-Protokolldatensatz hinzufügen oder daraus entfernen. Sie müssen in diesem Fall das Flow-Protokoll löschen und ein neues Protokoll mit der erforderlichen Konfiguration erstellen.
- Falls Ihre Netzwerkschnittstelle über mehrere IPv4-Adressen verfügt und Datenverkehr an eine sekundäre private IPv4-Adresse gesendet wird, zeigt das Flow-Protokoll die primäre private IPv4-Adresse im Feld `dstaddr` an. Erstellen Sie ein Flow-Protokoll mit dem Feld `pkt-dstaddr`, um die ursprüngliche Ziel-IP-Adresse zu erfassen.
- Falls der Datenverkehr an eine Netzwerkschnittstelle gesendet wird und es sich beim Ziel um keine IP-Adresse der Netzwerkschnittstelle handelt, wird im Flow-Protokoll die primäre private IPv4-Adresse im Feld `dstaddr` angezeigt. Erstellen Sie ein Flow-Protokoll mit dem Feld `pkt-dstaddr`, um die ursprüngliche Ziel-IP-Adresse zu erfassen.
- Falls der Datenverkehr von einer Netzwerkschnittstelle gesendet wird und es sich bei der Quelle um keine IP-Adresse der Netzwerkschnittstelle handelt, wird im Flow-Protokoll die primäre private IPv4-Adresse im Feld `srcaddr` angezeigt. Erstellen Sie ein Flow-Protokoll mit dem Feld `pkt-srcaddr`, um die ursprüngliche Quell-IP-Adresse zu erfassen.
- Falls der Datenverkehr von oder an eine Netzwerkschnittstelle gesendet wird, zeigen die Felder `srcaddr` und `dstaddr` im Flow-Protokoll unabhängig von Paketquelle oder -ziel stets die primäre

private IPv4-Adresse an. Erstellen Sie ein Flow-Protokoll mit den Feldern `pkt-srcaddr` und `pkt-dstaddr`, um Paketquelle oder -ziel zu erfassen.

- Wenn Ihre Netzwerkschnittstelle einer Nitro-basierten Instance zugewiesen ist, beträgt das Aggregationsintervall immer 1 Minute oder weniger, unabhängig vom angegebenen maximalen Aggregationsintervall.

Flow-Protokolle erfassen nicht alle Arten von IP-Datenverkehr. Für folgende Arten von Datenverkehr werden keine Daten erfasst:

- Datenverkehr von Instances, die den Amazon-DNS-Server kontaktieren. Wenn Sie einen eigenen DNS-Server verwenden, wird sämtlicher Datenverkehr zu diesem DNS-Server erfasst.
- Datenverkehr von Windows-Instances zur Lizenzaktivierung von Amazon Windows
- Datenverkehr zu und von `169.254.169.254` für Instance-Metadaten
- Datenverkehr zu und von `169.254.169.123` für den Amazon Time Sync Service.
- DHCP-Datenverkehr
- Gespiegelter Datenverkehr.
- Datenverkehr zur reservierten IP-Adresse des Standard-VPC-Routers.
- Datenverkehr zwischen einer Endpunkt-Netzwerkschnittstelle und einer Network Load Balancer-Netzwerkschnittstelle.

Spezifische Einschränkungen für ECS-Felder, die in Version 7 verfügbar sind:

- Um Flow-Log-Abonnements mit ECS-Feldern zu erstellen, muss Ihr Konto mindestens einen ECS-Cluster enthalten.
- ECS-Felder werden nicht berechnet, wenn die zugrunde liegenden ECS-Aufgaben nicht dem Besitzer des Flow-Log-Abonnements gehören. Wenn Sie beispielsweise ein Subnetz (`SubnetA`) mit einem anderen Konto (`AccountB`) gemeinsam nutzen und dann ein Flow-Log-Abonnement für den Fall erstellen`SubnetA`, dass ECS-Aufgaben im gemeinsam genutzten Subnetz `AccountB` gestartet werden, empfängt Ihr Abonnement Verkehrsprotokolle von ECS-Aufgaben, die von gestartet wurden, `AccountB` aber die ECS-Felder für diese Protokolle werden aus Sicherheitsgründen nicht berechnet.
- Wenn Sie Flow-Log-Abonnements mit ECS-Feldern auf VPC-/Subnetz-Ressourcenebene erstellen, wird jeglicher Datenverkehr, der für Nicht-ECS-Netzwerkschnittstellen generiert wird, auch für Ihre Abonnements bereitgestellt. Die Werte für ECS-Felder sind '-' für Nicht-ECS-IP-Verkehr. Sie haben

beispielsweise ein Subnetz (`subnet-000000`) und Sie erstellen ein Flow-Log-Abonnement für dieses Subnetz mit ECS-Feldern (). `fl-00000000` In `subnet-000000` starten Sie eine EC2-Instance (`i-0000000`), die mit dem Internet verbunden ist und aktiv IP-Verkehr generiert. Sie starten auch eine laufende ECS-Task (`ECS-Task-1`) im selben Subnetz. Da `i-0000000` sowohl `ECS-Task-1` als auch IP-Verkehr generieren, liefert Ihr `fl-00000000` Flow-Log-Abonnement Verkehrsprotokolle für beide Entitäten. Es enthält jedoch nur `ECS-Task-1` die tatsächlichen ECS-Metadaten für die ECS-Felder, die Sie in Ihr LogFormat aufgenommen haben. Für `i-0000000` verwandten Datenverkehr haben diese Felder den Wert '-'.

- `ecs-container-id`und `ecs-second-container-id` werden so bestellt, wie der VPC Flow Logs-Dienst sie vom ECS-Event-Stream empfängt. Es kann nicht garantiert werden, dass sie sich in derselben Reihenfolge befinden, in der Sie sie auf der ECS-Konsole oder im DescribeTask API-Aufruf sehen. Wenn ein Container in den Status GESTOPPT übergeht, während die Aufgabe noch läuft, wird er möglicherweise weiterhin in Ihrem Protokoll angezeigt.
- Die ECS-Metadaten und IP-Verkehrsprotokolle stammen aus zwei verschiedenen Quellen. Wir beginnen mit der Berechnung Ihres ECS-Datenverkehrs, sobald wir alle erforderlichen Informationen aus den Upstream-Abhängigkeiten erhalten haben. Nachdem Sie eine neue Aufgabe gestartet haben, beginnen wir mit der Berechnung Ihrer ECS-Felder, 1) wenn wir IP-Verkehr für die zugrunde liegende Netzwerkschnittstelle empfangen und 2) wenn wir das ECS-Ereignis erhalten, das die Metadaten für Ihre ECS-Aufgabe enthält, um anzuzeigen, dass die Aufgabe gerade läuft. Nachdem Sie eine Aufgabe beendet haben, beenden wir die Berechnung Ihrer ECS-Felder, 1) wenn wir keinen IP-Verkehr mehr für die zugrunde liegende Netzwerkschnittstelle erhalten oder wenn wir IP-Verkehr erhalten, der um mehr als einen Tag verzögert ist, und 2) wenn wir das ECS-Ereignis erhalten, das die Metadaten für Ihre ECS-Aufgabe enthält, um anzuzeigen, dass Ihre Aufgabe nicht mehr ausgeführt wird.
- Es werden nur ECS-Aufgaben unterstützt, die im `awsvpc` Netzwerkmodus gestartet wurden.

Preisgestaltung

Es fallen Datenerfassungs- und Archivierungsgebühren für Verkaufsprotokolle an, wenn Sie Flow-Protokolle veröffentlichen. Weitere Informationen zu den Preisen bei der Veröffentlichung von Verkaufslogs finden Sie unter Amazon CloudWatch Pricing, wählen Sie Logs aus und suchen Sie nach Vended Logs.

Um Gebühren für die Veröffentlichung von Flow-Protokollen in CloudWatch Logs zu verfolgen, können Sie auf Ihre CloudWatch-Logs-Zielprotokollgruppe Kostenzuordnungs-Tags anwenden. Danach umfasst Ihr AWS Kostenzuordnungsbericht die Nutzung und die Kosten, die nach diesen

Tags zusammengefasst sind. Sie können Tags anwenden, die geschäftliche Kategorien (wie Kostenstellen, Anwendungsnamen oder Besitzer) darstellen, um die Kosten zu organisieren. Weitere Informationen finden Sie hier:

- Verwenden von Kostenzuordnungs-Tags im AWS Billing - Benutzerhandbuch.
- Taggen Sie Protokollgruppen in Amazon CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch
- Verwenden von Kostenzuordnungs-Tags für S3-Buckets im Benutzerhandbuch zu Amazon Simple Storage Service
- Taggen Ihrer Lieferdatenströme im Amazon Data Firehose Developer Guide

Arbeiten mit Flow-Protokollen

Sie können mit Flow-Protokollen über die Konsolen von Amazon EC2 und Amazon VPC arbeiten.

Aufgaben

- Kontrollieren der Nutzung von Flow-Protokollen
- Erstellen eines Flow-Protokolls
- Anzeigen eines Flow-Protokolls
- Markieren eines Flow-Protokolls
- Löschen eines Flow-Protokolls
- API- und CLI-Übersicht

Kontrollieren der Nutzung von Flow-Protokollen

Standardmäßig haben -Benutzer keine Berechtigungen zum Arbeiten mit Flow-Protokollen. Sie können eine IAM-Rolle mit einer angefügten Richtlinie erstellen, über die Benutzer die Berechtigungen zum Erstellen, Ändern, Beschreiben und Löschen von Flow-Protokollen erhalten.

Nachfolgend finden Sie eine Beispielrichtlinie, die Benutzern uneingeschränkte Berechtigungen erteilt, um Flow-Protokolle zu erstellen, zu beschreiben und zu löschen.

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

```
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteFlowLogs",
        "ec2:CreateFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": "*"
    }
  ]
}
```

Weitere Informationen finden Sie unter the section called “Funktionsweise von der Amazon VPC mit IAM”.

Erstellen eines Flow-Protokolls

Sie können Flow-Protokolle für Ihre VPCs, Subnetze oder Netzwerkschnittstellen erstellen. Wenn Sie ein Flow-Protokoll erstellen, müssen Sie ein Ziel für das Flow-Protokoll angeben. Weitere Informationen finden Sie hier:

- the section called “Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch ”
- the section called “Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht”
- the section called “Erstellen Sie ein Flow-Protokoll, das in Amazon Data Firehose veröffentlicht wird”

Anzeigen eines Flow-Protokolls

Sie können Informationen zu den Flow-Protokollen für eine Ressource, z. B. eine Netzwerkschnittstelle, anzeigen. Es werden folgende Informationen angezeigt: die ID des Flow-Protokolls, die Flow-Protokollkonfiguration sowie Informationen zum Status des Flow-Protokolls.

So zeigen Sie Informationen zu Flow-Protokollen an

1. Führen Sie eine der folgenden Aktionen aus:
   - Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. Wählen Sie im Navigationsbereich Network Interfaces aus. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.

- Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus. Aktivieren Sie das Kontrollkästchen für die VPC.
- Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. Aktivieren Sie das Kontrollkästchen für das Subnetz.

2. Wählen Sie Flow Logs (Flow-Protokolle).
3. (Optional) Um die Flow-Protokolldaten anzuzeigen, öffnen Sie das Protokollziel.

Markieren eines Flow-Protokolls

Sie können jederzeit Tags für ein Flow-Protokoll hinzufügen oder entfernen.

So verwalten Sie Tags für ein Flow-Protokoll

1. Führen Sie eine der folgenden Aktionen aus:
   - Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. Wählen Sie im Navigationsbereich Network Interfaces aus. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
   - Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus. Aktivieren Sie das Kontrollkästchen für die VPC.
   - Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. Aktivieren Sie das Kontrollkästchen für das Subnetz.
2. Wählen Sie Flow Logs (Flow-Protokolle).
3. Klicken Sie auf Actions (Aktionen), Manage tags (Markierungen verwalten).
4. Um ein neues Tag hinzuzufügen, wählen Sie Add new Tag (Neuen Tag hinzufügen) und geben Sie dann den Markierungsschlüssel und -Wert ein. Klicken Sie zum Entfernen eines Tags auf Remove (Entfernen).
5. Wenn Sie mit dem Einfügen oder Entfernen der Tags fertig sind, wählen Sie Save (Speichern).

Löschen eines Flow-Protokolls

Sie können ein Flow-Protokoll jederzeit löschen. Nachdem Sie ein Flow-Protokolls gelöscht haben, kann es einige Minuten dauern, bis keine Daten mehr erfasst werden.

Durch das Löschen eines Flow-Protokolls werden die Protokolldaten nicht aus dem Ziel gelöscht und die Zielressource wird nicht geändert. Sie müssen die vorhandenen Flow-Protokolldaten direkt vom Ziel löschen und die Zielressource mithilfe der Konsole für den Zielservice bereinigen.

So löschen Sie ein Flow-Protokoll

1. Führen Sie eine der folgenden Aktionen aus:
   - Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. Wählen Sie im Navigationsbereich Network Interfaces aus. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
   - Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus. Aktivieren Sie das Kontrollkästchen für die VPC.
   - Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. Aktivieren Sie das Kontrollkästchen für das Subnetz.
2. Wählen Sie Flow Logs (Flow-Protokolle).
3. Wählen Sie Actions (Aktionen), Delete flow logs (Flow-Protokolle löschen).
4. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **`delete`** ein und wählen Sie dann Delete (Löschen) aus.

API- und CLI-Übersicht

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile oder API ausführen. Weitere Informationen über Befehlszeilenschnittstellen und eine Liste der verfügbaren API-Aktionen finden Sie unter Arbeiten mit Amazon VPC.

Erstellen eines Flow-Protokolls

- create-flow-logs (AWS CLI)
- New-EC2FlowLog (AWS Tools for Windows PowerShell)
- CreateFlowProtokolle (Amazon EC2 Query API)

Beschreiben eines Flow-Protokolls

- describe-flow-logs (AWS CLI)
- Get-EC2FlowLog (AWS Tools for Windows PowerShell)
- DescribeFlowProtokolle (Amazon EC2 Query API)

Markieren eines Flow-Protokolls

- create-tags und delete-tags (AWS CLI)
- New-EC2Tagund Remove-EC2Tag()AWS Tools for Windows PowerShell
- CreateTagsund DeleteTags(Amazon EC2 Query API)

Löschen eines Flow-Protokolls

- delete-flow-logs (AWS CLI)
- Remove-EC2FlowLog (AWS Tools for Windows PowerShell)
- DeleteFlowProtokolle (Amazon EC2 Query API)

Veröffentlichen Sie Flow-Protokolle in CloudWatch Logs

Flow Logs können Flow-Protokolldaten direkt auf Amazon veröffentlichen CloudWatch.

Bei der Veröffentlichung in CloudWatch Logs werden Flow-Protokolldaten in einer Protokollgruppe veröffentlicht, und jede Netzwerkschnittstelle hat einen eigenen Protokollstream in der Protokollgruppe. Protokollstreams enthalten Flow-Protokolldatensätze. Sie können mehrere Flow-Protokolle erstellen, die Daten in derselben Protokollgruppe veröffentlichen. Wenn dieselbe Netzwerkschnittstelle von mehreren Flow-Protokollen innerhalb derselben Protokollgruppe verwendet wird, wird für diese Schnittstelle ein kombinierter Protokollstream erstellt. Wenn Sie ein Flow-Protokoll zum Erfassen von abgelehntem Datenverkehr und ein weiteres Flow-Protokoll zum Erfassen von zulässigem Datenverkehr erstellt haben, erfasst der kombinierte Protokollstream sämtlichen Datenverkehr.

In CloudWatch Logs entspricht das Zeitstempelfeld der Startzeit, die im Flow-Protokolldatensatz erfasst wurde. Das Feld ingestionTime gibt das Datum und die Uhrzeit an, an dem der Flow-Protokolldatensatz von Logs empfangen wurde. CloudWatch Dieser Zeitstempel liegt später als die Endzeit, die im Flow-Protokolldatensatz erfasst wird.

Weitere Informationen zu CloudWatch Logs finden Sie unter Logs sent to CloudWatch Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

Preisgestaltung

Wenn Sie Flow-Logs in Logs veröffentlichen, fallen Gebühren für Datenaufnahme und Archivierung für verkaufte Logs an. CloudWatch Weitere Informationen finden Sie unter Amazon CloudWatch Pricing, wählen Sie Logs aus und suchen Sie nach Vended Logs.

Inhalt

IAM-Rolle für die Veröffentlichung von Flow-Protokollen in Logs CloudWatch

Die IAM-Rolle, die Ihrem Flow-Protokoll zugeordnet ist, muss über ausreichende Berechtigungen verfügen, um Flow-Logs in der angegebenen Protokollgruppe in CloudWatch Logs zu veröffentlichen. Die IAM-Rolle muss zu Ihrem AWS Konto gehören.

Die IAM-Richtlinie, die mit Ihrer IAM-Rolle verknüpft ist, muss mindestens folgende Berechtigungen enthalten:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

Stellen Sie sicher, dass Ihre Rolle die folgende Vertrauensrichtlinie hat, die es dem Flow-Protokollservice erlaubt, die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Wir empfehlen Ihnen, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zu verwenden, um sich vor dem Problem des verwirrten Stellvertreters zu schützen. Beispielsweise können Sie der vorherigen Vertrauensrichtlinie den folgenden Bedingungsblock hinzufügen. Das Quellkonto ist der Eigentümer des Flow-Protokolls und der Quell-ARN ist der Flow Protokoll-ARN. Wenn Sie die Flow-Protokoll-ID nicht kennen, können Sie diesen Teil des ARN durch einen Platzhalter (*) ersetzen und dann die Richtlinie aktualisieren, nachdem Sie das Flow-Protokoll erstellt haben.

```
"Condition": {
    "StringEquals": {
        "aws:SourceAccount": "account_id"
    },
    "ArnLike": {
        "aws:SourceArn": "arn:aws:ec2:region:account_id:vpc-flow-log/flow-log-id"
    }
}
```

Erstellen einer IAM-Rolle für Flow-Protokolle

Sie können eine vorhandene Rolle wie oben beschrieben aktualisieren. Alternativ können Sie mit dem folgenden Verfahren eine neue Rolle für Flow-Protokolle erstellen. Sie geben diese Rolle an, wenn Sie das Flow-Protokoll erstellen.

So erstellen Sie eine IAM-Rolle für Flow-Protokolle

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. Führen Sie auf der Seite Create policy (Richtlinie erstellen) die folgenden Schritte aus:
   a. Wählen Sie JSON.
   b. Ersetzen Sie den Inhalt dieses Fensters durch die Berechtigungsrichtlinie am Anfang dieses Abschnitts.
   c. Wählen Sie Weiter aus.
   d. Geben Sie einen Namen für Ihre Richtlinie sowie eine optionale Beschreibung und Tags ein und wählen Sie dann Richtlinie erstellen aus.
5. Wählen Sie im Navigationsbereich Rollen aus.
6. Wählen Sie Rolle erstellen aus.
7. Für Trusted entity type (Vertrauenstyp der Entität), wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). Für Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie), ersetzen Sie `"Principal": {},` mit Folgendem und wählen Sie Next (Weiter).

```
"Principal": {
   "Service": "vpc-flow-logs.amazonaws.com"
},
```

8. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die zuvor in diesem Verfahren erstellte Richtlinie und anschließend Next (Weiter).
9. Geben Sie einen Namen für die Rolle sowie optional eine Beschreibung ein.
10. Wählen Sie Rolle erstellen aus.

Berechtigungen für IAM-Prinzipale, die Flow-Logs in Logs veröffentlichen CloudWatch

Stellen Sie sicher, dass der IAM-Prinzipal, den Sie für die Anfrage verwenden, über die erforderlichen Berechtigungen verfügt, um die Aktion aufzurufen. `iam:PassRole`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["iam:PassRole"],
      "Resource": "arn:aws:iam::account-id:role/flow-log-role-name"
    }
  ]
}
```

Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch

Sie können Flow-Protokolle für Ihre VPCs, Subnetze oder Netzwerkschnittstellen erstellen. Wenn Sie diese Schritte als Benutzer ausführen, der eine bestimmte IAM-Rolle verwendet, stellen Sie sicher, dass die Rolle über Berechtigungen zum Verwenden der `iam:PassRole`-Aktion verfügt. Weitere Informationen finden Sie unter Berechtigungen für IAM-Prinzipale, die Flow-Logs in Logs veröffentlichen CloudWatch .

Voraussetzung

- Erstellen Sie eine IAM-Rolle, wie in the section called “IAM-Rolle für die Veröffentlichung von Flow-Protokollen in Logs CloudWatch ” beschrieben.

So erstellen Sie ein Flow-Protokoll mithilfe der Konsole

1. Führen Sie eine der folgenden Aktionen aus:
   - Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. Wählen Sie im Navigationsbereich Network Interfaces aus. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
   - Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus. Aktivieren Sie das Kontrollkästchen für die VPC.

- Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. Aktivieren Sie das Kontrollkästchen für das Subnetz.

2. Klicken Sie auf Actions (Aktionen), Create flow log (Flow-Protokoll erstellen).
3. Geben Sie für Filter den Typ des zu protokollierenden Verkehrs an. Wählen Sie All (Alle) aus, um sämtlichen akzeptierten und abgelehnten Datenverkehr, Reject (Ablehnen), um nur abgelehnten Datenverkehr, oder Accept (Akzeptieren), um nur akzeptierten Datenverkehr aufzuzeichnen.
4. Wählen Sie unter Maximum aggregation interval (Maximales Aggregationsintervall) den maximalen Zeitraum aus, in dem ein Flow erfasst und zu einem Flow-Protokolldatensatz aggregiert wird.
5. Wählen Sie als Ziel die Option An CloudWatchProtokolle senden aus.
6. Wählen Sie für Zielprotokollgruppe den Namen einer vorhandenen Protokollgruppe aus oder geben Sie den Namen einer neuen Protokollgruppe ein, die beim Erstellen dieses Ablaufprotokolls angelegt wird.
7. Geben Sie für die IAM-Rolle den Namen der Rolle an, die berechtigt ist, Logs in Logs zu CloudWatch veröffentlichen.
8. Für Log record format (Datensatzformat protokollieren) wählen Sie das Format für den Flow-Protokolldatensatz aus.

   - Wenn Sie das Standardformat verwenden möchten, wählen Sie AWS default format (-Standardformat) aus.
   - Um ein benutzerdefiniertes Format zu verwenden, wählen Sie Custom format (Benutzerdefiniertes Format) und dann Felder aus Log format (Format protokollieren) aus.

9. Wählen Sie unter Zusätzliche Metadaten aus, ob Sie Metadaten von Amazon ECS in das Protokollformat einbeziehen möchten.
10. (Optional) Wählen Sie Add new tag (Neuen Tag hinzufügen) aus, um Tags auf das Flow-Protokoll anzuwenden.
11. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

So erstellen Sie ein Flow-Protokoll mit der Befehlszeile

Verwenden Sie einen der folgenden Befehle.

- create-flow-logs (AWS CLI)

- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

Im folgenden AWS CLI Beispiel wird ein Flow-Protokoll erstellt, das den gesamten akzeptierten Datenverkehr für das angegebene Subnetz erfasst. Die Flow-Protokolle werden an die angegebene Protokollgruppe übermittelt. Der `--deliver-logs-permission-arn` Parameter gibt die IAM-Rolle an, die für die Veröffentlichung in Logs erforderlich ist. CloudWatch

```
aws ec2 create-flow-logs --resource-type Subnet --resource-ids subnet-1a2b3c4d --
traffic-type ACCEPT --log-group-name my-flow-logs --deliver-logs-permission-arn
 arn:aws:iam::123456789101:role/publishFlowLogs
```

Anzeigen von Flow-Protokolldatensätzen

Sie können Ihre Flow-Protokolldatensätze in der CloudWatch Logs-Konsole anzeigen. Es kann nach dem Erstellen eines Flow-Protokolls einige Minuten dauern, bis das Protokoll in der Konsole angezeigt wird.

Um die in Logs veröffentlichten CloudWatch Flow-Log-Datensätze mit der Konsole anzuzeigen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle), Log groups (Protokollgruppen) aus.
3. Wählen Sie den Namen der Protokollgruppe aus, die Ihre Flow-Protokolle enthält, um die Detailseite zu öffnen.
4. Wählen Sie den Namen des Protokollstreams aus, der die Flow-Protokolldatensätze enthält. Weitere Informationen finden Sie unter Flow-Protokolldatensätze.

Um die in CloudWatch Logs veröffentlichten Flow-Protokolldatensätze über die Befehlszeile anzuzeigen

- get-log-events (AWS CLI)
- Get-CWL (LogEvent)AWS Tools for Windows PowerShell

Suche nach Flow-Protokoll-Datensätzen

Sie können Ihre Flow-Protokolldatensätze, die in Logs veröffentlicht wurden, mithilfe der CloudWatch CloudWatch Logs-Konsole durchsuchen. Sie können Metrikfilter verwenden, um Flow-Protokolldatensätze zu filtern. Flow-Protokolldatensätze sind durch Leerzeichen getrennt.

So suchen Sie mit der CloudWatch Logs-Konsole nach Flow-Log-Datensätzen

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle), Log groups (Protokollgruppen) aus.
3. Wählen Sie die Protokollgruppe mit Ihrem Flow-Protokoll und danach den Protokollstream aus, wenn Sie die Netzwerkschnittstelle kennen, nach der Sie suchen. Als alternative Vorgehensweise wählen Sie Search log group (Protokollgruppe suchen). Dies kann einige Zeit in Anspruch nehmen, wenn sich viele Netzwerkschnittstellen in Ihrer Protokollgruppe befinden oder je nach ausgewähltem Zeitbereich.
4. Geben Sie unter Ereignisse filtern die folgende Zeichenfolge ein. Hierbei wird davon ausgegangen, dass der Flow-Protokolldatensatz das Standardformat verwendet.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport, protocol,
 packets, bytes, start, end, action, logstatus]
```

5. Ändern Sie den Filter nach Bedarf, indem Sie Werte für die Felder angeben. In den folgenden Beispielen wird nach bestimmten Quell-IP-Adressen gefiltert.

```
[version, accountid, interfaceid, srcaddr = 10.0.0.1, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr = 10.0.2.*, dstaddr, srcport, dstport,
 protocol, packets, bytes, start, end, action, logstatus]
```

Die folgenden Beispiele filtern nach Zielport, Anzahl der Bytes und ob der Datenverkehr abgelehnt wurde.

```
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes, start, end, action, logstatus]
[version, accountid, interfaceid, srcaddr, dstaddr, srcport, dstport = 80 ||
 dstport = 8080, protocol, packets, bytes >= 400, start, end, action = REJECT,
 logstatus]
```

Prozessflussprotokolldatensätze in CloudWatch Logs

Sie können mit Flow-Protokolldatensätzen genauso arbeiten wie mit allen anderen Protokollereignissen, die von CloudWatch Logs erfasst werden. Weitere Informationen zur Überwachung von Protokolldaten und Metrikfiltern finden Sie unter Suchen und Filtern von Protokolldaten im CloudWatch Amazon-Benutzerhandbuch.

Beispiel: Erstellen Sie einen CloudWatch metrischen Filter und einen Alarm für ein Flow-Protokoll

In diesem Beispiel haben Sie ein Flow-Protokoll für `eni-1a2b3c4d`. Sie möchten einen Alarm erstellen, um benachrichtigt zu werden, wenn ein Verbindungsversuch zu Ihrer Instance über den TCP-Port 22 (SSH) innerhalb einer Stunde mindestens 10 Mal fehlschlägt. Zuerst müssen Sie einen Metrikfilter erstellen, der mit dem Datenverkehrsmuster übereinstimmt, für das Sie den Alarm erstellen möchten. Danach können Sie einen Alarm für den Metrikfilter erstellen.

So erstellen Sie einen Metrikfilter für abgelehnten SSH-Datenverkehr und einen Alarm für den Filter

1. Öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie im Navigationsbereich Logs (Protokolle), Log groups (Protokollgruppen) aus.
3. Aktivieren Sie das Kontrollkästchen für die Protokollgruppe und wählen Sie dann Actions (Aktionen), Create metric filter (Metrikfilter erstellen).
4. Geben Sie für Filter pattern (Filtermuster) folgende Informationen ein.

   ```
   [version, account, eni, source, destination, srcport, destport="22", protocol="6",
    packets, bytes, windowstart, windowend, action="REJECT", flowlogstatus]
   ```

5. Wählen Sie für Select Log Data to Test (Die zu testenden Protokolldaten auswählen) den Protokollstream Ihrer Netzwerkschnittstelle aus. (Optional) Um die Zeilen der Protokolldaten anzuzeigen, die mit dem Filtermuster übereinstimmen, wählen Sie Test Pattern (Testmuster).
6. Wählen Sie danach Next (Weiter) aus.
7. Geben Sie einen Filternamen, einen Metrik-Namespace und einen Metriknamen ein. Legen Sie den Metrikwert auf 1 fest. Wenn Sie fertig sind, wählen Sie Next (Weiter) und dann Create metric filter (Metrikfilter erstellen) aus.
8. Wählen Sie im Navigationsbereich Alarms (Alarme) und All alarms (Alle Alarme) aus.
9. Wählen Sie Create alarm (Alarm erstellen) aus.
10. Wählen Sie den Metriknamen aus, den Sie erstellt haben, und klicken Sie dann auf Metrik auswählen.
11. Konfigurieren Sie den Alarm wie folgt, und wählen Sie dann Weiter:

    - Wählen Sie für Statistic (Statistik) Sum (Summe) aus. Dadurch wird sichergestellt, dass Sie die Gesamtzahl der Datenpunkte für den angegebenen Zeitraum erfassen.
    - Wählen Sie als Period (Zeitraum) 1 Hour (1 Stunde) aus.

- Für wann immer TimeSinceLastActive ist... , wählen Sie Größer/Gleich und geben Sie 10 als Schwellenwert ein.
- Belassen Sie für Additional configuration (Zusätzliche Konfiguration), Datapoints to alarm (Zu alarmierende Datenpunkte) den Standardwert 1.

12. Wählen Sie Weiter aus.
13. Wählen Sie für Notification (Benachrichtigung) ein vorhandenes SNS-Thema aus oder wählen Sie Create new topic (Neues Thema erstellen), um ein neues zu erstellen. Wählen Sie Weiter aus.
14. Geben Sie einen Namen und eine Beschreibung für den Alarm ein und wählen Sie Next (Weiter).
15. Wenn Sie mit der Vorschau des Alarms fertig sind, wählen Sie „Alarm erstellen“.

Veröffentlichen von Flow-Protokollen auf Amazon S3

Flow-Protokolle können Flow-Protokolldaten direkt in Amazon S3 veröffentlichen.

Beim Veröffentlichen in Amazon S3 werden Flow-Protokolldaten in einem vorhandenen Amazon S3-Bucket veröffentlicht, den Sie zuvor angegeben haben. Flow-Protokolldatensätze für alle überwachten Netzwerkschnittstellen werden in eine Reihe von Protokolldateiobjekten veröffentlicht, die im Bucket abgelegt sind. Wenn das Flow-Protokoll Daten für eine VPC erfasst, veröffentlicht das Flow-Protokoll Flow-Protokolldatensätze für alle Netzwerkschnittstellen in der ausgewählten VPC.

Informationen zum Erstellen eines Amazon-S3-Buckets für die Verwendung mit Flow-Protokollen finden Sie unter Erstellen eines Buckets im Benutzerhandbuch zu Amazon Simple Storage Service.

Weitere Informationen zur Protokollierung mehrerer Konten finden Sie unter Zentrale Protokollierung in der AWS Solutions Library.

Weitere Informationen zu CloudWatch Logs finden Sie unter An Amazon S3 gesendete Logs im Amazon CloudWatch Logs-Benutzerhandbuch.

Preisgestaltung

Für die Dateneingabe und Archivierung fallen Gebühren für angebotene Protokolle an, wenn Sie Flow-Protokolle in Amazon S3 veröffentlichen. Weitere Informationen finden Sie unter Amazon CloudWatch Pricing, wählen Sie Logs aus und suchen Sie nach Vended Logs.

Inhalt

- Berechtigungen für IAM-Prinzipale, die Flow-Protokolle in Amazon S3 veröffentlichen
- Amazon S3-Bucket-Berechtigungen für Flow-Protokolle
- Erforderliche Schlüsselrichtlinie zur Verwendung mit SSE-KMS
- Amazon S3-Protokolldateiberechtigungen
- Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht
- Anzeigen von Flow-Protokolldatensätzen
- Verarbeiten von Flow-Protokolldatensätzen in Amazon S3

Flow-Protokolldateien

VPC Flow Logs sammelt Daten über den IP-Verkehr zu und von Ihrer VPC in Protokolldatensätzen, fasst diese Datensätze in Protokolldateien zusammen und veröffentlicht die Protokolldateien dann in Intervallen von 5 Minuten im Amazon S3 S3-Bucket. Es können mehrere Dateien veröffentlicht werden, und jede Protokolldatei kann einige oder alle Flow-Protokolldatensätze für den IP-Verkehr enthalten, der in den letzten 5 Minuten aufgezeichnet wurde.

In Amazon S3 gibt das Feld Last modified (Zuletzt geändert) für die FLow-Protokolldatei Datum und Uhrzeit an, zu dem/der die Datei in den Amazon S3-Bucket hochgeladen wurde. Dieser Zeitpunkt ist später als der Zeitstempel im Dateinamen und die Differenz ist die Zeitspanne, die zum Upload der Datei in den Amazon S3-Bucket benötigt wird.

Protokolldateiformat

Sie können eines der folgenden Formate für die Protokolldateien festlegen. Jede Datei wird in eine einzelne Gzip-Datei komprimiert.

- Text – Klartext. Dies ist das Standardformat.
- Parquet – Apache Parquet ist ein spaltenförmiges Datenformat. Abfragen zu Daten im Parquet-Format sind 10 bis 100 Mal schneller im Vergleich zu Abfragen zu Daten im Klartext. Daten im Parquet-Format mit Gzip-Komprimierung benötigen 20 Prozent weniger Speicherplatz als Nur-Text bei Gzip-Komprimierung.

> **Note**
>
> Wenn Daten im Parquet-Format mit Gzip-Komprimierung weniger als 100 KB pro Aggregationszeitraum betragen, kann das Speichern von Daten im Parquet-Format aufgrund

der Speicheranforderungen für die Parquet-Datei mehr Speicherplatz beanspruchen als Klartext mit Gzip-Komprimierung.

Protokolldateioptionen

Optional können Sie folgende Optionen angeben.

- HIVE-kompatible S3-Präfixe – Aktivieren Sie HIVE-kompatible Präfixe, anstatt Partitionen in Ihre HIVE-kompatiblen Tools zu importieren. Bevor Sie Abfragen ausführen, verwenden Sie den MSCK REPAIR TABLE-Befehl.
- Stündliche Partitionen – Wenn Sie über eine große Anzahl von Protokollen verfügen und Abfragen normalerweise auf eine bestimmte Stunde richten, können Sie schnellere Ergebnisse erzielen und Abfragekosten sparen, indem Sie Protokolle stündlich partitionieren.

S3-Bucket-Struktur der Protokolldatei

Protokolldateien werden im angegebenen Amazon-S3-Bucket mit einer Ordnerstruktur gespeichert, die auf der ID, der Region, dem Erstellungsdatum und den Zieloptionen des Flow-Protokolls basiert.

Standardmäßig werden die Dateien an den folgenden Speicherort geliefert.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/
```

Wenn Sie HIVE-kompatible S3-Präfixe aktivieren, werden die Dateien an den folgenden Speicherort geliefert.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/
```

Wenn Sie stündliche Partitionen aktivieren, werden die Dateien an den folgenden Speicherort geliefert.

```
bucket-and-optional-prefix/AWSLogs/account_id/vpcflowlogs/region/year/month/day/hour/
```

Wenn Sie HIVE-kompatible Partitionen aktivieren und das Flow-Protokoll pro Stunde partitionieren, werden die Dateien an den folgenden Speicherort geliefert.

```
bucket-and-optional-prefix/AWSLogs/aws-account-id=account_id/aws-service=vpcflowlogs/
aws-region=region/year=year/month=month/day=day/hour=hour/
```

Protokolldateinamen

Der Dateiname einer Protokolldatei basiert auf der Flow-Protokoll-ID, der Region sowie dem Erstellungsdatum und der Uhrzeit. Dateinamen verwenden das folgende Format:

```
aws_account_id_vpcflowlogs_region_flow_log_id_YYYYMMDDTHHmmZ_hash.log.gz
```

Im Folgenden sehen Sie ein Beispiel für eine Protokolldatei für ein Flow-Protokoll, das von AWS - Konto 123456789012 für eine Ressource in der us-east-1-Region am June 20, 2018 um 16:20 UTC erstellt wurde. Die Datei enthält die Flow-Protokolldatensätze mit einer Endzeit zwischen 16:20:00 und 16:24:59.

```
123456789012_vpcflowlogs_us-east-1_fl-1234abcd_20180620T1620Z_fe123456.log.gz
```

Berechtigungen für IAM-Prinzipale, die Flow-Protokolle in Amazon S3 veröffentlichen

Der IAM-Prinzipal, der das Flow-Protokoll erstellt, muss eine IAM-Rolle verwenden, die über die folgenden Berechtigungen verfügt, die für die Veröffentlichung von Flow-Protokollen im Amazon-S3-Ziel-Bucket erforderlich sind.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs:DeleteLogDelivery"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon S3-Bucket-Berechtigungen für Flow-Protokolle

Standardmäßig sind Amazon S3-Buckets und die darin enthaltenen Objekte privat. Nur der Bucket-Besitzer kann auf den Bucket und die darin gespeicherten Objekte zugreifen. Der Bucket-Besitzer kann jedoch anderen Ressourcen und Benutzern Zugriffsberechtigungen erteilen, indem er eine Zugriffsrichtlinie schreibt.

Wenn der Benutzer, der das Flow-Protokoll erstellt, Eigentümer des Buckets ist und `PutBucketPolicy`- und `GetBucketPolicy`-Berechtigungen für den Bucket besitzt, fügen wir automatisch die folgende Richtlinie an den Bucket an. Diese Richtlinie überschreibt alle vorhandenen Richtlinien, die bereits an den Bucket angefügt sind.

Ansonsten muss der Bucket-Eigentümer diese Richtlinie zum Bucket hinzufügen und dabei die AWS -Konto-ID des Flow-Protokoll-Erstellers oder die Erstellung des Flow-Logs schlägt fehl. Weitere Informationen finden Sie unter Verwenden von Bucket-Richtlinien im Benutzerhandbuch für Amazon Simple Storage Service.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "my-s3-arn/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id,
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": [
                "s3:GetBucketAcl",
                "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::bucket_name",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": account_id
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:logs:region:account_id:*"
                }
            }
        }
    ]
}
```

Der ARN, den Sie für *meine-s3-arn* angeben hängt davon ab, ob Sie HIVE-kompatible S3-Präfixe verwenden.

- Standardpräfixe

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/account_id/*
```

- HIVE-kompatible S3-Präfixe

```
arn:aws:s3:::bucket_name/optional_folder/AWSLogs/aws-account-id=account_id/*
```

Es hat sich bewährt, diese Berechtigungen nicht einzelnen AWS-Konto ARNs, sondern dem Principal des Protokollzustellungsdienstes zu erteilen. Es ist auch eine bewährte Methode, die `aws:SourceAccount`- und `aws:SourceArn`-Bedingungsschlüssel zum Schutz vor dem Problem des verwirrten Stellvertreters zu verwenden. Das Quellkonto ist der Eigentümer des Flow-Protokolls und der Quell-ARN ist der Platzhalter-AARN (*) des Protokolldienstes.

Erforderliche Schlüsselrichtlinie zur Verwendung mit SSE-KMS

Sie können die Daten in Ihrem Amazon-S3-Bucket schützen, indem Sie entweder Serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) oder Serverseitige

Verschlüsselung mit KMS-Schlüsseln (SSE-KMS) für Ihr S3-Bucket aktivieren. Weitere Informationen finden Sie unter Schützen von Daten mithilfe serverseitiger Verschlüsselung im Amazon S3-Entwicklerhandbuch.

Wenn Sie SSE-S3 wählen, ist keine zusätzliche Konfiguration erforderlich. Amazon S3 verarbeitet den Verschlüsselungsschlüssel.

Wenn Sie sich für SSE-KMS entscheiden, müssen Sie einen vom Kunden verwalteten Schlüssel-ARN verwenden. Wenn Sie eine Schlüssel-ID verwenden, kann beim Erstellen eines Flow-Protokolls ein LogDestination nicht zustellbar-Fehler auftreten. Sie müssen die Schlüsselrichtlinie für Ihren vom Kunden verwalteten Schlüssel aktualisieren, damit das Protokollzustellungskonto in Ihren S3-Bucket schreiben kann. Weitere Informationen zur erforderlichen Schlüsselrichtlinie für die Verwendung mit SSE-KMS finden Sie unter serverseitige Verschlüsselung des Amazon S3 S3-Buckets im Amazon CloudWatch Logs-Benutzerhandbuch.

Amazon S3-Protokolldateiberechtigungen

Zusätzlich zu den erforderlichen Bucket-Richtlinien verwendet Amazon S3 Zugriffskontrolllisten (ACLs), um den Zugriff auf die durch ein Flow-Protokoll erzeugten Protokolldateien zu verwalten. Standardmäßig hat der Bucket-Eigentümer `FULL_CONTROL`-Berechtigungen für jede Protokolldatei. Der Protokollbereitstellungseigentümer hat keine Berechtigungen, wenn er nicht gleichzeitig der Bucket-Eigentümer ist. Das Konto für die Protokollbereitstellung hat `READ`- und `WRITE`-Berechtigungen. Weitere Informationen finden Sie unter Zugriffskontrollliste (ACL) – Übersicht im Benutzerhandbuch zu Amazon Simple Storage Service.

Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht

Nachdem Sie Ihren Amazon-S3-Bucket erstellt und konfiguriert haben, können Sie Flow-Protokolle für Ihre Netzwerkschnittstellen, Subnetze und VPCs erstellen.

So erstellen Sie ein Flow-Protokoll mithilfe der Konsole

1. Führen Sie eine der folgenden Aktionen aus:
   - Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. Wählen Sie im Navigationsbereich Network Interfaces aus. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
   - Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus. Aktivieren Sie das Kontrollkästchen für die VPC.

- Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. Aktivieren Sie das Kontrollkästchen für das Subnetz.

2. Klicken Sie auf Actions (Aktionen), Create flow log (Flow-Protokoll erstellen).
3. Geben Sie für Filter den Typ der zu protokollierenden IP-Verkehrsdaten an.

   - Akzeptieren — Nur akzeptierter Datenverkehr wird protokolliert.
   - Ablehnen — Nur abgelehnter Verkehr wird protokolliert.
   - Alle – Akzeptierten und abgelehnten Verkehr protokollieren.

4. Wählen Sie unter Maximum aggregation interval (Maximales Aggregationsintervall) den maximalen Zeitraum aus, in dem ein Flow erfasst und zu einem Flow-Protokolldatensatz aggregiert wird.
5. Wählen Sie für Destination (Ziel) die Option Send to an Amazon S3 bucket (An einen Amazon S3-Bucket senden).
6. Geben Sie für S3 bucket ARN (S3-Bucket-ARN) den Amazon-Ressourcennamen (ARN) eines vorhandenen Amazon S3-Buckets an. Sie können optional einen Unterordner einfügen. Um beispielsweise den Unterordner `my-logs` im Bucket `my-bucket` anzugeben, verwenden Sie den folgenden ARN:

   ```
   arn:aws:s3:::my-bucket/my-logs/
   ```

   Der Bucket kann als Unterordnername nicht `AWSLogs` verwenden, da dieser Begriff reserviert ist.

   Wenn Sie der Eigentümer des Buckets sind, erstellen wir automatisch eine Ressourcenrichtlinie und fügen sie dem Bucket hinzu. Weitere Informationen finden Sie unter Amazon S3-Bucket-Berechtigungen für Flow-Protokolle.
7. Für Log record format (Datensatzformat protokollieren) geben Sie das Format für den Flow-Protokolldatensatz an.

   - Wenn Sie das Standardformat für Flow-Protokolldatensätze verwenden möchten, wählen Sie AWS default format (-Standardformat).
   - Wenn Sie ein benutzerdefiniertes Format erstellen möchten, wählen Sie Custom format (Benutzerdefiniertes Format). Wählen Sie für Protokollformat die Felder, die im Flow-Protokolldatensatz berücksichtigt werden sollen.

8. Wählen Sie unter Zusätzliche Metadaten aus, ob Sie Metadaten von Amazon ECS in das Protokollformat einbeziehen möchten.

9. Geben Sie für Log file format (Protokolldateiformat) das Format für die Protokolldatei an.
   - Text – Klartext. Dies ist das Standardformat.
   - Parquet – Apache Parquet ist ein spaltenförmiges Datenformat. Abfragen zu Daten im Parquet-Format sind 10 bis 100 Mal schneller im Vergleich zu Abfragen zu Daten im Klartext. Daten im Parquet-Format mit Gzip-Komprimierung benötigen 20 Prozent weniger Speicherplatz als Nur-Text bei Gzip-Komprimierung.
10. (Optional) Um Hive-kompatible S3-Präfixe zu verwenden, wählen Sie Hive-compatible S3 prefix (Hive-kompatibles S3-Präfix), Enable (Aktivieren).
11. (Optional) Um Ihre Flow-Protokolle pro Stunde zu partitionieren, wählen Sie Every 1 hour (60 mins) (Jede 1 Stunde (60 Minuten)).
12. (Optional) Um dem Flow-Protokoll ein Tag hinzuzufügen, wählen Sie Add new tag (Neues Tag hinzufügen) und geben Sie den Tag-Schlüssel und -Wert an.
13. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

So erstellen Sie ein Flow-Protokoll, das mithilfe eines Befehlszeilen-Tools in Amazon S3 veröffentlicht

Verwenden Sie einen der folgenden Befehle:

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

Das folgende AWS CLI Beispiel erstellt ein Flow-Protokoll, das den gesamten Datenverkehr für die angegebene VPC erfasst und die Flow-Logs an den angegebenen Amazon S3 S3-Bucket übermittelt. Der Parameter `--log-format` legt ein benutzerdefiniertes Format für die Flow-Protokolldatensätze fest.

```
aws ec2 create-flow-logs --resource-type VPC --resource-ids vpc-00112233344556677 --
traffic-type ALL --log-destination-type s3 --log-destination arn:aws:s3:::flow-log-
bucket/custom-flow-logs/ --log-format '${version} ${vpc-id} ${subnet-id} ${instance-
id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${tcp-flags} ${type} ${pkt-
srcaddr} ${pkt-dstaddr}'
```

Anzeigen von Flow-Protokolldatensätzen

Sie können Ihre Flow-Protokolle mit der Amazon-S3-Konsole anzeigen. Es kann nach dem Erstellen eines Flow-Protokolls einige Minuten dauern, bis das Protokoll in der Konsole angezeigt wird.

So zeigen Sie in Amazon S3 veröffentlichte Flow-Protokolldatensätze an

1. Öffnen Sie die Amazon S3-Konsole unter https://console.aws.amazon.com/s3/.
2. Wählen Sie den Namen des Buckets aus, um seine Detailseite zu öffnen.
3. Navigieren Sie zu dem Ordner mit den Protokolldateien. *Beispiel: Präfix/ AWSLogs/account_id /vpcflowlogs/ region/year/month/day /.*
4. Aktivieren Sie das Kontrollkästchen neben dem Dateinamen und wählen Sie dann Download (Herunterladen).

Verarbeiten von Flow-Protokolldatensätzen in Amazon S3

Die Protokolldateien werden komprimiert. Wenn Sie die Protokolldateien unter Verwendung der Amazon S3-Konsole öffnen, werden sie dekomprimiert und die Flow-Protokolldatensätze werden angezeigt. Wenn Sie die Dateien herunterladen, müssen Sie sie dekomprimieren, um die Flow-Protokolldatensätze anzuzeigen.

Sie können die Flow-Protokolldatensätze in den Protokolldateien auch mit Amazon Athena abfragen. Amazon Athena ist ein interaktiver Abfrageservice, der die Analyse von Daten in Amazon S3 mit Standard-SQL erleichtert. Weitere Informationen finden Sie unter Abfragen von Amazon VPC Flow-Protokollen im Amazon Athena-Benutzerhandbuch.

Veröffentlichen Sie Flow-Logs in Amazon Data Firehose

Flow Logs können Flow-Protokolldaten direkt in Amazon Data Firehose veröffentlichen.

Bei der Veröffentlichung in Amazon Data Firehose werden die Flow-Protokolldaten in einem Amazon Data Firehose-Lieferstream im Klartextformat veröffentlicht.

Preisgestaltung

Es fallen die üblichen Kosten für Einnahme und Lieferung an. Weitere Informationen finden Sie unter Amazon CloudWatch Pricing, wählen Sie Logs aus und suchen Sie nach Vended Logs.

Inhalt

- IAM-Rollen für die kontoübergreifende Bereitstellung
- Erstellen Sie ein Flow-Protokoll, das in Amazon Data Firehose veröffentlicht wird
- Prozessflussprotokolldatensätze in Amazon Data Firehose

IAM-Rollen für die kontoübergreifende Bereitstellung

Wenn Sie auf Amazon Data Firehose veröffentlichen, können Sie einen Lieferstream auswählen, der sich im selben Konto wie die zu überwachende Ressource (das Quellkonto) oder in einem anderen Konto (das Zielkonto) befindet. Um die kontoübergreifende Übermittlung von Flow-Protokollen an Amazon Data Firehose zu ermöglichen, müssen Sie eine IAM-Rolle im Quellkonto und eine IAM-Rolle im Zielkonto erstellen.

Rollen

- Rolle des Quellkontos
- Rolle des Zielkontos

Rolle des Quellkontos

Erstellen Sie im Quellkonto eine Rolle, die die folgenden Berechtigungen gewährt. In diesem Beispiel lautet der Name der Rolle `mySourceRole`, allerdings können Sie einen anderen Namen für diese Rolle wählen. Die letzte Anweisung ermöglicht es der Rolle im Zielkonto, diese Rolle zu übernehmen. Die Bedingungsanweisungen stellen sicher, dass diese Rolle nur an den Protokollbereitstellungsservice und nur beim Überwachen der angegebenen Ressource übergeben wird. Geben Sie beim Erstellen Ihrer Richtlinie die VPCs, Netzwerkschnittstellen oder Subnetze, die Sie überwachen, mit dem Bedingungsschlüssel `iam:AssociatedResourceARN` an.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::source-account:role/mySourceRole",
      "Condition": {
          "StringEquals": {
              "iam:PassedToService": "delivery.logs.amazonaws.com"
          },
          "StringLike": {
              "iam:AssociatedResourceARN": [
                  "arn:aws:ec2:region:source-account:vpc/vpc-00112233344556677"
              ]
          }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
          "logs:CreateLogDelivery",
          "logs:DeleteLogDelivery",
          "logs:ListLogDeliveries",
          "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}
```

Stellen Sie sicher, dass Ihre Rolle die folgende Vertrauensrichtlinie hat, die es dem Protokollservice erlaubt, die Rolle zu übernehmen.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Führen Sie aus dem Quellkonto die folgenden Schritte zum Erstellen der Rolle aus.

So erstellen Sie die Rolle des Quellkontos

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. Führen Sie auf der Seite Create policy (Richtlinie erstellen) die folgenden Schritte aus:

   a. Wählen Sie JSON.

   b. Ersetzen Sie den Inhalt dieses Fensters durch die Berechtigungsrichtlinie am Anfang dieses Abschnitts.

   c. Wählen Sie Weiter aus.

   d. Geben Sie einen Namen für Ihre Richtlinie sowie eine optionale Beschreibung und Tags ein und wählen Sie dann Richtlinie erstellen aus.

5. Wählen Sie im Navigationsbereich Rollen aus.
6. Wählen Sie Rolle erstellen aus.
7. Für Trusted entity type (Vertrauenstyp der Entität), wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). Für Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie), ersetzen Sie `"Principal": {},` mit dem Folgenden, was den Protokollbereitstellungsdienst spezifiziert. Wählen Sie Weiter aus.

   ```
   "Principal": {
      "Service": "delivery.logs.amazonaws.com"
   },
   ```

8. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die zuvor in diesem Verfahren erstellte Richtlinie und anschließend Next (Weiter).
9. Geben Sie einen Namen für die Rolle sowie optional eine Beschreibung ein.
10. Wählen Sie Rolle erstellen aus.

Rolle des Zielkontos

Erstellen Sie im Zielkonto eine Rolle mit einem Namen, der mit beginnt AWSLogDeliveryFirehoseCrossAccountRole. Die Rolle muss die folgenden Berechtigungen enthalten.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iam:CreateServiceLinkedRole",
```

```
            "firehose:TagDeliveryStream"
        ],
        "Resource": "*"
      }
    ]
}
```

Stellen Sie sicher, dass diese Rolle über die folgende Vertrauensrichtlinie verfügt, mit der die Rolle, die Sie im Quellkonto erstellt haben, diese Rolle übernehmen kann.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
          "AWS": "arn:aws:iam::source-account:role/mySourceRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Führen Sie vom Quellkonto die folgenden Schritte zum Erstellen der Rolle aus.

So erstellen Sie die Rolle des Zielkontos

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. Führen Sie auf der Seite Create policy (Richtlinie erstellen) die folgenden Schritte aus:
   a. Wählen Sie JSON.
   b. Ersetzen Sie den Inhalt dieses Fensters durch die Berechtigungsrichtlinie am Anfang dieses Abschnitts.
   c. Wählen Sie Weiter aus.
   d. Geben Sie einen Namen für Ihre Richtlinie ein, der mit beginnt AWSLogDeliveryFirehoseCrossAccountRole, und wählen Sie dann Richtlinie erstellen aus.
5. Wählen Sie im Navigationsbereich Rollen aus.

6. Wählen Sie Rolle erstellen aus.
7. Für Trusted entity type (Vertrauenstyp der Entität), wählen Sie Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie). Für Custom trust policy (Benutzerdefinierte Vertrauensrichtlinie), ersetzen Sie `"Principal": {},` mit dem Folgenden, was die Rolle des Quellkontos angibt. Wählen Sie Weiter aus.

```
"Principal": {
   "AWS": "arn:aws:iam::source-account:role/mySourceRole"
},
```

8. Wählen Sie auf der Seite Add permissions (Berechtigungen hinzufügen) die zuvor in diesem Verfahren erstellte Richtlinie und anschließend Next (Weiter).
9. Geben Sie einen Namen für die Rolle sowie optional eine Beschreibung ein.
10. Wählen Sie Rolle erstellen aus.

Erstellen Sie ein Flow-Protokoll, das in Amazon Data Firehose veröffentlicht wird

Sie können Flow-Protokolle für Ihre VPCs, Subnetze oder Netzwerkschnittstellen erstellen.

Voraussetzungen

- Erstellen Sie den Amazon Data Firehose-Ziel-Lieferstream. Verwenden Sie Direct Put als Quelle. Weitere Informationen finden Sie unter Erstellen eines Amazon Data Firehose-Lieferdatenstroms.
- Wenn Sie Flow-Protokolle in einem anderen Konto veröffentlichen, erstellen Sie die erforderlichen IAM-Rollen, wie unter the section called “IAM-Rollen für die kontoübergreifende Bereitstellung” beschrieben.

Um ein Flow-Protokoll zu erstellen, das in Amazon Data Firehose veröffentlicht wird

1. Führen Sie eine der folgenden Aktionen aus:
   - Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/. Wählen Sie im Navigationsbereich Network Interfaces aus. Aktivieren Sie das Kontrollkästchen für die Netzwerkschnittstelle.
   - Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus. Aktivieren Sie das Kontrollkästchen für die VPC.

- Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/. Wählen Sie im Navigationsbereich Subnets (Subnetze) aus. Aktivieren Sie das Kontrollkästchen für das Subnetz.

2. Klicken Sie auf Actions (Aktionen), Create flow log (Flow-Protokoll erstellen).
3. Geben Sie für Filter den Typ des zu protokollierenden Verkehrs an.
   - Accept (Akzeptieren) – Nur akzeptierten Datenverkehr protokollieren
   - Reject (Ablehnen) – Nur abgelehnten Datenverkehr protokollieren
   - All (Alle) – Akzeptierten und abgelehnten Verkehr protokollieren
4. Wählen Sie unter Maximum aggregation interval (Maximales Aggregationsintervall) den maximalen Zeitraum aus, in dem ein Flow erfasst und zu einem Flow-Protokolldatensatz aggregiert wird.
5. Wählen Sie für Destination (Ziel) eine der folgenden Optionen:
   - Mit demselben Konto an Amazon Data Firehose senden — Der Lieferstream und die zu überwachende Ressource befinden sich auf demselben Konto.
   - Mit einem anderen Konto an Amazon Data Firehose senden — Der Lieferstream und die zu überwachende Ressource befinden sich in unterschiedlichen Konten.
6. Wählen Sie für den Amazon Data Firehose-Streamnamen den Lieferstream aus, den Sie erstellt haben.
7. [Nur kontoübergreifende Lieferung] Für IAM roles (IAM-Rollen) spezifizieren Sie die erforderlichen Rollen (siehe the section called “IAM-Rollen für die kontoübergreifende Bereitstellung”).
8. Für Log record format (Datensatzformat protokollieren) geben Sie das Format für den Flow-Protokolldatensatz an.
   - Wenn Sie das Standardformat für Flow-Protokolldatensätze verwenden möchten, wählen Sie AWS default format (-Standardformat).
   - Wenn Sie ein benutzerdefiniertes Format erstellen möchten, wählen Sie Custom format (Benutzerdefiniertes Format). Wählen Sie für Protokollformat die Felder, die im Flow-Protokolldatensatz berücksichtigt werden sollen.
9. Wählen Sie unter Zusätzliche Metadaten aus, ob Sie Metadaten von Amazon ECS in das Protokollformat einbeziehen möchten.
10. (Optional) Wählen Sie Tag hinzufügen, um Tags auf das Flow-Protokoll anzuwenden.

11. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

Um ein Flow-Protokoll zu erstellen, das mit einem Befehlszeilentool in Amazon Data Firehose veröffentlicht wird

Verwenden Sie einen der folgenden Befehle:

- create-flow-logs (AWS CLI)
- New-EC2FlowLogs (AWS Tools for Windows PowerShell)

Im folgenden AWS CLI Beispiel wird ein Flow-Protokoll erstellt, das den gesamten Datenverkehr für die angegebene VPC erfasst und die Flow-Protokolle an den angegebenen Amazon Data Firehose-Lieferstream im selben Konto übermittelt.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream
```

Das folgende AWS CLI Beispiel erstellt ein Flow-Protokoll, das den gesamten Datenverkehr für die angegebene VPC erfasst und die Flow-Protokolle an den angegebenen Amazon Data Firehose-Lieferstream in einem anderen Konto übermittelt.

```
aws ec2 create-flow-logs --traffic-type ALL \
  --resource-type VPC \
  --resource-ids vpc-00112233344556677 \
  --log-destination-type kinesis-data-firehose \
  --log-destination arn:aws:firehose:us-
east-1:123456789012:deliverystream:flowlogs_stream \
  --deliver-logs-permission-arn arn:aws:iam::source-account:role/mySourceRole \
  --deliver-cross-account-role arn:aws:iam::destination-account:role/
AWSLogDeliveryFirehoseCrossAccountRole
```

Prozessflussprotokolldatensätze in Amazon Data Firehose

Sie können die Flow-Protokolldaten von dem Ziel abrufen, das Sie für den Bereitstellungsstream konfiguriert haben.

Abfragen von Flow-Protokollen mit Amazon Athena

Amazon Athena ist ein interaktiver Abfrageservice, mit dem Sie Daten in Amazon S3, wie Ihre Flow-Protokolle, mithilfe von Standard-SQL analysieren können. Sie können Athena mit VPC Flow Logs verwenden, um schnell umsetzbare Einblicke in den Verkehr zu erhalten, der durch Ihre VPC fließt. Sie können beispielsweise ermitteln, welche Ressourcen in Ihren Virtual Private Clouds (VPCs) die Top-Talker sind, oder die IP-Adressen mit den meisten abgelehnten TCP-Verbindungen identifizieren.

Optionen

- Sie können die Integration Ihrer VPC-Flow-Logs mit Athena optimieren und automatisieren, indem Sie eine CloudFormation Vorlage generieren, die die erforderlichen AWS Ressourcen und vordefinierten Abfragen erstellt, die Sie ausführen können, um Einblicke in den Datenverkehr zu erhalten, der durch Ihre VPC fließt.
- Sie können eigene Abfragen mit Athena erstellen. Weitere Informationen finden Sie unter Abfragen von Flow-Protokollen mit Amazon Athena im Amazon Athena-Benutzerhandbuch.

Preisgestaltung

Für die Durchführung von Anfragen fallen Ihnen standardmäßige Amazon Athena-Gebühren an. Es fallen Ihnen standardmäßige AWS Lambda -Gebühren für die Lambda-Funktion an, die neue Partitionen nach einem wiederkehrenden Zeitplan lädt (wenn Sie eine Partitionsladehäufigkeit, aber kein Start- und Enddatum angeben).

Verwenden der vordefinierten Abfragen

- Generieren Sie die Vorlage mithilfe der Konsole CloudFormation
- Generieren Sie die CloudFormation Vorlage mit dem AWS CLI
- Ausführen einer vordefinierten Abfrage

Generieren Sie die Vorlage mithilfe der Konsole CloudFormation

Nachdem die ersten Flow-Logs an Ihren S3-Bucket geliefert wurden, können Sie Athena integrieren, indem Sie eine CloudFormation Vorlage generieren und die Vorlage verwenden, um einen Stack zu erstellen.

Voraussetzungen

- Die ausgewählte Region muss Amazon Athena unterstützen AWS Lambda .

- Die Amazon S3-Buckets müssen sich in der ausgewählten Region befinden.
- Das Protokollsatzformat für das Ablaufprotokoll muss die Felder enthalten, die von den spezifischen vordefinierten Abfragen, die Sie ausführen möchten, verwendet werden.

So generieren Sie die Vorlage mit der Konsole

1. Führen Sie eine der folgenden Aufgaben aus:
   - Öffnen Sie die Amazon VPC-Konsole. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) und dann Ihr VPC aus.
   - Öffnen Sie die Amazon VPC-Konsole. Wählen Sie im Navigationsbereich die Option Subnets (Subnetze) und dann Ihr Subnetz aus.
   - Öffnen Sie die Amazon EC2-Konsole. Klicken Sie im Navigationsbereich auf Network Interfaces (Netzwerkschnittstellen) und dann Ihre Netzwerkschnittstelle aus.
2. Wählen Sie auf der Registerkarte Flow logs (Flow-Protokolle) ein Flow-Protokoll aus, das in Amazon S3 veröffentlicht wird, und wählen Sie dann Actions (Aktionen), Generate Athena Integration (Athena-Integration generieren) aus.
3. Geben Sie die Ladehäufigkeit der Partition an. Wenn Sie None (Keine) wählen, müssen Sie das Start- und Enddatum der Partition unter Verwendung von in der Vergangenheit liegenden Daten angeben. Wenn Sie Daily (Täglich), Weekly (Wöchentlich) oder Monthly (Monatlich) auswählen, sind das Start- und Enddatum der Partition optional. Wenn Sie kein Start- und Enddatum angeben, erstellt die CloudFormation Vorlage eine Lambda-Funktion, die neue Partitionen nach einem wiederkehrenden Zeitplan lädt.
4. Wählen oder erstellen Sie einen S3-Bucket für die generierte Vorlage und einen S3-Bucket für die Abfrageergebnisse.
5. Wählen Sie Generate Athena Integration (Athena-Integration generieren aus.
6. (Optional) Wählen Sie in der Erfolgsmeldung den Link aus, um zu dem Bucket zu navigieren, den Sie für die CloudFormation Vorlage angegeben haben, und passen Sie die Vorlage an.
7. Wählen Sie in der Erfolgsmeldung Create CloudFormation Stack aus, um den Assistenten Create Stack in der AWS CloudFormation Konsole zu öffnen. Die URL für die generierte CloudFormation Vorlage ist im Abschnitt Vorlage angegeben. Schließen Sie den Assistenten ab, um die Ressourcen zu erstellen, die in der Vorlage angegeben sind.

Mit der CloudFormation Vorlage erstellte Ressourcen

- Eine Athena-Datenbank. Der Datenbankname lautet vpcflowlogsathenadatabase<flow-logs-subscription-id>.
- Eine Athena-Arbeitsgruppe. Der Arbeitsgruppenname lautet <flow-log-subscription-id><partition-load-frequency><start-date><end-date>workgroup.
- Eine partitionierte Athena-Tabelle, die Ihren Flow-Protokolldatensätzen entspricht. Der Tabellenname lautet <flow-log-subscription-id><partition-load-frequency><start-date><end-date>.
- Eine Gruppe von Athena-benannten Abfragen. Weitere Informationen finden Sie unter Vordefinierte Abfragen.
- Eine Lambda-Funktion, die neue Partitionen nach dem angegebenen Zeitplan (täglich, wöchentlich oder monatlich) in die Tabelle lädt.
- Eine IAM-Rolle, die die Berechtigung zum Ausführen der Lambda-Funktionen gewährt.

Generieren Sie die CloudFormation Vorlage mit dem AWS CLI

Nachdem die ersten Flow-Logs an Ihren S3-Bucket übermittelt wurden, können Sie eine CloudFormation Vorlage für die Integration mit Athena generieren und verwenden.

Verwenden Sie den folgenden Befehl get-flow-logs-integration-template, um die Vorlage zu generieren. CloudFormation

```
aws ec2 get-flow-logs-integration-template --cli-input-json file://config.json
```

Das folgende Beispiel zeigt eine `config.json`-Datei.

```
{
    "FlowLogId": "fl-12345678901234567",
    "ConfigDeliveryS3DestinationArn": "arn:aws:s3:::my-flow-logs-athena-integration/
templates/",
    "IntegrateServices": {
        "AthenaIntegrations": [
            {
                "IntegrationResultS3DestinationArn": "arn:aws:s3:::my-flow-logs-
analysis/athena-query-results/",
                "PartitionLoadFrequency": "monthly",
                "PartitionStartDate": "2021-01-01T00:00:00",
                "PartitionEndDate": "2021-12-31T00:00:00"
            }
```

```
        ]
    }
}
```

Verwenden Sie den folgenden create-stack-Befehl, um mithilfe der generierten Vorlage einen Stack zu erstellen. CloudFormation

```
aws cloudformation create-stack --stack-name my-vpc-flow-logs --template-body file://
my-cloudformation-template.json
```

Ausführen einer vordefinierten Abfrage

Die generierte CloudFormation Vorlage enthält eine Reihe vordefinierter Abfragen, die Sie ausführen können, um schnell aussagekräftige Einblicke in den Datenverkehr in Ihrem AWS Netzwerk zu erhalten. Nachdem Sie den Stack erstellt und überprüft haben, ob alle Ressourcen korrekt erstellt wurden, können Sie eine der vordefinierten Abfragen ausführen.

So führen Sie eine vordefinierte Abfrage mit der Konsole aus

1. Öffnen Sie die Athena-Konsole.
2. Wählen Sie im Navigationsbereich die Option Query Editor (Abfrage-Editor) aus. Wählen Sie unter Arbeitsgruppe die Arbeitsgruppe aus, die mit der CloudFormation Vorlage erstellt wurde.
3. Wählen Sie Saved queries (Gespeicherte Abfragen) aus, wählen Sie eine Abfrage aus, ändern Sie die Parameter nach Bedarf und führen Sie dann die Abfrage aus. Eine Liste der verfügbaren vordefinierten Abfragen finden Sie unter Predefined queries (Vordefinierte Abfragen).
4. Sehen Sie sich unter Query results (Abfrageergebnisse) die Abfrageergebnisse an.

Vordefinierte Abfragen

Das Folgende ist eine vollständige Liste der Athena-benannten Abfragen. Die vordefinierten Abfragen, die beim Generieren der Vorlage bereitgestellt werden, hängen von den Feldern ab, die Teil des Protokolldatensatzformats für das Ablaufprotokoll sind. Daher enthält die Vorlage möglicherweise nicht alle diese vordefinierten Abfragen.

- VpcFlowLogsAcceptedVerkehr — Die TCP-Verbindungen, die auf der Grundlage Ihrer Sicherheitsgruppen und Netzwerk-ACLs zugelassen wurden.
- VpcFlowLogsAdminPortTraffic— Die 10 IP-Adressen mit dem meisten Datenverkehr, aufgezeichnet von Anwendungen, die Anfragen an Administrator-Ports bearbeiten.

- VpcFlowLogsIPv4Traffic — Die Gesamtzahl der Byte des aufgezeichneten IPv4-Datenverkehrs.
- VpcFlowLogsIPv6Traffic — Die Gesamtzahl der Byte des aufgezeichneten IPv6-Verkehrs.
- VpcFlowLogsRejectedTCPTraffic — Die TCP-Verbindungen, die aufgrund Ihrer Sicherheitsgruppen oder Netzwerk-ACLs abgelehnt wurden.
- VpcFlowLogsRejectedVerkehr — Der Datenverkehr, der aufgrund Ihrer Sicherheitsgruppen oder Netzwerk-ACLs abgelehnt wurde.
- VpcFlowLogsSshRdpTraffic— Der SSH- und RDP-Verkehr.
- VpcFlowLogsTopTalkers — Die 50 IP-Adressen mit dem meisten aufgezeichneten Verkehr.
- VpcFlowLogsTopTalkersPacketLevel — Die 50 IP-Adressen auf Paketebene mit dem meisten aufgezeichneten Verkehr.
- VpcFlowLogsTopTalkingInstances— Die IDs der 50 Instances mit dem meisten aufgezeichneten Traffic.
- VpcFlowLogsTopTalkingSubnets— Die IDs der 50 Subnetze mit dem meisten aufgezeichneten Verkehr.
- VpcFlowLogsTopTCPTraffic — Der gesamte TCP-Verkehr, der für eine Quell-IP-Adresse aufgezeichnet wurde.
- VpcFlowLogsTotalBytesTransferred— Die 50 Paare von Quell- und Ziel-IP-Adressen mit den meisten aufgezeichneten Byte.
- VpcFlowLogsTotalBytesTransferredPacketLevel— Die 50 Paare von Quell- und Ziel-IP-Adressen auf Paketebene mit den meisten aufgezeichneten Byte.
- VpcFlowLogsTrafficFrmSrcAddr — Der für eine bestimmte Quell-IP-Adresse aufgezeichnete Verkehr.
- VpcFlowLogsTrafficToDstAddr — Der für eine bestimmte Ziel-IP-Adresse aufgezeichnete Verkehr.

Fehlerbehebung bei VPC Flow Logs

Im Folgenden finden Sie mögliche Probleme, die auftreten können, wenn Sie mit Flow-Protokollen arbeiten.

Problembereiche

- Unvollständige Flow-Protokolldatensätze
- Flow-Protokoll ist aktiv, aber keine Flow-Protokolldatensätze oder Protokollgruppen vorhanden
- Fehler „LogDestinationNotFoundAusnahme“ oder „Zugriff verweigert für“ LogDestination

- Überschreiten des Amazon S3-Bucket-Richtlinienlimits
- LogDestination nicht zustellbar

Unvollständige Flow-Protokolldatensätze

Problem

Ihre Flow-Protokolldatensätze sind unvollständig oder werden nicht mehr veröffentlicht.

Ursache

Möglicherweise liegt ein Problem bei der Übermittlung der Flow-Protokolle an die Protokollgruppe CloudWatch Logs vor.

Lösung

Wählen Sie in der Amazon EC2-Konsole oder in der Amazon VPC-Konsole die Registerkarte Flow Logs (Flow-Protokolle) der betroffenen Ressource. Weitere Informationen finden Sie unter Anzeigen eines Flow-Protokolls. In der Tabelle "Flow-Protokolle" werden sämtliche Fehler in der Spalte Status angezeigt. Sie können auch den Befehl describe-flow-logs ausführen und den Wert überprüfen, der im Feld `DeliverLogsErrorMessage` zurückgegeben wird. Einer der folgenden Fehler kann angezeigt werden:

- `Rate limited`: Dieser Fehler kann auftreten, wenn die CloudWatch Protokolldrosselung angewendet wurde, d. h. wenn die Anzahl der Datenflussprotokolleinträge für eine Netzwerkschnittstelle höher ist als die maximale Anzahl von Datensätzen, die innerhalb eines bestimmten Zeitraums veröffentlicht werden können. Dieser Fehler kann auch auftreten, wenn Sie das Kontingent für die Anzahl der CloudWatch Logs-Protokollgruppen, die Sie erstellen können, erreicht haben. Weitere Informationen finden Sie unter CloudWatchServicequotas im CloudWatch Amazon-Benutzerhandbuch.
- `Access error`: Dieser Fehler kann aus folgenden Gründen auftreten:
  - Die IAM-Rolle für Ihr Flow-Protokoll verfügt nicht über ausreichende Berechtigungen, um Flow-Protokolldatensätze in der CloudWatch Protokollgruppe zu veröffentlichen
  - Die IAM-Rolle hat keine Vertrauensbeziehung zum Flow-Protokoll-Service.
  - Die Vertrauensbeziehung legt den Flow-Protokoll-Service nicht als Prinzipal fest.

  Weitere Informationen finden Sie unter IAM-Rolle für die Veröffentlichung von Flow-Protokollen in Logs CloudWatch .

- `Unknown error`: Es ist ein interner Fehler im Flow-Protokoll-Service aufgetreten.

Flow-Protokoll ist aktiv, aber keine Flow-Protokolldatensätze oder Protokollgruppen vorhanden

Problem

Sie haben ein Flow-Protokoll erstellt und in der Amazon VPC- bzw. Amazon EC2-Konsole wird das Flow-Protokoll als `Active` angezeigt. Sie können jedoch keine Protokollstreams in CloudWatch Protokollen oder Protokolldateien in Ihrem Amazon S3 S3-Bucket sehen.

Mögliche Ursachen

- Das Flow-Protokoll wird noch erstellt. Es kann unter Umständen zehn Minuten oder länger dauern, bis nach dem Erstellen des Flow-Protokolls die Protokollgruppe erstellt bzw. Daten angezeigt werden.
- Es wurde noch kein Datenverkehr für Ihre Netzwerkschnittstellen erfasst. Die Protokollgruppe in CloudWatch Logs wird nur erstellt, wenn Datenverkehr aufgezeichnet wird.

Lösung

Warten Sie ein paar Minuten, bis die Protokollgruppe erstellt oder der Datenverkehr aufgezeichnet wird.

Fehler „LogDestinationNotFoundAusnahme“ oder „Zugriff verweigert für“ LogDestination

Problem

Sie erhalten, wenn Sie ein Flow-Protokoll erstellen einen `Access Denied for LogDestination`- oder einen `LogDestinationNotFoundException`-Fehler.

Mögliche Ursachen

- Wenn Sie ein Flow-Protokoll erstellen, das Daten in einem Amazon-S3-Bucket veröffentlicht, weist dieser Fehler darauf hin, dass der angegebene S3-Bucket nicht gefunden wurde oder dass die Bucket-Richtlinie die Zustellung von Protokollen nicht zulässt.

- Bei der Erstellung eines Flow-Protokolls, das Daten in Amazon CloudWatch Logs veröffentlicht, weist dieser Fehler darauf hin, dass die IAM-Rolle die Übermittlung von Protokollen an die Protokollgruppe nicht zulässt.

Lösung

- Stellen Sie beim Veröffentlichen in Amazon S3 sicher, dass Sie den ARN für einen vorhandenen S3-Bucket angegeben haben und dass der ARN das richtige Format hat. Wenn Sie nicht Eigentümer des S3-Buckets sind, überprüfen Sie, ob die Bucket-Richtlinie über die erforderlichen Berechtigungen verfügt und die richtige Konto-ID und den richtigen Bucket-Namen im ARN verwendet.
- Stellen Sie beim Veröffentlichen in CloudWatch Logs sicher, dass die IAM-Rolle über die erforderlichen Berechtigungen verfügt.

Überschreiten des Amazon S3-Bucket-Richtlinienlimits

Problem

Wenn Sie versuchen, ein Flow-Protokoll zu erstellen, wird die folgende Fehlermeldung angezeig: `LogDestinationPermissionIssueException`.

Mögliche Ursachen

Amazon S3 Bucket-Richtlinien sind auf eine Größe von 20 KB beschränkt.

Jedes Mal, wenn Sie ein Flow-Protokoll erstellen, das in einem Amazon S3-Bucket veröffentlicht, fügen wir den angegebenen Bucket-ARN, der den Ordnerpfad enthält, automatisch zum `Resource`-Element in der Richtlinie des Buckets hinzu.

Wenn mehrere Flow-Protokolle erstellt werden, die in den gleichen Bucket veröffentlichen, kann dies zu einer Überschreitung des Bucket-Richtlinienlimits führen.

Lösung

- Bereinigen Sie die Richtlinie des Buckets, indem Sie nicht mehr benötigte Flow-Protokolleinträge entfernen.
- Erteilen Sie Berechtigungen für den gesamten Bucket, indem Sie die einzelnen Protokolleinträge folgendermaßen ersetzen:

```
arn:aws:s3:::bucket_name/*
```

Wenn Sie Berechtigungen für den gesamten Bucket erteilen, fügen neue Flow-Protokollabonnements keine neuen Berechtigungen zur Bucket-Richtlinie hinzu.

LogDestination nicht zustellbar

Problem

Wenn Sie versuchen, ein Flow-Protokoll zu erstellen, wird die folgende Fehlermeldung angezeig: `LogDestination <bucket name> is undeliverable`.

Mögliche Ursachen

Der Amazon S3 S3-Ziel-Bucket wird mit serverseitiger Verschlüsselung mit AWS KMS (SSE-KMS) verschlüsselt, und die Standardverschlüsselung des Buckets ist eine KMS-Schlüssel-ID.

Lösung

Der Wert muss ein KMS-Schlüssel-ARN sein. Ändern Sie den standardmäßigen S3-Verschlüsselungstyp von KMS-Schlüssel-ID zu KMS-Schlüssel-ARN. Weitere Informationen finden Sie unter Standardverschlüsselung konfigurieren im Benutzerhandbuch für Amazon Simple Storage Service.

CloudWatch-Metriken für Ihre VPCs

Amazon VPC veröffentlicht Daten über Ihre VPCs auf Amazon CloudWatch. Sie können Statistiken über Ihre VPCs als geordneten Satz von Zeitreihendaten, den so genannten Metriken, abrufen. Betrachten Sie eine Metrik als eine zu überwachende Variable und die Daten als den Wert dieser Variable im Laufe der Zeit. Weitere Informationen finden Sie im Amazon-CloudWatch-Benutzerhandbuch.

Inhalt

NAU-Metriken und -Dimensionen

Network Address Usage (NAU) ist eine Metrik, die auf Ressourcen in Ihrem virtuellen Netzwerk angewendet wird und Sie bei der Planung und Überwachung der Größe Ihrer VPC unterstützt. Die Überwachung der NAU ist kostenlos. Die Überwachung von NAU ist hilfreich, denn wenn Sie die NAU- oder Peer-NAU-Kontingente für Ihre VPC ausgeschöpft haben, können Sie keine neuen EC2-Instances starten oder neue Ressourcen bereitstellen, beispielsweise Network Load Balancer, VPC-Endpunkte, Lambda-Funktionen, Transit-Gateway-Anhänge und NAT-Gateways.

Wenn Sie die Überwachung der Network Address Usage für eine VPC aktiviert haben, sendet Amazon VPC Metriken im Zusammenhang mit NAU an Amazon CloudWatch. Die Größe einer VPC wird anhand der Anzahl der in der VPC enthaltenen Network Address Usage (NAU)-Einheiten gemessen.

Sie können diese Metriken verwenden, um die Wachstumsrate Ihrer VPC zu ermitteln, vorherzusagen, wann Ihre VPC ihre Größenbeschränkung erreicht, oder Alarme zu erstellen, wenn Größengrenzwerte überschritten werden.

Der `AWS/EC2`-Namespace enthält die folgenden Metriken für die NAU-Überwachung.

Metrik	Beschreibung
`NetworkAddressUsage`	Die NAU-Anzahl pro VPC. Kriterien für die Berichterstattung • Alle 24 Stunden. Dimensions (Abmessungen) • Name: `Per-VPC Metrics`, Wert: Die VPC-ID.
`NetworkAddressUsagePeered`	Die NAU-Anzahl für die VPC und alle VPCs, mit denen sie durch Peering verbunden ist. Kriterien für die Berichterstattung • Alle 24 Stunden.

Metrik	Beschreibung
	Dimensions (Abmessungen) • Name: `Per-VPC Metrics`, Wert: Die VPC-ID.

Der `AWS/Usage`-Namespace enthält die folgenden Metriken für die NAU-Überwachung.

Metrik	Beschreibung
`ResourceCount`	Die NAU-Anzahl pro VPC. Kriterien für die Berichterstattung • Alle 24 Stunden. Dimensions (Abmessungen) • Name: `Service`, Wert: `EC2` • Name: `Type`, Wert: `Resource` • Name: `Resource`, Wert: Die VPC-ID. • Name: `Class`, Wert: `NetworkAddressUsage`
`ResourceCount`	Die NAU-Anzahl für die VPC und alle VPCs, mit denen sie durch Peering verbunden ist. Kriterien für die Berichterstattung • Alle 24 Stunden. Dimensions (Abmessungen) • Name: `Service`, Wert: `EC2` • Name: `Type`, Wert: `Resource` • Name: `Resource`, Wert: Die VPC-ID.

Metrik	Beschreibung
	• Name: `Class`, Wert: `NetworkAddressUsagePeered`
`ResourceCount`	Eine kombinierte Ansicht der NAU-Nutzung über VPCs hinweg. Kriterien für die Berichterstattung • Alle 24 Stunden. Dimensions (Abmessungen) • Name: `Service`, Wert: `EC2` • Name: `Type`, Wert: `Resource` • Name: `Resource`, Wert: `VPC` • Name: `Class`, Wert: `NetworkAddressUsage`
`ResourceCount`	Eine kombinierte Ansicht der NAU-Nutzung durch Peering verbundene VPCs hinweg. Kriterien für die Berichterstattung • Alle 24 Stunden. Dimensions (Abmessungen) • Name: `Service`, Wert: `EC2` • Name: `Type`, Wert: `Resource` • Name: `Resource`, Wert: `VPC` • Name: `Class`, Wert: `NetworkAddressUsagePeered`

Aktivieren oder Deaktivieren der NAU-Überwachung

Um NAU-Metriken in CloudWatch anzuzeigen, müssen Sie zunächst die Überwachung auf jeder zu überwachenden VPC aktivieren.

Um die NAU-Überwachung zu aktieren oder zu deaktivieren

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Your VPCs (Ihre VPCs) aus.
3. Aktivieren Sie das Kontrollkästchen für die VPC.
4. Wählen Sie Actions (Aktionen), Edit VPC settings (VPC-Einstellungen bearbeiten).
5. Führen Sie eine der folgenden Aktionen aus:

    - Um die Überwachung zu aktivieren, wählen Sie Network mapping units metrics settings (Einstellungen für Netzwerkzuordnungseinheiten), Enable network address usage metrics (Metriken der Network Address Usage aktivieren).
    - Um die Überwachung zu deaktivieren, wählen Sie Network mapping units metrics settings (Einstellungen für Netzwerkzuordnungseinheiten), Enable network address usage metrics (Metriken der Network Address Usage aktivieren) ab.

So aktivieren oder deaktivieren Sie die Überwachung mit der Befehlszeile

- modify-vpc-attribute (AWS CLI)
- Edit-EC2VpcAttribute (AWS Tools for Windows PowerShell)

Alarm-Beispiel für NAU CloudWatch

Sie können den AWS CLI-Befehl und Beispiel-`.json` verwenden, um einen Amazon-CloudWatch-Alarm und eine SNS-Benachrichtigung zu erstellen, welche die NAU-Auslastung der VPC mit einem Grenzwert von 50.000 NAUs verfolgen. Für dieses Beispiel müssen Sie zunächst ein Amazon-SNS-Thema erstellen. Weitere Informationen finden Sie unter Erste Schritte mit Amazon SNS im Benutzerhandbuch für Amazon Simple Notification Service.

```
aws cloudwatch put-metric-alarm --cli-input-json file://nau-alarm.json
```

Es folgt ein Beispiel für `nau-alarm.json`.

```
{
    "Namespace": "AWS/EC2",
    "MetricName": "NetworkAddressUsage",
    "Dimensions": [{
        "Name": "Per-VPC Metrics",
        "Value": "vpc-0123456798"
    }],
    "AlarmActions": ["arn:aws:sns:us-west-1:123456789012:my_sns_topic"],
    "ComparisonOperator": "GreaterThanThreshold",
    "Period": 86400,
    "EvaluationPeriods": 1,
    "Threshold": 50000,
    "AlarmDescription": "Tracks NAU utilization of the VPC with 50k NAUs as the
 threshold",
    "AlarmName": "VPC NAU Utilization",
    "Statistic": "Maximum"
}
```

Sicherheit in Amazon Virtual Private Cloud

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von einer Rechenzentrums- und 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 geteilten Verantwortung beschreibt dies als Sicherheit der Cloud selbst 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 Virtual Private Cloud gelten, finden Sie unter AWS Services im Umfang nach Compliance-Programm AWS .
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

In dieser Dokumentation wird erläutert, wie das Modell der übergreifenden Verantwortlichkeit bei der Verwendung von Amazon VPC zum Tragen kommt. Die folgenden Themen veranschaulichen, wie Sie Amazon VPC zur Erfüllung Ihrer Sicherheits- und Compliance-Ziele konfigurieren können. Sie lernen auch, wie Sie andere AWS Services nutzen können, die Sie bei der Überwachung und Sicherung Ihrer Amazon VPC-Ressourcen unterstützen.

Inhalt

Datenschutz in Amazon Virtual Private Cloud

Das AWS Modell der mit gilt für den Datenschutz in Amazon Virtual Private Cloud. Wie in diesem Modell beschrieben, AWS ist es 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 VPC 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.

Richtlinie für den Datenverkehr zwischen Netzwerken in Amazon VPC

Amazon Virtual Private Cloud stellt Features bereit, mit denen Sie die Sicherheit Ihrer Virtual Private Cloud (VPC) erhöhen und überwachen können:

- Sicherheitsgruppen: Sicherheitsgruppen erlauben bestimmten eingehenden und ausgehenden Datenverkehr auf Ressourcenebene (z. B. eine EC2-Instance). Wenn Sie eine Instance starten, können Sie sie mit einer oder mehreren Sicherheitsgruppen verknüpfen. Jede Instance in Ihrer VPC kann einer anderen Reihe von Sicherheitsgruppen zugeordnet werden. Wenn Sie beim Starten einer Instance keine Sicherheitsgruppe festlegen, wird die Instance automatisch mit der Standardsicherheitsgruppe für ihre VPC verknüpft. Weitere Informationen finden Sie unter Sicherheitsgruppen.
- Netzwerk-Zugriffssteuerungslisten (ACL): Netzwerk-ACLs erlauben oder verweigern bestimmten eingehenden oder ausgehenden Datenverkehr auf der Subnetzebene. Weitere Informationen finden Sie unter Datenverkehr in Subnetzen mit Netzwerk-ACLs steuern.
- Flow-Protokolle: Flow-Protokolle erfassen Informationen zum IP-Datenverkehr zu und von Netzwerkschnittstellen in der VPC. Sie können Flow-Protokolle für eine VPC, ein Subnetz oder eine bestimmte Netzwerkschnittstelle erstellen. Flow-Protokolldaten werden in CloudWatch Logs oder Amazon S3 veröffentlicht und können Ihnen helfen, zu restriktive oder zu freizügige Sicherheitsgruppen- und Netzwerk-ACL-Regeln zu diagnostizieren. Weitere Informationen finden Sie unter Protokollieren von IP-Datenverkehr mit VPC Flow Logs.
- Datenverkehrsspiegelung: Sie können den Netzwerkverkehr von einer Elastic Netzwork-Schnittstelle einer Amazon EC2-Instance kopieren. Anschließend können Sie den Datenverkehr an out-of-band Sicherheits- und Überwachungsgeräte senden. Weitere Informationen finden Sie im Leitfaden zur Datenspiegelung.

Identity and Access Management für Amazon VPC

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren steuern, wer authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) ist, Amazon VPC-Ressourcen zu nutzen. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Inhalt

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt davon ab, welche Arbeit Sie in Amazon VPC ausführen.

Servicebenutzer – Wenn Sie zur Ausführung Ihrer Aufgaben den Amazon VPC-Service verwenden, stellt Ihnen Ihr Administrator die erforderlichen Anmeldeinformationen und Berechtigungen bereit. Wenn Sie zur Ausführung von Aufgaben weitere Amazon VPC-Features verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle verstehen, kann Ihnen dies helfen, die richtigen Berechtigungen von Ihrem Administrator anzufordern. Wenn Sie nicht auf ein Feature in Amazon VPC zugreifen können, informieren Sie sich in Fehlerbehebung für Amazon VPC-Identität und -Zugriff.

Serviceadministrator – Wenn Sie in Ihrem Unternehmen die Verantwortung für Amazon VPC-Ressourcen haben, haben Sie wahrscheinlich vollständigen Zugriff auf Amazon VPC. Sie legen die Amazon VPC-Features und -Ressourcen fest, auf die Mitarbeiter zugreifen können. Sie beantragen bei Ihrem IAM-Administrator entsprechende Änderungen für die Berechtigungen Ihrer Service-Benutzer. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM zu verstehen. Weitere Informationen dazu, wie Ihr Unternehmen IAM mit Amazon VPC verwenden kann, finden Sie unter Funktionsweise von der Amazon VPC mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Amazon VPC verfassen können. Informationen zum Anzeigen von Beispielrichtlinien finden Sie unter Beispiele für Amazon VPC-Richtlinien.

Authentifizieren mit Identitäten

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

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

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

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

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

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-

Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

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

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

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

IAM-Rollen

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

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

- Verbundbenutzerzugriff – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter Erstellen von Rollen für externe Identitätsanbieter im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter Berechtigungssätze im AWS IAM Identity Center -Benutzerhandbuch.
- Temporäre IAM-Benutzerberechtigungen – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- Kontoübergreifender Zugriff – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.
- Serviceübergreifender Zugriff — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward Access Sessions (FAS) — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle – Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM

erstellen, ändern und löschen. Weitere Informationen finden Sie unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service im IAM-Benutzerhandbuch.

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

- Anwendungen, die auf Amazon EC2 ausgeführt werden — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden im IAM-Benutzerhandbuch.

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

Verwalten des Zugriffs mithilfe von Richtlinien.

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

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

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

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

Identitätsbasierte Richtlinien

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

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

Ressourcenbasierte Richtlinien

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

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

Zugriffssteuerungslisten (ACLs)

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

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

Weitere Richtlinientypen

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

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

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter Bewertungslogik für Richtlinien.

Funktionsweise von der Amazon VPC mit IAM

Bevor Sie mit IAM den Zugriff auf Amazon VPC verwalten können, sollten Sie sich darüber informieren, welche IAM-Features Sie mit Amazon VPC verwenden können. Einen allgemeinen Überblick darüber, wie Amazon VPC und andere AWS Services mit IAM zusammenarbeiten, finden Sie im AWS IAM-Benutzerhandbuch unter Services, die mit IAM funktionieren.

Inhalt

Mit identitätsbasierten IAM-Richtlinien können Sie zulässige oder abgelehnte Aktionen angeben. Für einige Aktionen können Sie die Ressourcen und Bedingungen angeben, unter denen Aktionen zulässig oder verweigert werden. Amazon VPC unterstützt bestimmte Aktionen, Ressourcen und Bedingungsschlüssel. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der IAM-Referenz für JSON-Richtlinienelemente im IAM-Benutzerhandbuch.

Aktionen

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

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

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

Amazon VPC teilt seinen API-Namespace mit Amazon EC2. Richtlinienaktionen in Amazon VPC verwenden das folgende Präfix vor der Aktion: `ec2:`. Um einem Benutzer beispielsweise die Berechtigung zum Erstellen einer VPC mithilfe der `CreateVpc`-API-Operation zu erteilen, gewähren Sie Zugriff auf die `ec2:CreateVpc`-Aktion. Richtlinienanweisungen müssen entweder ein `Action`- oder ein `NotAction`-Element enthalten.

Um mehrere Aktionen in einer einzelnen Anweisung anzugeben, trennen Sie sie durch Kommata, wie im folgenden Beispiel gezeigt.

```
"Action": [
      "ec2:action1",
      "ec2:action2"
]
```

Sie können auch Platzhalter (*) verwenden, um mehrere Aktionen anzugeben. Beispielsweise können Sie alle Aktionen festlegen, die mit dem Wort `Describe` beginnen, einschließlich der folgenden Aktion:

```
"Action": "ec2:Describe*"
```

Eine Liste von Amazon-VPC-Aktionen finden Sie unter von Amazon EC2 definierte Aktionen in der Service-Autorisierungs-Referenz.

Ressourcen

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

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

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

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

Die VPC-Ressource hat den im folgenden Beispiel gezeigten ARN.

```
arn:${Partition}:ec2:${Region}:${Account}:vpc/${VpcId}
```

Um beispielsweise die VPC `vpc-1234567890abcdef0` in Ihrer Anweisung anzugeben, verwenden Sie den im folgenden Beispiel gezeigten ARN.

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
```

Um alle VPCs in einer bestimmten Region anzugeben, die zu einem bestimmten Konto gehören, verwenden Sie den Platzhalter (*).

```
"Resource": "arn:aws:ec2:us-east-1:123456789012:vpc/*"
```

Einige Amazon VPC-Aktionen, z. B. das Erstellen von Ressourcen, können auf bestimmten Ressourcen nicht ausgeführt werden. In diesen Fällen müssen Sie den Platzhalter (*) verwenden.

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

Viele Amazon EC2-API-Aktionen umfassen mehrere Ressourcen. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie die ARNs durch Kommata voneinander.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Eine Liste von Ressourcentypen und deren ARNs finden Sie unter Von Amazon EC2 definierte Ressourcen in der Service-Autorisierungs-Referenz.

Bedingungsschlüssel

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

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

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

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

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

Alle Amazon EC2-Aktionen unterstützen die Bedingungsschlüssel `aws:RequestedRegion` und `ec2:Region`. Weitere Informationen finden Sie unter Beispiel: Einschränken des Zugriffs auf eine bestimmte Region.

Amazon VPC definiert einen eigenen Satz von Bedingungsschlüsseln und unterstützt auch einige globale Bedingungsschlüssel. Eine Liste von Amazon-VPC-Bedingungsschlüsseln finden Sie unter

Bedingungsschlüssel für Amazon EC2 in der Service-Autorisierungs-Referenz. Informationen dazu, für welche Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon EC2 definierte Aktionen.

Ressourcenbasierte Amazon VPC-Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die angeben, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für die Amazon VPC-Ressource ausführen kann.

Um kontoübergreifenden Zugriff zu ermöglichen, können Sie ein gesamtes Konto oder IAM-Entitäten in einem anderen Konto als Prinzipal in einer ressourcenbasierten Richtlinie angeben. Durch das Hinzufügen eines kontoübergreifenden Auftraggebers zu einer ressourcenbasierten Richtlinie ist nur die halbe Vertrauensbeziehung eingerichtet. Wenn sich der Principal und die Ressource in unterschiedlichen AWS Konten befinden, müssen Sie der Prinzipalentität auch die Erlaubnis erteilen, auf die Ressource zuzugreifen. Sie erteilen Berechtigungen, indem Sie der Entität eine identitätsbasierte Richtlinie anfügen. Wenn jedoch eine ressourcenbasierte Richtlinie Zugriff auf einen Prinzipal in demselben Konto gewährt, ist keine zusätzliche identitätsbasierte Richtlinie erforderlich. Weitere Informationen finden Sie unter Wie sich IAM-Rollen von ressourcenbasierten Richtlinien unterscheiden im IAM-Benutzerhandbuch.

Autorisierung auf der Basis von Markierungen

Sie können Markierungen an Amazon VPC-Ressourcen anfügen oder in einer Anforderung an Amazon VPC übergeben. Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungselement einer Richtlinie mithilfe von Bedingungsschlüsseln Tag-Informationen an. Weitere Informationen finden Sie unter Markieren von Ressourcen während der Erstellung und Kontrollieren des Zugriffs auf EC2-Ressourcen mit Ressourcen-Tags im Amazon-EC2-Benutzerhandbuch.

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter Starten von Instances in einer bestimmten VPC.

IAM-Rollen

Eine IAM-Rolle ist eine Entität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt.

Verwenden temporärer Anmeldeinformationen

Sie können temporäre Anmeldeinformationen verwenden, um sich über einen Verbund anzumelden, eine IAM-Rolle anzunehmen oder eine kontenübergreifende Rolle anzunehmen. Sie erhalten temporäre Sicherheitsanmeldedaten, indem Sie AWS STS API-Operationen wie AssumeRoleoder GetFederationToken aufrufen.

Amazon VPC unterstützt die Verwendung temporärer Anmeldeinformationen.

Service-verknüpfte Rollen

Mit dienstbezogenen Rollen können AWS Dienste auf Ressourcen in anderen Diensten zugreifen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem IAM-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverknüpfte Rollen anzeigen, aber nicht bearbeiten.

Transit-Gateways unterstützen serviceverknüpfte Rollen.

Servicerollen

Dieses Feature ermöglicht einem Service das Annehmen einer Servicerolle in Ihrem Namen. Diese Rolle gewährt dem Service Zugriff auf Ressourcen in anderen Diensten, um eine Aktion in Ihrem Namen auszuführen. Servicerollen werden in Ihrem IAM-Konto angezeigt und gehören zum Konto. Dies bedeutet, dass ein IAM-Administrator die Berechtigungen für diese Rolle ändern kann. Dies kann jedoch die Funktionalität des Services beeinträchtigen.

Amazon VPC unterstützt Servicerollen für Flow-Protokolle. Wenn Sie ein Flow-Protokoll erstellen, müssen Sie eine Rolle auswählen, die dem Flow-Logs-Dienst den Zugriff auf CloudWatch Logs ermöglicht. Weitere Informationen finden Sie unter the section called “IAM-Rolle für die Veröffentlichung von Flow-Protokollen in Logs CloudWatch ”.

Beispiele für Amazon VPC-Richtlinien

IAM-Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von VPC-Ressourcen. Sie können auch keine Aufgaben mit der AWS Management Console AWS CLI, oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Rollen die Berechtigung zum Ausführen bestimmter API-Operationen für die angegebenen Ressourcen gewähren, die diese benötigen. Der Administrator muss diese Richtlinien anschließend den IAM-Rollen anfügen, die diese Berechtigungen benötigen.

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

Inhalt

Bewährte Methoden für Richtlinien

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

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

Anwenden von Berechtigungen finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.
- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Konfigurieren eines MFA-geschützten API-Zugriffs im IAM-Benutzerhandbuch.

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

Verwenden der Amazon VPC-Konsole.

Um auf die Amazon VPC-Konsole zugreifen zu können, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon VPC-Ressourcen in Ihrem AWS Konto aufzulisten und einzusehen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (IAM-Rollen) mit dieser Richtlinie.

Die folgende Richtlinie gewährt einer Rolle die Berechtigung, Ressourcen in der VPC-Konsole aufzulisten, nicht jedoch, sie zu erstellen, zu aktualisieren oder zu löschen.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeClassicLinkInstances",
                "ec2:DescribeClientVpnEndpoints",
                "ec2:DescribeCustomerGateways",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeEgressOnlyInternetGateways",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeManagedPrefixLists",
                "ec2:DescribeMovingAddresses",
                "ec2:DescribeNatGateways",
                "ec2:DescribeNetworkAcls",
                "ec2:DescribeNetworkInterfaceAttribute",
                "ec2:DescribeNetworkInterfacePermissions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribePrefixLists",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroupReferences",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeStaleSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeTrafficMirrorFilters",
                "ec2:DescribeTrafficMirrorSessions",
                "ec2:DescribeTrafficMirrorTargets",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeTransitGatewayVpcAttachments",
                "ec2:DescribeTransitGatewayRouteTables",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcClassicLink",
                "ec2:DescribeVpcClassicLinkDnsSupport",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeVpcEndpointConnectionNotifications",
                "ec2:DescribeVpcEndpointConnections",
```

```
                "ec2:DescribeVpcEndpointServiceConfigurations",
                "ec2:DescribeVpcEndpointServicePermissions",
                "ec2:DescribeVpcEndpointServices",
                "ec2:DescribeVpcPeeringConnections",
                "ec2:DescribeVpcs",
                "ec2:DescribeVpnConnections",
                "ec2:DescribeVpnGateways",
                "ec2:GetManagedPrefixListAssociations",
                "ec2:GetManagedPrefixListEntries"
            ],
            "Resource": "*"
        }
    ]
}
```

Sie müssen Rollen, die nur die AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die den API-Operation entsprechen, die die Rolle ausführen muss.

Erstellen einer VPC mit einem öffentlichen Subnetz

Im folgenden Beispiel können Rollen VPCs, Subnetze, Routing-Tabellen und Internet-Gateways erstellen. Rollen können auch ein Internet-Gateway an eine VPC anfügen und Routen in Routing-Tabellen erstellen. Die `ec2:ModifyVpcAttribute`-Aktion ermöglicht Rollen, DNS-Hostnamen für die VPC zu aktivieren, so dass jede Instance, die in einer VPC gestartet wird, einen DNS-Hostnamen erhält.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": [
        "ec2:CreateVpc",
        "ec2:CreateSubnet",
        "ec2:DescribeAvailabilityZones",
        "ec2:CreateRouteTable",
        "ec2:CreateRoute",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:AssociateRouteTable",
        "ec2:ModifyVpcAttribute"
      ],
```

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

Die vorangehende Richtlinie ermöglicht es Rollen auch, eine VPC in der Amazon-VPC-Konsole zu erstellen.

Ändern und Löschen von VPC-Ressourcen

Sie können bei Bedarf steuern, welche VPC-Ressourcen Rollen ändern oder löschen können. Mit der folgenden Richtlinie können Rollen beispielsweise mit Routing-Tabellen, die die Markierung `Purpose=Test` haben, arbeiten und diese löschen. Die Richtlinie legt außerdem fest, dass Rollen nur Internet-Gateways mit der Markierung `Purpose=Test` löschen können. Rollen können nicht mit Routing-Tabellen oder Internet-Gateways arbeiten, die diese Markierung nicht haben.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:DeleteInternetGateway",
            "Resource": "arn:aws:ec2:*:*:internet-gateway/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteRouteTable",
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": "arn:aws:ec2:*:*:route-table/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Purpose": "Test"
                }
```

```
            }
        }
    ]
}
```

Verwalten von Sicherheitsgruppen

Mit der folgenden Richtlinie können Rollen Sicherheitsgruppen verwalten. Die erste Anweisung ermöglicht es Rollen, jede Sicherheitsgruppe mit der Markierung `Stack=test` zu löschen und die eingehenden und ausgehenden Regeln für jede Sicherheitsgruppe mit der Markierung `Stack=test` zu verwalten. Die zweite Anweisung erfordert, dass Rollen alle von ihnen erstellten Sicherheitsgruppen mit der Markierung `Stack=Test` kennzeichnen. Die dritte Anweisung ermöglicht es Rollen, Markierungen zu erstellen, wenn eine Sicherheitsgruppe erstellt wird. Die vierte Anweisung ermöglicht es Rollen, jede Sicherheitsgruppe und Sicherheitsgruppenregel anzuzeigen. Die fünfte Anweisung ermöglicht es Rollen, eine Sicherheitsgruppe in einer VPC zu erstellen.

> **Note**
>
> Diese Richtlinie kann vom AWS CloudFormation Dienst nicht verwendet werden, um eine Sicherheitsgruppe mit den erforderlichen Tags zu erstellen. Wenn Sie die Bedingung für die Aktion `ec2:CreateSecurityGroup` entfernen, für die das Tag erforderlich ist, funktioniert die Richtlinie.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:ModifySecurityGroupRules",
                "ec2:UpdateSecurityGroupRuleDescriptionsIngress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
```

```
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Stack": "test"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Stack": "test"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "Stack"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateTags",
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateSecurityGroup"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeSecurityGroupRules",
                "ec2:DescribeVpcs",
                "ec2:DescribeSecurityGroups"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:CreateSecurityGroup",
            "Resource": "arn:aws:ec2:*:*:vpc/*"
        }
    ]
```

```
}
```

Damit Rollen die Sicherheitsgruppe ändern können, die einer Instance zugeordnet ist, fügen Sie Ihrer Richtlinie die `ec2:ModifyInstanceAttribute`-Aktion hinzu.

Um Rollen das Ändern von Sicherheitsgruppen für eine Netzwerkschnittstelle zu ermöglichen, fügen Sie der Richtlinie die `ec2:ModifyNetworkInterfaceAttribute`-Aktion hinzu.

Sicherheitsgruppenregeln verwalten

Die folgende Richtlinie erteilt Rollen die Berechtigung, alle Sicherheitsgruppen und Sicherheitsgruppenregeln anzuzeigen, Regeln für ein- und ausgehenden Datenverkehr für die Sicherheitsgruppen für eine bestimmte VPC hinzuzufügen und zu entfernen und Regelbeschreibungen für die angegebene VPC zu ändern. Die erste Anweisung verwendet den Bedingungsschlüssel `ec2:Vpc`, um Berechtigungen für eine bestimmte VPC festzulegen.

Die zweite Anweisung erteilt Rollen die Berechtigung zum Beschreiben aller Sicherheitsgruppen, Sicherheitsgruppenregeln und Markierungen. Auf diese Weise können Rollen Sicherheitsgruppenregeln anzeigen, um sie zu ändern.

```
{
  "Version": "2012-10-17",
  "Statement":[{
    "Effect":"Allow",
    "Action": [
       "ec2:AuthorizeSecurityGroupIngress",
       "ec2:RevokeSecurityGroupIngress",
       "ec2:UpdateSecurityGroupRuleDescriptionsIngress",
       "ec2:AuthorizeSecurityGroupEgress",
       "ec2:RevokeSecurityGroupEgress",
       "ec2:UpdateSecurityGroupRuleDescriptionsEgress",
       "ec2:ModifySecurityGroupRules"
    ],
     "Resource": "arn:aws:ec2:region:account-id:security-group/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
        }
      }
    },
    {
      "Effect": "Allow",
```

```
      "Action": [
          "ec2:DescribeSecurityGroups",
          "ec2:DescribeSecurityGroupRules",
          "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
          "ec2:ModifySecurityGroupRules"
      ],
      "Resource": "arn:aws:ec2:region:account-id:security-group-rule/*"
    }
  ]
}
```

Starten von Instances in einem bestimmten Subnetz

Mit der folgenden Richtlinie wird Rollen die Berechtigung zum Starten von Instances in einem bestimmten Subnetz sowie die Nutzung einer bestimmten Sicherheitsgruppe in der Anfrage gewährt. Die Richtlinie tut dies, indem sie den ARN für das Subnetz und den ARN für die Sicherheitsgruppe angibt. Wenn Rollen versuchen, eine Instance in einem anderen Subnetz zu starten oder eine andere Sicherheitsgruppe zu verwenden, schlägt die Anfrage fehl, sofern Rollen nicht durch andere Richtlinien oder Anweisungen eine entsprechende Erlaubnis dafür gewährt wird.

Außerdem wird in der Richtlinie die Berechtigung zum Verwenden der Netzwerkschnittstellenressource gewährt. Beim Starten einer Instance in einem Subnetz wird mithilfe der Anfrage `RunInstances` standardmäßig eine primäre Netzwerkschnittstelle erstellt. Daher benötigt die Rolle die Berechtigung zum Erstellen dieser Ressource beim Starten der Instance.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:region::image/ami-*",
        "arn:aws:ec2:region:account:instance/*",
        "arn:aws:ec2:region:account:subnet/subnet-id",
        "arn:aws:ec2:region:account:network-interface/*",
        "arn:aws:ec2:region:account:volume/*",
```

```
        "arn:aws:ec2:region:account:key-pair/*",
        "arn:aws:ec2:region:account:security-group/sg-id"
      ]
    }
  ]
}
```

Starten von Instances in einer bestimmten VPC

Mit der folgenden Richtlinie wird Rollen die Berechtigung zum Starten von Instances in beliebigen Subnetzen einer bestimmten VPC gewährt. Hierfür wird ein Bedingungsschlüssel (`ec2:Vpc`) auf die Subnetzressource angewendet.

Außerdem wird mit der Richtlinie Rollen die Berechtigung zum Starten von Instances ausschließlich mit AMIs mit der Markierung „`department=dev`“ gewährt.

```
{
   "Version": "2012-10-17",
   "Statement": [{
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region:account-id:subnet/*",
        "Condition": {
         "ArnEquals": {
            "ec2:Vpc": "arn:aws:ec2:region:account-id:vpc/vpc-id"
         }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:region::image/ami-*",
      "Condition": {
         "StringEquals": {
            "ec2:ResourceTag/department": "dev"
            }
      }
   },
   {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
         "arn:aws:ec2:region:account:instance/*",
```

```
            "arn:aws:ec2:region:account:volume/*",
            "arn:aws:ec2:region:account:network-interface/*",
            "arn:aws:ec2:region:account:key-pair/*",
            "arn:aws:ec2:region:account:security-group/*"
            ]
        }
    ]
}
```

Weitere Beispiele für Amazon VPC-Richtlinien

Weitere IAM-Beispielrichtlinien zu Amazon VPC finden Sie in der folgenden Dokumentation:

- Verwaltete Präfixlisten
- Datenverkehrsspiegelung
- Transit-Gateways
- VPC-Endpunkte und VPC-Endpunktservices
- VPC-Endpunktrichtlinien
- VPC-Peering
- AWS Wavelength

Fehlerbehebung für Amazon VPC-Identität und -Zugriff

Diagnostizieren und beheben Sie mithilfe der folgenden Informationen gängige Probleme, die bei der Verwendung von Amazon VPC und IAM auftreten können.

Problembereiche

- Ich bin nicht autorisiert, eine Aktion in Amazon VPC auszuführen
- Ich bin nicht berechtigt, iam auszuführen: PassRole
- Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Amazon VPC-Ressourcen ermöglichen

Ich bin nicht autorisiert, eine Aktion in Amazon VPC auszuführen

Wenn Ihnen AWS Management Console mitgeteilt wird, dass Sie nicht berechtigt sind, eine Aktion auszuführen, müssen Sie sich an Ihren Administrator wenden, um Unterstützung zu erhalten. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Der folgende Beispielfehler tritt auf, wenn der `mateojackson`-IAM-Benutzer versucht, die Konsole zum Anzeigen von Details zu einem Subnetz zu verwenden, das jedoch zu einer IAM-Rolle gehört, die nicht über `ec2:DescribeSubnets`-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 ec2:DescribeSubnets on resource: subnet-id
```

In diesem Fall bittet Mateo seinen Administrator um die Aktualisierung der Richtlinie, um auf das Subnetz zugreifen zu können.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zur Ausführung der Aktion `iam:PassRole` autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Amazon VPC übergeben zu können.

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

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

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

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

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

Ich möchte Personen außerhalb meines AWS Kontos den Zugriff auf meine Amazon VPC-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem

die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen finden Sie hier:

- Informationen dazu, ob Amazon VPC diese Features unterstützt, finden Sie unter Funktionsweise von der Amazon VPC mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien im IAM-Benutzerhandbuch.

AWS verwaltete Richtlinien für Amazon Virtual Private Cloud

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

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

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

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

AWS verwaltete Richtlinie: AmazonVPC FullAccess

Sie können die `AmazonVPCFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die vollen Zugriff auf Amazon VPC ermöglichen.

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonVPC FullAccess in der AWS Referenz zu verwalteten Richtlinien.

AWS verwaltete Richtlinie: AmazonVPC Access ReadOnly

Sie können die `AmazonVPCReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die einen schreibgeschützten Zugriff auf Amazon VPC erlauben.

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonVPC ReadOnly Access in der AWS Referenz für verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonVPC Operations CrossAccount NetworkInterface

Sie können die `AmazonVPCCrossAccountNetworkInterfaceOperations`-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die es der Identität ermöglichen, Netzwerkschnittstellen zu erstellen und an kontoübergreifende Ressourcen anzuhängen.

Die Berechtigungen für diese Richtlinie finden Sie unter AmazonVPC CrossAccount NetworkInterface Operations in der AWS Referenz für verwaltete Richtlinien.

Amazon VPC-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon VPC an, seit dieser Service im März 2021 damit begonnen hat, diese Änderungen zu verfolgen.

Änderung	Beschreibung	Datum
the section called “Amazon VPC FullAccess” – Aktualisierung auf eine bestehende Richtlinie	Die GetSecurityGroupsForVpc Aktion wurde hinzugefügt, mit der Sie Sicherheitsgruppen abrufen können, die in Ihrer VPC verwendet werden können.	8. Februar 2024

Änderung	Beschreibung	Datum
the section called “AmazonVPC-Zugriff ReadOnly” – Aktualisierung auf eine bestehende Richtlinie	Die GetSecurityGroupsForVpc Aktion wurde hinzugefügt, mit der Sie Sicherheitsgruppen abrufen können, die in Ihrer VPC verwendet werden können.	8. Februar 2024
the section called “AmazonVPC-Betrieb CrossAccount NetworkInterface” – Aktualisierung auf eine bestehende Richtlinie	Es wurden die Aktionen AssignIpv6Addresses und UnassignIpv6Addresses hinzugefügt, mit denen Sie die IPv6-Adressen verwalten können, die Netzwerkschnittstellen zugeordnet sind.	25. September 2023
the section called “AmazonVPC-Zugriff ReadOnly” – Aktualisierung auf eine bestehende Richtlinie	Die DescribeSecurityGroupRules-Aktion wurde hinzugefügt, mit der Sie Sicherheitsgruppenregeln anzeigen können.	2. August 2021
the section called “Amazon VPC FullAccess” – Aktualisierung auf eine bestehende Richtlinie	Die DescribeSecurityGroupRules- und ModifySecurityGroupRules-Aktionen wurden hinzugefügt, mit denen Sie Sicherheitsgruppenregeln anzeigen und ändern können.	2. August 2021
the section called “Amazon VPC FullAccess” – Aktualisierung auf eine bestehende Richtlinie	Es wurden Aktionen für Carrier-Gateways, IPv6-Pools, lokale Gateways und Routing-Tabellen des lokalen Gateways hinzugefügt.	23. Juni 2021

Änderung	Beschreibung	Datum
the section called “AmazonVPC-Zugriff ReadOnly” – Aktualisierung auf eine bestehende Richtlinie	Es wurden Aktionen für Carrier-Gateways, IPv6-Pools, lokale Gateways und Routing-Tabellen des lokalen Gateways hinzugefügt.	23. Juni 2021

Infrastruktursicherheit in Amazon VPC

Als verwalteter Service ist Amazon Virtual Private 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 VPC 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.

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.

Sie können AWS PrivateLinkdamit Ressourcen in Ihrer VPC so einrichten, dass sie AWS-Services über private IP-Adressen eine Verbindung herstellen, als ob diese Dienste direkt in Ihrer VPC gehostet würden. Daher müssen Sie für den Zugriff kein Internet-Gateway oder NAT-Gerät verwenden. AWS-Services

Kontrollieren des Netzwerkverkehrs

Erwägen Sie die folgenden Optionen für die Kontrolle des Netzwerkverkehrs zu den Ressourcen in Ihrer VPC, wie beispielsweise EC2-Instances:

- Nutzen Sie Sicherheitsgruppen als primären Mechanismus zur Steuerung des Netzwerkzugriffs auf VPCs. 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 als sekundäre Kontrolle (z. B. zum Verweigern einer bestimmten Teilmenge des Datenverkehrs) oder als übergeordnete Subnetzleitplanken wirksam sein. Da Netzwerk-ACLs für ein ganzes Subnetz gelten, können sie außerdem so verwendet werden, als ob defense-in-depth eine Instance jemals ohne die richtige Sicherheitsgruppe gestartet würde.
- Verwenden Sie für Ihre Instances private Subnetze, wenn Sie nicht direkt aus dem Internet erreichbar sein sollen. Verwenden Sie einen Bastion-Host oder ein NAT-Gateway für den Internetzugriff von Instances in einem privaten Subnetz.
- Konfigurieren Sie Subnetz-Routing-Tabellen mit den minimalen Netzwerkrouten, um Ihre Konnektivitätsanforderungen zu erfüllen.
- Erwägen Sie, zusätzliche Sicherheitsgruppen oder Netwerk-Schnittstellen, um den Datenverkehr der Amazon Ec2-Instance-Verwaltung getrennt vom regulären Anwendungsdatenverkehr zu steuern und zu prüfen. So können Sie spezielle IAM-Richtlinien für die Änderungskontrolle implementieren, die die Prüfung von Änderungen an Sicherheitsgruppenregeln oder automatischen Skripten zur Regelüberprüfung erleichtern. Mehrere Netzwerk-Schnittstellen bieten außerdem zusätzliche Optionen zur Steuerung des Netzwerkdatenverkehrs, einschließlich der Möglichkeit, hostbasierte Routing-Richtlinien zu erstellen oder verschiedene VPC-Subnetz-Routing-Regeln basierend auf einer einem Subnetz zugewiesenen Netzwerkschnittstelle zu nutzen.

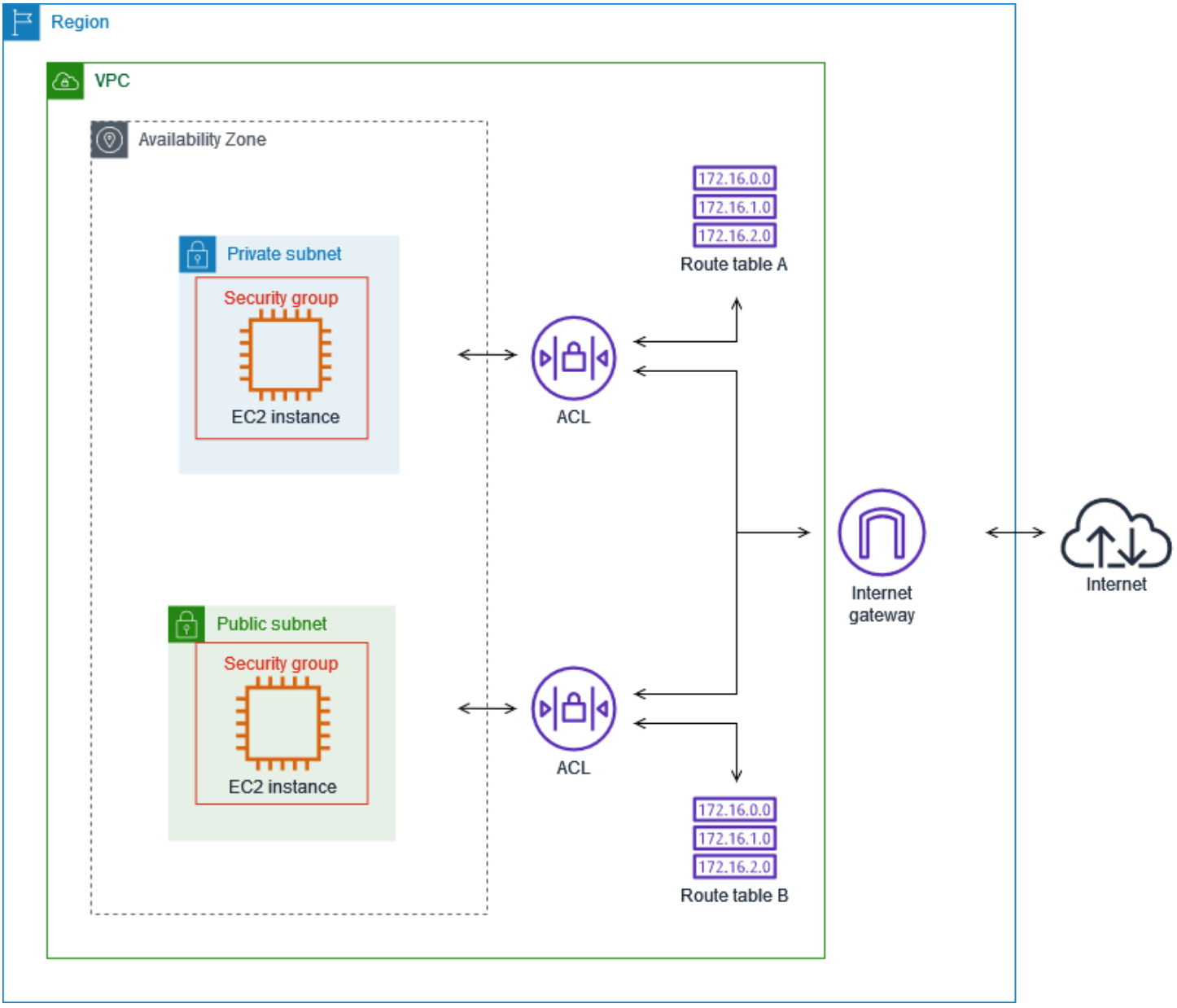
- Verwenden Sie AWS Virtual Private Network oder AWS Direct Connect , um private Verbindungen von Ihren Remote-Netzwerken zu Ihren VPCs herzustellen. Weitere Informationen finden Sie unter Verbindungsoptionen zwischen Netzwerk und Amazon VPC.
- Verwenden Sie VPC Flow-Protokolle, um den Datenverkehr zu überwachen, der Ihre Instances erreicht.
- Verwenden Sie AWS Security Hub, um nach unbeabsichtigten Netzwerkzugriffsmöglichkeiten von Ihren Instances zu suchen.
- Verwenden Sie AWS Network Firewall, um die Subnetze in Ihrer VPC vor allgemeinen Netzwerkbedrohungen zu schützen.

Vergleichen von Sicherheitsgruppen und Netzwerk-ACLs

In der folgenden Tabelle sind die grundlegenden Unterschiede zwischen Sicherheitsgruppen und Netzwerk-ACLs zusammengefasst.

Sicherheitsgruppe	Netzwerk-ACL
Wird auf Instance-Ebene ausgeführt	Wird auf Subnetz-Ebene ausgeführt
Wird nur auf eine Instance angewendet, wenn sie mit der Instance verknüpft ist	Wird auf alle Instances angewendet, die in dem zugeordneten Subnetz bereitgestellt werden (dadurch entsteht eine zusätzliche Verteidig ungsebene, wenn die Sicherheitsgruppenregeln zu viele Rechte gewähren)
Unterstützt nur Regeln zum Erlauben	Unterstützt Regeln zum Erlauben und Verweigern
Alle Regeln werden vor dem Erlauben von Datenverkehr ausgewertet.	Bewertet bei der Entscheidung, ob Datenverk ehr zugelassen werden soll, Regeln der Reihe nach und beginnt mit der niedrigsten nummerierten Regel
Zustandsbehaftet: Rückfließender Datenverk ehr ist unabhängig von Regeln immer erlaubt	Zustandslos: Rückfließender Datenverkehr muss ausdrücklich durch die Regeln zugelasse n werden

Die folgende Abbildung stellt die Sicherheitsebenen dar, die von Sicherheitsgruppen und Netzwerk-ACLs bereitgestellt werden. Datenverkehr von einem Internet-Gateway wird beispielsweise mithilfe der Routen aus der Routing-Tabelle an das entsprechende Subnetz weitergeleitet. Über die Regeln der dem Subnetz zugeordneten Netzwerk-ACL wird festgelegt, welcher Datenverkehr auf das Subnetz zugreifen kann. Über die Regeln der einer Instance zugeordneten Sicherheitsgruppe wird festgelegt, welcher Datenverkehr auf die Instance zugreifen kann.



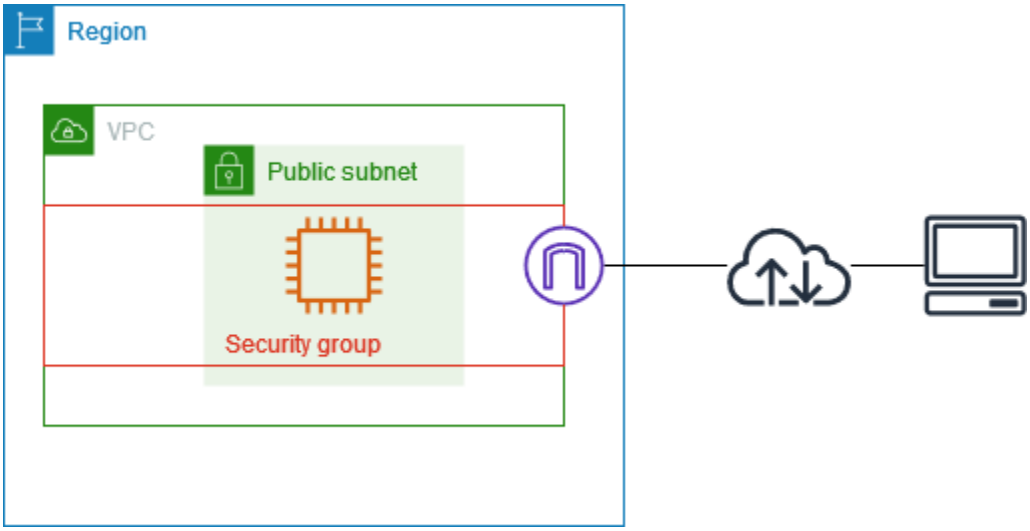
Sie können Ihre Instances nur mit Sicherheitsgruppen sichern. Sie können jedoch Netzwerk-ACLs als zusätzliche Verteidigungsebene hinzufügen. Weitere Informationen finden Sie unter Beispiel: Steuern des Zugriffs auf Instances in einem Subnetz.

Steuern Sie den Datenverkehr zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen

Eine Sicherheitsgruppe steuert den Datenverkehr, der die Ressourcen erreichen und verlassen darf, mit denen er verknüpft ist. Nachdem Sie beispielsweise eine Sicherheitsgruppe mit einer EC2-Instance verknüpft haben, steuert sie den ein- und ausgehenden Datenverkehr für die Instance.

Wenn Sie eine VPC erstellen, verfügt diese über eine Standardsicherheitsgruppe. Sie können für eine VPC zusätzliche Sicherheitsgruppen erstellen, jede mit ihren eigenen Regeln für eingehenden und ausgehenden Datenverkehr. Sie können die Quelle, den Portbereich und das Protokoll für jede Regel für eingehenden Datenverkehr angeben. Sie können das Ziel, den Portbereich und das Protokoll für jede Regel für ausgehenden Datenverkehr angeben.

Das folgende Diagramm zeigt eine VPC mit einer Sicherheitsgruppe, einem Internet-Gateway und einem Subnetz. Das Subnetz enthält eine EC2-Instance. Die Sicherheitsgruppe ist der Instance zugeordnet. Die Sicherheitsgruppe fungiert als virtuelle Firewall. Der einzige Datenverkehr, der die Instance erreicht, ist der Datenverkehr, der nach den Sicherheitsgruppenregeln zulässig ist. Wenn die Sicherheitsgruppe beispielsweise eine Regel enthält, die ICMP-Datenverkehr von Ihrem Netzwerk zur Instance zulässt, können Sie die Instance von Ihrem Computer aus anpingen. Wenn die Sicherheitsgruppe keine Regel enthält, die SSH-Datenverkehr zulässt, konnten Sie mit SSH keine Verbindung zu Ihrer Instance herstellen.



Inhalt

- Sicherheitsgruppenregeln
- Standardsicherheitsgruppen für Ihre VPCs
- Arbeiten mit Sicherheitsgruppen

Preisgestaltung

Für die Nutzung von Sicherheitsgruppen fallen keine zusätzlichen Gebühren an.

Sicherheitsgruppengrundlagen

- Sie können eine Sicherheitsgruppe nur den Ressourcen zuweisen, die in derselben VPC erstellt wurden wie die Sicherheitsgruppe. Sie können einer Ressource mehrere Sicherheitsgruppen zuweisen.
- Wenn Sie eine Sicherheitsgruppe erstellen, müssen Sie einen Namen und eine Beschreibung dafür angeben. Die folgenden Regeln gelten:
  - Der Name einer Sicherheitsgruppe muss innerhalb der VPC eindeutig sein.
  - Namen und Beschreibungen können bis zu 255 Zeichen lang sein.
  - Namen und Beschreibungen dürfen nur die folgenden Zeichen enthalten: a-z, A-Z, 0-9, Leerzeichen und ._-:/()#,@[]+=&;{}!$*.
  - Wenn der Name nachgestellte Leerzeichen enthält, schneiden wir das Leerzeichen am Ende des Namens ab. Wenn Sie beispielsweise „Sicherheitsgruppe testen“ als Namen eingeben, wird er als „Sicherheitsgruppe testen“ gespeichert.
  - Ein Sicherheitsgruppenname darf nicht mit `sg-` beginnen.
- Sicherheitsgruppen sind zustandsbehaftet. Wenn Sie zum Beispiel von Ihrer Instance eine Anforderung senden, wird der Antwortdatenverkehr für diese Anforderung zugelassen, unabhängig der für diese Sicherheitsgruppe geltenden eingehenden Regeln. Antworten auf zulässigen eingehenden Datenverkehr dürfen unabhängig von den Regeln für ausgehenden Datenverkehr die Instance verlassen.
- Sicherheitsgruppen filtern keinen Datenverkehr, der für die folgenden Ziele bestimmt ist oder von diesen ausgeht:
  - Amazon Domain Name Services (DNS)
  - Amazon Dynamic Host Configuration Protocol (DHCP)
  - Amazon EC2-Instance-Metadaten
  - Amazon-ECS-Endpunkte für Aufgabenmetadaten

  - Lizenzaktivierung für Windows-Instances
  - Amazon Time Sync Service
  - Reservierte IP-Adressen, die vom Standard-VPC-Router verwendet werden
- Es gibt Kontingente für die Anzahl der Sicherheitsgruppen, die Sie pro VPC erstellen können, für die Anzahl der Regeln, die Sie den einzelnen Sicherheitsgruppen hinzufügen können, und für die Anzahl der Sicherheitsgruppen, die Sie einer Netzwerkschnittstelle zuordnen können. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.

Bewährte Methoden

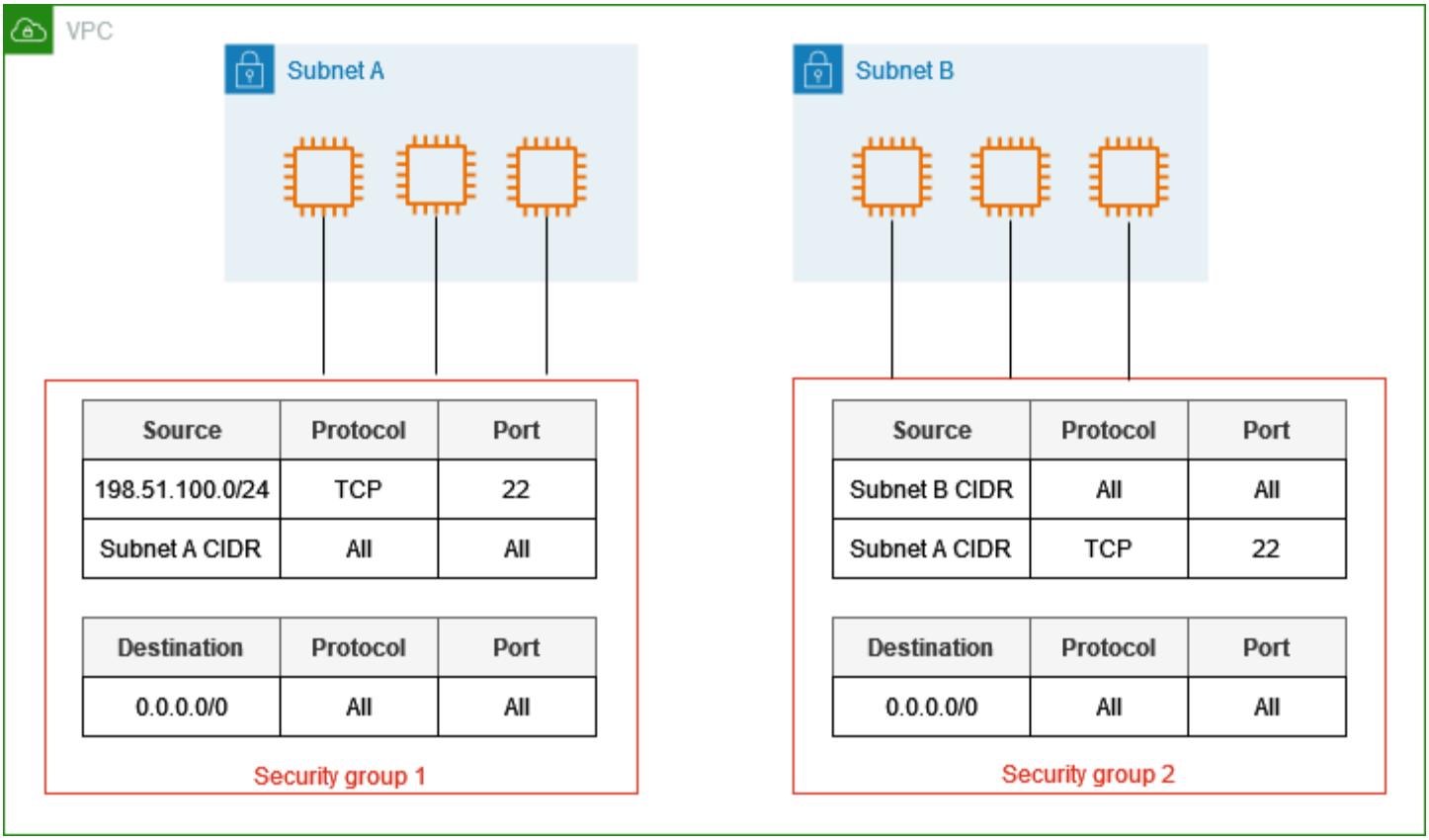
- Autorisieren Sie nur bestimmte IAM-Prinzipale zum Erstellen und Ändern von Sicherheitsgruppen.
- Erstellen Sie die Mindestanzahl von Sicherheitsgruppen, die Sie benötigen, um das Fehlerrisiko zu verringern. Verwenden Sie jede Sicherheitsgruppe, um den Zugriff auf Ressourcen mit ähnlichen Funktionen und Sicherheitsanforderungen zu verwalten.
- Wenn Sie eingehende Regeln für die Ports 22 (SSH) oder 3389 (RDP) hinzufügen, damit Sie auf Ihre EC2-Instances zugreifen können, lassen Sie nur bestimmte IP-Adressbereiche zu. Wenn Sie 0.0.0.0/0 (IPv4) und: ::/ (IPv6) angeben, können alle Benutzer über eine beliebige IP-Adresse mit dem angegebenen Protokoll auf Ihre Instances zugreifen.
- Öffnen Sie keine großen Portbereiche. Stellen Sie sicher, dass der Zugriff über jeden Port auf die Quellen oder Ziele beschränkt ist, die ihn benötigen.
- Ziehen Sie in Erwägung, Netzwerk-ACLs mit ähnlichen Regeln wie Ihre Sicherheitsgruppen zu erstellen, um Ihrer VPC eine zusätzliche Sicherheitsebene hinzuzufügen. Weitere Informationen zu den Unterschieden zwischen Sicherheitsgruppen und Netzwerk-ACLs finden Sie unter Vergleichen von Sicherheitsgruppen und Netzwerk-ACLs.

Beispiel für eine Sicherheitsgruppe

Das folgende Diagramm zeigt eine VPC mit zwei Sicherheitsgruppen und zwei Subnetzen. Die Instances in Subnetz A haben dieselben Konnektivitätsanforderungen und sind daher der Sicherheitsgruppe 1 zugewiesen. Die Instances in Subnetz B haben dieselben Konnektivitätsanforderungen und sind daher der Sicherheitsgruppe 2 zugewiesen. Die Sicherheitsgruppenregeln lassen Datenverkehr wie folgt zu:

- Die erste eingehende Regel in Sicherheitsgruppe 1 erlaubt SSH-Datenverkehr zu den Instances in Subnetz A aus dem angegebenen Adressbereich (z. B. einem Bereich in Ihrem eigenen Netzwerk).

- Die zweite Regel für eingehenden Datenverkehr in Sicherheitsgruppe 1 ermöglicht es den Instances in Subnetz A, über ein beliebiges Protokoll und einen beliebigen Port miteinander zu kommunizieren.
- Die zweite Regel für eingehenden Datenverkehr in Sicherheitsgruppe 2 ermöglicht es den Instances in Subnetz B, über ein beliebiges Protokoll und einen beliebigen Port miteinander zu kommunizieren.
- Die zweite Regel für eingehenden Datenverkehr in Sicherheitsgruppe 2 ermöglicht es den Instances in Subnetz A, über SSH mit den Instances in Subnetz B zu kommunizieren.
- Beide Sicherheitsgruppen nutzen die Standardregel für ausgehenden Datenverkehr, die den gesamten Datenverkehr zulässt.



Sicherheitsgruppenregeln

Die Regeln einer Sicherheitsgruppe steuern den eingehenden Datenverkehr, der die Ressourcen erreichen darf, die der Sicherheitsgruppe zugeordnet sind. Die Regeln steuern auch den ausgehenden Datenverkehr, der sie verlassen darf.

Sie können einer Sicherheitsgruppe Regeln hinzufügen oder diese entfernen (auch als Autorisieren oder Widerrufen des eingehenden bzw. ausgehenden Zugriffs bezeichnet). Eine Regel bezieht sich entweder auf den eingehenden Datenverkehr (Eingang) oder den ausgehenden Datenverkehr (Ausgang). Sie können Zugriff auf eine bestimmte Quelle oder ein bestimmtes Ziel gewähren.

Inhalt

Sicherheitsgruppen – Grundlagen für Regeln

- Sie können Regeln zum Erlauben, aber nicht zum Ablehnen einrichten.
- Wenn Sie eine Sicherheitsgruppe zuerst erstellen, verfügt sie über keine Regeln für den eingehenden Datenverkehr. Aus diesem Grund ist kein eingehender Verkehr erlaubt, bis Sie der Sicherheitsgruppe Regeln für eingehenden Verkehr hinzufügen.
- Wenn Sie zum ersten Mal eine Sicherheitsgruppe erstellen, verfügt diese über eine Regel für ausgehenden Datenverkehr, die den gesamten ausgehenden Datenverkehr von der Ressource zulässt. Sie können die Regel entfernen und ausgehende Regeln hinzufügen, die nur bestimmten ausgehenden Datenverkehr erlauben. Wenn Ihre Sicherheitsgruppe keine Regeln für den ausgehenden Datenverkehr hat, ist kein ausgehender Datenverkehr erlaubt.
- Wenn Sie mehrere Sicherheitsgruppen mit einer Ressource verbinden, werden die Regeln jeder Sicherheitsgruppe effektiv zu einem einzigen Regelsatz zusammengeführt, der verwendet wird um zu bestimmen, ob ein Zugriff zugelassen werden soll.
- Wenn Sie Regeln hinzufügen, aktualisieren oder entfernen, gelten diese Änderungen automatisch für alle Ressourcen, die der Sicherheitsgruppe zugewiesen sind. Die Auswirkung einiger Regeländerungen kann davon abhängen, wie der Datenverkehr nachverfolgt wird. Weitere Informationen finden Sie unter Verbindungsverfolgung im Amazon EC2 EC2-Benutzerhandbuch.

- 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.

Einschränkung

Sicherheitsgruppen können DNS-Anfragen an oder vom Route 53 Resolver nicht blockieren, der manchmal als „VPC+2-IP-Adresse“ bezeichnet wird (siehe Amazon Route 53 Resolverim Amazon Route 53 Developer Guide) oder als DNS bezeichnet. AmazonProvided Um DNS-Anfragen durch den Route 53 Resolver zu filtern, verwenden Sie die DNS-Firewall des Route 53 Resolver.

Komponenten einer Sicherheitsgruppenregel

- 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 the section called “Verwaltete Präfixlisten”.
  - Die ID einer Sicherheitsgruppe. z. B. `sg-1234567890abcdef0`. Weitere Informationen finden Sie unter the section called “Referenzierung von Sicherheitsgruppen”.
- (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 ._-:/()#,@[]+=;{}!$*.

Referenzierung von Sicherheitsgruppen

Wenn Sie eine Sicherheitsgruppe als Quelle oder Ziel für eine Regel angeben, wirkt sich die Regel auf alle Instances aus, die den Sicherheitsgruppen zugeordnet sind. Die Instances können unter Verwendung der privaten IP-Adressen der Instances über das festgelegte Protokoll und den angegebenen Port in die vorgegebene Richtung kommunizieren.

Das Folgende stellt beispielsweise eine Regel für eingehenden Datenverkehr für eine Sicherheitsgruppe dar, die auf die Sicherheitsgruppe sg-0abcdef1234567890 verweist. Diese Regel erlaubt eingehenden SSH-Datenverkehr von den Instances, die mit sg-0abcdef1234567890 verknüpft sind.

Quelle	Protocol (Protokoll)	Port-Bereich
sg-0abcdef1234567890	TCP	22

Berücksichtigen Sie Folgendes, wenn Sie in einer Sicherheitsgruppenregel auf eine Sicherheitsgruppe verweisen:

- Beide Sicherheitsgruppen müssen zur gleichen VPC oder zu per Peering verbundenen VPCs gehören.
- Es werden keine Regeln aus der referenzierten Sicherheitsgruppe der Sicherheitsgruppe hinzugefügt, die darauf verweist.
- Bei Regeln für eingehenden Datenverkehr können die EC2-Instances, die einer Sicherheitsgruppe zugewiesen sind, eingehenden Datenverkehr von den privaten IP-Adressen der EC2-Instances empfangen, die der referenzierten Sicherheitsgruppe zugewiesen sind.
- Bei Regeln für ausgehenden Datenverkehr können die einer Sicherheitsgruppe zugewiesenen EC2-Instances ausgehenden Datenverkehr an die privaten IP-Adressen der EC2-Instances senden, die der referenzierten Sicherheitsgruppe zugewiesen sind.

Einschränkung

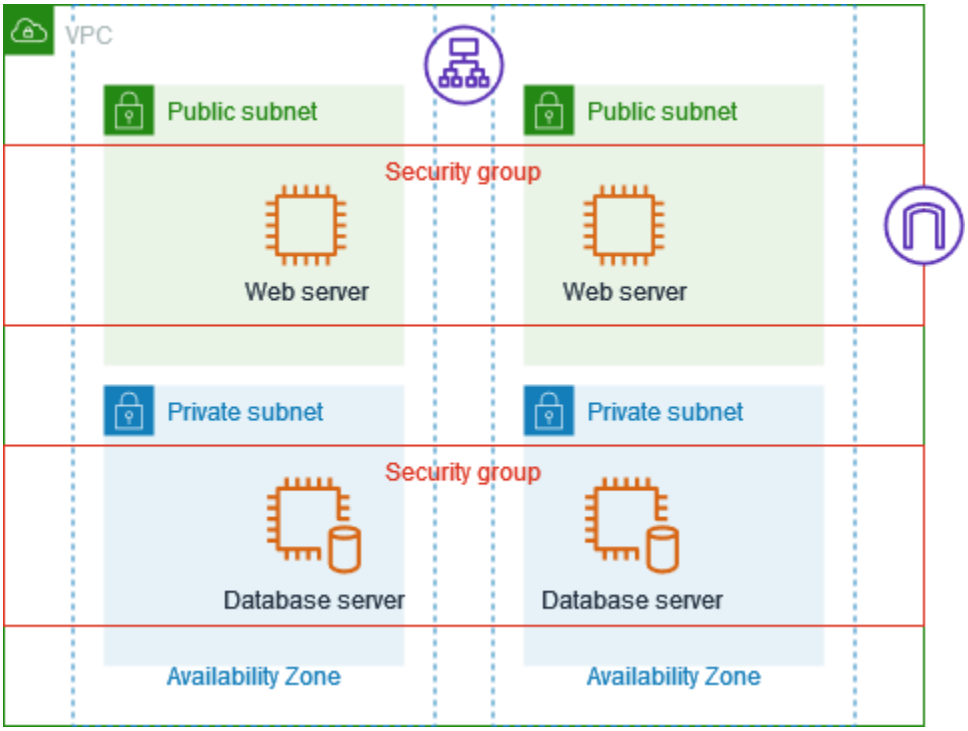
Wenn Sie Routen konfigurieren, um den Datenverkehr zwischen zwei Instances in unterschiedlichen Subnetzen über eine Middlebox-Appliance weiterzuleiten, müssen Sie sicherstellen, dass die Sicherheitsgruppen für beide Instances den Datenverkehr zwischen den Instances zulassen. Die Sicherheitsgruppe für 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.

Beispiel

Das folgende Diagramm zeigt eine VPC mit Subnetzen in zwei Availability Zones, einem Internet-Gateway und einem Application Load Balancer. Jede Availability Zone hat ein öffentliches Subnetz für Webserver und ein privates Subnetz für Datenbankserver. Es gibt separate Sicherheitsgruppen für den Load Balancer, die Webserver und die Datenbankserver. Erstellen Sie die folgenden Sicherheitsgruppenregeln, um Datenverkehr zuzulassen.

- Fügen Sie der Sicherheitsgruppe des Load Balancer Regeln hinzu, um HTTP- und HTTPS-Datenverkehr aus dem Internet zuzulassen. Die Quelle ist 0.0.0.0/0.
- Fügen Sie der Sicherheitsgruppe für die Webserver Regeln hinzu, um nur HTTP- und HTTPS-Datenverkehr vom Load Balancer zuzulassen. Die Quelle ist die Sicherheitsgruppe für den Load Balancer.
- Fügen Sie der Sicherheitsgruppe Regeln für die Datenbankserver Regeln hinzu, um nur Datenbankanforderungen von den Webservern zuzulassen. Die Quelle ist die Sicherheitsgruppe für die Webserver.



Größe der Sicherheitsgruppe

Der Typ der Quelle oder des Ziels bestimmt, wie jede Regel auf die maximale Anzahl von Regeln angerechnet wird, die Sie pro Sicherheitsgruppe haben können.

- Eine Regel, die auf einen CIDR-Block verweist, gilt als eine Regel.
- Eine Regel, die auf eine andere Sicherheitsgruppe verweist, gilt als eine Regel, und zwar unabhängig von der Größe der referenzierten Sicherheitsgruppe.
- Eine Regel, die auf eine vom Kunden verwaltete Präfixliste verweist, gilt als maximale Größe der Präfixliste. Wenn die maximale Größe Ihrer Präfixliste beispielsweise 20 beträgt, gilt eine Regel, die auf diese Präfixliste verweist, als 20 Regeln.
- Eine Regel, die auf eine von AWS-verwaltete Präfixliste verweist, zählt als Gewichtung der Präfixliste. Wenn die Gewichtung der Präfixliste beispielsweise 10 beträgt, zählt eine Regel, die auf diese Präfixliste verweist, als 10 Regeln. Weitere Informationen finden Sie unter the section called “Verfügbare von AWS verwaltete Präfixlisten”.

Veraltete Sicherheitsgruppenregeln

Wenn Ihre VPC über eine VPC-Peering-Verbindung mit einer anderen VPC verfügt oder eine von einem anderen Konto freigegebene VPC verwendet, kann eine Sicherheitsgruppenregel in Ihrer VPC auf eine Sicherheitsgruppe in dieser Peer-VPC oder freigegebenen VPC verweisen. Dadurch können Ressourcen, die der referenzierten Sicherheitsgruppe zugeordnet sind, und solche, die der referenzierenden Sicherheitsgruppe zugeordnet sind, miteinander kommunizieren.

Wenn die Sicherheitsgruppe in der freigegebenen VPC oder die VPC-Peering-Verbindung gelöscht wird, wird die Sicherheitsgruppenregel als veraltet markiert. Sie können veraltete Sicherheitsgruppenregeln genau wie alle anderen Sicherheitsgruppenregeln löschen. Weitere Informationen finden Sie unter Arbeiten mit veralteten Sicherheitsgruppenregeln im Amazon VPC Peering Guide.

Arbeiten mit Sicherheitsgruppenregeln

Die folgenden Aufgaben veranschaulichen, wie Sie mit Sicherheitsgruppenregeln arbeiten.

Erforderliche Berechtigungen

- Sicherheitsgruppenregeln verwalten

Aufgaben

- Hinzufügen von Regeln zu einer Sicherheitsgruppe
- Aktualisieren veralteter Sicherheitsgruppenregeln
- Sicherheitsgruppenregeln markieren
- Löschen von Sicherheitsgruppenregeln

Hinzufügen von Regeln zu einer Sicherheitsgruppe

Wenn Sie eine Regel zu einer Sicherheitsgruppe hinzufügen, wird die neue Regel automatisch auf alle Ressourcen angewendet, die der Sicherheitsgruppe zugeordnet sind.

Wenn Sie über eine VPC-Peering-Verbindung verfügen, können Sie in Ihren Sicherheitsgruppenregeln Sicherheitsgruppen der VPC als Quelle oder Ziel referenzieren. Weitere Informationen finden Sie unter Aktualisieren der Sicherheitsgruppen, um auf Peer-VPC-Gruppen zu verweisen im Amazon VPC-Peering-Handbuch.

Informationen zu den Berechtigungen, die zum Verwalten von Sicherheitsgruppenregeln erforderlich sind, finden Sie unter Sicherheitsgruppenregeln verwalten.

> **Warning**
>
> Wenn Sie Anywhere-IPv4 wählen, lassen Sie Datenverkehr von allen IPv4-Adressen zu. Wenn Sie Anywhere-IPv6 wählen, lassen Sie Datenverkehr von allen IPv6-Adressen zu. Wenn Sie eingehende Regeln für die Ports 22 (SSH) oder 3389 (RDP) hinzufügen, lassen Sie nur bestimmten IP-Adressbereichen Zugriff auf Ihre Instances zu.

Hinzufügen einer Regel mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie die Sicherheitsgruppe aus.
4. Wählen Sie Actions (Aktionen), Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) oder Actions (Aktionen), Edit outbound rules (Regeln für ausgehenden Datenverkehr bearbeiten).
5. 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 TCP oder UDP müssen Sie den zuzulassenden Portbereich eingeben.
   - Für ein benutzerdefiniertes ICMP müssen Sie den Namen des ICMP-Typs aus Protocol (Protokoll= und, falls zutreffend, den Codenamen aus Port range (Portbereich) wählen.
   - Für einen anderen Typ werden das Protokoll und der Portbereich automatisch konfiguriert.

b. Führen Sie unter Source type (Ursprungstyp) (eingehende Regeln) oder Destination type (Zieltyp) (ausgehende Regeln) 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 Anywhere-IPv4, um Datenverkehr von jeder IPv4-Adresse zuzulassen (eingehende Regeln) oder um Datenverkehr zu erlauben, der alle IPv4-Adressen erreicht (ausgehende Regeln). Dies fügt automatisch eine Regel für den IPv4-CIDR-Block 0.0.0.0/0 hinzu.
   - Wählen Sie Anywhere-IPv6, um Datenverkehr von jeder IPv6-Adresse zuzulassen (eingehende Regeln) oder um Datenverkehr zu erlauben, der alle IPv6-Adressen erreicht (ausgehende Regeln). Dies fügt automatisch eine Regel für den ::/0 IPv6-CIDR-Block hinzu.
   - Wählen Sie My IP (Meine IP), um Datenverkehr nur von (eingehende Regeln) oder zu (ausgehende Regeln) der öffentlichen IPv4-Adresse Ihres lokalen Computers zu erlauben.

c. (Optional) Geben Sie für Description (Beschreibung) eine kurze Beschreibung für die Regel an.

6. Wählen Sie Save rules (Regeln speichern) aus.

Um einer Sicherheitsgruppe eine Regel hinzuzufügen, verwenden Sie AWS CLI

Verwenden Sie die Befehle authorize-security-group-ingress und authorize-security-group-egress .

Aktualisieren veralteter Sicherheitsgruppenregeln

Wenn Sie eine Regel aktualisieren, gilt die aktualisierte Regel automatisch für alle Ressourcen, die der Sicherheitsgruppe zugewiesen sind.

Informationen zu den Berechtigungen, die zum Verwalten von Sicherheitsgruppenregeln erforderlich sind, finden Sie unter Sicherheitsgruppenregeln verwalten.

Aktualisieren einer Regel mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie die Sicherheitsgruppe aus.
4. Wählen Sie Actions (Aktionen), Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) oder Actions (Aktionen), Edit outbound rules (Regeln für ausgehenden Datenverkehr bearbeiten).
5. Aktualisieren Sie die Regel nach Bedarf.
6. Wählen Sie Save rules (Regeln speichern) aus.

Um eine Sicherheitsgruppenregel mit dem zu aktualisieren AWS CLI

Verwenden Sie die Befehle modify-security-group-rules, update-security-group-rule-descriptions-ingress, und update-security-group-rule-descriptions-egress.

Sicherheitsgruppenregeln markieren

Fügen Sie Ihren Ressourcen Markierungen hinzu, um sie einfacher ordnen und identifizieren zu können, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können Sicherheitsgruppenregeln Markierungen hinzufügen. Tag-schlüssel müssen für jede Sicherheitsgruppe eindeutig sein. Wenn Sie eine Markierung mit einem Schlüssel hinzufügen, der der Sicherheitsgruppenregel bereits zugeordnet ist, ändert sich der Wert dieser Markierung.

Hinzufügen einer Markierung mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich 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.

Um eine Regel mit dem zu kennzeichnen AWS CLI

Verwenden Sie den Befehl create-tags.

Löschen von Sicherheitsgruppenregeln

Wenn Sie eine Regel aus einer Sicherheitsgruppe löschen, wird die Änderung automatisch auf alle Instances der Sicherheitsgruppe angewendet.

So löschen Sie eine Sicherheitsgruppenregel mithilfe der Konsole:

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie die Sicherheitsgruppe aus.
4. 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.
5. Wählen Sie die Schaltfläche Delete (Löschen) neben der zu löschenden Regel.
6. Wählen Sie Save rules (Regeln speichern) aus. Alternativ können Sie Änderungen in der Vorschau anzeigen wählen, Ihre Änderungen überprüfen und dann Bestätigen auswählen.

Um eine Sicherheitsgruppenregel mit dem zu löschen AWS CLI

Verwenden Sie die Befehle revoke-security-group-ingress und revoke-security-group-egress.

Beispielregeln

Web-Server

Die folgende Tabelle beschreibt Beispielregeln für eine Sicherheitsgruppe für Webserver. Die Webserver können HTTP- und HTTPS-Datenverkehr von allen IPv4- und IPv6-Adressen empfangen und SQL- oder MySQL-Datenverkehr an Ihre Datenbankserver senden.

> **Warning**
>
> Wenn Sie Regeln für die Ports 22 (SSH) oder 3389 (RDP) hinzufügen, damit Sie auf Ihre EC2-Instances zugreifen können, empfehlen wir Ihnen, nur bestimmte IP-Adressbereiche zuzulassen. Wenn Sie 0.0.0.0/0 (IPv4) und: ::/ (IPv6) angeben, können alle Benutzer über eine beliebige IP-Adresse mit dem angegebenen Protokoll auf Ihre Instances zugreifen.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Beschreibung
0.0.0.0/0	TCP	80	Lässt eingehenden HTTP-Zugriff von allen IPv4-Adressen zu
::/0	TCP	80	Lässt eingehenden HTTP-Zugriff von allen IPv6-Adressen zu
0.0.0.0/0	TCP	443	Lässt eingehenden HTTPS-Zugriff von allen IPv4-Adressen zu
::/0	TCP	443	Lässt eingehenden HTTPS-Zugriff von allen IPv6-Adressen zu
Öffentlicher IPv4-Adressbereich Ihres Netzwerks	TCP	22	(Optional) Lässt eingehenden SSH-Zugriff von IPv4-IP-Adressen in Ihrem Netzwerk zu
IPv6-Adressbereich Ihres Netzwerks	TCP	22	(Optional) Lässt eingehenden SSH-Zugriff von IPv6-

Source	Protocol (Protokoll)	Port-Bereich	Beschreibung
			IP-Adressen in Ihrem Netzwerk zu
Öffentlicher IPv4-Adressbereich Ihres Netzwerks	TCP	3389	(Optional) Lässt eingehend en RDP-Zugriff von IPv4-IP-Adressen in Ihrem Netzwerk zu
IPv6-Adressbereich Ihres Netzwerks	TCP	3389	(Optional) Lässt eingehend en RDP-Zugriff von IPv6-IP-Adressen in Ihrem Netzwerk zu
ID dieser Sicherhei tsgruppe	Alle	Alle	(Optional) Lässt eingehend en Datenverkehr von anderen Servern zu, die dieser Sicherheitsgruppe zugeordnet sind

Ausgehend

Ziel	Protocol (Protokoll)	Port-Bereich	Beschreibung
ID der Sicherhei tsgruppe für Instances, auf denen Microsoft SQL Server ausgeführt wird	TCP	1433	Lässt ausgehenden Zugriff auf Microsoft SQL Server zu
ID der Sicherhei tsgruppe für Instances,	TCP	3306	Erlaubt ausgehenden MySQL-Zugriff

Ziel	Protocol (Protokoll)	Port-Bereich	Beschreibung
auf denen MySQL ausgeführt wird			

Datenbankserver

Datenbankserver benötigen Regeln, die spezifische Protokolle für eingehenden Datenverkehr zulassen, z. B. MySQL oder Microsoft SQL Server. Beispiele finden Sie unter Datenbankserverregeln im Benutzerhandbuch für Amazon EC2. Weitere Informationen zu Sicherheitsgruppen für Amazon RDS-DB-Instances finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen im Amazon RDS-Benutzerhandbuch.

Beheben Sie Probleme mit der Erreichbarkeit

Reachability Analyzer ist ein Tool zur statischen Konfigurationsanalyse. Verwenden Sie Reachability Analyzer, um die Netzwerkerreichbarkeit zwischen zwei Ressourcen in Ihrer VPC zu analysieren und zu debuggen. Reachability Analyzer erzeugt hop-by-hop Details zum virtuellen Pfad zwischen diesen Ressourcen, wenn sie erreichbar sind, und identifiziert andernfalls die blockierende Komponente. Es kann beispielsweise fehlende oder falsch konfigurierte Sicherheitsgruppenregeln identifizieren.

Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

Standardsicherheitsgruppen für Ihre VPCs

Ihre Standard-VPCs und alle VPCs, die Sie erstellen, verfügen über eine Standardsicherheitsgruppe. Der Namen der Standard-Sicherheitsgruppe ist „default“.

Es wird empfohlen, Sicherheitsgruppen für bestimmte Ressourcen oder Ressourcengruppen zu erstellen, anstatt die Standardsicherheitsgruppe zu verwenden. Wenn Sie jedoch einigen Ressourcen bei der Erstellung keine Sicherheitsgruppe zuordnen, ordnen wir sie der Standardsicherheitsgruppe zu. Wenn Sie beispielsweise beim Starten einer EC2-Instance keine Sicherheitsgruppe festlegen, wird die Standardsicherheitsgruppe für die zugehörige VPC zugeordnet.

Grundlagen für Standard-Sicherheitsgruppen

- Sie können die Regeln für eine Standardsicherheitsgruppe ändern.

- Sie können eine Standardsicherheitsgruppe nicht löschen. Wenn Sie versuchen, eine Standardsicherheitsgruppe zu löschen, sehen Sie die folgende Fehlermeldung: `Client.CannotDelete`.

Standardregeln

Die folgenden Tabellen beschreiben die Standardregeln für eine 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.

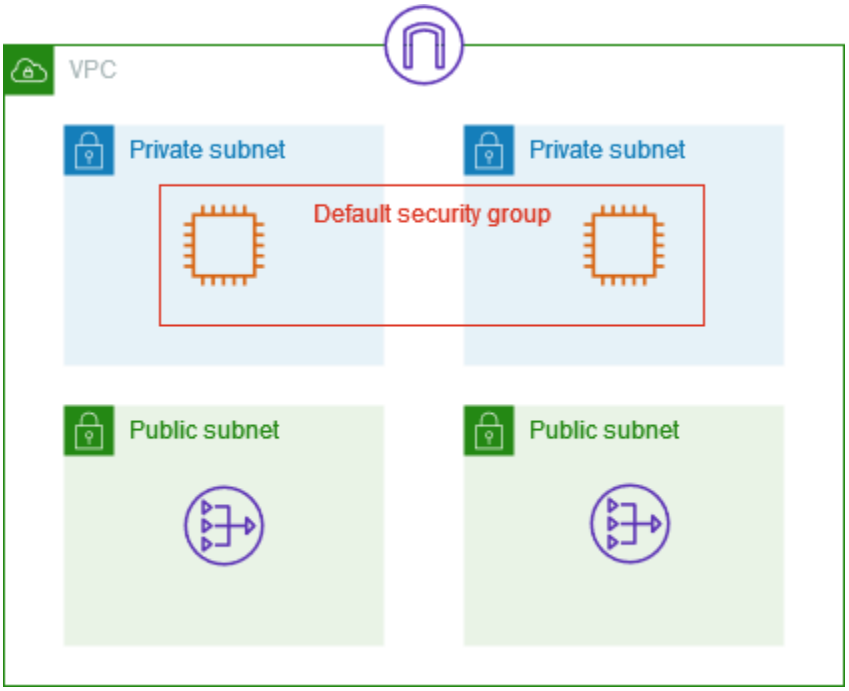
Ausgehend

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.

Beispiel

Das folgende Diagramm zeigt eine VPC mit einer Standard-Sicherheitsgruppe, einem Internet-Gateway und einem NAT-Gateway. Die Standardsicherheit enthält nur ihre Standardregeln und

ist zwei EC2-Instances zugeordnet, die in der VPC ausgeführt werden. In diesem Szenario kann jede Instance eingehenden Datenverkehr von der anderen Instance auf allen Ports und Protokollen empfangen. Die Standardregeln erlauben es den Instances nicht, Datenverkehr vom Internet-Gateway oder vom NAT-Gateway zu empfangen. Wenn Ihre Instances zusätzlichen Datenverkehr erhalten müssen, empfehlen wir Ihnen, eine Sicherheitsgruppe mit den erforderlichen Regeln zu erstellen und die neue Sicherheitsgruppe den Instances anstelle der Standardsicherheitsgruppe zuzuweisen.



Arbeiten mit Sicherheitsgruppen

Die folgenden Aufgaben veranschaulichen, wie Sie mit Sicherheitsgruppen arbeiten.

Aufgaben

- Eine Sicherheitsgruppe erstellen
- Anzeigen Ihrer Sicherheitsgruppen
- Markieren Ihrer Sicherheitsgruppen
- Löschen einer Sicherheitsgruppe
- Verwalten von Sicherheitsgruppen mit Firewall Manager

Erforderliche Berechtigungen

Stellen Sie zuerst sicher, dass Sie über die erforderlichen Berechtigungen verfügen.

- Verwalten von Sicherheitsgruppen
- Sicherheitsgruppenregeln verwalten

Die Regeln einer Sicherheitsgruppe steuern den eingehenden Datenverkehr, der die Ressourcen erreichen darf, die der Sicherheitsgruppe zugeordnet sind. Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppenregeln.

Eine Sicherheitsgruppe erstellen

Standardmäßig enthält jede Sicherheitsgruppe am Anfang nur eine Regel für ausgehenden Datenverkehr, die sämtlichen von der Ressource ausgehenden Datenverkehr zulässt. Sie müssen Regeln hinzufügen, um eingehenden Datenverkehr zuzulassen oder den ausgehenden Datenverkehr einzuschränken.

Erstellen einer Sicherheitsgruppe mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie Create security group (Sicherheitsgruppe erstellen) aus.
4. Geben Sie einen Namen und eine Beschreibung für die Sicherheitsgruppe ein. Sie können den Namen und die Beschreibung einer Regelgruppe nach der Erstellung nicht mehr ändern.
5. Wählen Sie unter VPC eine VPC aus. Die Sicherheitsgruppe kann nur in der VPC verwendet werden, für die sie erstellt wird.
6. 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.
7. 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.
8. Wählen Sie Sicherheitsgruppe erstellen aus.

Nachdem Sie eine Sicherheitsgruppe erstellt haben, möchten Sie möglicherweise einen der folgenden Schritte ausführen:

- Weisen Sie die Sicherheitsgruppe einer EC2-Instance zu, wenn Sie die Instance starten, oder ändern Sie die Sicherheitsgruppe, die derzeit einer Instance zugewiesen ist. Weitere Informationen

finden Sie unter Starten einer Instance oder Ändern von Sicherheitsgruppen im Amazon EC2 EC2-Benutzerhandbuch.

- Fügen Sie Sicherheitsgruppenregeln hinzu. Die Regeln einer Sicherheitsgruppe steuern den eingehenden Datenverkehr, der die Ressourcen erreichen darf, die der Sicherheitsgruppe zugeordnet sind. Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter Arbeiten mit Sicherheitsgruppenregeln.

Um eine Sicherheitsgruppe mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl create-security-group.

Anzeigen Ihrer Sicherheitsgruppen

Sie können Informationen zu Ihren Sicherheitsgruppen wie folgt anzeigen.

So zeigen Sie Ihre Sicherheitsgruppen über die Konsole an

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Ihre Sicherheitsgruppen werden aufgelistet. So zeigen Sie die Details für eine bestimmte Sicherheitsgruppe, einschließlich ihrer eingehenden und ausgehenden Regeln, an. Weitere Informationen zum Aktualisieren von Sicherheitsgruppenregeln finden Sie unter Aktualisieren veralteter Sicherheitsgruppenregeln.

So zeigen Sie alle Sicherheitsgruppen in Regionen an

Öffnen Sie die Amazon EC2 Global View-Konsole unter https://console.aws.amazon.com/ec2globalview/home. Weitere Informationen finden Sie unter Ressourcen mithilfe von Amazon EC2 Global View auflisten und filtern im Amazon EC2 EC2-Benutzerhandbuch.

Um Ihre Sicherheitsgruppen anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie die Befehle describe-security-groups und describe-security-group-rules.

Markieren Ihrer Sicherheitsgruppen

Fügen Sie Ihren Ressourcen Markierungen hinzu, um sie einfacher ordnen und identifizieren zu können, beispielsweise nach Zweck, Besitzer oder Umgebung. Sie können Ihren Sicherheitsgruppe

Markierungen hinzufügen. Markierungsschlüssel müssen für jede Sicherheitsgruppe eindeutig sein. Wenn Sie eine Markierung mit einem Schlüssel hinzufügen, der der Regel bereits zugeordnet ist, ändert sich der Wert dieser Markierung.

So markieren Sie eine Sicherheitsgruppe mit der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Aktivieren Sie das Kontrollkästchen für die Sicherheitsgruppe.
4. Klicken Sie auf Actions (Aktionen), Manage tags (Markierungen verwalten). Auf der Seite Manage tags (Markierungen verwalten) werden alle Markierungen angezeigt, die der Sicherheitsgruppe zugeordnet sind.
5. Um eine Markierung hinzuzufügen, wählen Sie Neues Tag hinzufügen und geben Sie dann den Tagschlüssel und -Wert ein. Um ein Tag (Markierungen) zu löschen, wählen Sie Remove (Entfernen) neben dem zu löschenden Tag (Markierung).
6. Wählen Sie Änderungen speichern aus.

Um eine Sicherheitsgruppe mit dem zu kennzeichnen AWS CLI

Verwenden Sie den Befehl create-tags.

Löschen einer Sicherheitsgruppe

Sie können eine Sicherheitsgruppe nur dann löschen, wenn sie mit keiner Ressource mehr verbunden ist. Sie können eine Standardsicherheitsgruppe nicht löschen.

Wenn Sie die Konsole verwenden, können Sie mehrere Sicherheitsgruppen gleichzeitig löschen. Wenn Sie die Befehlszeile oder die API verwenden, können Sie jeweils nur eine Sicherheitsgruppe löschen.

Löschen einer Sicherheitsgruppe mithilfe der Konsole

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie die Sicherheitsgruppe und dann Aktionen, Sicherheitsgruppe löschen aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Delete (Löschen).

Um eine Sicherheitsgruppe mit dem zu löschen AWS CLI

Verwenden Sie den Befehl delete-security-group.

Verwalten von Sicherheitsgruppen mit Firewall Manager

AWS Firewall Manager vereinfacht die Verwaltung und Wartung Ihrer Sicherheitsgruppe für mehrere Konten und Ressourcen. Mit Firewall Manager können Sie die Sicherheitsgruppen für Ihr Unternehmen von einem einzigen zentralen Administratorkonto aus konfigurieren und überwachen. Danach wendet der Firewall Manager die Regeln und Schutzmaßnahmen automatisch auf Ihre Konten und Ressourcen an, selbst wenn Sie diese erst später hinzufügen. Firewall Manager ist besonders nützlich, wenn Sie Ihre gesamte Organisation schützen möchten oder wenn Sie häufig neue Ressourcen hinzufügen, die Sie vor einem zentralen Administratorkonto schützen möchten.

Sie können Sicherheitsgruppen auf folgende Weise mit Firewall Manager zentral verwalten:

- Konfigurieren allgemeiner Baseline-Sicherheitsgruppen in der gesamten Organisation: Sie können eine gemeinsame Sicherheitsgruppenrichtlinie verwenden, um eine zentral gesteuerte Zuordnung von Sicherheitsgruppen zu Konten und Ressourcen in der gesamten Organisation bereitzustellen. Sie geben an, wo und wie die Richtlinie in Ihrer Organisation angewendet werden soll.
- Prüfen vorhandener Sicherheitsgruppen in Ihrer Organisation: Sie können eine Prüfungssicherheitsgruppenrichtlinie verwenden, um die vorhandenen Regeln zu überprüfen, die in den Sicherheitsgruppen Ihrer Organisation verwendet werden. Sie können die Richtlinie so gestalten, dass alle Konten, bestimmte Konten oder Ressourcen, die in Ihrer Organisation markiert sind, geprüft werden. Firewall Manager erkennt automatisch neue Konten und Ressourcen und prüft diese. Sie können Prüfungsregeln erstellen, um Leitlinien dafür festzulegen, welche Sicherheitsgruppenregeln innerhalb Ihrer Organisation zugelassen oder nicht zugelassen werden sollen, und um nach nicht verwendeten oder redundanten Sicherheitsgruppen zu suchen.
- Abrufen von Berichten über nicht konforme Ressourcen und Beseitigen der Nichtkonformität: Sie können Berichte und Warnungen für nicht konforme Ressourcen für Ihre Baseline- und Prüfungsrichtlinien abrufen. Sie können auch Workflows für die automatische Behebung des Problems festlegen, um alle von Firewall Manager erkannten nicht konformen Ressourcen zu korrigieren.

Weitere Informationen zur Verwendung von Firewall Manager zur Verwaltung Ihrer Sicherheitsgruppen finden Sie in den folgenden Ressourcen im AWS Firewall Manager Entwicklerhandbuch:

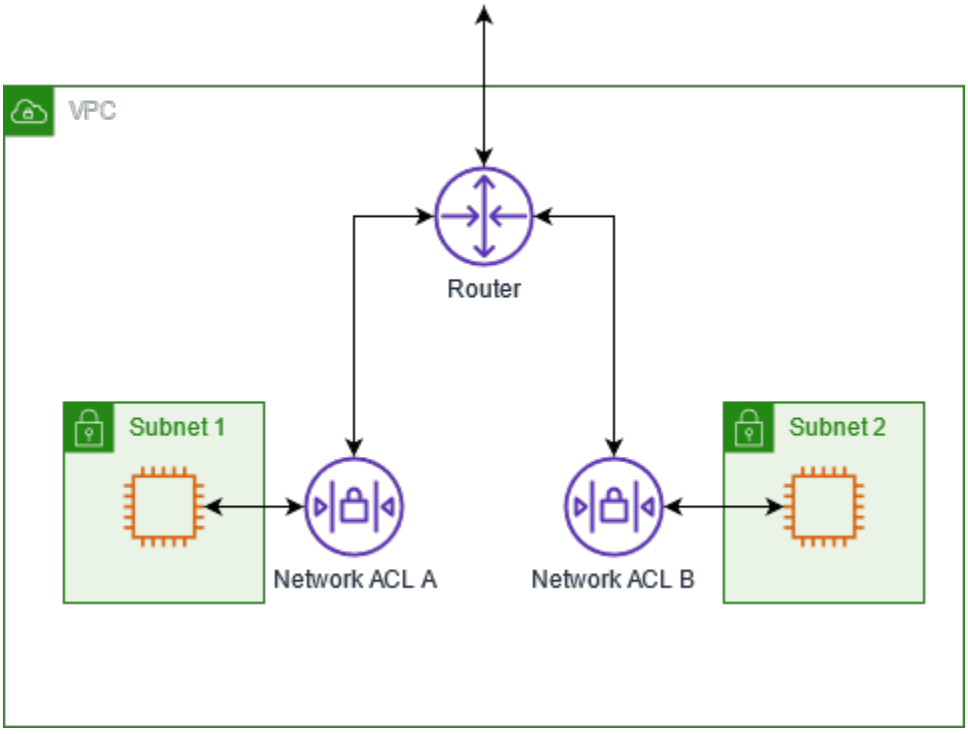
- AWS Firewall Manager Voraussetzungen
- Erste Schritte mit AWS Firewall Manager Amazon VPC-Sicherheitsgruppenrichtlinien
- Wie funktionieren Sicherheitsgruppenrichtlinien in AWS Firewall Manager
- Anwendungsfälle für Sicherheitsgruppenrichtlinien

Datenverkehr in Subnetzen mit Netzwerk-ACLs steuern

Eine Netzwerk-Zugriffssteuerungsliste (ACL) erlaubt oder verweigert bestimmten eingehenden oder ausgehenden Datenverkehr auf der Subnetzebene. Sie können die Standard-Netzwerk-ACL für Ihre VPC verwenden, oder Sie können eine benutzerdefinierte Netzwerk-ACL für Ihre VPC mit Regeln erstellen, die den Regeln für Ihre Sicherheitsgruppen ähneln, um Ihrer VPC eine zusätzliche Sicherheitsebene hinzuzufügen.

Für die Nutzung von Netzwerk-ACLs fallen keine zusätzlichen Gebühren an.

Das folgende Diagramm zeigt eine VPC mit zwei Subnetzen. Jedes Subnetz hat eine Netzwerk-ACL. Wenn Datenverkehr in die VPC gelangt (z. B. von einer durch Peering verbundenen VPC, einer VPN-Verbindung oder dem Internet), sendet der Router den Datenverkehr an das Ziel. Netzwerk-ACL A bestimmt, welcher Datenverkehr, der für Subnetz 1 bestimmt ist, in Subnetz 1 gelangen darf und welcher Datenverkehr, der für einen Standort außerhalb von Subnetz 1 bestimmt ist, Subnetz 1 verlassen darf. In ähnlicher Weise bestimmt Netzwerk-ACL B, welcher Datenverkehr in Subnetz 2 ein- und ausgehen darf.



Weitere Informationen zu den Unterschieden zwischen Sicherheitsgruppen und Netzwerk-ACLs finden Sie unter Vergleichen von Sicherheitsgruppen und Netzwerk-ACLs.

Inhalt

Grundlagen von Netzwerk-ACLs

Nachfolgend werden die Grundlagen von Netzwerk-ACLs beschrieben:

- Ihre VPC verfügt automatisch über eine Standardnetzwerk-ACL, die Sie bearbeiten können. Standardmäßig wird der gesamte eingehende und ausgehende IPv4-Datenverkehr und gegebenenfalls IPv6-Datenverkehr erlaubt.
- Sie können eine benutzerdefinierte Netzwerk-ACL erstellen und einem Subnetz zuordnen. So können Sie bestimmten eingehenden oder ausgehenden Datenverkehr auf der Subnetzebene verweigern.
- Jedes Subnetz in Ihrer VPC muss mit einer Netzwerk-ACL verknüpft werden. Sofern Sie einem Subnetz nicht explizit eine Netzwerk-ACL zuordnen, gilt für das Subnetz automatisch die Standardnetzwerk-ACL.
- Sie können eine Netzwerk-ACL mehreren Subnetzen zuordnen. Ein Subnetz kann jedoch jeweils nur einer Netzwerk-ACL zugeordnet werden. Wenn Sie einem Subnetz eine Netzwerk-ACL zuordnen, wird die bisherige Zuordnung gelöscht.
- Eine Netzwerk-ACL hat Regeln für eingehenden und ausgehenden Datenverkehr. Jede Regel kann Datenverkehr entweder erlauben oder verweigern. Jede Regel hat eine Nummer von 1 bis 32.766. Die Regeln werden der Reihe nach ausgewertet, beginnend mit der Regel mit der niedrigsten Nummer, um zu entscheiden, ob der Verkehr zugelassen oder abgelehnt wird. Wenn der Datenverkehr mit einer Regel übereinstimmt, wird die Regel angewendet und wir werten keine zusätzlichen Regeln aus. Wir empfehlen, zunächst Regeln in Abschnitten zu erstellen (z. B. Abschnitte von 10 oder 100). So können Sie später neue Regeln einfach in Ihre Rangordnung einfügen.
- Wir werten die Netzwerk-ACL-Regeln aus, wenn Datenverkehr in das Subnetz ein- und ausläuft, nicht wenn er innerhalb eines Subnetzes geroutet wird.
- NACLs sind zustandslos, das heißt, Informationen über zuvor gesendeten oder empfangenen Datenverkehr werden nicht gespeichert. Wenn Sie beispielsweise eine NACL-Regel erstellen, um bestimmten eingehenden Datenverkehr zu einem Subnetz zuzulassen, werden Antworten auf diesen Datenverkehr nicht automatisch zugelassen. Dies steht im Gegensatz zur Funktionsweise von Sicherheitsgruppen. Sicherheitsgruppen sind zustandsbehaftet, das heißt, dass Informationen über zuvor gesendeten oder empfangenen Datenverkehr gespeichert werden. Wenn beispielsweise eine Sicherheitsgruppe eingehenden Datenverkehr zu einer EC2-Instance zulässt, werden Antworten unabhängig von den Regeln der ausgehenden Sicherheitsgruppe automatisch zugelassen.
- Netzwerk-ACLs können DNS-Anfragen an oder vom Route 53 Resolver (auch bekannt als VPC+2-IP-Adresse oder DNS) nicht blockieren. AmazonProvided Um DNS-Anfragen durch den Route 53 Resolver zu filtern, können Sie die Route 53 Resolver DNS Firewall im Entwicklerhandbuch für Amazon Route 53 aktivieren.

- Netzwerk-ACLs können den Datenverkehr zum Instance Metadata Service (IMDS) nicht blockieren. Informationen zur Verwaltung des Zugriffs auf IMDS finden Sie unter Konfiguration der Instance-Metadatenoptionen im Benutzerhandbuch für Amazon EC2.
- Netzwerk-ACLs filtern keinen Datenverkehr, der für die folgenden Ziele bestimmt ist oder von diesen ausgeht:
  - Amazon Domain Name Services (DNS)
  - Amazon Dynamic Host Configuration Protocol (DHCP)
  - Amazon EC2-Instance-Metadaten
  - Amazon-ECS-Endpunkte für Aufgabenmetadaten
  - Lizenzaktivierung für Windows-Instances
  - Amazon Time Sync Service
  - Reservierte IP-Adressen, die vom Standard-VPC-Router verwendet werden
- Es gibt Kontingente (bekannt als Grenzwerte) für die Anzahl der Netzwerk-ACLs pro VPC und die Anzahl der Regeln pro Netzwerk-ACL. Weitere Informationen finden Sie unter Amazon VPC-Kontingente.

Regeln für Netzwerk-ACLs

Sie können der Standardnetzwerk-ACL Regeln hinzufügen oder Regeln entfernen oder zusätzliche Netzwerk-ACLs für Ihre VPC erstellen. Wenn Sie Regeln zu einer Netzwerk-ACL hinzufügen oder daraus entfernen, werden die Änderungen automatisch auf die mit der Netzwerk-ACL verknüpften Subnetze angewendet.

Eine Netzwerk-ACL-Regel besteht aus folgenden Bestandteilen:

- Rule number (Regelnummer. Regeln werden nacheinander beginnend mit der niedrigsten Nummer ausgewertet. Sobald der Datenverkehr mit einer Regel übereinstimmt, wird die Regel angewendet. Dabei werden Regeln mit höherer Nummer, die dieser Regel möglicherweise widersprechen, ignoriert.
- Typ. Die Art des Datenverkehrs, z. B. SSH. Sie können auch den gesamten Datenverkehr oder einen benutzerdefinierten Bereich angeben.
- Protocol (Protokoll. Sie können ein beliebiges Protokoll mit einer Standardprotokollnummer auswählen. Weitere Informationen finden Sie unter Protocol Numbers. Wenn Sie als Protokoll ICMP auswählen, können Sie beliebige bzw. alle ICMP-Typen und -Codes angeben.

- Port-Bereich. Der Listening-Port oder Portbereich für den Datenverkehr. Beispiel: 80 für HTTP-Datenverkehr.
- Quelle. [Nur eingehende Regeln] Die Quelle des Datenverkehrs (CIDR-Bereich).
- Ziel. [Nur ausgehende Regeln] Das Ziel für den Datenverkehr (CIDR-Bereich).
- Erlauben/Verweigern. Gibt an, ob der angegebene Datenverkehr erlaubt oder verweigert werden soll.

Wenn Sie eine Regel mit einem Befehlszeilen-Tool oder der Amazon EC2-API hinzufügen, wird der CIDR-Bereich automatisch in die kanonische Form geändert. Wenn Sie beispielsweise `100.68.0.18/18` für den CIDR-Bereich angeben, erstellen wir eine Regel mit dem CIDR-Bereich `100.68.0.0/18`.

Standardnetzwerk-ACL

Die Standardnetzwerk-ACL ist so konfiguriert, dass der gesamte ein- und ausgehende Datenverkehr für die mit ihr verknüpften Subnetze erlaubt wird. Jede Netzwerk-ACL enthält auch eine Regel, deren Regelnummer ein Sternchen (*) ist. Über diese Regel wird sichergestellt, dass Pakete, die mit keiner anderen Regel übereinstimmen, abgelehnt werden. Diese Regel kann weder bearbeitet noch gelöscht werden.

Nachfolgend finden Sie ein Beispiel für eine Standardnetzwerk-ACL für eine VPC, die ausschließlich IPv4 unterstützt.

Eingehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/ Verweigern
100	Gesamter IPv4-Datenverkehr	Alle	Alle	0.0.0.0/0	ERLAUBEN
*	Gesamter IPv4-Datenverkehr	Alle	Alle	0.0.0.0/0	DENY

Ausgehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/ Verweigern
100	Gesamter IPv4-Datenverkehr	Alle	Alle	0.0.0.0/0	ERLAUBEN
*	Gesamter IPv4-Datenverkehr	Alle	Alle	0.0.0.0/0	DENY

Wenn Sie eine VPC mit einem IPv6 CIDR-Block erstellen oder Ihrer vorhandenen VPC einen IPv6 CIDR-Block zuordnen, werden automatisch Regeln hinzugefügt, über die der gesamte IPv6-Datenverkehr für das Subnetz erlaubt wird. Außerdem werden Regeln mit einem Sternchen als Nummer hinzugefügt, um sicherzustellen, dass Pakete, die mit keiner anderen nummerierten Regel übereinstimmen, abgelehnt werden. Diese Regeln können weder bearbeitet noch gelöscht werden. Nachfolgend finden Sie ein Beispiel für eine Standardnetzwerk-ACL für eine VPC, die IPv4 und IPv6 unterstützt.

> **Note**
>
> Wenn Sie die Eingangsregeln Ihrer Standard-Netzwerk-ACL geändert haben, fügen wir nicht automatisch eine `ALLOW`-Regel für eingehenden IPv6-Verkehr hinzu, wenn Sie einen IPv6-Block mit Ihrer VPC verknüpfen. Ebenso fügen wir nicht automatisch eine `ALLOW`-Regel für ausgehenden IPv6-Verkehr hinzu, wenn Sie die Regeln für ausgehenden Verkehr geändert haben.

Eingehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/ Verweigern
100	Gesamter IPv4-Datenverkehr	Alle	Alle	0.0.0.0/0	ERLAUBEN

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/ Verweigern
101	Gesamter IPv6-Datenverkehr	Alle	Alle	::/0	ERLAUBEN
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY
*	Gesamter IPv6-Datenverkehr	Alle	Alle	::/0	VERWEIGERN

Ausgehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/ Verweigern
100	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	ERLAUBEN
101	Gesamter IPv6-Datenverkehr	Alle	Alle	::/0	ERLAUBEN
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY
*	Gesamter IPv6-Datenverkehr	Alle	Alle	::/0	VERWEIGERN

Benutzerdefinierte Netzwerk-ACL

Das folgende Beispiel illustriert eine benutzerdefinierte Netzwerk-ACL für eine VPC, die nur IPv4 unterstützt. Es enthält eingehende Regeln, die HTTP- und HTTPS-Verkehr zulassen (100 und 110).

Es gibt eine entsprechende Ausgangsregel, die Antworten auf diesen eingehenden Verkehr (140) zulässt, der die ephemeren Ports 32768-65535 abdeckt. Weitere Informationen zur Auswahl des passenden Bereichs für flüchtige Ports finden Sie unter Flüchtige Ports.

Die Netzwerk-ACL enthält außerdem Regeln für eingehenden Datenverkehr, die SSH- und RDP-Datenverkehr für das Subnetz zulassen. Die Regel für ausgehenden Datenverkehr 120 ermöglicht Antworten, das Subnetz zu verlassen.

Die Netzwerk-ACL verfügt über Regeln für ausgehenden Datenverkehr (Regeln 100 und 110), über die ausgehender HTTP- und HTTPS-Datenverkehr für das Subnetz erlaubt wird. Es gibt eine entsprechende Eingangsregel, die Antworten auf diesen eingehenden Verkehr (140) zulässt, der die ephemeren Ports 32768-65535 abdeckt.

Jede Netzwerk-ACL enthält eine Standardregel mit der Nummer "*". Über diese Regel wird sichergestellt, dass Pakete, die mit keiner anderen Regel übereinstimmen, abgelehnt werden. Diese Regel kann weder bearbeitet noch gelöscht werden.

Eingehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigern	Kommentare
100	HTTP	TCP	80	0.0.0.0/0	ERLAUBEN	Lässt eingehenden HTTP-Datenverkehr von jeder IPv4-Adresse zu.
110	HTTPS	TCP	443	0.0.0.0/0	ERLAUBEN	Lässt eingehenden HTTPS-Datenverkehr von jeder IPv4-Adresse zu.
120	SSH	TCP	22	192.0.2.0/24	ERLAUBEN	Lässt eingehenden SSH-Datenverkehr vom öffentlichen IPv4-Adressbereich Ihres Heimnetzwerks (über

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigern	Kommentare
						das Internet-Gateway) zu.
130	RDP	TCP	3389	192.0.2.0/24	ERLAUBEN	Lässt eingehenden RDP-Datenverkehr vom öffentlichen IPv4-Adressbereich Ihres Heimnetzwerks (über das Internet-Gateway) zu den Webservern zu.
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ERLAUBEN	Lässt eingehenden zurückfließenden IPv4-Datenverkehr vom Internet (also für Anfragen aus dem Subnetz) zu. Dieser Bereich dient nur der Veranschaulichung.
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	VERWEIGERN	Verweigert den gesamten eingehenden IPv4-Datenverkehr, der nicht von einer vorangehenden Regel gehandhabt wird. (Kann nicht verändert werden.)

Ausgehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/Verweigern	Kommentare
100	HTTP	TCP	80	0.0.0.0/0	ERLAUBEN	Lässt ausgehenden HTTP-Datenverkehr über IPv4 vom Subnetz zum Internet zu.
110	HTTPS	TCP	443	0.0.0.0/0	ERLAUBEN	Lässt ausgehenden HTTPS-Datenverkehr über IPv4 vom Subnetz zum Internet zu.
120	SSH	TCP	1024 - 65535	192.0.2.0/24	ERLAUBEN	Ermöglicht ausgehenden SSH-Rückverkehr in den öffentlichen IPv4-Adressbereich Ihres Heimnetzwerks (über das Internet-Gateway).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ERLAUBEN	Lässt ausgehende IPv4-Antworten an Clients im Internet zu (beispielsweise zur Bereitstellung von Webseiten an Personen, die die Webserver im Subnetz besuchen).

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/Verweigern	Kommentare
						Dieser Bereich dient nur der Veranschaulichung.
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY	Verweigert den gesamten ausgehenden IPv4-Datenverkehr, der nicht von einer vorangehenden Regel gehandhabt wird. (Kann nicht verändert werden.)

Wenn ein Paket im Subnetz eingeht, werden die Regeln für eingehenden Datenverkehr der ACL, mit der das Subnetz verknüpft ist, nacheinander (von oben am Anfang der Liste bis unten) ausgewertet. Die Auswertung für ein Paket für den HTTPS-Port (443) sieht wie folgt aus. Das Paket stimmt nicht mit der ersten ausgewerteten Regel (Regel 100) überein. Es stimmt mit der zweiten Regel (Regel 110) überein, die das Paket in das Subnetz lässt. Wenn das Paket für Port 139 (NetBIOS) bestimmt gewesen wäre, stimmt es mit keiner der Regeln überein und die Regel * lehnt das Paket letztlich ab.

Es kann sinnvoll sein, eine deny (verweigern)-Regel zu erstellen, wenn Sie aus einem bestimmten Grund einen großen Portbereich freigeben müssen, einzelne Ports innerhalb dieses Bereichs jedoch gesperrt werden sollen. Platzieren Sie die deny (verweigern)-Regel in der Tabelle vor der Regel, die den gesamten Portbereich freigibt.

Sie fügen allow (erlauben)-Regeln je nach Anwendungsfall hinzu. Sie können beispielsweise eine Regel hinzufügen, die ausgehenden TCP- und UDP-Zugriff auf Port 53 für die DNS-Auflösung zulässt. Für jede hinzugefügte Regel müssen Sie sicherstellen, dass eine entsprechende Regel für ausgehenen oder eingehenden Datenverkehr existiert, die Antworten ermöglicht.

Im folgenden Beispiel wird eine benutzerdefinierte Netzwerk-ACL für eine VPC gezeigt, die einen zugehörigen IPv6-CIDR-Block hat. Diese Netzwerk-ACL enthält Regeln für den gesamten HTTP- und

HTTPS-Datenverkehr über IPv6. In diesem Fall wurden neue Regeln zwischen den bestehenden Regeln für IPv4-Datenverkehr eingefügt. Sie können die Regeln auch als Regeln mit höheren Nummern nach den IPv4-Regeln hinzufügen. IPv4- und IPv6-Datenverkehr wird separat bearbeitet. Daher sind die Regeln für den IPv4-Datenverkehr für IPv6-Datenverkehr nicht anwendbar.

Eingehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigern	Kommentare
100	HTTP	TCP	80	0.0.0.0/0	ERLAUBEN	Lässt eingehenden HTTP-Datenverkehr von jeder IPv4-Adresse zu.
105	HTTP	TCP	80	::/0	ERLAUBEN	Lässt eingehenden HTTP-Datenverkehr von jeder IPv6-Adresse zu.
110	HTTPS	TCP	443	0.0.0.0/0	ERLAUBEN	Lässt eingehenden HTTPS-Datenverkehr von jeder IPv4-Adresse zu.
115	HTTPS	TCP	443	::/0	ERLAUBEN	Lässt eingehenden HTTPS-Datenverkehr von jeder IPv6-Adresse zu.
120	SSH	TCP	22	192.0.2.0/24	ERLAUBEN	Lässt eingehenden SSH-Datenverkehr vom öffentlichen IPv4-Adressbereich Ihres Heimnetzwerks (über das Internet-Gateway) zu.

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigern	Kommentare
130	RDP	TCP	3389	192.0.2.0/24	ERLAUBEN	Lässt eingehenden RDP-Datenverkehr vom öffentlichen IPv4-Adressbereich Ihres Heimnetzwerks (über das Internet-Gateway) zu den Webservern zu.
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ERLAUBEN	Lässt eingehenden zurückfließenden IPv4-Datenverkehr vom Internet (also für Anfragen aus dem Subnetz) zu. Dieser Bereich dient nur der Veranschaulichung.
145	Custom TCP	TCP	32768-65535	::/0	ERLAUBEN	Lässt eingehenden zurückfließenden IPv6-Datenverkehr vom Internet (also für Anfragen aus dem Subnetz) zu. Dieser Bereich dient nur der Veranschaulichung.

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigern	Kommentare
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	VERWEIGERN	Verweigert den gesamten eingehenden IPv4-Datenverkehr, der nicht von einer vorangehenden Regel gehandhabt wird. (Kann nicht verändert werden.)
*	Gesamter Datenverkehr	Alle	Alle	::/0	VERWEIGERN	Verweigert den gesamten eingehenden IPv6-Datenverkehr, der nicht von einer vorangehenden Regel gehandhabt wird. (Kann nicht verändert werden.)

Ausgehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/Verweigern	Kommentare
100	HTTP	TCP	80	0.0.0.0/0	ERLAUBEN	Lässt ausgehenden HTTP-Datenverkehr über IPv4 vom Subnetz zum Internet zu.

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/Verweigern	Kommentare
105	HTTP	TCP	80	::/0	ERLAUBEN	Lässt ausgehenden HTTP-Datenverkehr über IPv6 vom Subnetz zum Internet zu.
110	HTTPS	TCP	443	0.0.0.0/0	ERLAUBEN	Lässt ausgehenden HTTPS-Datenverkehr über IPv4 vom Subnetz zum Internet zu.
115	HTTPS	TCP	443	::/0	ERLAUBEN	Lässt ausgehenden HTTPS-Datenverkehr über IPv6 vom Subnetz zum Internet zu.
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ERLAUBEN	Lässt ausgehende IPv4-Antworten an Clients im Internet zu (beispielsweise zur Bereitstellung von Webseiten an Personen, die die Webserver im Subnetz besuchen). Dieser Bereich dient nur der Veranschaulichung.

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/Verweigern	Kommentare
145	Custom TCP	TCP	32768-65535	::/0	ERLAUBEN	Lässt ausgehende IPv6-Antworten an Clients im Internet zu (beispielsweise zur Bereitstellung von Webseiten an Personen, die die Webserver im Subnetz besuchen). Dieser Bereich dient nur der Veranschaulichung.
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY	Verweigert den gesamten ausgehenden IPv4-Datenverkehr, der nicht von einer vorangehenden Regel gehandhabt wird. (Kann nicht verändert werden.)
*	Gesamter Datenverkehr	Alle	Alle	::/0	VERWEIGERN	Verweigert den gesamten ausgehenden IPv6-Datenverkehr, der nicht von einer vorangehenden Regel gehandhabt wird. (Kann nicht verändert werden.)

Benutzerdefinierte Netzwerk-ACLs und andere Dienste AWS

Wenn Sie eine benutzerdefinierte Netzwerk-ACL erstellen, sollten Sie sich darüber im Klaren sein, wie sich dies auf Ressourcen auswirken kann, die Sie mit anderen AWS Diensten erstellen.

Wenn Sie für Ihre Backend-Instances eine Netzwerk-ACL konfiguriert haben, die eine deny (verweigern)-Regel für den gesamten Datenverkehr mit der Quelle `0.0.0.0/0` oder den CIDR-Bereich des Subnetzes enthält, kann der Load Balancer mit Elastic Load Balancing keine Zustandsprüfung für die Instances durchführen. Weitere Informationen zu den empfohlenen Netzwerk-ACL-Regeln für Load Balancer und Backend-Instances finden Sie unter Netzwerk-ACLs für Load Balancer in einer VPC im Benutzerhandbuch für Classic Load Balancer.

Flüchtige Ports

Die Beispiel-Netzwerk-ACL im vorhergehenden Abschnitt verwendet den flüchtigen Portbereich 32768 bis 65535. Abhängig vom Client-Typ, den Sie verwenden oder mit dem Sie kommunizieren, kann es jedoch sinnvoll sein, einen anderen Bereich für Ihre Netzwerk-ACL zu verwenden.

Der flüchtige Portbereich wird vom Client festgelegt, von dem die Anfrage ausgeht. Der Bereich ist abhängig vom Betriebssystem des Clients.

- Viele Linux-Kernel (einschließlich des Amazon Linux-Kernels) verwenden Ports 32768-61000.
- Anforderungen, die von Elastic Load Balancing stammen, verwenden Ports 1024-65535.
- Windows-Betriebssysteme bis Windows Server 2003 verwenden die Ports 1025 bis 5000.
- Ab Windows Server 2008 werden die Ports 49152 bis 65535 verwendet.
- NAT-Gateways verwenden die Ports 1024 bis 65535.
- AWS Lambda Funktionen verwenden die Ports 1024-65535.

Wenn eine Anfrage beispielsweise von einem Windows 10-Client im Internet auf einem Webserver in Ihrer VPC eingeht, muss Ihre Netzwerk-ACL über eine Regel für ausgehenden Datenverkehr verfügen, die Datenverkehr für die Ports 49152-65535 erlaubt.

Wenn die Anforderung von einer Instance in Ihrer VPC ausgeht, muss Ihre Netzwerk-ACL über eine Regel für eingehenden Datenverkehr verfügen, um Datenverkehr zu den flüchtigen Ports des Instance-Typs zuzulassen (Amazon Linux, Windows Server 2008 usw.).

In der Praxis empfiehlt es sich, die flüchtigen Ports 1024 bis 65535 zu öffnen, um die unterschiedlichen Client-Typen abzudecken, von denen Datenverkehr an öffentliche Instances in

Ihrer VPC gelangen kann. Sie können der ACL jedoch auch Regeln hinzufügen, um Datenverkehr für böswillige Ports innerhalb dieses Bereichs zu verweigern. Platzieren Sie die deny (verweigern)-Regeln in der Tabelle vor den allow (erlauben)-Regeln, die den gesamten flüchtigen Portbereich freigeben.

Path MTU Discovery

Path MTU Discovery 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 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.

Wenn die maximale Übertragungseinheit (MTU) zwischen Hosts in Ihren Subnetzen unterschiedlich ist oder Ihre Instances mit Peers über das Internet kommunizieren, müssen Sie die folgende Netzwerk-ACL-Regel sowohl ein- als auch ausgehend hinzufügen. Dadurch wird sichergestellt, dass Path MTU Discovery ordnungsgemäß funktioniert und Paketverlust verhindert wird. Wählen Sie Custom ICMP Rule (Benutzerdefinierte ICMP-Regel) für den Typ und Destination Unreachable (Zielbereich nicht erreichbar), Fragmentation required (Fragmentierung erforderlich) und DF flag set (DF-Markierung gesetzt) für den Portbereich (Typ 3, Code 4). Wenn Sie Traceroute verwenden, fügen Sie außerdem die folgende Regel hinzu: wählen Sie als Typ Custom ICMP Rule (Benutzerdefinierte ICMP-Regel) und als Port-Bereich Time Exceeded (Zeit überschritten), TTL expired transit (TTL bei Übertragung abgelaufen) (Typ 11, Code 0). Weitere Informationen finden Sie unter Network Maximum Transmission Unit (MTU) für Ihre EC2-Instance im Amazon EC2 EC2-Benutzerhandbuch.

Arbeiten mit Netzwerk-ACLs

Die folgenden Aufgaben veranschaulichen, wie Sie unter Verwendung der Amazon VPC-Konsole mit Netzwerk-ACLs arbeiten.

Aufgaben

Bestimmen der Netzwerk-ACL-Zuordnungen

Über die Amazon VPC-Konsole können Sie herausfinden, welche Netzwerk-ACL mit einem Subnetz verknüpft ist. Netzwerk-ACLs können mehreren Subnetzen zugeordnet werden, daher können Sie auch feststellen, welche Subnetze einer Netzwerk-ACL zugeordnet sind.

So bestimmen Sie, welche Netzwerk-ACL einem Subnetz zugeordnet ist

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets und dann das Subnetz aus.

   Sie finden die dem Subnetz zugeordnete Netzwerk-ACL einschließlich der Netzwerk-ACL-Regeln auf der Registerkarte Network ACL.

So bestimmen Sie, welche Subnetze einer Netzwerk-ACL zugeordnet sind

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Network ACLs aus. Der Spalte Associated With können Sie entnehmen, wie viele Subnetze einer Netzwerk-ACL zugeordnet sind.
3. Wählen Sie eine Netzwerk-ACL aus.

4. Wählen Sie im Detailbereich Subnet Associations (Subnetzzuordnungen) aus, um die Subnetze anzuzeigen, die der Netzwerk-ACL zugeordnet sind.

Erstellen einer Netzwerk-ACL

Sie können für Ihre VPC benutzerdefinierte Netzwerk-ACLs erstellen. Standardmäßig verweigern benutzerdefinierte Netzwerk-ACLs den gesamten Datenverkehr, bis Sie Regeln hinzufügen. Neu erstellte Netzwerk-ACLs müssen einem Subnetz erst zugeordnet werden.

So erstellen Sie eine Netzwerk-ACL

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Network ACLs aus.
3. Klicken Sie auf Create Network ACL.
4. Im Dialogfeld Create Network ACL (Netzwerk-ACL erstellen) können Sie der Netzwerk-ACL einen Namen geben. Wählen Sie dann die ID Ihrer VPC in der Liste VPC aus. Wählen Sie dann Yes, Create (Ja, erstellen) aus.

Hinzufügen und Löschen von Regeln

Wenn Sie eine Regel zu einer ACL hinzufügen oder daraus löschen, sind alle Subnetze, die der ACL zugeordnet sind, von dieser Änderung betroffen. Sie müssen die Instances im Subnetz nicht beenden und neu starten. Die Änderungen werden nach kurzer Zeit wirksam.

> **Important**
>
> Seien Sie sehr vorsichtig, wenn Sie Regeln gleichzeitig hinzufügen und löschen. Netzwerk-ACL-Regeln definieren die Arten des ein- und ausgehenden Netzwerkverkehrs Ihrer VPCs. Wenn Sie eingehende oder ausgehende Regeln löschen und dann mehr neue Einträge hinzufügen, als in Amazon VPC-Kontingente erlaubt sind, werden die zum Löschen ausgewählten Einträge entfernt und neue Einträge werden nicht hinzugefügt. Dies kann zu unerwarteten Verbindungsproblemen führen und versehentlich den Zugriff auf und von Ihren VPCs verhindern.

Wenn Sie die Amazon EC2-API oder ein Befehlszeilen-Tool verwenden, können Sie keine Regeln ändern. Sie können nur Regeln hinzufügen und löschen. Wenn Sie die Amazon VPC-Konsole

verwenden, können Sie die Einträge für vorhandene Regeln ändern. Die Konsole entfernt die vorhandene Regel und fügt eine neue Regel für Sie hinzu. Wenn Sie die Reihenfolge von Regeln innerhalb der ACL ändern möchten, müssen Sie eine neue Regel mit der neuen Regelnummer hinzufügen und die ursprüngliche Regel löschen.

So fügen Sie einer Netzwerk-ACL Regeln hinzu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Network ACLs aus.
3. Klicken Sie im Detailbereich abhängig von der hinzuzufügenden Regel entweder auf die Registerkarte Inbound Rules oder die Registerkarte Outbound Rules und anschließend auf Edit.
4. Geben Sie unter Rule # eine Regelnummer (z. B. 100) ein. Die Regelnummer darf nicht bereits in der Netzwerk-ACL vorhanden sein. Regeln werden von der niedrigsten Nummer an der Reihe nach abgearbeitet.

   Wir empfehlen, zwischen den Regelnummern Lücken zu lassen (z. B. 100, 200, 300), statt aufeinanderfolgende Nummern zu verwenden (101, 102, 103). So können Sie jederzeit problemlos neue Regeln hinzufügen, ohne die vorhandenen Regeln neu nummerieren zu müssen.
5. Wählen Sie aus der Liste Type eine Regel aus. Wenn Sie beispielsweise eine Regel für HTTP hinzufügen möchten, wählen Sie HTTP aus. Um eine Regel zu erstellen, die den gesamten TCP-Datenverkehr erlaubt, wählen Sie All TCP aus. Für einige dieser Optionen (beispielsweise HTTP) wird der Port automatisch ausgefüllt. Wenn Sie ein Protokoll verwenden möchten, das nicht in der Liste enthalten ist, wählen Sie Custom Protocol Rule aus.
6. (Optional) Wenn Sie eine benutzerdefinierte Protokollregel erstellen, wählen Sie die Protokollnummer und den Namen aus der Liste Protocol aus. Weitere Informationen finden Sie unter IANA List of Protocol Numbers.
7. (Optional) Wenn für das ausgewählte Protokoll eine Portnummer erforderlich ist, geben Sie die Portnummer oder den Portbereich durch einen Bindestrich getrennt (z. B. 49152-65535) ein.
8. Geben Sie im Feld Source oder Destination (je nachdem, ob es sich um eine Regel für eingehenden oder ausgehenden Datenverkehr handelt) den CIDR-Bereich ein, auf den die Regel angewendet werden soll.
9. Wählen Sie in der Liste Allow/Deny ALLOW aus, um den ausgewählten Datenverkehr zu erlauben, oder DENY, um den ausgewählten Datenverkehr zu verweigern.
10. (Optional) Um eine weitere Regel hinzuzufügen, wählen Sie Add another rule aus und wiederholen Sie die Schritte 4 bis 9.

11. Klicken Sie abschließend auf Save.

So löschen Sie eine Regel aus einer Netzwerk-ACL

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Network ACLs und wählen Sie dann die Netzwerk-ACL aus.
3. Klicken Sie im Detailbereich entweder auf die Registerkarte Inbound Rules oder die Registerkarte Outbound Rules und anschließend auf Edit. Klicken Sie für die gewünschte Regel auf Remove und anschließend auf Save.

Zuweisen eines Subnetzes zu einer Netzwerk-ACL

Damit die Regeln einer Netzwerk-ACL auf ein bestimmtes Subnetz angewendet werden können, müssen Sie das Subnetz der Netzwerk-ACL zuordnen. Sie können eine Netzwerk-ACL mehreren Subnetzen zuordnen. Ein Subnetz kann jedoch nur einer Netzwerk-ACL zugeordnet werden. Subnetze, die keiner bestimmten ACL zugewiesen sind, werden standardmäßig der Standardnetzwerk-ACL zugewiesen.

So weisen Sie ein Subnetz einer Netzwerk-ACL zu

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im Navigationsbereich auf Network ACLs und wählen Sie dann die Netzwerk-ACL aus.
3. Klicken Sie im Detailbereich auf der Registerkarte Subnet Associations auf Edit. Aktivieren Sie das Kontrollkästchen Associate für das Subnetz, um es der Netzwerk-ACL zuzuordnen, und klicken Sie auf Save.

Aufheben der Zuordnung einer Netzwerk-ACL zu einem Subnetz

Sie können die Zuordnung einer benutzerdefinierten Netzwerk-ACL zu einem Subnetz aufheben. Wenn das Subnetz von der benutzerdefinierten Netzwerk-ACL getrennt wurde, wird es dann automatisch der Standard-Netzwerk-ACL zugeordnet.

So heben Sie die Zuordnung eines Subnetzes zu einer Netzwerk-ACL auf

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

2. Klicken Sie im Navigationsbereich auf Network ACLs und wählen Sie dann die Netzwerk-ACL aus.
3. Klicken Sie im Detailbereich auf die Registerkarte Subnet Associations.
4. Klicken Sie auf Edit und deaktivieren Sie das Kontrollkästchen Associate neben dem Subnetz. Wählen Sie Speichern.

Ändern der Netzwerk-ACL eines Subnetzes

Sie können die einem Subnetz zugeordnete Netzwerk-ACL ändern. Wenn Sie beispielsweise ein Subnetz erstellen, wird dieses zunächst der Standardnetzwerk-ACL zugeordnet. Möglicherweise möchten Sie es jedoch einer eigenen, benutzerdefinierten Netzwerk-ACL zuordnen.

Nachdem Sie die Netzwerk-ACL eines Subnetzes geändert haben, müssen Sie die Instances im Subnetz nicht beenden und neu starten. Die Änderungen werden nach kurzer Zeit wirksam.

So ändern Sie die Netzwerk-ACL-Zuordnung eines Subnetzes

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Subnets und dann das Subnetz aus.
3. Wählen Sie die Registerkarte Network ACL aus und klicken Sie auf Edit.
4. Wählen Sie aus der Liste Change to (Ändern zu) die Netzwerk-ACL aus, die Sie dem Subnetz zuordnen möchten, und klicken Sie auf Save (Speichern).

Löschen einer Netzwerk-ACL

Sie können eine Netzwerk-ACL nur löschen, wenn ihr keine Subnetze zugeordnet sind. Die Standardnetzwerk-ACL kann nicht gelöscht werden.

So löschen Sie eine Netzwerk-ACL

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie im Navigationsbereich Network ACLs aus.
3. Wählen Sie die Netzwerk-ACL aus und klicken Sie auf Delete.
4. Wählen Sie im Bestätigungsdialogfeld Yes, Delete aus.

Überblick über die API und Befehlszeile

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile oder eine API ausführen. Weitere Informationen über Befehlszeilenschnittstellen und eine Liste der verfügbaren APIs finden Sie unter Arbeiten mit Amazon VPC.

Erstellen einer Netzwerk-ACL für Ihre VPC

- create-network-acl (AWS CLI)
- New-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Beschreiben Ihrer Netzwerk-ACLs

- describe-network-acls (AWS CLI)
- Get-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Hinzufügen von Regeln zu einer Netzwerk-ACL

- create-network-acl-entry (AWS CLI)
- New-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Löschen von Regeln aus einer Netzwerk-ACL

- delete-network-acl-entry (AWS CLI)
- Remove-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Ersetzen von vorhandenen Regeln innerhalb einer Netzwerk-ACL

- replace-network-acl-entry (AWS CLI)
- Set-EC2NetworkAclEntry (AWS Tools for Windows PowerShell)

Ersetzen einer Netzwerk-ACL-Zuordnung

- replace-network-acl-association (AWS CLI)
- Set-EC2NetworkAclAssociation (AWS Tools for Windows PowerShell)

Löschen einer Netzwerk-ACL

- delete-network-acl (AWS CLI)
- Remove-EC2NetworkAcl (AWS Tools for Windows PowerShell)

Netzwerk-ACLs mit Firewall Manager verwalten

AWS Firewall Manager vereinfacht Ihre Netzwerk-ACL-Administrations- und Wartungsaufgaben für mehrere Konten und Subnetze. Sie können den Firewall Manager verwenden, um Konten und Subnetze in Ihrer Organisation zu überwachen und die von Ihnen definierten Netzwerk-ACL-Konfigurationen automatisch anzuwenden. Firewall Manager ist besonders nützlich, wenn Sie Ihre gesamte Organisation schützen möchten oder wenn Sie häufig neue Subnetze hinzufügen, die Sie automatisch von einem zentralen Administratorkonto aus schützen möchten.

Mit einer Firewall Manager Manager-Netzwerk-ACL-Richtlinie können Sie mit einem einzigen Administratorkonto die Mindestregelsätze konfigurieren, überwachen und verwalten, die Sie in den Netzwerk-ACLs, die Sie in Ihrem Unternehmen verwenden, definiert haben möchten. Sie geben an, welche Konten und Subnetze in Ihrer Organisation in den Geltungsbereich der Firewall Manager Manager-Richtlinie fallen. Firewall Manager meldet den Konformitätsstatus der Netzwerk-ACLs für Subnetze im Geltungsbereich, und Sie können Firewall Manager so konfigurieren, dass nicht konforme Netzwerk-ACLs automatisch behoben werden, um sie konform zu machen.

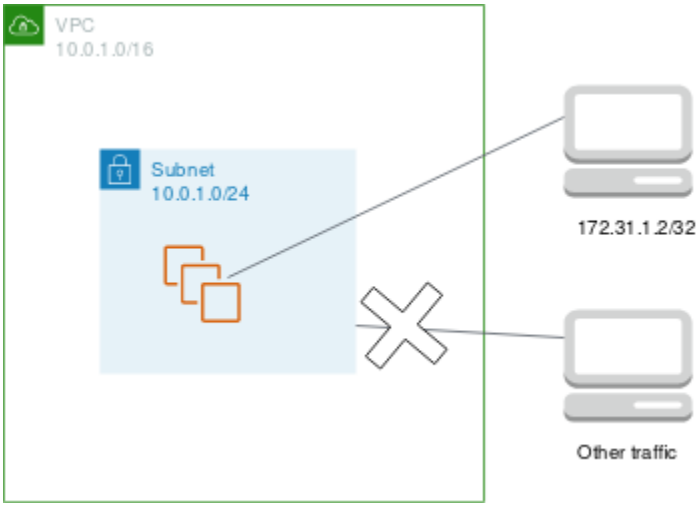
Weitere Informationen zur Verwendung von Firewall Manager zur Verwaltung Ihrer Netzwerk-ACLs finden Sie in den folgenden Ressourcen im AWS Firewall Manager Entwicklerhandbuch:

- AWS Firewall Manager Voraussetzungen
- Erste Schritte mit AWS Firewall Manager Amazon VPC-Netzwerk-ACL-Richtlinien
- Richtlinien für die Netzwerkzugriffskontrollliste (ACL) von Amazon Virtual Private Cloud

Beispiel: Steuern des Zugriffs auf Instances in einem Subnetz

In diesem Beispiel können die Instances in Ihrem Subnetz miteinander kommunizieren und sind von vertrauenswürdigen Remote-Computern aus zugreifbar. Der Remotecomputer kann ein Computer in Ihrem lokalen Netzwerk oder eine Instance in einem anderen Subnetz oder VPC sein. Sie verwenden ihn, um eine Verbindung zu Ihren Instances herzustellen, um administrative Aufgaben auszuführen. Die Sicherheitsgruppenregeln und Netzwerk-ACL-Regeln erlauben den Zugriff von der IP-Adresse Ihres Remote-Computers (172.31.1.2/32). Der gesamte Datenverkehr aus dem Internet oder

anderen Netzwerken wird verweigert. Dieses Szenario bietet die Flexibilität, Sicherheitsgruppen oder Sicherheitsgruppenregeln für Instances zu ändern und die Netzwerk-ACL als zusätzliche Schutzebene zu nutzen.



Im Folgenden finden Sie ein Beispiel für eine Sicherheitsgruppe, die mit den Instances verknüpft werden soll. Sicherheitsgruppen sind zustandsbehaftet. Daher benötigen Sie keine Regel, die Antworten auf eingehenden Datenverkehr zulässt.

Eingehend

Protokolltyp	Protocol (Protokoll)	Port-Bereich	Source	Kommentare
Gesamter Datenverkehr	Alle	Alle	sg-1234567890abcdef0	Alle mit dieser Sicherheitsgruppe verbundenen Instances können miteinander kommunizieren.
SSH	TCP	22	172.31.1.2/32	Lässt eingehenden SSH-Zugriff von dem Remote-Computer zu.

Ausgehend

Protokolltyp	Protocol (Protokoll)	Port-Bereich	Zielbereich	Kommentare
Gesamter Datenverkehr	Alle	Alle	sg-1234567890abcdef0	Alle mit dieser Sicherheitsgruppe verbundenen Instances können miteinander kommunizieren.

Im Folgenden finden Sie ein Beispiel für eine Netzwerk-ACL, die mit den Subnetzen für die Instances verknüpft wird. Die Netzwerk-ACL-Regeln gelten für alle Instances im Subnetz. Netzwerk-ACLs sind zustandslos. Daher benötigen Sie eine Regel, die Antworten auf eingehenden Datenverkehr zulässt.

Eingehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigern	Kommentare
100	SSH	TCP	22	172.31.1.2/32	ERLAUBEN	Lässt eingehenden Datenverkehr von dem Remote-Computer zu.
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	VERWEIGERN	Verweigert jeglichen anderen eingehenden

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigern	Kommentare
						Datenverkehr.

Ausgehend

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/Verweigern	Kommentare
100	Custom TCP	TCP	1024 - 65535	172.31.1.2/32	ERLAUBEN	Lässt ausgehende Antworten an den Remote-Computer zu.
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	VERWEIGERN	Verweigert jeglichen anderen ausgehenden Datenverkehr.

Wenn Sie versehentlich Ihre Sicherheitsgruppenregeln zu offen gestalten, erlaubt die Netzwerk-ACL in diesem Beispiel weiterhin den Zugriff nur über die angegebene IP-Adresse. Die folgende Sicherheitsgruppe enthält beispielsweise eine Regel, die eingehenden SSH-Zugriff von jeder IP-Adresse aus zulässt. Wenn Sie diese Sicherheitsgruppe jedoch einer Instance in einem Subnetz zuordnen, das die Netzwerk-ACL verwendet, können nur andere Instances im Subnetz und Ihr Remote-Computer auf die Instance zugreifen, da die Netzwerk-ACL-Regeln anderen eingehenden Datenverkehr im Subnetz verweigern.

Eingehend

Typ	Protocol (Protokoll)	Port-Bereich	Source	Kommentare
Gesamter Datenverkehr	Alle	Alle	sg-123456 7890abcdef0	Alle mit dieser Sicherhei tsgruppe verbunden en Instances können miteinander kommunizieren.
SSH	TCP	22	0.0.0.0/0	Lässt SSH-Zugri ff von beliebigen IP-Adressen zu.

Ausgehend

Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Kommentare
Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	Lässt den gesamten ausgehenden Datenverkehr zu.

Beheben Sie Probleme mit der Erreichbarkeit

Reachability Analyzer ist ein Tool zur statischen Konfigurationsanalyse. Verwenden Sie Reachability Analyzer, um die Netzwerkerreichbarkeit zwischen zwei Ressourcen in Ihrer VPC zu analysieren und zu debuggen. Reachability Analyzer erzeugt hop-by-hop Details zum virtuellen Pfad zwischen diesen Ressourcen, wenn sie erreichbar sind, und identifiziert andernfalls die blockierende Komponente. Es kann beispielsweise fehlende oder falsch konfigurierte Netzwerk-ACL-Regeln identifizieren.

Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

Ausfallsicherheit in Amazon Virtual Private Cloud

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

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

Sie können Ihre VPCs so konfigurieren, dass sie die Resilienzanforderungen für Ihre Workloads erfüllen. Weitere Informationen finden Sie hier:

- Machen Sie sich mit Resilienzmustern und Kompromissen vertraut (Architektur-Blog)AWS
- Planen Sie Ihre Netzwerktopologie (AWS Well-Architected Framework)
- Verbindungsoptionen für Amazon Virtual Private Cloud (AWS Whitepapers)

Compliance-Validierung für Amazon Virtual Private Cloud

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.

Bewährte Methoden für die Sicherheit für Ihre VPC

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

- Wenn Sie Ihrer VPC-Subnetze hinzufügen, um Ihre Anwendung zu hosten, erstellen Sie diese in mehreren Availability Zones. Eine Availability Zone besteht aus einem oder mehreren diskreten Rechenzentren mit redundanter Stromversorgung, Vernetzung und Konnektivität in einer AWS Region. Die Verwendung mehrerer Availability Zones macht Ihre Produktionsanwendungen hochverfügbar, fehlertolerant und skalierbar. Weitere Informationen finden Sie unter Amazon VPC in AWS.
- Verwenden Sie Sicherheitsgruppen, um den Datenverkehr zu EC2-Instances in Ihren Subnetzen zu steuern. Weitere Informationen finden Sie unter Sicherheitsgruppen.
- Verwenden Sie Netzwerk-ACLs, um den ein- und ausgehenden Datenverkehr auf Subnetzebene zu steuern. Weitere Informationen finden Sie unter Datenverkehr in Subnetzen mit Netzwerk-ACLs steuern.
- Verwalten Sie den Zugriff auf AWS Ressourcen in Ihrer VPC mithilfe von AWS Identity and Access Management (IAM) -Identitätsverbund, Benutzern und Rollen. Weitere Informationen finden Sie unter Identity and Access Management für Amazon VPC.
- Verwenden Sie VPC-Flow-Protokolle, um den IP-Datenverkehr zu und von einer VPC, einem Subnetz oder einer Netzwerkschnittstelle zu überwachen. Weitere Informationen finden Sie unter VPC Flow Logs.
- Verwenden Sie Network Access Analyzer, um unbeabsichtigten Netzwerkzugriff auf Ressourcen in unseren VPCs zu identifizieren. Weitere Informationen finden Sie im Handbuch für Network Access Analyzer.
- Wird verwendet AWS Network Firewall , um Ihre VPC zu überwachen und zu schützen, indem eingehender und ausgehender Datenverkehr gefiltert wird. Weitere Informationen finden Sie im AWS Network Firewall -Handbuch.
- Verwenden Sie Amazon GuardDuty , um potenzielle Bedrohungen für Ihre Konten, Container, Workloads und Daten in Ihrer AWS Umgebung zu erkennen. Die grundlegende Bedrohungserkennung umfasst die Überwachung der VPC-Flow-Protokolle, die Ihren Amazon EC2 EC2-Instances zugeordnet sind. Weitere Informationen finden Sie unter VPC Flow Logs im GuardDuty Amazon-Benutzerhandbuch.

Antworten auf häufig gestellte Fragen zur VPC-Sicherheit finden Sie unter Sicherheit und Filterung in den Häufig gestellte Fragen zu Amazon VPC.

Verwenden von Amazon VPC mit anderen AWS-Services

Sie können Amazon VPC mit anderen verwenden, AWS-Services um Lösungen zu entwickeln, die Ihren Anforderungen entsprechen.

Inhalt

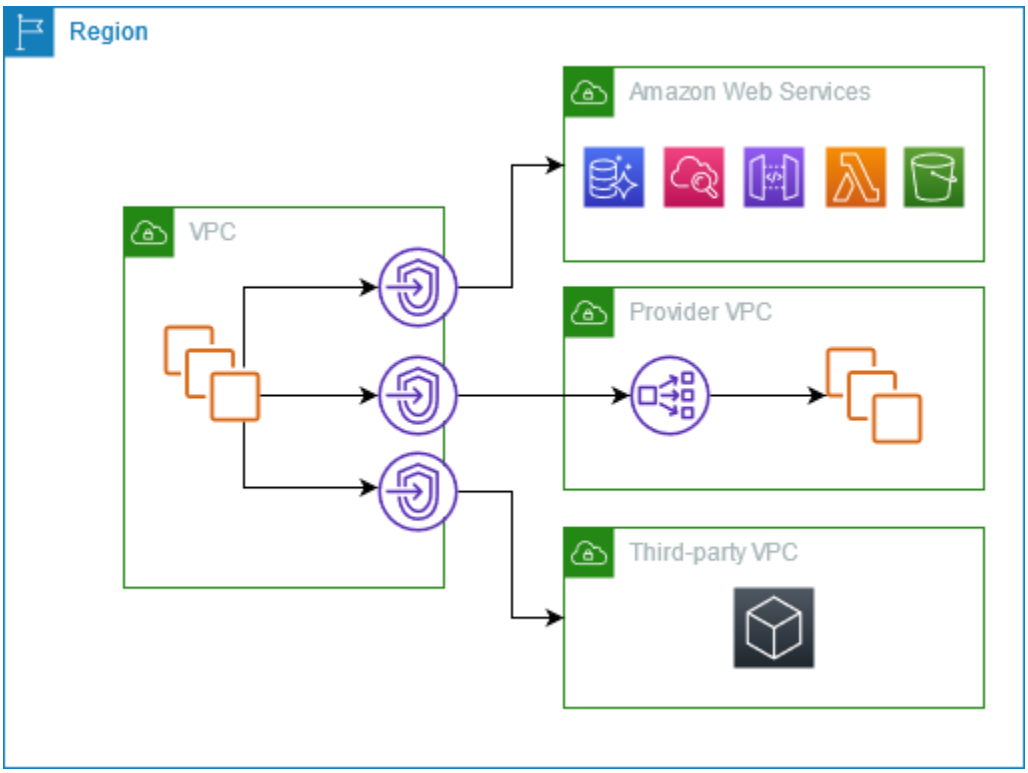
Verbinden Ihrer VPC mit anderen Services mithilfe von AWS PrivateLink

AWS PrivateLink stellt eine private Verbindung zwischen Virtual Private Clouds (VPCs) und unterstützten AWS-Services, von anderen AWS-Konten gehosteten Services und unterstützten AWS Marketplace-Services her. Sie benötigen kein Internet-Gateway, kein NAT-Gerät und auch keine AWS Direct Connect- oder AWS Site-to-Site VPN-Verbindung, um mit dem Service zu kommunizieren.

Zur Nutzung von AWS PrivateLink erstellen Sie einen VPC-Endpunkt in Ihrer VPC. Geben Sie dabei den Namen des Service und ein Subnetz an. Damit wird eine Elastic-Network-Schnittstelle im Subnetz erstellt, die als Eintrittspunkt des für den Service bestimmten Datenverkehrs dient.

Sie können Ihren eigenen von AWS PrivateLink gestützten VPC-Endpunkt-Service erstellen und anderen AWS-Kunden Zugriff auf Ihren Service erteilen.

Das folgende Diagramm veranschaulicht die gängigen Anwendungsfälle für AWS PrivateLink. Die VPC auf der linken Seite weist mehrere EC2-Instances in einem privaten Subnetz und drei Schnittstellen-VPC-Endpunkte auf. Der oberste VPC-Endpunkt ist mit einem AWS-Service verbunden. Der mittlere VPC-Endpunkt ist mit einem von einem anderen AWS-Konto gehosteten Service (einem VPC-Endpunktservice) verbunden. Der untere VPC-Endpunkt ist mit einem AWS Marketplace-Partnerservice verbunden.



Weitere Informationen finden Sie unter AWS PrivateLink.

Filtern von Netzwerkverkehr mit AWS Network Firewall

Sie können den Netzwerkverkehr auf der Perimeterebene Ihrer VPC mithilfe der AWS Network Firewall filtern. Die Network Firewall ist eine zustandsbehafteter, verwalteter Netzwerk-Firewall sowie ein Service zur Angriffserkennung und -verhinderung. Weitere Informationen finden Sie im AWS Network Firewall-Entwicklerhandbuch.

Sie implementieren die Network Firewall mit den folgenden AWS-Ressourcen.

Network Firewall-Ressource	Beschreibung
Firewall	Eine Firewall verbindet das Filterverhalten einer Firewall-Richtlinie für den Netzwerkverkehr mit der VPC, die Sie schützen möchten. Die Firewall-Konfiguration enthält Spezifikationen für die Availability Zones und Subnetze, in denen die Firewall-Endpunkte platziert werden. Sie definiert auch allgemeine Einstellungen wie die Konfiguration der

Network Firewall-Ressource	Beschreibung
	Firewall-Protokollierung und das Tagging auf der AWS-Firewall-Ressource. Weitere Informationen finden Sie unter Firewalls in AWS Network Firewall.
Firewall-Richtlinie	Eine Firewall-Richtlinie definiert das Überwachungs- und Schutzverhalten für eine Firewall. Die Details des Verhaltens werden in den Regelgruppen definiert, die Sie Ihrer Richtlinie hinzufügen, sowie in einigen Richtlinien-Standardeinstellungen. Um eine Firewall-Richtlinie zu verwenden, verknüpfen Sie sie mit einer oder mehreren Firewalls. Weitere Informationen finden Sie unter Firewall-Richtlinien in AWS Network Firewall.
Regelgruppe	Eine Regelgruppe ist ein wiederverwendbarer Satz von Kriterien für die Überprüfung und Handhabung des Netzwerkverkehrs. Im Rahmen Ihrer Richtlinienkonfiguration fügen Sie einer Firewall-Richtlinie eine oder mehrere Regelgruppen hinzu. Sie können zustandslose Regelgruppen definieren, um jedes Netzwerkpaket isoliert zu untersuchen. Zustandslose Regelgruppen ähneln in ihrem Verhalten und in der Verwendung den Amazon VPC-Netzwerkzugriffssteuerungslisten (ACLs). Sie können auch statusbehaftete Regelgruppen definieren, um Pakete im Kontext ihres Verkehrsflusses zu untersuchen. Zustandsbehaftete Regelgruppen ähneln in ihrem Verhalten und in der Verwendung den Amazon VPC-Sicherheitsgruppen. Weitere Informationen finden Sie unter Regelgruppen in AWS Network Firewall.

Sie können AWS Firewall Manager auch verwenden, um Network-Firewall-Ressourcen für Ihre Konten und Anwendungen in AWS Organizations zentral zu konfigurieren und zu verwalten. Firewalls für mehrere Konten können Sie mit einem einzigen Konto in Firewall Manager verwalten. Weitere Informationen finden Sie unter AWS Firewall Manager im AWS WAF, AWS Firewall Manager und AWS Shield Advanced-Benutzerhandbuch.

Filtern von DNS-Datenverkehr mit Route 53 Resolver DNS Firewall

Mit DNS Firewall definieren Sie Filterregeln für Domänennamen in Regelgruppen, die Sie Ihren VPCs zuordnen. Sie können Listen von Domänennamen angeben, die Sie zulassen oder blockieren möchten, und Sie können die Antworten für die blockierten DNS-Abfragen anpassen. Weitere Informationen finden Sie in der DNS-Firewall-Dokumentation zu Route 53 Resolver.

Sie implementieren die DNS-Firewall mit den folgenden AWS-Ressourcen.

DNS-Firewall-Resource	Beschreibung
DNS Firewall-Regelgruppe	Eine DNS Firewall-Regelgruppe ist eine benannte, wiederverwendbare Sammlung von DNS-Firewall-Regeln zum Filtern von DNS-Abfragen. Sie füllen die Regelgruppe mit den Filterregeln auf und verknüpfen dann die Regelgruppe mit einer oder mehreren VPCs von Amazon VPC. Wenn Sie eine Regelgruppe mit einer VPC verknüpfen, aktivieren Sie die DNS-Firewall-Filterung für die VPC. Wenn Resolver dann eine DNS-Abfrage für eine VPC erhält, mit der eine Regelgruppe verknüpft ist, übergibt Resolver die Abfrage zur Filterung an die DNS Firewall. Jede Regel innerhalb der Regelgruppe gibt eine Domänenliste und eine Aktion für DNS-Abfragen an, deren Domänen mit den Domänenspezifikationen in der Liste übereinstimmen. Sie können übereinstimmende Abfragen zulassen, blockieren oder warnen. Sie können auch benutzerdefinierte Antworten für blockierte Abfragen definieren. Weitere Informationen finden Sie unter Regelgruppen und Regeln in der Route 53 Resolver DNS Firewall.
Domänenliste	Eine Domänenliste ist ein wiederverwendbarer Satz von Domänenspezifikationen, die Sie in einer DNS Firewall-Regel innerhalb einer Regelgruppe verwenden. Weitere Informationen finden Sie unter Domänenlisten in der DNS-Firewall von Route 53 Resolver.

Sie können auch AWS Firewall Manager verwenden, um DNS-Firewall-Ressourcen in Ihren Konten und Organisationen in AWS Organizations zentral zu konfigurieren und zu verwalten. Firewalls für mehrere Konten können Sie mit einem einzigen Konto in Firewall Manager verwalten. Weitere Informationen finden Sie unter AWS Firewall Manager im AWS WAF, AWS Firewall Manager und AWS Shield Advanced-Benutzerhandbuch.

Beheben von Erreichbarkeitsproblemen mit Reachability Analyzer

Reachability Analyzer ist ein Tool zur statischen Konfigurationsanalyse. Verwenden Sie Reachability Analyzer, um die Erreichbarkeit des Netzwerks zwischen zwei Ressourcen in Ihrer VPC zu analysieren und zu debuggen. Reachability Analyzer erzeugt hop-by-hop Details zum virtuellen Pfad zwischen diesen Ressourcen, wenn sie erreichbar sind, und identifiziert andernfalls die blockierende Komponente.

Sie können Reachability Analyzer verwenden, um die Erreichbarkeit zwischen den folgenden Ressourcen zu analysieren:

- Instances
- Internet-Gateways
- Netzwerkschnittstellen
- Transit Gateways
- Transit-Gateway-Anhänge
- VPC-Endpunkt-Services
- VPC-Endpunkte
- VPC-Peering-Verbindungen
- VPN-Gateways

Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

VPC-Beispiele

Im Folgenden finden Sie Beispielkonfigurationen für Ihre Virtual Private Clouds (VPCs).

Beispiele

- Beispiel: VPC für eine Testumgebung
- Beispiel: VPC für Web- und Datenbankserver
- Beispiel: VPC mit Servern in privaten Subnetzen und NAT

Verbundene Beispiele

- Informationen zum Verbinden Ihrer VPCs miteinander finden Sie unter VPC-Peering-Konfigurationen im Leitfaden für Amazon-VPC-Peering.
- Informationen zum Verbinden Ihrer VPCs mit Ihrem eigenen Netzwerk finden Sie unter Site-to-Site-VPN-Architekturen im AWS Site-to-Site VPN-Benutzerhandbuch.
- Um Ihre VPCs miteinander und mit Ihrem eigenen Netzwerk zu verbinden, sehen Sie sich die Transit-Gateway-Beispiele in den Amazon VPC Transit Gateways an.

Weitere Ressourcen

- Resilienzmuster und Kompromisse verstehen (AWS-Architektur-Blog)
- Planen Sie Ihre Netzwerktopologie (AWS Well-Architected Framework)
- Optionen für Verbindungen der Amazon Virtual Private Cloud (AWS-Whitepaper)

Beispiel: VPC für eine Testumgebung

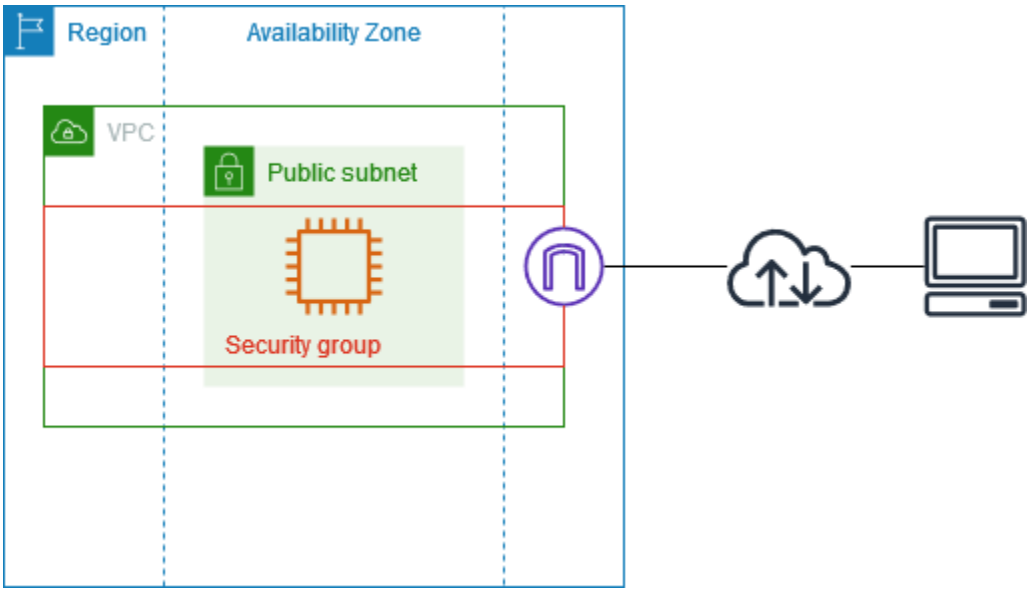
Dieses Beispiel zeigt, wie Sie eine VPC erstellen, die Sie als Entwicklungs- oder Testumgebung verwenden können. Da diese VPC nicht für den Einsatz in der Produktion vorgesehen ist, müssen Sie die Server nicht in mehreren Availability Zones bereitstellen. Der geringeren Kosten und der Einfachheit halber können Sie die Server stattdessen in einer einzigen Availability Zone bereitstellen.

Inhalt

- Bereitstellen der Anwendung
- Testen Sie Ihre Konfiguration
- Bereinigen

Übersicht

Das folgende Diagramm bietet einen Überblick über die in diesem Beispiel enthaltenen Ressourcen. Die VPC verfügt über ein öffentliches Subnetz in einer einzelnen Availability Zone und ein Internet-Gateway. Der Server ist eine EC2-Instance, die im öffentlichen Subnetz läuft. Die Sicherheitsgruppe für die Instance erlaubt SSH-Verkehr von Ihrem eigenen Computer sowie jeglichen anderen Datenverkehr, der speziell für Ihre Entwicklungs- oder Testaktivitäten erforderlich ist.



Routing

Wenn Sie diese VPC über die Amazon-VPC-Konsole erstellen, erstellen wir eine Routing-Tabelle für das öffentliche Subnetz mit lokalen Routen und Routen zum Internet-Gateway. Im Folgenden finden Sie ein Beispiel für eine Routing-Tabelle mit Routen für IPv4 und IPv6. Wenn Sie Nur-IPv4-Subnetze anstelle von Dual-Stack-Subnetzen erstellen, enthält Ihre Routing-Tabelle nur die IPv4-Routen.

Ziel	Ziel
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Lokal

Ziel	Ziel
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Sicherheit

Für diese Beispielkonfiguration müssen Sie eine Sicherheitsgruppe für Ihre Instance erstellen, die den von Ihrer Anwendung benötigten Datenverkehr ermöglicht. Beispielsweise müssen Sie u. U. eine Regel hinzufügen, die SSH-Verkehr von Ihrem Computer oder HTTP-Verkehr aus Ihrem Netzwerk zulässt.

Im Folgenden finden Sie Beispiele für eingehende Regeln für eine Sicherheitsgruppe mit Regeln für IPv4 und IPv6. Wenn Sie reine IPv4-Subnetze anstelle von Dual-Stack-Subnetzen erstellen, benötigen Sie nur Regeln für IPv4.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Beschreibung
0.0.0.0/0	TCP	80	Lässt eingehenden HTTP-Zugriff von allen IPv4-Adressen zu
::/0	TCP	80	Lässt eingehenden HTTP-Zugriff von allen IPv6-Adressen zu
0.0.0.0/0	TCP	443	Lässt eingehenden HTTPS-Zugriff von allen IPv4-Adressen zu
::/0	TCP	443	Lässt eingehenden HTTPS-Zugriff von allen IPv6-Adressen zu
Öffentlicher IPv4-Adressbereich Ihres Netzwerks	TCP	22	(Optional) Lässt eingehenden SSH-Zugriff von IPv4-IP-Adressen in Ihrem Netzwerk zu

Source	Protocol (Protokoll)	Port-Bereich	Beschreibung
IPv6-Adressbereich Ihres Netzwerks	TCP	22	(Optional) Lässt eingehend en SSH-Zugriff von IPv6-IP-A dressen in Ihrem Netzwerk zu
Öffentlicher IPv4-Adressbereich Ihres Netzwerks	TCP	3389	(Optional) Lässt eingehend en RDP-Zugriff von IPv4-IP-A dressen in Ihrem Netzwerk zu
IPv6-Adressbereich Ihres Netzwerks	TCP	3389	(Optional) Lässt eingehend en RDP-Zugriff von IPv6-IP-A dressen in Ihrem Netzwerk zu

Erstellen Sie die VPC

Verwenden Sie das folgende Verfahren, um eine VPC mit einem öffentlichen Subnetz in einer Availability Zone zu erstellen. Diese Konfiguration ist geeignet für eine Entwicklungs- oder Testumgebung.

So erstellen Sie die VPC

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie auf dem VPC-Dashboard VPC erstellen aus.
3. Wählen Sie unter Resources to create (Zu erstellende Ressourcen) die Option VPC and more (VPC und mehr) aus.
4. Konfigurieren Sie die VPC

    a. Geben Sie unter Name tag auto-generation (Automatische Generierung des Namens-Tags) einen Namen für die VPC ein.

    b. Behalten Sie für den IPv4-CIDR-Block entweder den Standardvorschlag bei oder geben Sie den für Ihre Anwendung oder Ihr Netzwerk erforderlichen CIDR-Block ein. Weitere Informationen finden Sie unter the section called “VPC-CIDR-Blöcke”.

c. (Optional) Wenn die Anwendung über IPv6-Adressen kommuniziert, wählen Sie den IPv6-CIDR-Block und den von Amazon bereitgestellten IPv6-CIDR-Block.

5. Konfiguration der Subnetze

   a. Wählen Sie für Anzahl der Availability Zones (AZs) 1 aus. Sie können die standardmäßige Availability Zone beibehalten oder alternativ die Option AZs anpassen erweitern und eine Availability Zone auswählen.

   b. Wählen Sie für Number of public subnets (Anzahl der öffentlichen Subnetze) 1 aus.

   c. Wählen Sie für Anzahl der öffentlichen Subnetze (Number of private subnets) 0 aus.

   d. Sie können die standardmäßigen CIDR-Blöcke für die Subnetze beibehalten oder alternativ CIDR-Blöcke des Subnetzes anpassen erweitern und einen CIDR-Block eingeben. Weitere Informationen finden Sie unter the section called “Subnetz-CIDR-Blöcke”.

6. Behalten Sie für NAT-Gateways den Standardwert Keine bei.

7. Wählen Sie für VPC endpoints (VPC-Endpunkte) None (Keine) aus. Ein Gateway-VPC-Endpunkt für S3 wird nur für den Zugriff auf Amazon S3 von privaten Subnetzen aus verwendet.

8. Behalten Sie beide Optionen unter DNS-Optionen ausgewählt. Infolgedessen erhält Ihre Instance einen öffentlichen DNS-Hostnamen, der ihrer öffentlichen IP-Adresse entspricht.

9. Wählen Sie Create VPC aus.

Bereitstellen der Anwendung

Es gibt eine Vielzahl von Möglichkeiten für die Bereitstellung von EC2-Instances. Beispiel:

- Amazon-EC2-Assistent zum Starten von Instances
- Amazon EC2 Auto Scaling
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Nachdem Sie eine EC2-Instance bereitgestellt haben, können Sie eine Verbindung mit der Instance herstellen, die Software installieren, die Sie für Ihre Anwendung benötigen, und dann ein Image für die zukünftige Verwendung erstellen. Weitere Informationen finden Sie unter Erstellen eines Linux-AMI oder Erstellen eines Windows-AMI in der Amazon-EC2-Dokumentation. Alternativ können Sie EC2 Image Builder verwenden, um Ihr Amazon Machine Image (AMI) zu erstellen und zu verwalten.

Testen Sie Ihre Konfiguration

Nachdem Sie Ihre Anwendung bereitgestellt haben, können Sie sie testen. Wenn Sie keine Verbindung zu Ihrer EC2-Instance herstellen können oder wenn Ihre Anwendung den erwarteten Datenverkehr nicht senden oder empfangen kann, können Sie Reachability Analyzer verwenden, um Sie bei der Fehlerbehebung zu unterstützen. Reachability Analyzer kann beispielsweise Konfigurationsprobleme mit Ihren Routing-Tabellen oder Sicherheitsgruppen identifizieren. Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

Bereinigen

Wenn Sie mit dieser Konfiguration fertig sind, können Sie sie löschen. Bevor Sie die VPC löschen können, müssen Sie Ihre Instance beenden. Weitere Informationen finden Sie unter the section called “Löschen der VPC”.

Beispiel: VPC für Web- und Datenbankserver

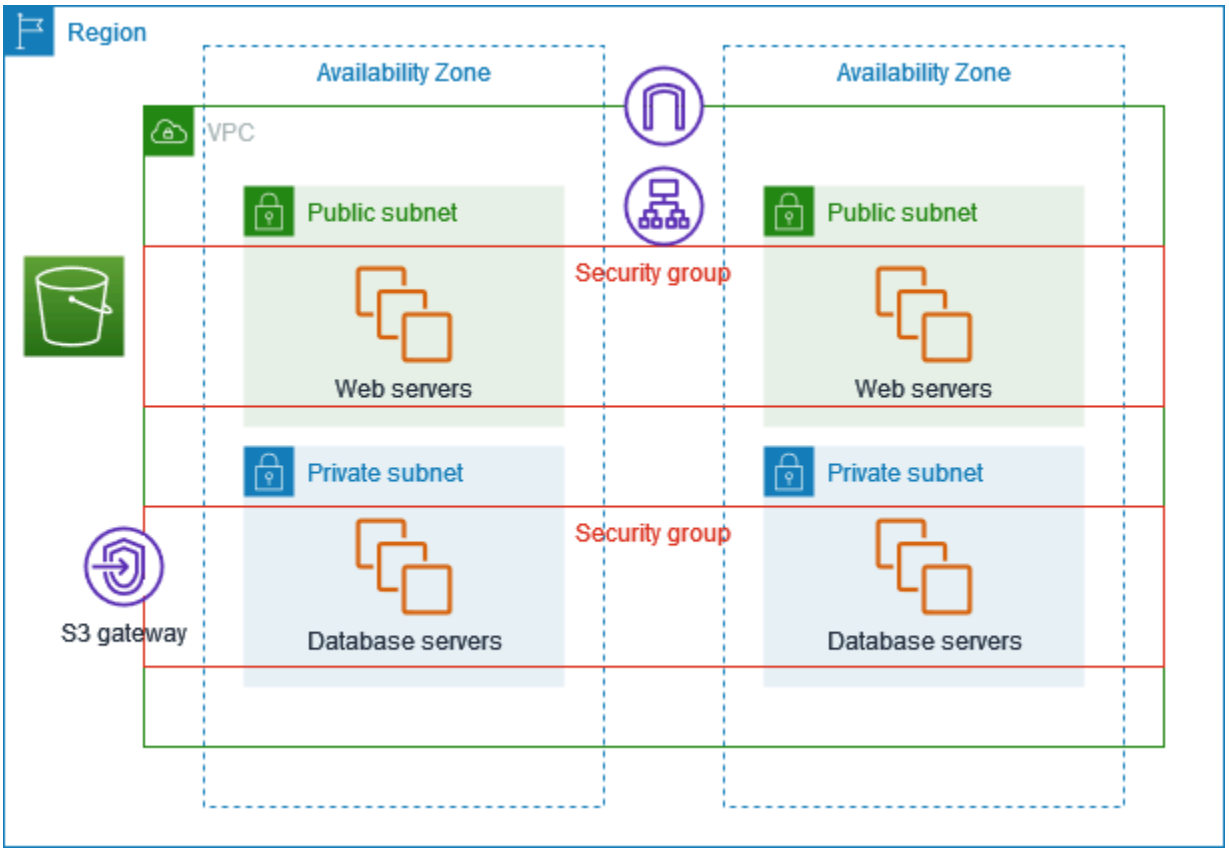
Dieses Beispiel zeigt, wie Sie eine VPC erstellen, die Sie für eine zweistufige Architektur in einer Produktionsumgebung verwenden können. Um die Ausfallsicherheit zu erhöhen, stellen Sie die Server in zwei Availability Zones bereit.

Inhalt

Übersicht

Das folgende Diagramm bietet einen Überblick über die in diesem Beispiel enthaltenen Ressourcen. Die VPC hat öffentliche Subnetze und private Subnetze in zwei Availability Zones. Die Webserver laufen in den öffentlichen Subnetzen und empfangen Datenverkehr von Clients über einen Load Balancer. Sie können der Sicherheitsgruppe für die Webserver Regeln hinzufügen, um den Datenverkehr nur vom Load Balancer zuzulassen. Die Datenbankserver laufen in den privaten Subnetzen und empfangen Datenverkehr von den Webservern. Die Sicherheitsgruppe für die

Datenbankserver ermöglicht den Datenverkehr von den Webservern. Die Datenbankserver können über einen Gateway-VPC-Endpunkt eine Verbindung zu Amazon S3 herstellen.



Routing

Wenn Sie diese VPC über die Amazon-VPC-Konsole erstellen, erstellen wir eine Routing-Tabelle für die öffentlichen Subnetze mit lokalen Routen und Routen zum Internet-Gateway sowie eine Routing-Tabelle für jedes private Subnetz mit lokalen Routen und einer Route zum Gateway-VPC-Endpunkt.

Im Folgenden finden Sie ein Beispiel für eine Routing-Tabelle für die öffentlichen Subnetze mit Routen für IPv4 und IPv6. Wenn Sie reine IPv4-Subnetze anstelle von Dual-Stack-Subnetzen erstellen, enthält Ihre Routing-Tabelle nur die IPv4-Routen.

Bestimmungsort	Ziel
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Lokal
0.0.0.0/0	*igw-id*

Bestimmungsort	Ziel
::/0	*igw-id*

Im Folgenden finden Sie ein Beispiel für eine Routing-Tabelle für die privaten Subnetze mit Routen für IPv4 und IPv6. Wenn Sie reine IPv4-Subnetze erstellen, enthält Ihre Routing-Tabelle nur die IPv4-Routen. Die letzte Route sendet Datenverkehr für Amazon S3 an den Gateway-VPC-Endpunkt.

Bestimmungsort	Ziel
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	local
S3-Präfix-Listen-ID	*s3-gateway-id*

Sicherheit

Für diese Beispielkonfiguration erstellen Sie eine Sicherheitsgruppe für den Load Balancer, eine Sicherheitsgruppe für die Webserver und eine Sicherheitsgruppe für die Datenbankserver.

Load Balancer

Die Sicherheitsgruppe für Ihren Application Load Balancer oder Network Load Balancer muss eingehenden Datenverkehr von Clients am Load-Balancer-Listener-Port zulassen. Um Datenverkehr von überall im Internet zu akzeptieren, geben Sie 0.0.0.0/0 als Quelle ein. Die Load-Balancer-Sicherheitsgruppe muss auch ausgehenden Datenverkehr vom Load Balancer zu den Ziel-Instances auf dem Instance-Listener-Port und dem Zustandsprüfungsport zulassen.

Web-Server

Die folgenden Sicherheitsgruppenregeln ermöglichen Webservern, HTTP- und HTTPS-Datenverkehr vom Load Balancer zu empfangen. Sie können den Webservern optional erlauben, SSH- oder RDP-Verkehr von Ihrem Netzwerk zu empfangen. Die Webserver können SQL- bzw. MySQL-Datenverkehr an Ihre Datenbankserver senden.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Beschreibung
ID der Sicherheitsgruppe für den Load Balancer	TCP	80	Lässt eingehenden HTTP-Zugriff vom Load Balancer zu
ID der Sicherheitsgruppe für den Load Balancer	TCP	443	Lässt eingehenden HTTP-Zugriff vom Load Balancer zu
Öffentlicher IPv4-Adressbereich Ihres Netzwerks	TCP	22	(Optional) Lässt eingehenden SSH-Zugriff von IPv4-IP-Adressen in Ihrem Netzwerk zu
IPv6-Adressbereich Ihres Netzwerks	TCP	22	(Optional) Lässt eingehenden SSH-Zugriff von IPv6-IP-Adressen in Ihrem Netzwerk zu
Öffentlicher IPv4-Adressbereich Ihres Netzwerks	TCP	3389	(Optional) Lässt eingehenden RDP-Zugriff von IPv4-IP-Adressen in Ihrem Netzwerk zu
IPv6-Adressbereich Ihres Netzwerks	TCP	3389	(Optional) Lässt eingehenden RDP-Zugriff von IPv6-IP-Adressen in Ihrem Netzwerk zu

Ausgehend

Ziel	Protocol (Protokoll)	Port-Bereich	Beschreibung
ID der Sicherheitsgruppe für	TCP	1433	Lässt ausgehenden Microsoft-SQL-Server-Zugriff auf die Datenbankserver zu

Ziel	Protocol (Protokoll)	Port-Bereich	Beschreibung
Instances, auf denen Microsoft SQL Server ausgeführt wird			
ID der Sicherheitsgruppe für Instances, auf denen MySQL ausgeführt wird	TCP	3306	Lässt ausgehenden MySQL-Server-Zugriff auf die Datenbankserver zu

Datenbankserver

Die folgenden Sicherheitsgruppenregeln berechtigen die Datenbankserver, Lese- und Schreibanforderungen von den Webservern zu empfangen.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Kommentare
Die ID der Webserver-Sicherheitsgruppe	TCP	1433	Lässt eingehenden Microsoft SQL Server-Zugriff von Webservern zu
Die ID der Webserver-Sicherheitsgruppe	TCP	3306	Lässt eingehenden MySQL-Zugriff von den Webservern zu

Ausgehend

Ziel	Protocol (Protokoll)	Port-Bereich	Kommentare
0.0.0.0/0	TCP	80	Lässt ausgehenden HTTP-Zugriff auf das Internet über IPv4 zu
0.0.0.0/0	TCP	443	Lässt ausgehenden HTTP-Zugriff auf das Internet über IPv4 zu

Weitere Informationen zu Sicherheitsgruppen für Amazon RDS-DB-Instances finden Sie unter Zugriffskontrolle mit Sicherheitsgruppen im Amazon RDS-Benutzerhandbuch.

Erstellen Sie die VPC

Gehen Sie wie folgt vor, um eine VPC mit einem öffentlichen Subnetz und einem privaten Subnetz in zwei Availability Zones zu erstellen.

So erstellen Sie die VPC

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie auf dem VPC-Dashboard VPC erstellen aus.
3. Wählen Sie unter Zu erstellende Ressourcen die Option VPC und mehr aus.
4. Konfigurieren Sie die VPC:

    a. Lassen Sie die automatische Generierung von Namenstags aktiviert, um Namenstags für die VPC-Ressourcen zu erstellen, oder deaktivieren Sie die Option, um Ihre eigenen Namenstags für die VPC-Ressourcen bereitzustellen.

    b. Behalten Sie für den IPv4-CIDR-Block entweder den Standardvorschlag bei oder geben Sie den für Ihre Anwendung oder Ihr Netzwerk erforderlichen CIDR-Block ein. Weitere Informationen finden Sie unter the section called “VPC-CIDR-Blöcke”.

    c. (Optional) Wenn die Anwendung über IPv6-Adressen kommuniziert, wählen Sie den IPv6-CIDR-Block und den von Amazon bereitgestellten IPv6-CIDR-Block.

    d. Wählen Sie eine Tenancy-Option aus. Diese Option definiert, ob in der VPC gestartete EC2-Instances auf Hardware ausgeführt werden, die gemeinsam mit anderen AWS-Konten genutzt wird, oder auf Hardware, die ausschließlich für Ihre Verwendung bestimmt ist. Wenn

Sie die Tenancy der VPC als Tenancy wählen, verwenden EC2-Instances`Default`, die in dieser VPC gestartet werden, das Tenancy-Attribut, das Sie beim Starten der Instance angegeben haben. Weitere Informationen finden Sie unter Starten einer Instance mithilfe definierter Parameter im Amazon EC2 EC2-Benutzerhandbuch. Wenn Sie für die Tenancy der VPC `Dedicated` auswählen, werden die Instances immer als Dedicated Instances auf Hardware ausgeführt, die für Ihre Verwendung bestimmt ist.

5. Konfigurieren Sie die Subnetze:
   a. Wählen Sie für Anzahl der Availability Zones die Option 2, so dass Sie Instances in mehreren Availability Zones starten können, um die Ausfallsicherheit zu erhöhen.
   b. Wählen Sie für Number of public subnets (Anzahl der öffentlichen Subnetze) 2 aus.
   c. Wählen Sie für Number of private subnets (Anzahl der privaten Subnetze) 2 aus.
   d. Sie können die Standard-CIDR-Blöcke für die Subnetze beibehalten oder alternativ die Option CIDR-Blöcke für Subnetze anpassen erweitern und einen CIDR-Block eingeben. Weitere Informationen finden Sie unter the section called “Subnetz-CIDR-Blöcke”.
6. Behalten Sie für NAT-Gateways den Standardwert Keine bei.
7. Behalten Sie für VPC-Endpunkte den Standardwert S3-Gateway bei. Obwohl es keine Auswirkungen hat, solange Sie nicht auf einen S3-Bucket zugreifen, entstehen keine Kosten für die Aktivierung dieses VPC-Endpunkts.
8. Behalten Sie beide Optionen unter DNS-Optionen ausgewählt. Infolgedessen erhalten Ihre Webserver öffentliche DNS-Hostnamen, die ihren öffentlichen IP-Adressen entsprechen.
9. Wählen Sie VPC erstellen aus.

Bereitstellen der Anwendung

Idealerweise haben Sie Ihre Web- und Datenbankserver bereits in einer Entwicklungs- oder Testumgebung getestet und die Skripts oder Images erstellt, die Sie für die Bereitstellung Ihrer Anwendung in der Produktion verwenden werden.

Sie können EC2-Instances für Ihre Webserver verwenden. Es gibt eine Vielzahl von Möglichkeiten für die Bereitstellung von EC2-Instances. Beispielsweise:

- Amazon-EC2-Assistent zum Starten von Instances
- AWS CloudFormation
- Amazon Elastic Container Service (Amazon ECS)

Um die Verfügbarkeit zu verbessern, können Sie Amazon EC2 Auto Scaling verwenden, um Server in mehreren Availability Zones bereitzustellen und die für die Anwendung erforderliche Mindestserverkapazität aufrechtzuerhalten.

Sie können Elastic Load Balancing verwenden, um den Traffic gleichmäßig auf Ihre Server zu verteilen. Sie können Ihre Load Balancer an eine Auto-Scaling-Gruppe anhängen.

Sie können EC2-Instances für Ihre Datenbankserver oder einen unserer speziell entwickelten Datenbanktypen verwenden. Weitere Informationen finden Sie unter Datenbanken unter: So wählen Sie aus. AWS

Testen Sie Ihre Konfiguration

Nachdem Sie Ihre Anwendung bereitgestellt haben, können Sie sie testen. Wenn Ihre Anwendung den erwarteten Datenverkehr nicht senden oder empfangen kann, können Sie den Reachability Analyzer verwenden, um Sie bei der Fehlerbehebung zu unterstützen. Reachability Analyzer kann beispielsweise Konfigurationsprobleme mit Ihren Routing-Tabellen oder Sicherheitsgruppen identifizieren. Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

Bereinigen

Wenn Sie mit dieser Konfiguration fertig sind, können Sie sie löschen. Bevor Sie die VPC löschen können, müssen Sie Ihre Instances beenden und den Load Balancer löschen. Weitere Informationen finden Sie unter the section called “Löschen der VPC”.

Beispiel: VPC mit Servern in privaten Subnetzen und NAT

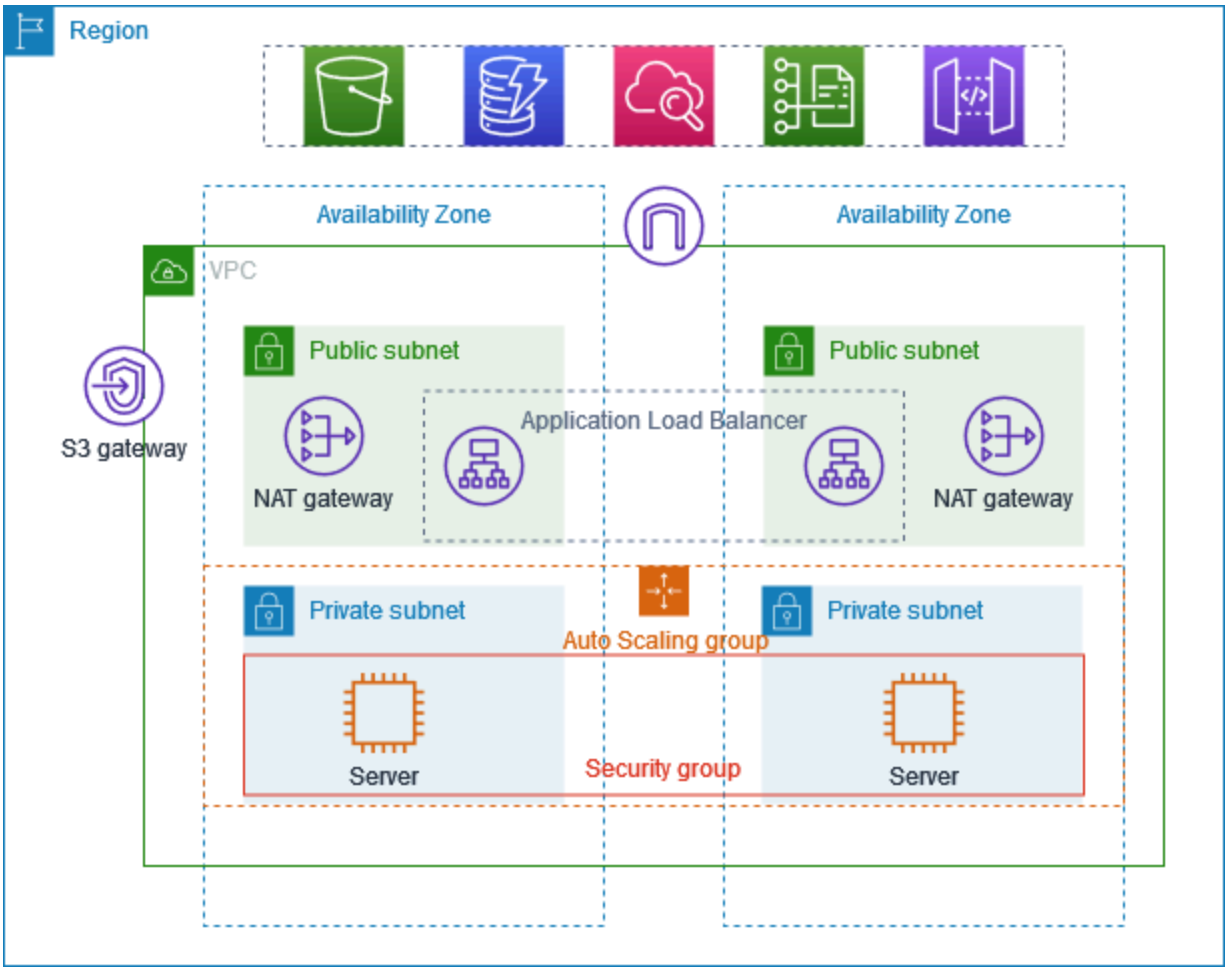
Dieses Beispiel zeigt, wie Sie eine VPC erstellen, die Sie für eine zweistufige Architektur in einer Produktionsumgebung verwenden können. Um die Ausfallsicherheit zu erhöhen, stellen Sie die Server in zwei Availability Zones bereit und verwenden dabei eine Auto-Scaling-Gruppe und einen Application Load Balancer. Zur zusätzlichen Sicherheit stellen Sie die Server in privaten Subnetzen bereit. Die Server empfangen Anfragen über den Load Balancer. Die Server können über ein NAT-Gateway eine Verbindung zum Internet herstellen. Um die Ausfallsicherheit zu erhöhen, stellen Sie das NAT-Gateway in beiden Availability Zones bereit.

Inhalt

- Erstellen Sie die VPC
- Bereitstellen der Anwendung
- Testen Sie Ihre Konfiguration
- Bereinigen

Übersicht

Das folgende Diagramm bietet einen Überblick über die in diesem Beispiel enthaltenen Ressourcen. Die VPC hat öffentliche Subnetze und private Subnetze in zwei Availability Zones. Jedes öffentliche Subnetz enthält ein NAT-Gateway und einen Load-Balancer-Knoten. Die Server werden in den privaten Subnetzen ausgeführt, werden mithilfe einer Auto-Scaling-Gruppe gestartet und beendet und empfangen Datenverkehr vom Load Balancer. Die Server können über das NAT-Gateway eine Verbindung zum Internet herstellen. Die Server können über einen Gateway-VPC-Endpunkt eine Verbindung zu Amazon S3 herstellen.



Routing

Wenn Sie diese VPC über die Amazon-VPC-Konsole erstellen, erstellen wir eine Routing-Tabelle für die öffentlichen Subnetze mit lokalen Routen und Routen zum Internet-Gateway. Wir erstellen auch eine Routing-Tabelle für die privaten Subnetze mit lokalen Routen und Routen zum NAT-Gateway, zum reinen Ausgangs-Internet-Gateway und zum Gateway-VPC-Endpunkt.

Im Folgenden finden Sie ein Beispiel für eine Routing-Tabelle für die öffentlichen Subnetze mit Routen sowohl für IPv4 und IPv6. Wenn Sie reine IPv4-Subnetze anstelle von Dual-Stack-Subnetzen erstellen, enthält Ihre Routing-Tabelle nur die IPv4-Routen.

Ziel	Ziel
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Lokal
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Im Folgenden finden Sie ein Beispiel für eine Routing-Tabelle für die privaten Subnetze mit Routen sowohl für IPv4 und IPv6. Wenn Sie reine IPv4-Subnetze erstellen, enthält Ihre Routing-Tabelle nur die IPv4-Routen. Die letzte Route sendet Datenverkehr für Amazon S3 an den Gateway-VPC--Endpunkt.

Ziel	Ziel
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Lokal
0.0.0.0/0	*nat-gateway-id*
::/0	*eigw-id*
S3-Präfix-Listen-ID	*s3-gateway-id*

Sicherheit

Im Folgenden finden Sie ein Beispiel für die Regeln, die Sie für die Sicherheitsgruppe erstellen können, die Sie Ihren Servern zuordnen. Die Sicherheitsgruppe muss Datenverkehr vom Load Balancer über den Listener-Port und das Protokoll zulassen. Es muss auch den Verkehr mit Zustandsprüfungen ermöglichen.

Eingehend

Source	Protocol (Protokoll)	Port-Bereich	Kommentare
ID der Load Balancer-Sicherheitsgruppe	*Listener-Protokoll*	*Listener-Ports*	Erlaubt eingehenden Datenverkehr vom Load Balancer auf dem Listener-Port
ID der Load Balancer-Sicherheitsgruppe	*Zustandsprüfungsprotokoll*	*Pfad für die Zustandsprüfung*	Erlaubt Zustandsüberprüfungs-Datenverkehr vom Load Balancer

Erstellen Sie die VPC

Gehen Sie wie folgt vor, um eine VPC mit einem öffentlichen Subnetz und einem privaten Subnetz in zwei Availability Zones und einem NAT-Gateway in jeder Availability Zone zu erstellen.

So erstellen Sie die VPC

1. Öffnen Sie die Amazon-VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Wählen Sie auf dem VPC-Dashboard VPC erstellen aus.
3. Wählen Sie unter Resources to create (Zu erstellende Ressourcen) die Option VPC and more (VPC und mehr) aus.
4. Konfigurieren Sie die VPC
    a. Geben Sie unter Name tag auto-generation (Automatische Generierung des Namens-Tags) einen Namen für die VPC ein.

b. Behalten Sie für den IPv4-CIDR-Block entweder den Standardvorschlag bei oder geben Sie den für Ihre Anwendung oder Ihr Netzwerk erforderlichen CIDR-Block ein.

c. Wenn die Anwendung über IPv6-Adressen kommuniziert, wählen Sie IPv6-CIDR-Block und Von Amazon bereitgestellter IPv6-CIDR-Block aus.

5. Konfiguration der Subnetze

   a. Wählen Sie für Anzahl der Availability Zones die Option 2, so dass Sie Instances in mehreren Availability Zones starten können, um die Resilienz zu verbessern.

   b. Wählen Sie für Number of public subnets (Anzahl der öffentlichen Subnetze) 2 aus.

   c. Wählen Sie für Number of private subnets (Anzahl der privaten Subnetze) 2 aus.

   d. Sie können die standardmäßigen CIDR-Blöcke für die Subnetze beibehalten oder alternativ CIDR-Blöcke des Subnetzes anpassen erweitern und einen CIDR-Block eingeben. Weitere Informationen finden Sie unter the section called “Subnetz-CIDR-Blöcke”.

6. Wählen Sie für NAT-Gateways 1 pro AZ aus, um die Resilienz zu verbessern.

7. Wenn die Anwendung über IPv6-Adressen kommuniziert, wählen Sie unter Internet-Gateway nur für ausgehenden Datenverkehr die Option Ja aus.

8. Wenn die Instances für VPC-Endpunkte auf einen S3-Bucket zugreifen müssen, behalten Sie die Standardeinstellung S3-Gateway bei. Andernfalls können Instances in Ihrem privaten Subnetz nicht auf Amazon S3 zugreifen. Für diese Option fallen keine Kosten an, sodass Sie die Standardeinstellung beibehalten können, falls Sie in Zukunft möglicherweise einen S3-Bucket verwenden. Wenn Sie Keine wählen, können Sie später jederzeit einen Gateway-VPC-Endpunkt hinzufügen.

9. Deaktivieren Sie für DNS-Optionen die Option DNS-Hostnamen aktivieren.

10. Wählen Sie Create VPC aus.

Bereitstellen der Anwendung

Idealerweise haben Sie die Tests Ihrer Server in einer Entwicklungs- oder Testumgebung abgeschlossen und die Skripte oder Images erstellt, die Sie für die Bereitstellung Ihrer Anwendung in der Produktion verwenden werden.

Sie können Amazon EC2 Auto Scaling verwenden, um Server in mehreren Availability Zones bereitzustellen und die Mindestkapazität des Servers zu erhalten, die für Ihre Anwendung erforderlich ist.

So starten Sie Instances mithilfe einer Auto-Scaling-Gruppe

1. Erstellen Sie eine Startvorlage, um die Konfigurationsinformationen anzugeben, die zum Starten der EC2-Instances mithilfe von Amazon EC2 Auto Scaling erforderlich sind. Weitere Informationen finden Sie unter Erstellen einer Startvorlage für eine Auto-Scaling-Gruppe im Benutzerhandbuch für Amazon EC2 Auto Scaling.
2. Erstellen Sie eine Auto-Scaling-Gruppe, bei der es sich um eine Sammlung von EC2-Instances mit einer minimalen, maximalen und gewünschten Größe handelt. Schritt-für-Schritt-Anleitungen finden Sie unter Erstellen einer Auto-Scaling-Gruppe mithilfe einer Startvorlage im Benutzerhandbuch für Amazon EC2 Auto Scaling.
3. Erstellen Sie einen Load Balancer, der den Datenverkehr gleichmäßig über die Instances in Ihrer Auto-Scaling-Gruppe verteilt, und fügen Sie den Load Balancer an Ihre Auto-Scaling-Gruppe an. Weitere Informationen finden Sie im Benutzerhandbuch für Elastic Load Balancing und Verwendung von Elastic Load Balancing im Benutzerhandbuch für Amazon EC2 Auto Scaling.

Testen Sie Ihre Konfiguration

Nachdem Sie Ihre Anwendung bereitgestellt haben, können Sie sie testen. Wenn Ihre Anwendung den erwarteten Datenverkehr nicht senden oder empfangen kann, können Sie den Reachability Analyzer verwenden, um Sie bei der Fehlerbehebung zu unterstützen. Reachability Analyzer kann beispielsweise Konfigurationsprobleme mit Ihren Routing-Tabellen oder Sicherheitsgruppen identifizieren. Weitere Informationen finden Sie im Leitfaden Reachability Analyzer.

Bereinigen

Wenn Sie mit dieser Konfiguration fertig sind, können Sie sie löschen. Bevor Sie die VPC löschen können, müssen Sie die Auto-Scaling-Gruppe löschen, Ihre Instances beenden, die NAT-Gateways löschen und den Load Balancer löschen. Weitere Informationen finden Sie unter the section called “Löschen der VPC”.

Amazon VPC-Kontingente

In den folgenden Tabellen sind die Kontingente, früher als Limits bezeichnet, für Amazon VPC-Ressourcen für Ihr AWS Konto aufgeführt. Sofern nicht anders angegeben, gelten diese Kontingente pro Region.

Wenn Sie eine Erhöhung des pro Ressource geltenden Kontingents beantragen, erhöhen wir das Kontingent für alle Ressourcen in der Region.

VPC und Subnetze

Name	Standard	Anpassbar	Kommentare
VPCs pro Region	5	Ja	Durch Erhöhung dieses Kontingents erhöht sich auch das Kontingents für Internet-Gateways pro Region um dieselbe Menge. Sie können diesen Grenzwert erhöhen, so dass Sie über Hunderte von VPCs pro Region verfügen können.
Subnetze pro VPC	200	Ja	
IPv4 CIDR-Blöcke pro VPC	5	Ja (bis zu 50)	Der primäre CIDR-Block und alle sekundären CIDR-Blöcke werden auf dieses Kontingent angerechnet.
IPv6 CIDR-Blöcke pro VPC	5	Ja (bis zu 50)	Die Anzahl der -CIDRs, die Sie einer einzelnen VPC zuordnen können.

DNS

Jede EC2-Instance kann 1 024 Pakete pro Sekunde pro Netzwerkschnittstelle an Route 53 Resolver senden (insbesondere die .2-Adresse, z. B. 10.0.0.2 und 169.254.169.253). Dieses Kontingent kann nicht erhöht werden. Die Zahl der DNS-Abfragen, die pro Sekunde vom Route 53 Resolver unterstützt werden, ist vom Typ der Abfrage, von der Größe der Antwort und dem verwendeten Protokoll abhängig. Weitere Informationen und Empfehlungen für eine skalierbare DNS-Architektur finden Sie im technischen Handbuch AWS -Hybrid-DNS mit Active Directory.

Elastic-IP-Adressen

Name	Standard	Anpassbar	Kommentare
Elastische IP-Adressen pro Region	5	Ja	Dieses Kontingent gilt für einzelne AWS-Konto VPCs und gemeinsam genutzte VPCs.
Elastic-IP-Adressen pro öffentlichem NAT-Gateway	2	Ja	Sie können eine Erhöhung des Kontingents auf bis zu 8 beantragen.

Gateways

Name	Standard	Anpassbar	Kommentare
Internet-Gateways pro Region nur für ausgehenden Verkehr	5	Ja	Um dieses Kontingent zu erhöhen, erhöhen Sie das Kontingent für VPCs pro Region. Sie können nur jeweils ein Internet-Gateway nur für ausgehenden Verkehr an eine VPC anfügen.
Internet-Gateways pro Region	5	Ja	Um dieses Kontingent zu erhöhen, erhöhen Sie das Kontingent für VPCs pro Region.

Name	Standard	Anpassbar	Kommentare
			Sie können nur jeweils ein Internet-Gateway nur für eine VPC anfügen.
NAT-Gateways pro Availability Zone	5	Ja	NAT-Gateways zählen nur zu Ihrem Kontingent im Status `pending`, `active` oder `deleting`.
Kontingent an privaten IP-Adressen pro NAT-Gateway	8	Nein	
Carrier-Gateways pro VPC	1	Nein	

Vom Kunden verwaltete Präfixlisten

Während die Standard-Quotas für kundenverwaltete Präfixlisten anpassbar sind, können Sie eine Erhöhung nicht über die Konsole für Service-Quotas anfordern. Sie müssen einen Fall zur Erhöhung des Servicelimits mit der AWS Support Center Console eröffnen.

Name	Standard	Anpassbar	Kommentare
Präfixlisten pro Region	100	Ja	
Versionen pro Präfixliste	1.000	Ja	Wenn eine Präfixliste 1 000 gespeicherte Versionen enthält und Sie eine neue Version hinzufügen, wird die älteste Version entfernt, damit die neue Version hinzugefügt werden kann.
Maximale Anzahl von Einträgen pro Präfixliste	1.000	Ja	Sie können die Größe einer vom Kunden verwalteten Präfixliste auf bis zu 1.000 ändern. Weitere Informationen finden Sie unter Größe einer Präfixliste ändern. Wenn Sie in einer Ressource auf eine Präfixliste verweisen, zählt die maximale Anzahl von Einträgen für die Präfixlisten zu, Kontingent für die Einträge für die

Name	Standard	Anpassbar	Kommentare
			Ressource. Wenn Sie beispielsweise eine Präfixliste mit maximal 20 Einträgen erstellen und in einer Sicherheitsgruppenregel auf diese Präfixliste verweisen, zählt dies als 20 Regeln für die Sicherheitsgruppe.
Verweise auf eine Präfixliste pro Ressourcentyp	5,000	Ja	Dieses Kontingent gilt pro Ressourcentyp, der auf eine Präfixliste verweisen kann. Beispielsweise können Sie 5.000 Verweise auf eine Präfixliste für alle Sicherheitsgruppen sowie 5.000 Verweise auf eine Präfixliste in allen Subnetz-Routing-Tabellen verwenden. Wenn Sie eine Präfixliste mit anderen AWS Konten teilen, werden die Verweise der anderen Konten auf Ihre Präfixliste auf dieses Kontingent angerechnet.

Netzwerk-ACLs

Name	Standard	Anpassbar	Kommentare
Netzwerk-ACLs pro VPC	200	Ja	Sie können eine Netzwerk-ACL mit einem oder mehreren Subnetzen in einer VPC verknüpfen.
Regeln pro Netzwerk-ACL	20	Ja	Dieses Kontingent bestimmt die Höchstzahl von Regeln für ein- und ausgehenden Datenverkehr. Das Kontingent kann auf maximal 40 Regeln für eingehenden und 40 Regeln für ausgehenden Datenverkehr (also insgesamt 80 Regeln) erhöht werden,

Name	Standard	Anpassbar	Kommentare
			was aber die Netzwerkleistung beeinträchtigen kann.

Netzwerkschnittstellen

Name	Standard	Anpassbar	Kommentare
Netzwerkschnittstellen pro Instance	Variiert je nach Instance-Typ	Nein	Weitere Informationen finden Sie unter Netzwerkschnittstellen pro Instance-Typ.
Netzwerkschnittstellen pro Region	5,000	Ja	Dieses Kontingent gilt für einzelne AWS-Konto VPCs und gemeinsam genutzte VPCs. Dieses Limit wird pro Availability Zone (AZ) durchgesetzt. Wenn sich die Netzwerkschnittstellen beispielsweise in drei AZs befinden, gilt für jede AZ ein Limit von 5.000 und für die Region ein Limit von 15.000.

Routing-Tabellen

Name	Standard	Anpassbar	Kommentare
Routing-Tabellen pro VPC	200	Ja	Die Haupt-Routing-Tabelle wird auf dieses Kontingent angerechnet. Beachten Sie, dass Sie, wenn Sie eine Kontingenterhöhung für Routing-Tabellen anfordern, möglicherweise auch eine Kontingenterhöhung für Subnetze anfordern sollten. Routing-Tabelle können zwar mit mehreren Subnetzen

Name	Standard	Anpassbar	Kommentare
			geteilt werden, ein Subnetz kann aber jeweils nur mit einer Routing-Tabelle verknüpft sein.
Routen pro Routing-Tabelle (nicht verteilte Routen)	50	Ja	Sie können dieses Kontingent auf maximal 1.000 erhöhen; dies beeinträchtigt jedoch möglicherweise die Netzwerkleistung. Dieses Kontingent wird für IPv4-Routen und IPv6-Routen getrennt durchgesetzt. Wenn Sie mehr als 125 Routen haben, empfehlen wir die Paginierung von Aufrufen zur Beschreibung Ihrer Routing-Tabellen, um eine bessere Leistung zu erzielen.
Propagierte Routen pro Routing-Tabelle	100	Nein	Wenn Sie weitere Präfixe benötigen, kündigen Sie eine standardmäßige Route an.

Sicherheitsgruppen

Name	Standard	Anpassbar	Kommentare
VPC-Sicherheitsgruppen pro Region	2.500	Ja	Dieses Kontingent gilt für einzelne AWS-Konto VPCs und gemeinsam genutzte VPCs. Wenn Sie dieses Kontingent auf mehr als 5 000 Sicherheitsgruppen in einer Region erweitern, empfehlen wir die Paginierung von Aufrufen zur Beschreibung Ihrer Sicherheitsgruppen, um eine bessere Leistung zu erzielen.

Name	Standard	Anpassbar	Kommentare
Regeln für ein- und ausgehenden Datenverkehr pro Sicherheitsgruppe	60	Ja	Dieses Kontingent wird für Regeln für eingehenden und ausgehenden Datenverkehr getrennt erzwungen. Für ein Konto mit dem Standardkontingent von 60 Regeln kann eine Sicherhei tsgruppe 60 Regeln für eingehend e Datenverkehr und 60 Regeln für ausgehenden Datenverkehr haben. Außerdem wird dieses Kontingent für IPv4-Regeln und IPv6-Regeln getrennt erzwungen. Für ein Konto mit dem Standardkontingent von 60 Regeln kann eine Sicherheitsgruppe 60 Regeln für eingehenden IPv4-Datenverkehr und 60 Regeln für eingehenden IPv6-Datenverkehr haben. Weitere Informati onen finden Sie unter the section called “Größe der Sicherheitsgruppe”. Eine Änderung des Kontingents wirkt sich auf die Regeln für den ein- und ausgehenden Datenverkehr aus. Dieses Kontingent, multipliziert mit dem Kontingent für Sicherheitsgruppen pro Netzwerkschnittstelle, darf 1 000 nicht überschreiten.
Sicherheitsgruppen pro Netzwerkschnittstelle	5	Ja (bis zu 16)	Dieses Kontingent multipliziert mit dem Kontingent für Regeln pro Sicherhei tsgruppe darf 1.000 nicht überschreiten.

VPC-Freigabe

Für eine freigegebene VPC gelten alle VPC-Standardkontingente.

Name	Standard	Anpassbar	Kommentare
Teilnehmerkonten pro VPC	100	Ja	Dies ist die maximale Anzahl unterschi edlicher Teilnehmerkonten, mit denen Subnetze in einer VPC freigegeben werden können. Dies ist ein Pro-VPC-K ontingent, und es gilt für alle in einer VPC freigegebenen Subnetze. VPC-Besitzer können die Netzwerks chnittstellen und Sicherheitsgruppen anzeigen, die den Teilnehmerressourcen angefügt sind.
Subnetze, die für ein Konto freigegeben werden können	100	Ja	Dies ist die maximale Anzahl von Subnetzen, die mit einem Konto gemeinsam genutzt werden können. AWS

Netzwerkadressennutzung

Network Address Usage (NAU, Netzwerkadressennutzung) setzt sich aus IP-Adressen, Netzwerkschnittstellen und CIDRs in verwalteten Präfixlisten zusammen. NAU ist eine Metrik, die auf die Ressourcen in einer VPC angewandt wird, um Sie bei der Planung und Überwachung der Größe Ihrer VPC zu unterstützen. Weitere Informationen finden Sie unter Network Address Usage.

Die Ressourcen, aus denen sich die NAU-Anzahl zusammensetzt, haben ihre eigenen individuellen Servicekontigente. Selbst wenn für eine VPC NAU-Kapazität verfügbar ist, können Sie keine Ressourcen in die VPC bringen, wenn die Ressourcen ihre Servicekontigente überschritten haben.

Name	Standard	Anpassbar	Kommentare
Network Address Usage	64.000	Ja (bis zu 256 000)	Die maximale Anzahl von NAU-Einheiten pro VPC.
Peered Network Address Usage	128.000	Ja (bis zu 512 000)	Die maximale Anzahl von NAU-Einheiten für eine VPC und alle ihre intraregionalen

Name	Standard	Anpassbar	Kommentare
			Peering-VPCs. VPCs, die über verschied ene Regionen per Peering verbunden sind, tragen nicht zu dieser Anzahl bei.

Amazon EC2-API-Drosselung

Weitere Informationen zur Drosselung von Amazon EC2 finden Sie unter API Request Throttling in der Amazon EC2 API Reference.

Zusätzliche Kontingentressourcen

Weitere Informationen finden Sie hier:

- AWS Client VPN Kontingente im AWS Client VPN Administratorhandbuch
- AWS Direct Connect -KontingenteimAWS Direct Connect Benutzerhandbuch
- Peering-Kontingente im Amazon VPC Peering Guide
- PrivateLink Kontingente im AWS PrivateLink Leitfaden
- Site-to-Site VPN-Kontingente im AWS Site-to-Site VPN Benutzerhandbuch
- Traffic Mirroring-Kontingente im Amazon VPC Traffic Mirroring Guide
- Kontingente für Transit Gateway im Amazon VPC Transi -Gateways Guide.

Dokumentverlauf

In der folgenden Tabelle sind die wichtigen Änderungen in jeder Version des Benutzerhandbuchs zu Amazon VPC beschrieben.

Änderung	Beschreibung	Datum
Bevorzugte IPv6-Lease-Zeit	Sie können jetzt auswählen, wie oft eine laufende Instance, deren IPv6 zugewiesen ist, eine DHCPv6-Lease-Erneuerung durchläuft.	20. Februar 2024
AWS Aktualisierung der von verwalteten Richtlinie	Amazon VPC hat die von AmazonVPCFullAccess und AmazonVPCReadOnlyAccess verwalteten Richtlinien aktualisiert.	8. Februar 2024
AWS Aktualisierung der von verwalteten Richtlinie	Amazon VPC hat die AmazonVPCCrossAccountNetworkInterfaceOperations von verwaltete Richtlinie aktualisiert.	25. September 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.	31. Juli 2023

Hinzufügen von sekundären IPv4-Adressen zu NAT-Gateways	Sie können sekundäre private IPv4-Adressen öffentlichen und privaten NAT-Gateways hinzufügen. Sekundäre IPv4-Adressen erhöhen die Anzahl der verfügbaren Ports und damit auch die Begrenzung der Anzahl gleichzeitiger Verbindungen, die Ihre Workloads mithilfe eines NAT-Gateways herstellen können.	31. Januar 2023
Anpassung an die bewährten IAM-Methoden	Aktualisierter Leitfaden, angepasst an die bewährten IAM-Methoden. Weitere Informationen finden Sie unter Bewährte IAM-Methoden.	4. Januar 2023
Auswählen der privaten IP-Adresse des NAT-Gateways	Wenn Sie ein NAT-Gateway erstellen, können Sie jetzt die private IP-Adresse auswählen, die dem NAT-Gateway zugewiesen ist. Bisher wurde die private IP-Adresse automatisch vom IP-Adressbereich des Subnetzes zugewiesen.	17. November 2022
IPv6-Standard-Gateway-Router-Konfiguration	Drei IPv6-Adressen sind jetzt für die Verwendung durch den Standard-VPC-Router reserviert.	11. November 2022
Übertragen von Elastic-IP-Adressen	Sie können jetzt Elastic IP-Adressen von einem AWS Konto auf ein anderes übertragen.	31. Oktober 2022

Metriken für Network Address Usage	Sie können Metriken zur Network Address Usage für Ihre VPC aktivieren, um die Größe Ihrer VPC zu planen und zu überwachen.	04. Oktober 2022
Veröffentlichen von Flow-Protokollen in Amazon Data Firehose	Sie können einen Amazon-Data-Firehose-Bereitstellungsdatenstrom als Ziel für Flow-Protokolldaten angeben.	8. September 2022
NAT-Gateway-Bandbreite	NAT-Gateways unterstützen jetzt eine Bandbreite von bis zu 100 Gbit/s (ein Anstieg von 45 Gbit/s) und können bis zu zehn Millionen Pakete pro Sekunde verarbeiten (gegenüber vier Millionen Paketen).	15. Juni 2022
Mehrere IPv6-CIDR-Blöcke	Sie können einer VPC bis zu fünf IPv6-CIDR-Blöcke zuordnen.	12. Mai 2022
Reorganisation	Allgemeine Reorganisation des Benutzerhandbuchs von Amazon Virtual Private Cloud.	2. Januar 2022
NAT-Gateway IPv6 zu IPv4	NAT-Gateway unterstützt die Übersetzung von Netzwerkadressen von IPv6 nach IPv4, im Volksmund als NAT64 bekannt.	24. November 2021
IPv6–only Subnetze in VPCs	Sie können IPv6–only Subnetze erstellen, in die Sie nur IPv6-EC2-Instances starten können.	23. November 2021

Lieferoptionen von VPC-Flow-Protokollen an Amazon S3	Sie können das Apache-Parquet-Protokolldateiformat, stündliche Partitionen und HIVE-kompatible S3-Präfixe angeben.	13. Oktober 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
Spezifischere Routen	Sie können Ihren Routing-Tabellen eine Route hinzufügen, die spezifischer als die lokale Route ist. Sie können spezifischere Routen verwenden, um Datenverkehr zwischen Subnetzen innerhalb einer VPC (Ost-West-Verkehr) zu einer Middlebox-Appliance umzuleiten. Sie können festlegen, dass das Ziel einer Route mit einem gesamten IPv4- oder IPv6-CIDR-Block eines Subnetzes in Ihrer VPC übereinstimmt.	30. August 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

Private NAT-Gateways	Sie können ein privates NAT-Gateway für die ausgehende private Kommunikation zwischen VPCs oder zwischen einer VPC und Ihrem On-Premises-Netzwerk verwenden.	10. Juni 2021
Tag beim Erstellen	Sie können Markierungen hinzufügen, wenn Sie eine VPC, DHCP-Optionen, ein Internet-Gateway, ein Gateway nur für ausgehenden Verkehr, eine Netzwerk-ACL und eine Sicherheitsgruppe erstellen.	30. Juni 2020
Verwaltete Präfixlisten	Sie können eine Gruppe von CIDR-Blöcken in einer Präfixliste erstellen und verwalten.	29. Juni 2020
Flow-Protokoll-Erweiterungen	Neue Flow-Protokollfelder sind verfügbar, und Sie können ein benutzerdefiniertes Format für Flow-Protokolle angeben, die in - CloudWatch Protokollen veröffentlicht werden.	4. Mai 2020
Markierungsunterstützung für Flow-Protokolle	Sie können Ihren Flow-Protokollen Markierungen hinzufügen.	16. März 2020
Tag zur Erstellung des NAT-Gateways	Sie können eine Markierung hinzufügen, wenn Sie ein NAT-Gateway erstellen.	9. März 2020

Maximales Aggregationsintervall für Flow-Protokolle	Sie können den maximalen Zeitraum angeben, in dem ein Flow erfasst und zu einem Flow-Protokolldatensatz aggregiert wird.	4. Februar 2020
Konfiguration von Netzwerkgrenzgruppen	Sie können Netzwerkgrenzgruppen für Ihre VPCs über die Amazon Virtual Private Cloud Console konfigurieren.	22. Januar 2020
Privater DNS-Name	Sie können privat von Ihrer VPC aus mit privaten DNS-Namen auf - AWS PrivateLink basierte Services zugreifen.	6. Januar 2020
Gateway-Routing-Tabellen	Sie können eine Routing-Tabelle einem Gateway zuordnen und eingehenden VPC-Datenverkehr an eine bestimmte Netzwerkschnittstelle in Ihrer VPC weiterleiten.	03. Dezember 2019
Flow-Protokoll-Erweiterungen	Sie können ein benutzerdefiniertes Format für Ihr Flow-Protokoll angeben und auswählen, welche Felder in den Flow-Protokolldatenstätzen ausgegeben werden sollen.	11. September 2019
VPC Sharing	Sie können Subnetze, die sich in derselben VPC befinden, für mehrere Konten in derselben AWS Organisation freigeben.	27. November 2018

Ein Standard-Subnetz erstellen	Sie können ein Standards ubnetz in einer Availability Zone erstellen, in der es noch kein solches gibt.	9. November 2017
Unterstützung einer Markierung für NAT-Gateways	Sie können Ihren NAT-Gateway markieren.	7. September 2017
Amazon- CloudWatch Metriken für NAT-Gateways	Sie können CloudWatch Metriken für Ihr NAT-Gateway anzeigen.	7. September 2017
Beschreibungen der Sicherheitsgruppenregel	Sie können Ihren Sicherheitsgruppenregeln Beschreibungen hinzufügen.	31. August 2017
Sekundäre IPv4-CIDR-Blöcke für Ihre VPC	Sie können Ihrer VPC mehrere IPv4-CIDR-Blöcke hinzufügen.	29. August 2017
Wiederherstellen von Elastic-IP-Adressen	Wenn Sie eine Elastic-IP-Adresse freigeben, können Sie sie möglicherweise wiederherstellen.	11. August 2017
Eine Standard-VPC erstellen	Wenn Sie Ihre vorhandenen Standard-VPC löschen, können Sie eine neue Standard-VPC erstellen.	27. Juli 2017
IPv6-Support	Sie können Ihrer VPC einen IPv6 CIDR-Block zuordnen und Ihren Ressourcen in der VPC IPv6-Adressen zuweisen.	1. Dezember 2016
Support für DNS-Auflösung für IP-Adressbereiche außerhalb von RFC 1918	Der Amazon DNS-Server kann jetzt für alle Adressräume private DNS-Hostnamen in private IP-Adressen auflösen.	24. Oktober 2016

NAT-Gateways	Sie können NAT-Gateways in einem öffentlichen Subnetz erstellen und Instances in einem privaten Subnetz ermöglichen, ausgehenden Datenverkehr zum Internet und anderen AWS -Services zu initiieren.	17. Dezember 2015
VPC Flow Logs	Sie können Flow-Protokolle erstellen, um Informationen über den IP-Datenverkehr zu und von Netzwerkschnittstellen in Ihrer VPC zu erfassen.	10. Juni 2015
ClassicLink	Sie können verwenden ClassicLink , um 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.	7. Januar 2015
Verwenden von privat gehosteten Zonen	Sie können über benutzerdefinierte DNS-Domainnamen, die Sie in einer privat gehosteten Zone in Route 53 definieren, auf Ressourcen in Ihrer VPC zugreifen.	5. November 2014

Ändern des öffentlichen IP-Adressierungsattributs eines Subnetzes	Sie können das öffentliche IP-Adressierungsattribut eines Subnetzes ändern, um festzulegen, ob Instances in diesem Subnetz eine öffentliche IP-Adresse erhalten sollen.	21. Juni 2014
Zuweisen einer öffentlichen IP-Adresse	Sie können einer Instance beim Start eine öffentliche IP-Adresse zuweisen.	20. August 2013
Aktivieren von DNS-Hostnamen und Deaktivieren von DNS-Auflösung	Sie können VPC-Standardwerte ändern und die DNS-Auflösung deaktivieren und DNS-Hostnamen aktivieren.	11. März 2013
VPC Everywhere	Unterstützung für VPC in fünf AWS Regionen, VPCs in mehreren Availability Zones, mehrere VPCs pro AWS Konto und mehrere VPN-Verbindungen pro VPC hinzugefügt.	3. August 2011
Dedicated Instances	Dedicated Instances sind Amazon EC2-Instances, die innerhalb Ihrer VPC gestartet werden und nur zur Ausführung der Hardware eines einzigen Kunden dienen.	27. März 2011

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.