



Benutzer-Leitfaden

Amazon Virtual Private Cloud



Amazon Virtual Private Cloud: Benutzer-Leitfaden

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist Amazon VPC?	1
Features	1
Erste Schritte mit Amazon VPC	3
Arbeiten mit Amazon VPC	3
Preise für Amazon VPC	4
Funktionsweise von Amazon VPC	6
VPCs und Subnetze	7
Standardmäßige und nicht standardmäßige VPCs	7
Routing-Tabellen	8
Zugriff auf das Internet	8
Zugriff auf ein Unternehmens- oder Heimnetzwerk	9
Verbinden von VPCs und Netzwerken	10
Privates globales Netzwerk von AWS	10
Planen der VPC	12
Melde dich an für eine AWS-Konto	12
Überprüfen der Berechtigungen	13
Ermitteln Sie Ihre IP-Adressbereiche	13
Wählen Sie Ihre Availability Zones	13
Planen Sie Ihre Internetverbindung	14
Erstellen Sie Ihre VPC	14
Bereitstellen der Anwendung	15
IP-Adressierung	16
Private Adressen IPv4	17
Öffentliche Adressen IPv4	18
IPv6 Adressen	19
Öffentliche Adressen IPv6	20
Private Adressen IPv6	21
Verwenden Sie Ihre eigenen IP-Adressen	22
Amazon VPC IP Address Manager	23
VPC-CIDR-Blöcke	23
IPv4 VPC CIDR-Blöcke	23
IPv4 CIDR-Blöcke für eine VPC verwalten	25
IPv4 Einschränkungen der CIDR-Blockzuweisung	27
IPv6 VPC CIDR-Blöcke	30

Subnetz-CIDR-Blöcke	31
Größe der Subnetze für IPv4	32
Größe des Subnetzes für IPv6	32
Vergleich von IPv4 und IPv6	33
Verwaltete Präfixlisten	35
Konzepte und Regeln für Präfixlisten	36
Identitäts- und Zugriffsverwaltung für Präfixlisten	37
Vom Kunden verwaltete Präfixlisten	38
AWS Von verwaltete Präfixlisten	48
Optimieren Sie das AWS Infrastrukturmanagement mit Präfixlisten	51
AWS-IP-Adressbereiche	54
Herunterladen	54
Kontrolle des ausgehenden Datenverkehrs	55
Geolokalisierungs-Feed	55
IPv4-Adressbereiche finden	55
Syntax	62
Abonnieren von -Benachrichtigungen	68
IPv6-Unterstützung für Ihre VPC	70
Hinzufügen der IPv6-Unterstützung für Ihre VPC	71
Beispiel für eine Dual-Stack-VPC	76
IPv6 Unterstützung auf AWS	78
Dienste, die unterstützen IPv6	78
Zusätzliche IPv6 Unterstützung	92
Weitere Informationen	93
Virtual Private Clouds	94
VPC-Grundlagen	95
IP-Adressbereich der VPC	95
VPC-Diagramm	95
VPC-Ressourcen	96
VPC-Konfigurationsoptionen	97
Standard VPCs	99
Komponenten von Standard-VPCs	99
Standard-Subnetze	102
Arbeiten mit Ihrer Standard-VPC und Standard-Subnetzen	103
Erstellen einer VPC	107
Erstellen Sie eine VPC und andere VPC-Ressourcen	107

Ausschließliches Erstellen einer VPC	109
Erstellen einer VPC mithilfe der AWS CLI	112
Visualisierung der Ressourcen in Ihrer VPC	117
CIDR-Block hinzufügen oder entfernen	118
DHCP-Optionssätze	121
Was ist DHCP?	122
DHCP-Optionssatzkonzepte	123
Arbeiten mit DHCP-Optionslisten	127
DNS-Attribute	131
Grundlagen von Amazon DNS	132
Anzeigen von DNS-Hostnamen für EC2-Instances	137
Anzeigen und Aktualisieren von DNS-Attributen für Ihre VPC	138
Network Address Usage	140
Wie NAU berechnet wird	140
NAU-Beispiele	141
Freigeben eines VPC-Subnetzes	143
Voraussetzungen für die Arbeit mit freigegebenen Subnetzen	143
Arbeiten mit freigegebenen Subnetzen	144
Fakturierung und Messung für den Eigentümer und Teilnehmer	147
Verantwortlichkeiten und Berechtigungen für Besitzer und Teilnehmer	147
AWS-Ressourcen und freigegebene VPC-Subnetze	151
Eine VPC auf andere Zonen erweitern	152
Subnetze in AWS Local Zones	153
Subnetze in AWS Wavelength	159
Subnetze in AWS Outposts	162
Löschen der VPC	163
Löschen mithilfe der Konsole	164
Mit der CLI löschen	165
IaC aus Konsolenaktionen generieren	166
Subnetze	168
Subnetze-Grundlagen	168
Subnetz-IP-Adressbereiche	168
Subnetz-Typen	169
Subnetzdiagramm	170
Subnetz-Routing	170
Subnetz-Einstellungen	170

Subnetz-sicherheit	171
Erstellen eines Subnetzes	172
Hinzufügen oder Entfernen eines IPv6-CIDR-Blocks aus Ihrem Subnetz	174
Ändern der IP-Adressierungsattribute Ihres Subnetzes	175
Subnetz-CIDR-Reservierungen	176
Arbeiten mit Subnetz-CIDR-Reservierungen mithilfe der Konsole	177
Arbeiten mit Subnetz-CIDR-Reservierungen mithilfe von AWS CLI	178
Routing-Tabellen	179
Routing-Tabellen-Konzepte	180
Subnetz-Routingtabellen	182
Gateway-Routing-Tabellen	190
Routenpriorität	193
Beispiele für Routing-Optionen	195
Erstellen einer Routing-Tabelle mit Routen	212
Verwalten von Subnetz-Routing-Tabellen	214
So ersetzen Sie die Routing-Haupttabelle	218
Zuordnen einer Routing-Tabelle zu einem Gateway	219
Ersetzen oder Wiederherstellen des Ziels für eine lokale Route	220
Erweitertes Routing	221
Beheben von Problemen mit der Erreichbarkeit	271
Middlebox-Routing-Assistent	271
Voraussetzungen für Middlebox-Routing-Assistent	272
Weiterleiten des VPC-Datenverkehrs an eine Sicherheits-Appliance	272
Überlegungen des Middlebox-Routing-Assistenten	275
Middlebox-Szenarien	276
Löschen eines Subnetzes	286
Verbinden Ihrer VPC	288
Internet-Gateways	290
Grundlagen zu Internet-Gateways	290
Ein Internet-Gateway erstellen	293
Löschen eines Internet-Gateways	296
Internet-Gateways nur für ausgehenden Datenverkehr	297
Grundlagen des Internet-Gateways für ausgehenden Verkehr	298
Hinzufügen eines auf ausgehenden Verkehr beschränkten Internetzugriffs zu einem Subnetz	299
NAT-Geräte	302

NAT gateways (NAT-Gateways)	304
NAT-Instances	361
Vergleich von NAT-Geräten	374
Elastic-IP-Adressen	377
Elastic-IP-Adresskonzepte und -Regeln	378
Erste Schritte zum Verwenden von Elastic-IP-Adressen	380
AWS Transit Gateway	390
AWS Virtual Private Network	392
VPC-Peering-Verbindungen	393
Überwachen	395
VPC Flow Logs	396
Grundlagen zu Flow-Protokollen	397
Flow-Protokolldatensätze	401
Beispiele für Flow-Protokolldatensätze	417
Einschränkungen von Flow-Protokollen	428
Preisgestaltung	431
Arbeiten mit Flow-Protokollen	432
In CloudWatch Logs veröffentlichen	435
Auf Amazon S3 veröffentlichen	444
Veröffentlichen in Amazon Data Firehose	454
Abfragen mit Athena	462
Fehlerbehebung	467
CloudWatch-Metriken	472
NAU-Metriken und -Dimensionen	472
Aktivieren oder Deaktivieren der NAU-Überwachung	475
Alarm-Beispiel für NAU CloudWatch	476
Fakturierungs- und Nutzungsberichte	477
IP-Adressverwaltung	478
VPC-Endpunkte	478
Transit Gateways	479
Netzwerkanalyse	480
Datenverkehrsspiegelung	480
VPC Lattice	480
Konto- und regionsübergreifende Ressourcen	481
Beschreiben Ihres VPC-Netzwerks	482
Geografischer Standort	483

Subnets	484
Netzwerkonnktivität	486
Sicherheitskontrollen	491
Verwaltung des Datenverkehrs	493
Zugehörige Ressourcen	496
Sicherheit	497
Datenschutz	498
Richtlinie für den Datenverkehr zwischen Netzwerken	499
VPC-Verschlüsselung bei der Übertragung erzwingen	500
Die Verschlüsselung steuert die Modi	500
Überwachung des Verschlüsselungsstatus von Verkehrsströmen	501
Ausnahmen von VPC-Verschlüsselungskontrollen	502
Arbeitsablauf bei der Implementierung	503
Status der VPC-Verschlüsselung steuert	504
AWS Serviceunterstützung und Kompatibilität	504
Preisgestaltung	4
AWS CLI Befehlsreferenz	509
Weitere Ressourcen	509
Identitäts- und Zugriffsverwaltung	509
Zielgruppe	510
Authentifizieren mit Identitäten	511
Verwalten des Zugriffs mithilfe von Richtlinien.	512
Funktionsweise von der Amazon VPC mit IAM	514
Beispiele für Richtlinien	518
Fehlerbehebung	532
AWS verwaltete Richtlinien	534
Verwenden von servicegebundenen Rollen	538
Sicherheit der Infrastruktur	543
Netzwerkisolierung	543
Kontrollieren des Netzwerkverkehrs	544
Vergleichen Sie Sicherheitsgruppen und Netzwerk ACLs	545
Sicherheitsgruppen	547
Sicherheitsgruppengrundlagen	548
Beispiel für eine Sicherheitsgruppe	550
Sicherheitsgruppenregeln	551
Standardsicherheitsgruppen	557

Eine Sicherheitsgruppe erstellen	559
Konfigurieren von Sicherheitsgruppenregeln	561
Löschen einer Sicherheitsgruppe	563
Ordnen Sie Sicherheitsgruppen mehreren zu VPCs	564
Sicherheitsgruppen mit AWS Organizations teilen	568
Netzwerk ACLs	574
Grundlagen von Netzwerk-ACLs	576
Regeln für Netzwerk-ACLs	577
Standardnetzwerk-ACL	579
Benutzerdefiniertes Netzwerk ACLs	580
Path MTU Discovery	586
Erstellen einer Netzwerk-ACL	587
Verwalten von Netzwerk-ACL-Zuordnungen	591
Löschen einer Netzwerk-ACL	594
Beispiel: Steuern des Zugriffs auf Instances in einem Subnetz	595
Ausfallsicherheit	599
Compliance-Validierung	601
Sperrern Sie den öffentlichen Zugriff VPCs auf Subnetze	601
VPC-BPA-Grundlagen	602
Bewerten der Auswirkungen von VPC-BPA und Überwachen von VPC-BPA	609
Erweitertes Beispiel	614
Best Practices	670
Verwendung mit anderen Services	672
AWS PrivateLink	673
AWS Network Firewall	674
Route 53 Resolver DNS Firewall	676
Reachability Analyzer	677
Beispiele	679
Testumgebungen	680
Übersicht	680
1. Erstellen Sie die VPC	683
2. Bereitstellen der Anwendung	684
3. Testen Sie Ihre Konfiguration	684
4. Bereinigen	684
Web- und Datenbankserver	684
-Übersicht	685

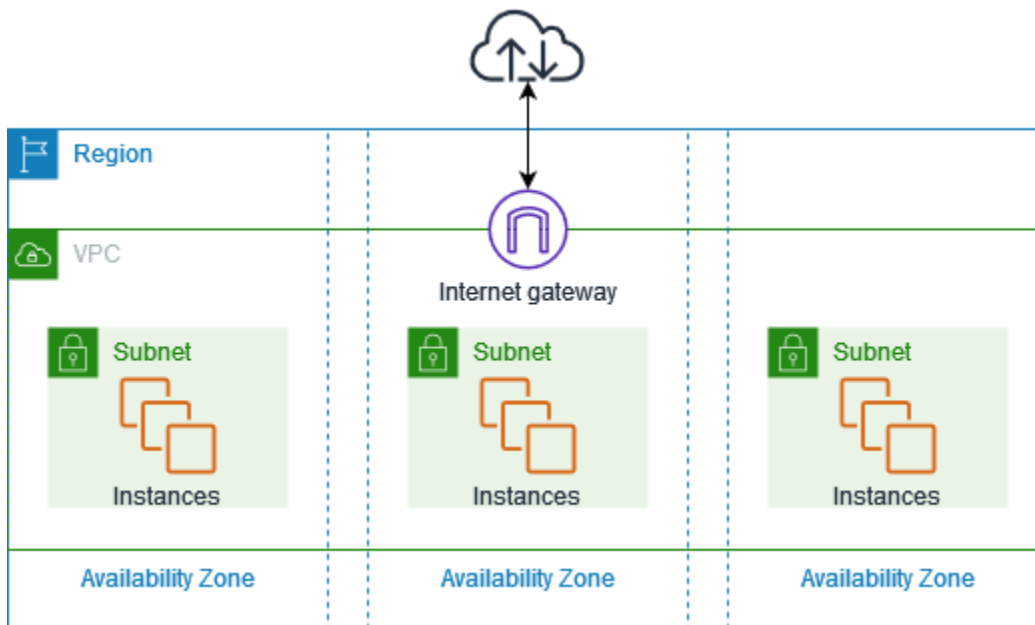
1. Erstellen Sie die VPC	689
2. Bereitstellen der Anwendung	690
3. Testen Sie Ihre Konfiguration	691
4. Bereinigen	691
Private Server	691
-Übersicht	692
1. Erstellen Sie die VPC	694
2. Bereitstellen der Anwendung	695
3. Testen Sie Ihre Konfiguration	696
4. Bereinigen	696
Tutorials	697
Erste Schritte mit Amazon VPC mithilfe der AWS CLI	697
Voraussetzungen	698
Erstellen einer VPC	699
Erstellen von Subnetzen	699
Konfigurieren der Internetverbindung	701
Erstellen eines NAT-Gateways	702
Konfigurieren der Subnetz-Einstellungen	703
Erstellen von Sicherheitsgruppen	704
Ihre VPC-Konfiguration überprüfen	705
Stellen Sie EC2 Instanzen bereit	706
Fehlerbehebung	236
Bereinigen von Ressourcen	709
In die Produktion übergehen	711
Nächste Schritte	711
Erstellen einer VPC mit privaten Subnetzen und NAT-Gateways mit der AWS CLI	712
Voraussetzungen	698
Erstellen der VPC und der Subnetze	714
Erstellen und konfigurieren der Internetverbindung	716
Erstellen von NAT-Gateways	718
Erstellen eines VPC-Endpunkts für Amazon S3	719
Configure Security Groups (Sicherheitsgruppen konfigurieren)	720
Erstellen einer Startvorlage für EC2-Instances	721
Erstellen eines Load Balancers und einer Zielgruppe	723
Erstellen einer Auto-Scaling-Gruppe	724
Testen Sie Ihre Konfiguration	725

Bereinigen von Ressourcen	709
Nächste Schritte	711
Kontingente	728
VPC und Subnetze	728
DNS	729
Elastic-IP-Adressen	729
Gateways	730
Vom Kunden verwaltete Präfixlisten	730
Netzwerk ACLs	732
Netzwerkschnittstellen	732
Routing-Tabellen	733
Route Server	734
Sicherheitsgruppen	736
VPC-Subnetz-Freigabe	737
Netzwerkadressennutzung	738
Drosselung der EC2 Amazon-API	738
Zusätzliche Kontingentressourcen	739
Dokumentverlauf	740
.....	dccliii

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 hat ein Subnetz in jeder Availability Zones in der Region, EC2 Instances in jedem Subnetz und ein Internet-Gateway, um die Kommunikation zwischen den Ressourcen in Ihrer VPC und dem Internet zu ermöglichen.



Weitere Informationen finden Sie unter [Amazon Virtual Private Cloud \(Amazon VPC\)](#).

Features

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

Virtual Private Clouds (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.

Subnets

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 Subnetzen IPv4 und IPv6 IP-Adressen](#) sowohl als auch zuweisen. Sie können Ihre öffentlichen IPv4 Adressen und IPv6 GUA-Adressen auch zu Ressourcen in Ihrer VPC übertragen AWS und sie Ressourcen wie EC2 Instances, NAT-Gateways und Network Load Balancers 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 Verkehr zwischen den Ressourcen in zwei zu leiten. VPCs

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 Knotenpunkt fungiert, um den Verkehr zwischen Ihren VPCs VPN-Verbindungen und 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

Stellen Sie mithilfe von [AWS Virtual Private Network \(Site-to-Site VPN\)](#) eine Verbindung VPCs zu Ihren lokalen Netzwerken her.

Erste Schritte mit Amazon VPC

Ihre AWS-Konto enthält jeweils AWS-Region eine [Standard-VPC](#). Ihre Standardeinstellungen VPCs sind so konfiguriert, dass Sie sofort mit dem Starten und Herstellen einer Verbindung zu EC2 Instances beginnen können. Weitere Informationen finden Sie unter [Planen der VPC](#).

Sie können wählen, ob Sie zusätzliche VPCs Subnetze, IP-Adressen, Gateways und Routing erstellen möchten, 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-Managementkonsole**— Bietet eine Weboberfläche, über die Sie auf Ihre zugreifen können 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**— Bietet sprachspezifische Funktionen APIs 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 Amazon EC2 API-Referenz.

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 bereit. Die überwiegende Mehrheit der Ressourcen in Ihrer VPC verwendet private IPv4 Adressen. Ressourcen, für die ein direkter Zugriff auf das Internet erforderlich ist IPv4, verwenden jedoch öffentliche IPv4 Adressen.

Mit Amazon VPC können Sie verwaltete Services wie ELB, Amazon RDS und Amazon EMR starten, ohne zuvor eine VPC einrichten zu müssen. Dazu wird die [Standard-VPC](#) in Ihrem Konto verwendet, falls Sie eine haben. Alle öffentlichen IPv4 Adressen, die Ihrem Konto durch den verwalteten Service zur Verfügung gestellt wurden, werden in Rechnung gestellt. Diese Gebühren werden mit dem Amazon VPC-Service in Ihrem AWS Cost and Usage Report verknüpft.

Preise für öffentliche Adressen IPv4

Eine öffentliche IPv4 Adresse ist eine IPv4 Adresse, die aus dem Internet geroutet werden kann. Eine öffentliche IPv4 Adresse ist notwendig, damit eine Ressource direkt vom Internet IPv4 aus erreichbar ist.

Wenn Sie bereits Kunde oder neuer Kunde des [AWS kostenlosen Kontingents](#) sind, können Sie mit dem EC2 Service 750 Stunden lang öffentliche IPv4 Adressen kostenlos nutzen. Wenn Sie den EC2 Service nicht im Rahmen des AWS kostenlosen Kontingents nutzen, werden öffentliche IPv4 Adressen berechnet. Spezifische Preisinformationen finden Sie auf der Registerkarte Öffentliche IPv4 Adresse in der [Amazon VPC-Preisgestaltung](#).

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

Es gibt die folgenden Typen von öffentlichen IPv4 Adressen:

- **Elastische IP-Adressen (EIPs):** Von Amazon bereitgestellte statische, öffentliche IPv4 Adressen, die Sie einer EC2 Instance, einer elastic network interface oder einer AWS Ressource zuordnen können.
- **EC2 öffentliche IPv4 Adressen:** Öffentliche IPv4 Adressen, die einer EC2 Instance von Amazon zugewiesen wurden (wenn die EC2 Instance in einem Standardsubnetz gestartet wird oder

wenn die Instance in einem Subnetz gestartet wird, das für die automatische Zuweisung einer öffentlichen IPv4 Adresse konfiguriert wurde).

- BYOIPv4 Adressen: Öffentliche IPv4 Adressen im IPv4 Adressbereich, zu dem Sie AWS mithilfe von [Bring Your Own IP Addresses \(BYOIP\)](#) gewechselt haben.
- Vom Dienst verwaltete IPv4 Adressen: Öffentliche IPv4 Adressen, die automatisch auf AWS Ressourcen bereitgestellt und von einem Dienst verwaltet werden. AWS Zum Beispiel öffentliche IPv4 Adressen auf Amazon ECS, Amazon RDS oder Amazon WorkSpaces.

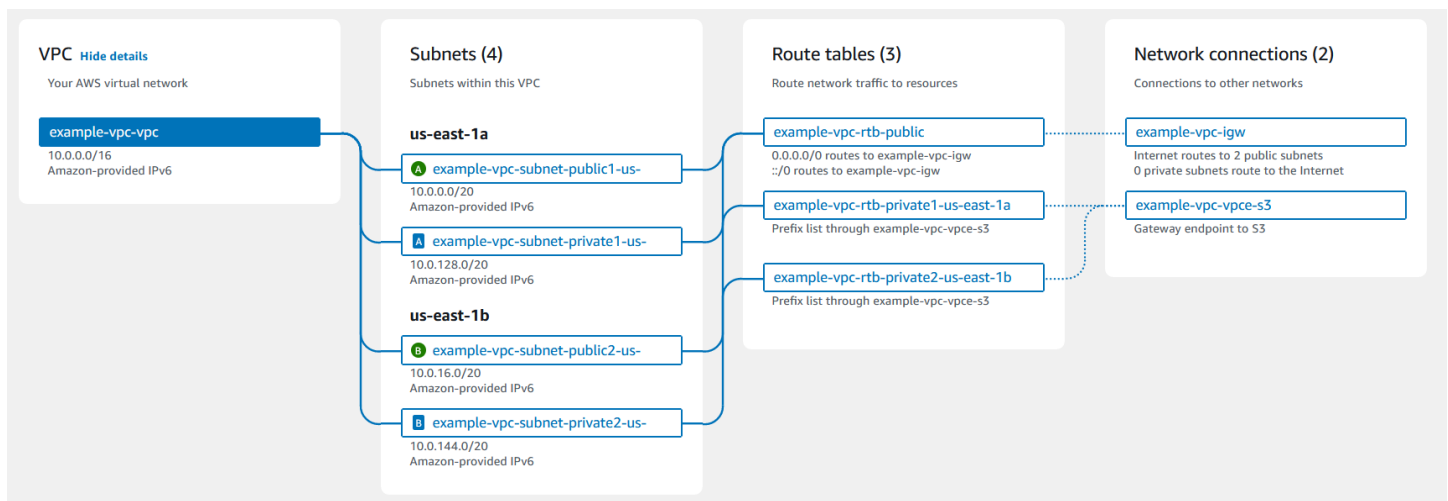
Die folgende Liste zeigt die gängigsten AWS Dienste, die öffentliche IPv4 Adressen verwenden können.

- WorkSpaces Amazon-Anwendungen
- [AWS Client VPN](#)
- AWS Database Migration Service
- Amazon EC2
- Amazon Elastic Container Service
- Amazon EKS
- Amazon EMR
- GameLift Amazon-Server
- 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

Sie können Amazon Virtual Private Cloud (Amazon VPC) verwenden, um AWS-Ressourcen in einem logisch isoliertem virtuellen Netzwerk zu 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 nutzen AWS.

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-Managementkonsole 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](#)

- [Privates globales Netzwerk von AWS](#)

VPCs und Subnetze

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk für Ihr AWS-Konto. Es ist von anderen virtuellen Netzwerken in der AWS Cloud getrennt. 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 für Ihre 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

- [Aktivieren des Internetzugangs für eine VPC mithilfe eines Internet-Gateways](#)
- [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 mithilfe einer IPsec-AWS Site-to-Site VPN-Verbindung mit Ihrem firmeneigenen Rechenzentrum verbinden und so die AWS-Cloud als Erweiterung Ihres Rechenzentrums nutzen.

Eine Site-to-Site-VPN-Verbindung besteht aus zwei VPN-Tunneln zwischen einem Virtual Private Gateway oder Transit-Gateway auf 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 möglicherweise angefügten VPCs, VPN-Verbindungen, Direct Connect-Gateways und Transit-Gateway-Peering-Verbindungen.

Weitere Informationen

- [Amazon VPC Peering Guide](#)
- [Amazon VPC Transit Gateways](#)

Privates globales Netzwerk von AWS

AWS bietet ein privates Hochleistungsnetzwerk mit geringer Latenz, das eine sichere Cloud Computingumgebung bereitstellt, die Ihre Netzwerkanforderungen unterstützt. AWS Die Regionen sind mit mehreren Internetdiensteanbietern sowie einem privaten Netzwerk-Backbone verbunden, die die Netzwerkleistung des durch die Kunden erzeugten regionsübergreifenden Datenverkehrs verbessern.

Pakete, die ihren Ursprung im privaten globalen Netzwerk und ein Ziel im privaten globalen Netzwerk haben, verbleiben im privaten globalen Netzwerk und durchlaufen nicht das öffentliche Internet. Das gilt unabhängig davon, ob es sich bei dem Ziel um eine private IP-Adresse oder eine öffentliche IP-Adresse handelt. Wenn beispielsweise EC2-Instances in zwei VPCs über öffentliche IP-Adressen kommunizieren, bleibt der Datenverkehr im privaten globalen Netzwerk. Das Ziel kann sich in derselben Availability Zone, einer anderen Availability Zone in derselben Region oder in einer anderen Region befinden, mit Ausnahme der Regionen 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 den gesamten globalen Backbone, der die AWS-Regionen verbindet. Wir betreiben unser Backbone-Netzwerk mit dem Ziel von p99 der stündlichen PLR von weniger als 0,0001 %.

Planen der VPC

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

Aufgaben

- [Melde dich an für eine 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 eine 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/die Anmeldung](https://portal.aws.amazon.com/billing/die-Anmeldung).
2. Folgen Sie den Online-Anweisungen.

Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um [Aufgaben auszuführen, die Root-Benutzerzugriff erfordern](#).

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu <https://aws.amazon.com/> gehst und Mein Konto auswählst.

Überprüfen der Berechtigungen

Um Amazon VPC verwenden zu können, benötigen Sie die erforderlichen Berechtigungen. Weitere Informationen erhalten 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 Subnetze erstellen VPCs , können Sie deren IP-Adressbereiche auswählen. Wenn Sie Ressourcen in einem Subnetz bereitstellen, z. B. EC2 Instances, erhalten sie IP-Adressen aus dem IP-Adressbereich des Subnetzes. Weitere Informationen finden Sie unter [IP-Adressierung](#).

Denken Sie bei der Auswahl der Größe für Ihre VPC darüber nach, wie viele IP-Adressen Sie in Ihrem AWS-Konten Land benötigen. VPCs Stellen Sie sicher, dass sich die IP-Adressbereiche für VPCs Sie nicht mit den IP-Adressbereichen für Ihr eigenes Netzwerk überschneiden. Wenn Sie Konnektivität zwischen mehreren benötigen VPCs, müssen Sie sicherstellen, dass sie 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, die als Availability Zones bezeichnet werden. 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. Beispiel:

- 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 [ELB](#). 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 die Anzahl VPCs und Subnetze, die Sie benötigen, bestimmt haben, welche CIDR-Blöcke Ihren VPCs 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-

Managementkonsole 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 EC2 Amazon-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 individuelle IPv4 Adresse ist 32 Bit lang und besteht aus 4 Gruppen mit bis zu 3 Dezimalziffern (0-255). Zum Beispiel 10.0.1.0.
- Ein IPv4 CIDR-Block hat eine IPv4 Adresse, gefolgt von einem Schrägstrich und einer Zahl von 0 bis 32. Beispielsweise steht 10.0.0.0/16 für 65.536 Adressen von 10.0.0.0 bis 10.0.255.255 IPv4 .
- Eine einzelne IPv6 Adresse ist 128 Bit lang und besteht aus 8 Segmenten mit 4 Hexadezimalziffern. Zum Beispiel: 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Es ist nicht notwendig, die führenden Nullen in ein Segment aufzunehmen. Sie können in einer Adresse auch aufeinanderfolgende Segmente, die nur Null enthalten, einmal durch doppelte Doppelpunkte (::) ersetzen. Daher kann die Beispieladresse zu 2001:db8:85a3::8a2e:370:7334 komprimiert werden.
- Ein IPv6 CIDR-Block hat eine IPv6 Adresse, die mit Segmenten endet, die nur Null sind, wobei die Segmente, die nur Null sind, durch einen doppelten Doppelpunkt ersetzt werden, gefolgt von einem Schrägstrich und einer Zahl von 0 bis 128. Beispielsweise steht 2001:db 8:1234:1 a00: :/56 für 2⁷² IPv6 Adressen von 2001:db 8:1234:1 a 00:0000:0000:0000 bis 2001:db 8:1234:1 aff:ffff:ffff:ffff.

Weitere Informationen finden Sie unter [Was ist CIDR?](#)

Inhalt

- [Private Adressen IPv4](#)
- [Öffentliche Adressen IPv4](#)
- [IPv6 Adressen](#)
- [Verwenden Sie Ihre eigenen IP-Adressen](#)
- [Amazon VPC IP Address Manager](#)
- [VPC-CIDR-Blöcke](#)
- [Subnetz-CIDR-Blöcke](#)
- [Vergleich von IPv4 und IPv6](#)

- [Konsolidierung und Verwaltung von Netzwerk-CIDR-Blöcken mit verwalteten Präfixlisten](#)
- [AWS-IP-Adressbereiche](#)
- [IPv6-Unterstützung für Ihre VPC](#)
- [AWS Dienste, die unterstützen IPv6](#)

Private Adressen IPv4

Private IPv4 Adressen (in diesem Thema auch als private IP-Adressen bezeichnet) sind über das Internet nicht erreichbar und können für die Kommunikation zwischen den Instances in Ihrer VPC verwendet werden. Wenn Sie eine Instance in einer VPC starten, wird der primären Netzwerkschnittstelle (z. B. eth0) der Instance eine primäre private IP-Adresse aus dem IPv4 Adressbereich des Subnetzes zugewiesen. 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 Instanzbenennung. EC2](#) 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 EC2 Amazon-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 EC2 Amazon-Benutzerhandbuch.

Wir bezeichnen private IP-Adressen als IP-Adressen, die sich innerhalb des IPv4 CIDR-Bereichs der VPC befinden. 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. Direct Connect

Wir geben den IPv4 Adressbereich eines Subnetzes niemals im Internet bekannt.

Öffentliche Adressen IPv4

Alle Subnetze verfügen über ein Attribut, das bestimmt, ob eine im Subnetz erstellte Netzwerkschnittstelle automatisch eine öffentliche IPv4 Adresse erhält (in diesem Thema auch als öffentliche IP-Adresse bezeichnet). Wenn Sie daher eine Instance in einem Subnetz starten, in dem dieses Attribut aktiviert ist, wird der primären Netzwerkschnittstelle, 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 [Amazon VPC-Preisseite](#) auf der Registerkarte Öffentliche IPv4 Adresse.

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 der IP-Adressierungsattribute 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 für Ihre Instance nach dem Start aufheben, indem Sie die mit einer Netzwerkschnittstelle verbundenen IP-Adressen verwalten. Weitere Informationen finden Sie unter [IP-Adressen verwalten](#) im EC2 Amazon-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. Wir trennen in bestimmten Fällen die öffentliche IP-Adresse von Ihrer Instance oder weisen ihr eine neue IP-Adresse zu. Weitere Informationen finden Sie unter [Öffentliche IP-Adressen](#) im EC2 Amazon-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](#).

Wenn Sie Amazon VPC IP Address Manager (IPAM) verwenden, können Sie einen zusammenhängenden Block von öffentlichen IPv4 Adressen abrufen AWS und ihn verwenden, um Ressourcen sequentielle Elastic IP-Adressen zuzuweisen. AWS Durch die Verwendung zusammenhängender IPv4 Adressblöcke kann der Verwaltungsaufwand für Sicherheitszugriffskontrolllisten erheblich reduziert und die Zuweisung und Nachverfolgung von IP-Adressen für Unternehmen, die darauf skalieren, vereinfacht werden. AWS Weitere Informationen finden Sie unter [Zuweisen sequenzieller Elastic-IP-Adressen aus einem IPAM-Pool](#) im Benutzerhandbuch zu Amazon VPC IPAM.

IPv6 Adressen

Mit dem weiteren Wachstum des Internets steigt auch der Bedarf an IP-Adressen. Das gängigste Format für IP-Adressen ist IPv4. Das neue Format für IP-Adressen ist IPv6, welches einen größeren Adressraum bietet als IPv4. IPv6 behebt das Problem der IPv4 Adressüberlastung und ermöglicht es Ihnen, mehr Geräte mit dem Internet zu verbinden. Die Umstellung erfolgt schrittweise, aber mit zunehmender IPv6 Akzeptanz können Sie Ihre Netzwerke vereinfachen und IPv6 erweiterte Funktionen für bessere Konnektivität, Leistung und Sicherheit nutzen.

Viele AWS Dienste, wie Amazon EC2, Amazon S3 und Amazon CloudFront, bieten entweder Dual-Stack-Support (IPv4 und IPv6) oder IPv6 Nur-Unterstützung, sodass Ressourcen IPv6 Adressen zugewiesen und über IPv6 das Protokoll abgerufen werden können. Dies vereinfacht die Netzwerkkonfiguration und -verwaltung für Kunden, die dies nutzen. IPv6 Andere Dienste bieten eingeschränkten oder teilweisen Dual-Stack-and-Support. IPv6

Weitere Informationen zu Diensten, die diese Unterstützung IPv6 bieten, finden Sie unter. [AWS Dienste, die unterstützen IPv6](#)

Beachten Sie, dass einige IPv6 Adressen von der Internet Engineering Task Force reserviert sind. Weitere Informationen zu reservierten IPv6 Adressbereichen finden Sie unter [IANA IPv6 Special-Purpose Address](#) Registry und. [RFC4291](#)

Note

Sowohl öffentliche als auch private IPv6 Adressierung sind in verfügbar. AWS definiert öffentliche IP-Adressen als solche, von denen aus im Internet Werbung gemacht wird AWS, wohingegen private IP-Adressen nicht im Internet beworben werden und können. AWS

Inhalt

- [Öffentliche Adressen IPv6](#)
- [Private Adressen IPv6](#)

Öffentliche Adressen IPv6

Von Amazon bereitgestellte IPv6 Adressen werden immer im Internet beworben. Sie sind global eindeutig und daher über das Internet erreichbar. Sie können kontrollieren, ob Ressourcen wie EC2 Instances über ihre IPv6 Adressen erreichbar sind, indem Sie das Routing für Ihre Subnetze steuern oder Sicherheitsgruppen und Netzwerke verwenden. ACLs

Dies sind einige der Möglichkeiten, wie Sie sich darauf vorbereiten können, öffentliche IPv6 Adressen für Ihre Workloads zu verwenden:

- Erstellen Sie ein IPAM mit Amazon VPC IP Address Manager und stellen Sie einen öffentlichen Adressbereich von Amazon für einen IPv6 IPAM-Adresspool bereit. Weitere Informationen finden Sie unter [Create IPv6 Pools](#) im Amazon VPC IPAM-Benutzerhandbuch.
- Wenn Sie über ein IPAM verfügen und einen öffentlichen IPv6 Adressbereich besitzen, stellen Sie einen Teil oder den gesamten öffentlichen IPv6 Adressbereich auf IPAM um und stellen Sie den öffentlichen IPv6 Adressbereich einem IPAM-Adresspool zur Verfügung. Weitere Informationen finden Sie unter [Tutorial: Mitbringen eigener IP-Adressen in IPAM](#) im Amazon-VPC-IPAM-Benutzerhandbuch.
- Wenn Sie kein IPAM haben, aber einen öffentlichen IPv6 Adressbereich besitzen, bringen Sie einen Teil oder den gesamten öffentlichen IPv6 Adressbereich zu. AWS Weitere Informationen finden Sie unter [Bringen Sie Ihre eigenen IP-Adressen \(BYOIP\) zu Amazon EC2 im EC2 Amazon-Benutzerhandbuch](#).

Wenn Sie bereit sind, öffentliche IPv6 Adressen zu verwenden, können Sie Instances öffentliche IPv6 Adressen zuweisen (siehe [IPv6 Adressen](#) im EC2 Amazon-Benutzerhandbuch), Sie können Ihrer VPC einen öffentlichen IPv6 CIDR-Block zuweisen (siehe [Hinzufügen oder Entfernen eines IPv4-CIDR-Blocks zu bzw. aus Ihrer VPC](#)) und den IPv6 CIDR-Block Ihren Subnetzen zuordnen (siehe). [Ändern der IP-Adressierungsattribute Ihres Subnetzes](#)

Private Adressen IPv6

IPv6 Privatadressen sind IPv6 Adressen, die nicht beworben werden und von denen aus im Internet auch nicht beworben werden kann. AWS

Sie können eine private IPv6 Adresse verwenden, wenn Sie möchten, dass Ihre privaten Netzwerke dies unterstützen IPv6 und Sie nicht beabsichtigen, den Datenverkehr von diesen Adressen ins Internet weiterzuleiten. Wenn Sie von einer Ressource mit einer privaten IPv6 Adresse aus eine Verbindung mit dem Internet herstellen möchten, können Sie dies tun, aber Sie müssen den Datenverkehr dazu über eine Ressource in einem anderen Subnetz mit einer öffentlichen IPv6 Adresse weiterleiten.

Es gibt zwei Arten von privaten IPv6 Adressen:

- IPv6 ULA-Bereiche: IPv6 Adressen wie in definiert [RFC4193](#). Diese Adressbereiche beginnen immer mit „fc“ oder „fd“, wodurch sie leicht identifizierbar sind. Gültiger IPv6 ULA-Speicherplatz ist alles unter fd00: :/8, das sich nicht mit dem von Amazon reservierten Bereich fd00: :/16 überschneidet.
- IPv6 GUA-Bereiche: Adressen wie in definiert. IPv6 [RFC3587](#) Die Option, IPv6 GUA-Bereiche als private IPv6 Adressen zu verwenden, ist standardmäßig deaktiviert und muss aktiviert werden, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter [Enable Provisioning private IPv6 GUA CIDRs](#) im Amazon VPC IPAM-Benutzerhandbuch.

Beachten Sie Folgendes:

- Private IPv6 Adressen sind nur über [Amazon VPC IP Address Manager \(IPAM\)](#) verfügbar. IPAM erkennt Ressourcen mit IPv6 ULA- und GUA-Adressen und überwacht Pools auf sich überschneidende IPv6 ULA- und GUA-Adressräume.
- Wenn Sie private IPv6 GUA-Bereiche verwenden, setzen wir voraus, dass Sie IPv6 GUA-Bereiche verwenden, die Ihnen gehören.
- Private IPv6 Adressen werden und können nicht im Internet von AWS beworben werden. AWS erlaubt keinen direkten Ausgang in das öffentliche Internet von einem privaten IPv6 Bereich aus,

selbst wenn in der VPC ein Internet-Gateway oder ein Internet-Gateway nur für ausgehenden Datenverkehr vorhanden ist. Private IPv6 Adressen werden am Rand des Internet-Gateways automatisch gelöscht, um sicherzustellen, dass sie nicht öffentlich weitergeleitet werden.

- AWS reserviert die ersten 4 privaten IPv6 Subnetzadressen und die letzte.
- Gültige Bereiche für private IPv6 ULA sind /9 bis /60, beginnend mit fd80: :/9.
- Wenn Sie einer VPC einen privaten IPv6 GUA-Bereich zugewiesen haben, können Sie keinen öffentlichen IPv6 GUA-Bereich verwenden, der sich mit dem privaten IPv6 GUA-Bereich in derselben VPC überschneidet.
- Die Kommunikation zwischen Ressourcen mit privaten IPv6 ULA- und GUA-Adressbereichen wird unterstützt (z. B. über Direct Connect-, VPC-Peering-, Transit-Gateway- oder VPN-Verbindungen).
- [Sie können private IPv6 Adressen mit IPv6 Nur-VPC-Subnetzen und Dual-Stack-VPC-Subnetzen, Elastic Load Balancern und Endpunkten verwenden.](#) [AWS Global Accelerator](#)
- Für private Adressen fallen keine Gebühren an. IPv6

Dies sind einige der Möglichkeiten, wie Sie sich darauf vorbereiten können, private IPv6 Adressen für Ihre Workloads zu verwenden:

- Erstellen Sie ein IPAM mit Amazon VPC IP Address Manager und stellen Sie einen privaten IPv6 ULA-Bereich für einen IPAM-Adresspool bereit. Weitere Informationen finden Sie unter [Create IPv6 Pools](#) im Amazon VPC IPAM-Benutzerhandbuch.
- Erstellen Sie ein IPAM mit Amazon VPC IP Address Manager und stellen Sie einen privaten IPv6 GUA-Bereich für einen IPAM-Adresspool bereit. Die Option, IPv6 GUA-Bereiche als private IPv6 Adressen zu verwenden, ist standardmäßig deaktiviert und muss auf Ihrem IPAM aktiviert werden, bevor Sie sie verwenden können. Weitere Informationen finden Sie unter [Enable Provisioning private IPv6 GUA CIDRs](#) im Amazon VPC IPAM-Benutzerhandbuch.

Wenn Sie bereit sind, private IPv6 Adressen zu verwenden, können Sie Ihrer VPC einen privaten IPv6 CIDR-Block aus einem IPAM-Pool zuweisen (siehe [Hinzufügen oder Entfernen eines IPv4-CIDR-Blocks zu bzw. aus Ihrer VPC](#)) und den IPv6 CIDR-Block Ihren Subnetzen zuordnen (siehe). [Ändern der IP-Adressierungsattribute Ihres Subnetzes](#)

Verwenden Sie Ihre eigenen IP-Adressen

Sie können Ihren eigenen öffentlichen IPv4 Adressbereich oder Adressbereich ganz oder teilweise in Ihr Konto übernehmen. IPv6 AWS Der Adressbereich gehört weiterhin Ihnen, wird jedoch von

AWS standardmäßig im Internet veröffentlicht. Nachdem Sie den Adressbereich hinzugefügt 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 EC2 Amazon-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 IP-Adressen CIDRs anhand bestimmter Geschäftsregeln zuzuweisen. VPCs

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. Eine VPC muss über einen zugehörigen IPv4 CIDR-Block verfügen. 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](#)
- [IPv4 CIDR-Blöcke für eine VPC verwalten](#)
- [IPv4 Einschränkungen der CIDR-Blockzuweisung](#)
- [IPv6 VPC CIDR-Blöcke](#)

IPv4 VPC CIDR-Blöcke

Wenn Sie eine VPC erstellen, 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 der VPC weitere IPv4 CIDR-Blöcke zuordnen. Weitere Informationen finden Sie unter [Hinzufügen oder Entfernen eines IPv4-CIDR-Blocks zu bzw. aus Ihrer VPC](#).

Wenn Sie eine VPC erstellen, empfehlen wir, einen CIDR-Block aus den privaten IPv4 Adressbereichen gemäß [RFC 1918](#) anzugeben.

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

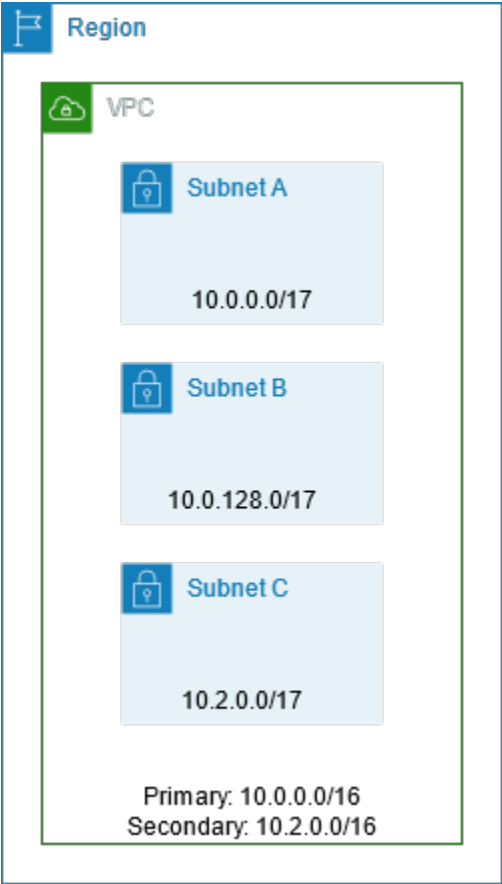
Überlegungen

- Sie können die folgenden CIDR-Blöcke nicht für Ihren angeben: VPCs
 - 0.0.0.0/8
 - 127.0.0.0/8 (interner Host-Loopback-Adressbereich)
 - 169.254.0.0/16 ([Link-lokaler Adressbereich](#))
 - 224.0.0.0/4 (Multicast-Adressbereich)
- Wenn Sie eine VPC für die Verwendung mit einem AWS Service erstellen, überprüfen Sie in der Servicedokumentation, ob bestimmte Anforderungen für die Konfiguration gelten.
- Einige AWS Dienste verwenden den 172.17.0.0/16 CIDR-Bereich. Bei Services können IP-Adresskonflikte auftreten, wenn der IP-Adressbereich bereits in Ihrem Netzwerk verwendet wird. Zum Beispiel AWS Cloud9 und Amazon SageMaker AI verwenden 172.17.0.0/16. Um zukünftige Konflikte zu vermeiden, verwenden Sie nicht diesen Bereich beim Erstellen Ihrer VPC. Weitere Informationen finden Sie im AWS Cloud9 Benutzerhandbuch unter [Es kann keine Verbindung zur EC2 Umgebung hergestellt werden, da die IP-Adressen der VPC von Docker verwendet werden](#).
- Sie können eine VPC mit einem öffentlich routbaren CIDR-Block erstellen, der außerhalb der in RFC 1918 angegebenen privaten IPv4 Adressbereiche liegt. Für die Zwecke dieser Dokumentation bezeichnen wir private IP-Adressen jedoch als Adressen, die IPv4 sich innerhalb des CIDR-Bereichs Ihrer VPC befinden.
- Wenn Sie eine VPC mit einem Befehlszeilentool oder der EC2 Amazon-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.

IPv4 CIDR-Blöcke für eine VPC verwalten

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
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 hinsichtlich der IPv4 Adressbereiche, die Sie verwenden können. Weitere Informationen finden Sie unter [IPv4 Einschränkungen der CIDR-Blockzuweisung](#).
- 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.
- Die folgenden Regeln gelten, wenn Sie IPv4 CIDR-Blöcke zu einer VPC hinzufügen, die Teil einer VPC-Peering-Verbindung ist:
 - 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 VPCs über ein Direct Connect-Gateway eine Verbindung Direct Connect zu mehreren Connect, dürfen VPCs die mit dem Direct Connect-Gateway verknüpften Verbindungen keine

überlappenden CIDR-Blöcke haben. Wenn Sie einen CIDR-Block zu einem der Blöcke hinzufügen VPCs , die dem Direct Connect-Gateway zugeordnet sind, stellen Sie sicher, dass sich der neue CIDR-Block nicht mit einem vorhandenen CIDR-Block einer anderen zugehörigen VPC überschneidet. Weitere Informationen finden Sie unter [Direct Connect-Gateways](#) im 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 den primären CIDR für Ihre VPC in der Amazon VPC-Konsole anzuzeigen, wählen Sie Ihr VPCs, aktivieren Sie das Kontrollkästchen für Ihre VPC und wählen Sie die Registerkarte. CIDRs [Um den primären 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
```

IPv4 Einschränkungen der CIDR-Blockzuweisung

Die folgende Tabelle gibt einen Überblick über zulässige und eingeschränkte VPC-CIDR-Blockzuordnungen für bestehende VPC-CIDR-Blöcke. 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

Bestehender Adressbereich IPv4	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 nicht zugewiesen werden. VPCs	
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.

Bestehender Adressbereich IPv4	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 einer /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 einer /28-Netzmaske oder ein CIDR-Block aus dem 100.64.0.0/10-Bereich zwischen einer /16-Netzmaske und einer /28-Netzmaske.

Bestehender Adressbereich IPv4	Beschränkte Verknüpfungen	Zugelassene Verknüpfungen
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. Sie können auch CIDR in einem der RFC-1918-Bereiche zuordnen. Dazu müssen Sie jedoch zuerst dieses CIDR ergänzen, wenn Sie die VPC erstellen, und dann Nicht-RFC-1918-CIDR ergänzen.

* IPv4 RFC 1918-Bereiche sind [dieser](#) privaten Adressbereiche, die in RFC 1918 spezifiziert 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 zuordnen. /4 Sie können einen IPv6 CIDR-Block aus dem Adresspool von Amazon anfordern. IPv6 Weitere Informationen finden Sie unter [Hinzufügen oder Entfernen eines IPv4-CIDR-Blocks zu bzw. aus Ihrer VPC](#).

Wenn Sie Ihrer VPC einen IPv6 CIDR-Block zugeordnet haben, können Sie einen IPv6 CIDR-Block einem vorhandenen Subnetz in Ihrer VPC oder beim Erstellen eines neuen Subnetzes zuordnen. Weitere Informationen finden Sie unter [the section called "Größe des Subnetzes für IPv6"](#).

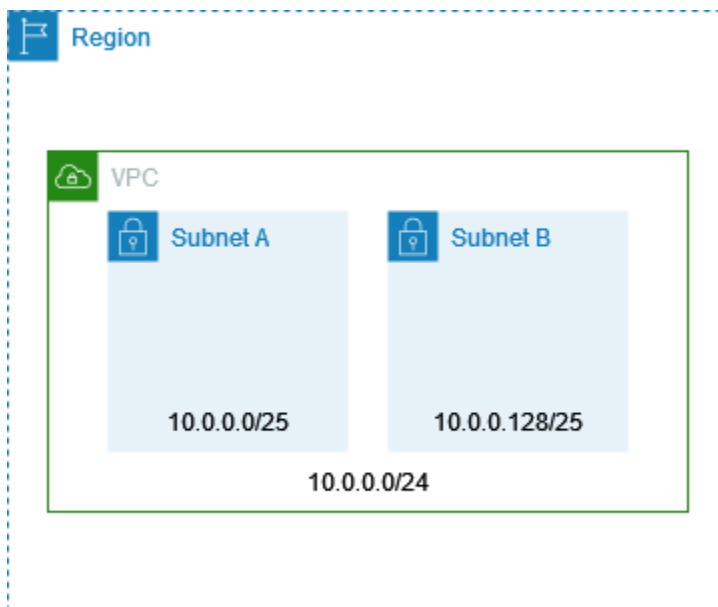
Sie erstellen beispielsweise eine VPC und geben an, dass Sie der VPC einen von Amazon bereitgestellten IPv6 CIDR-Block zuordnen möchten. Amazon weist Ihrer VPC den folgenden IPv6 CIDR-Block zu: 2001:db8:1234:1a00::/56 Sie können den Bereich der IP-Adressen nicht selbst auswählen. Sie können ein Subnetz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

Sie können einen IPv6 CIDR-Block von einer VPC trennen. Nachdem Sie einen IPv6 CIDR-Block von einer VPC getrennt haben, können Sie nicht erwarten, denselben CIDR zu erhalten, wenn Sie Ihrer VPC später erneut einen IPv6 CIDR-Block zuordnen.

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, die Ihnen bei der Berechnung und Erstellung IPv4 von CIDR-Blöcken sowie bei der IPv6 Subnetzerstellung helfen. Sie können Tools finden, die Ihren Bedürfnissen entsprechen, indem Sie nach Begriffen wie „Subnetzrechner“ oder „CIDR-Rechner“ suchen. Ihre Netzwerktechnikgruppe kann Ihnen auch dabei helfen, die CIDR-Blöcke IPv4 und die IPv6 CIDR-Blöcke zu bestimmen, die Sie für Ihre Subnetze angeben müssen.

Größe der Subnetze für IPv4

Die zulässige IPv4 CIDR-Blockgröße für ein Subnetz liegt zwischen einer Netzmaske und einer /28 Netzmaske. /16 Die ersten vier IP-Adressen und die letzte IP-Adresse in jedem CIDR-Block des Subnetzes stehen Ihnen nicht zur Verfügung und können keiner Ressource, z. B. einer Instanz, zugewiesen werden. EC2 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. VPCs Bei 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 Befehlszeilentool oder der EC2 Amazon-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 mit [BYOIP](#) einen IPv4 Adressbereich einrichten, können Sie alle IP-Adressen im Bereich verwenden, einschließlich der ersten Adresse (der Netzwerkadresse) und der letzten Adresse (der Broadcast-Adresse).

Größe des Subnetzes für IPv6

Wenn Sie Ihrer VPC einen IPv6 CIDR-Block zugeordnet haben, können Sie einen IPv6 CIDR-Block einem vorhandenen Subnetz in Ihrer VPC zuordnen oder wenn Sie ein neues Subnetz erstellen. Mögliche IPv6 Netzmaskenlängen liegen zwischen und in Schritten von. /44 /64 /4

Im Internet stehen Tools zur Verfügung, mit denen Sie CIDR-Blöcke für IPv6 Subnetze berechnen und erstellen können. Sie können Tools finden, die Ihren Anforderungen entsprechen, indem Sie nach Begriffen wie „IPv6Subnetzrechner“ oder „CIDR-Rechner“ suchen. IPv6 Ihre Netzwerktechnikgruppe kann Ihnen auch dabei helfen, die IPv6 CIDR-Blöcke zu ermitteln, die Sie für Ihre Subnetze angeben müssen.

Die ersten vier IPv6 Adressen und die letzte IPv6 Adresse in jedem CIDR-Block des Subnetzes stehen Ihnen nicht zur Verfügung und können keiner Instanz zugewiesen werden. EC2 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 Bereich `FE80::/10`, die mit EUI-64 generiert wurde. Weitere Informationen zu Link-lokalen Adressen finden Sie unter [Link-lokale Adresse](#).
- Die verknüpfungslokale IPv6 Adresse `FE80::ec2::1`.

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

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-Services, die eine Dual-Stack-Konfiguration (IPv4 und IPv6) und reine IPv6-Konfigurationen unterstützen, finden Sie unter [Dienste, die unterstützen IPv6](#).

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.

Merkmal	IPv4	IPv6
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 für Ihre VPC einen eigenen IPv6-CIDR-Block für AWS verwenden, einen von Amazon bereitgestellten IPv6-CIDR-Block 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.
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 öffentliche IPv4-Adresse.	Nicht unterstützt EIPs halten die öffentliche IPv4-Adresse einer Instance bei deren Neustart statisch. IPv6-Adressen sind standardmäßig statisch.
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.

Merkmal	IPv4	IPv6
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.

Konsolidierung und Verwaltung von Netzwerk-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. Mithilfe von Resource Access Manager (RAM) können Sie verwaltete Präfixlisten auch mit anderen AWS Konten verwenden.

Es gibt zwei Arten von Präfixlisten:

- Vom Kunden verwaltete Präfixlisten – Sätze von IP-Adressbereichen, die Sie definieren und verwalten. Sie können Ihre Präfixliste mit anderen AWS Konten teilen, sodass diese Konten in ihren eigenen Ressourcen auf die Präfixliste verweisen können.
- AWS-verwaltete Präfixlisten — Gruppen von IP-Adressbereichen für AWS Dienste. Sie können eine von AWS verwaltete Präfixliste nicht erstellen, ändern, freigeben oder löschen.

Inhalt

- [Konzepte und Regeln für Präfixlisten](#)
- [Identitäts- und Zugriffsverwaltung für Präfixlisten](#)
- [Vom Kunden verwaltete Präfixlisten](#)

- [AWS Von verwaltete Präfixlisten](#)
- [Optimieren Sie das AWS Infrastrukturmanagement mit Präfixlisten](#)

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 Typ der IP-Adressierung (IPv4 oder IPv6). Sie können IPv6 CIDR-Blöcke nicht in einer einzigen Präfixliste kombinieren IPv4 .
- 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 für 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](#).
- Von Kunden verwaltete Präfixlisten sind in allen [AWS Handelsregionen](#) (einschließlich Regionen GovCloud (USA) und China) verfügbar.

AWS Von verwaltete Präfixlisten

Die folgenden Regeln gelten für Präfixlisten, die AWS-verwaltet werden:

- Sie können eine Liste mit AWS verwalteten Präfixen nicht erstellen, ändern, teilen oder löschen.
- Unterschiedlich AWS verwaltete Präfixlisten haben eine unterschiedliche Gewichtung, wenn Sie sie verwenden. Weitere Informationen finden Sie unter [Von AWS verwaltete Präfixlistengewicht](#).
- Sie können die Versionsnummer einer Liste mit AWS verwalteten Präfixen 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 sowie der Ressourcen und Bedingungsschlüssel, die Sie in einer IAM-Richtlinie verwenden können, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon EC2](#) in der Service Authorization Reference.

Mit der folgenden Beispielrichtlinie können Benutzer nur die Präfixliste p1-123456abcde123456 anzeigen und mit ihr arbeiten. Benutzer können keine Präfixlisten erstellen oder löschen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:GetManagedPrefixListAssociations",
        "ec2:GetManagedPrefixListEntries",
        "ec2:ModifyManagedPrefixList",
        "ec2:RestoreManagedPrefixListVersion"
      ],
      "Resource": "arn:aws:ec2:us-east-1:123456789012:prefix-
list/p1-123456abcde123456"
    },
    {
      "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](#).

Vom Kunden verwaltete Präfixlisten

Mit von Kunden verwalteten Präfixlisten können Sie Ihre eigenen Gruppen von IP-Adressbereichen, sogenannten Präfixen, in AWS definieren und verwalten. Anstatt diese IP-Adressen in Ihren verschiedenen Ressourcen fest zu kodieren, können Sie eine zentrale Präfixliste erstellen und bei Bedarf darauf verweisen. Dies vereinfacht nicht nur die Verwaltung Ihrer IP-Adressen, sondern fördert auch die Konsistenz und Wiederverwendbarkeit in Ihrer gesamten AWS Landschaft.

Eines der herausragenden Merkmale von kundenverwalteten Präfixlisten ist die Möglichkeit, sie mit anderen Konten zu teilen. AWS Indem Sie Zugriff auf Ihre Präfixlisten gewähren, können Sie es anderen Teams oder Organisationen ermöglichen, Ihre definierten IP-Adressbereiche in ihren eigenen Ressourcen zu nutzen. Dieser kollaborative Ansatz fördert ein einheitlicheres und effizienteres Cloud-Erlebnis, bei dem die IP-Adressverwaltung freigegeben und synchronisiert wird.

In den folgenden Abschnitten werden wir uns eingehender mit den praktischen Aspekten der Arbeit mit von Kunden verwalteten Präfixlisten befassen, einschließlich step-by-step Anleitungen zur Erstellung, Verwaltung und Weitergabe Ihrer IP-Adressbereiche.

Note

Sie können die Verwaltung von Präfixlisten mithilfe von Amazon VPC IPAM automatisieren, um die automatische Synchronisierung auf der CIDRs Grundlage von von Ihnen definierter Regeln durchzuführen. Dadurch entfallen manuelle Aktualisierungen bei Änderungen Ihrer Infrastruktur. Weitere Informationen finden Sie unter [Automatisieren der Aktualisierungen von Präfixlisten mit IPAM](#) im Amazon-VPC-IPAM-Benutzerhandbuch.

Aufgaben

- [Arbeiten mit vom Kunden verwalteten Präfixlisten](#)

Arbeiten mit vom Kunden verwalteten Präfixlisten

In diesem Abschnitt wird beschrieben, wie Sie mit von Kunden verwalteten Präfixlisten arbeiten.

Inhalt

- [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](#)
- [Freigeben von vom Kunden verwalteten Präfixlisten](#)

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 für die Adressfamilie aus, ob die Präfixliste OR-Einträge unterstützt IPv4 . IPv6
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).

Um eine Präfixliste mit dem zu erstellen AWS CLI

Verwenden Sie den Befehl [create-managed-prefix-list](#).

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 AWSdie Besitzer-ID.

Um Präfixlisten anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den Befehl [describe-managed-prefix-lists](#).

Anzeigen der Einträge für eine Präfixliste

Sie können die Einträge für Ihre Präfixlisten, Präfixlisten, die mit Ihnen geteilt wurden, und AWS verwaltete 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.

Um die Einträge für eine Präfixliste anzuzeigen, verwenden Sie AWS CLI

Verwenden Sie den Befehl [get-managed-prefix-list-entries](#).

Anzeigen von Zuordnungen (Referenzen) für Ihre Präfixliste

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

Einschränkung

Sie können die zugehörigen Ressourcen für eine von AWS-verwaltete Präfixliste nicht 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.

Um Zuordnungen von Präfixlisten anzuzeigen, verwenden Sie den 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. Wenn die verwaltete Präfixliste als Resolver-Ziel für die IPAM-Präfixliste konfiguriert wurde, wird eine Option zur Synchronisation des IPAM-Präfixlisten-Resolvers dargestellt.

Wählen Sie aus, ob die Synchronisation mit IPAM-Präfixlisten-Resolver aktiviert oder deaktiviert werden soll. Wenn diese Option aktiviert ist, wird die Präfixliste CIDRs automatisch auf der Grundlage der CIDR-Auswahlregeln des zugehörigen Resolvers aktualisiert. Wenn diese Option deaktiviert ist, wird die Präfixliste CIDRs nicht automatisch aktualisiert. Weitere Informationen über dieses Feature finden Sie unter [Automatisieren der Aktualisierungen von Präfixlisten mit IPAM](#) im Amazon-VPC-IPAM-Benutzerhandbuch.

6. 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.
7. Wählen Sie Save prefix list (Präfixliste speichern).

Um eine Präfixliste mit dem zu ändern AWS CLI

Verwenden Sie den Befehl [modify-managed-prefix-list](#).

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.

Um die Größe einer Präfixliste zu ändern, verwenden Sie AWS CLI

Verwenden Sie den Befehl [modify-managed-prefix-list](#).

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).

Um eine frühere Version einer Präfixliste wiederherzustellen, verwenden Sie 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).

Um eine Präfixliste mit dem zu löschen AWS CLI

Verwenden Sie den Befehl [delete-managed-prefix-list](#).

Freigeben von vom Kunden verwalteten Präfixlisten

Mit AWS Resource Access Manager (AWS RAM) kann der Besitzer einer vom Kunden verwalteten Präfixliste die Präfixliste mit folgenden Personen teilen:

- Bestimmte AWS Konten innerhalb oder außerhalb der Organisation in AWS Organizations
- Eine Organisationseinheit innerhalb ihrer Organisation in AWS Organizations
- Eine ganze Organisation in AWS Organizations

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

Weitere Informationen zu AWS RAM finden Sie im [AWS RAM Benutzerhandbuch](#). Weitere Informationen zu Kontingenten finden Sie unter [Servicekontingenten](#) im AWS RAM Benutzerhandbuch.

 Important

Für die Freigabe von Präfixlisten fallen keine zusätzlichen Gebühren an.

Inhalt

- [Berechtigungen für freigegebene Präfixlisten](#)

- [Arbeiten mit freigegebenen Präfixlisten](#)

Berechtigungen für freigegebene Präfixlisten

Berechtigungen für Besitzer

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

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

Berechtigungen für Konsumenten

Verbraucher können die Einträge in einer gemeinsamen Präfixliste einsehen und in ihren AWS Ressourcen auf eine gemeinsame Präfixliste verweisen. Konsumenten können jedoch eine freigegebene Präfixliste nicht ändern, wiederherstellen oder löschen.

Arbeiten mit freigegebenen Präfixlisten

AWS Präfixlisten bieten eine bequeme Möglichkeit, die von verschiedenen AWS Diensten verwendeten IP-Adressbereiche zu verwalten und zu referenzieren. Zusätzlich zu den von AWS-verwalteten Präfixlisten können Sie auch Ihre eigenen, vom Kunden verwalteten Präfixlisten erstellen und mit anderen AWS Konten teilen.

Die gemeinsame Nutzung von Präfixlisten kann besonders für Unternehmen mit komplexen Netzwerkanforderungen oder für Unternehmen nützlich sein, die die Nutzung von IP-Adressen über mehrere AWS Workloads hinweg koordinieren müssen. Durch die Freigabe einer Präfixliste können Sie eine konsistente IP-Adressverwaltung sicherstellen und die Netzwerkkonfigurationen für Ihre Mitarbeiter vereinfachen.

In diesem Abschnitt wird beschrieben, wie Sie Präfixlisten freigeben und wie Sie Präfixlisten identifizieren und verwenden, die für Ihr Konto freigegeben wurden.

Inhalt

- [Teilen einer Präfixliste](#)
- [Aufheben der Freigabe einer freigegebenen Präfixliste](#)
- [Identifizieren einer freigegebenen Präfixliste](#)

- [Identifizieren von Verweisen auf eine freigegebene Präfixliste](#)

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 sind und die gemeinsame Nutzung innerhalb Ihrer Organisation aktiviert ist, erhalten Verbraucher in Ihrer Organisation automatisch Zugriff auf die gemeinsame Präfixliste. AWS Organizations 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.

Important

- 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 teilen.
- 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.

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.

Um eine Präfixliste, die Sie besitzen, mit dem AWS CLI

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

- [create-resource-share](#)
- [associate-resource-share](#)
- [update-resource-share](#)

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 gemeinsame Nutzung einer gemeinsamen Präfixliste, deren Eigentümer Sie sind, rückgängig zu machen, müssen Sie sie mithilfe AWS RAM von aus der Ressourcenfreigabe entfernen.

Um die gemeinsame Nutzung einer gemeinsamen Präfixliste, deren Eigentümer Sie sind, mithilfe der Konsole rückgängig zu machen AWS RAM

Siehe [Aktualisieren einer Ressourcenfreigabe](#) im AWS RAM -Benutzerhandbuch.

Um die gemeinsame Nutzung einer gemeinsamen Präfixliste, die Sie besitzen, rückgängig zu machen, verwenden Sie die AWS CLI

Verwenden Sie den Befehl [disassociate-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) .

Um eine gemeinsam genutzte Präfixliste zu identifizieren, verwenden Sie den AWS CLI

Verwenden Sie den Befehl [describe-managed-prefix-lists](#). Der Befehl gibt die Präfixlisten zurück, die Sie besitzen, und die Präfixlisten, die mit Ihnen geteilt wurden. 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 Ressourcen, die auf die Präfixliste verweisen, sind in der Spalte Ressourcen-ID aufgeführt. Die Besitzer der Ressourcen werden in der Spalte Resource Owner (Ressourcenbesitzer) aufgeführt.

Um Verweise auf eine gemeinsam genutzte Präfixliste zu identifizieren, verwenden Sie den AWS CLI

Verwenden Sie den Befehl [get-managed-prefix-list-associations](#).

AWS Von verwaltete Präfixlisten

AWS-verwaltete Präfixlisten sind Gruppen von IP-Adressbereichen für AWS Dienste. Diese Präfixlisten werden von Amazon Web Services verwaltet und bieten eine Möglichkeit, auf die IP-Adressen zu verweisen, die von verschiedenen AWS Angeboten verwendet werden. Das kann besonders nützlich sein, wenn Sicherheitsgruppen oder andere Kontrollen auf Netzwerkebene innerhalb einer VPC konfiguriert werden.

Die Präfixlisten decken eine Vielzahl von AWS Diensten ab, darunter S3 und DynamoDB und viele andere. Mithilfe der verwalteten Präfixlisten können Sie sicherstellen, dass Ihre Netzwerkconfigurationen die IP-Adressen, die von den AWS Diensten, auf die Sie angewiesen sind up-to-date, verwendet werden, korrekt berücksichtigen. Dies kann dazu beitragen, Netzerkennungsaufgaben zu vereinfachen und den Verwaltungsaufwand für die manuelle Verwaltung von IP-Adresslisten zu verringern.

Neben den praktischen Vorteilen entspricht die Verwendung der verwalteten Präfixlisten auch den bewährten AWS Sicherheitsmethoden. Indem Sie sich auf die verlässlichen IP-Adressinformationen von verlassen AWS, können Sie das Risiko einer Fehlkonfiguration oder unerwarteter Verbindungsprobleme minimieren. Dies kann besonders für geschäftskritische Anwendungen oder Workloads mit strengen Compliance-Anforderungen wichtig sein.

Inhalt

- [Verfügbare verwaltete AWS Präfixlisten](#)
- [Von AWS verwaltete Präfixlistengewicht](#)
- [Verwenden Sie eine von AWS-verwaltete Präfixliste](#)

Verfügbare verwaltete AWS Präfixlisten

Die folgenden Dienste stellen AWS verwaltete Präfixlisten bereit.

AWS-Service	Name der Präfixliste	Gewicht
Amazon CloudFront	com.amazonaws.global.cloudfront.origin-facing () IPv4	55
	com.amazonaws.global.ipv6.cloudfront.origin-facing () IPv6	
Amazon DynamoDB	com.amazonaws. <i>region</i> .dynamodb	1
Amazon EC2 Instance Connect	com.amazonaws. <i>region</i> .ec2-instanzenverbindung	2
	com.amazonaws. <i>region</i> .ipv6.ec2-instanzenverbindung	2

AWS-Service	Name der Präfixliste	Gewicht
AWS Ground Station	com.amazonaws.global.groundstation	5
Amazon Route 53	com.amazonaws. <i>region</i> .ipv6.route53 - Gesundheitschecks	25
	com.amazonaws. <i>region</i> .route53 - Gesundheitschecks	25
Amazon S3	com.amazonaws. <i>region</i> . 3	1
Amazon S3 Express One Zone	com.amazonaws. <i>region</i> .s3 Express	6
Amazon VPC Lattice	com.amazonaws. <i>region</i> .vpc-Gitter	10
	com.amazonaws. <i>region</i> .ipv6.vpc-Gitter	10

Um die von -verwalteten Präfixlisten mit der Konsole anzuzeigen AWS

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.

Um die mit AWS-verwalteten Präfixlisten anzuzeigen, verwenden Sie die AWS CLI

Verwenden Sie den [describe-managed-prefix-lists](#)-Befehl wie folgt:

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

Von AWS verwaltete Präfixlistengewicht

Die Gewichtung einer mit AWS-verwalteten Präfixlisten bezieht sich auf die Anzahl der Einträge, die sie in einer Ressource einnimmt.

Das Gewicht 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.

Verwenden Sie eine von AWS-verwaltete Präfixliste

AWS-verwaltete Präfixlisten werden von jedem Benutzer mit einem AWS Konto erstellt und verwaltet und können von jedem verwendet werden. AWS Sie können eine Liste mit AWS verwalteten Präfixen nicht erstellen, ändern, teilen oder löschen.

Wie bei kundenverwalteten Präfixlisten können Sie AWS-verwaltete Präfixlisten für AWS Ressourcen wie Sicherheitsgruppen und Routing-Tabellen verwenden. Weitere Informationen finden Sie unter [Optimieren Sie das AWS Infrastrukturmanagement mit Präfixlisten](#).

Optimieren Sie das AWS Infrastrukturmanagement mit Präfixlisten

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

Ressourcen

- [VPC-Sicherheitsgruppen](#)
- [Subnetz-Routingtabellen](#)
- [Transit-Gateway-Routing-Tabellen](#)
- [AWS Network Firewall Regelgruppen](#)
- [Netzwerkzugriffskontrolle von Amazon Managed Grafana](#)
- [AWS Outposts Lokale Gateways im Rack](#)

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](#).

 Important

Sie können eine bestehende Regel nicht ändern, um eine Präfixliste zu verwenden. Sie müssen eine neue Regel erstellen, um eine Präfixliste verwenden zu können.

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 Quelle (eingehende Regeln) oder Ziel (ausgehende Regeln) Benutzerdefiniert aus. Wählen Sie dann im nächsten Feld unter Präfixlisten die ID der Präfixliste aus.
6. Wählen Sie Regeln speichern aus.

Um auf eine Präfixliste in einer Sicherheitsgruppenregel zu verweisen, verwenden Sie den AWS CLI

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

Subnetz-Routingtabelle

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.

Um auf eine Präfixliste in einer Routentabelle zu verweisen, verwenden Sie 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 Prüfung und Bearbeitung von Netzwerkverkehr. 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.

Netzwerkzugriffskontrolle 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 Gateways im Rack

Jedes AWS Outposts Rack bietet ein lokales Gateway, über das Sie Ihre Outpost-Ressourcen mit Ihren lokalen Netzwerken verbinden können. Sie können CIDRs die häufig verwendeten Daten in einer Präfixliste gruppieren und diese Liste als Routenziel in Ihrer lokalen Gateway-Routentabelle referenzieren. Weitere Informationen finden Sie unter [Routing-Tabellen für lokale Gateways verwalten](#) im AWS Outposts -Benutzerhandbuch für Racks.

AWS-IP-Adressbereiche

AWS veröffentlicht seine aktuellen IP-Adressbereiche im JSON-Format. Mit diesen Informationen können Sie den Datenverkehr von AWS identifizieren. Sie können diese Informationen auch verwenden, um den Datenverkehr zu oder von bestimmten AWS-Services zuzulassen oder zu verweigern.

Überlegungen

- Wir veröffentlichen die IP-Adressbereiche für Services, die Kunden häufig zur Filterung ausgehender Daten verwenden. Wir veröffentlichen nicht die IP-Adressbereiche für alle Services.
- Services verwenden ihre IP-Adressbereiche, um mit anderen Services oder mit einem Kundennetzwerk zu kommunizieren.
- Die IP-Adressbereiche, die Sie über Ihre eigenen IP-Adressen zu AWS mitbringen (BYOIP), sind nicht in der `.json`-Datei enthalten. Weitere Informationen finden Sie unter [Veröffentlichen des Adressbereichs über AWS](#) im Amazon EC2-Benutzerhandbuch.

Einige Services veröffentlichen ihre Adressbereiche mithilfe von AWS-verwalteten Präfixlisten. Weitere Informationen finden Sie unter [the section called “Verfügbare verwaltete AWS Präfixlisten”](#).

Inhalt

- [Laden Sie die JSON-Datei herunter](#)
- [Kontrolle des ausgehenden Datenverkehrs](#)
- [Geolokalisierungs-Feed](#)
- [Finden der IP-Adressbereiche für AWS-Services](#)
- [Syntax für den AWS-IP-Adressbereich in der JSON-Datei](#)
- [AWSBenachrichtigungen für -IP-Adressbereiche](#)

Laden Sie die JSON-Datei herunter

Um die aktuellen Adressbereiche einzusehen, laden Sie Folgendes herunter: [ip-ranges.json](#). Um einen Verlauf zu pflegen, speichern Sie nachfolgende Versionen der JSON-Datei auf Ihrem eigenen Computer. 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.

Im Folgenden finden Sie einen curl-Beispielbefehl, mit dem die JSON-Datei im aktuellen Verzeichnis gespeichert wird.

```
curl -O https://ip-ranges.amazonaws.com/ip-ranges.json
```

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.

Informationen zum Empfangen von Benachrichtigungen über Aktualisierungen der JSON-Datei finden Sie unter [AWSBenachrichtigungen für -IP-Adressbereiche](#).

Kontrolle des ausgehenden Datenverkehrs

Damit Ressourcen, die Sie mit einem AWS-Service erstellt haben, nur auf andere AWS-Services 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-Services basieren auf EC2 und verwenden die EC2-IP-Adressumgebung. Wenn Sie den Verkehr zur EC2-IP-Adressumgebung blockieren, blockieren Sie auch den Verkehr zu diesen Nicht-EC2-Diensten.

Geolokalisierungs-Feed

Die IP-Adressbereiche in `ip-ranges.json` sind nach AWS-Region sortiert. Eine lokale Zone befindet sich jedoch nicht am gleichen physischen Standort wie ihre übergeordnete Region. Die in [geo-ip-feed.csv](#) veröffentlichten Geolokalisierungsdaten beziehen sich auf lokale Zonen. Die Daten entsprechen [RFC 8805](#).

Finden der IP-Adressbereiche für AWS-Services

Die JSON-Datei für den AWS-IP-Adressbereich, die von AWS bereitgestellt wird, kann eine wertvolle Ressource sein, um die IP-Adressen verschiedener AWS-Services zu ermitteln und diese

Informationen zur Verbesserung Ihrer Netzwerksicherheit und Zugriffskontrolle zu nutzen. Durch die Analyse der in dieser JSON-Datei enthaltenen detaillierten Daten können Sie die IP-Adressbereiche, die bestimmten AWS-Services und Regionen zugeordnet sind, genau identifizieren.

Sie können die IP-Adressbereiche beispielsweise verwenden, um robuste Netzwerksicherheitsrichtlinien zu konfigurieren und detaillierte Firewallregeln einzurichten, um den Zugriff auf bestimmte AWS-Ressourcen zuzulassen oder zu verweigern. Diese Informationen können auch für eine Vielzahl von AWS Network Firewall-Aufgaben nützlich sein. Dieses Maß an Kontrolle ist entscheidend für den Schutz Ihrer Anwendungen und Daten und stellt sicher, dass nur autorisierter Datenverkehr die erforderlichen AWS-Services erreichen kann. Zudem können Sie mit dieser IP-Intelligenz sicherstellen, dass Ihre Anwendungen für die Kommunikation mit den richtigen AWS-Endpunkten ordnungsgemäß konfiguriert sind, wodurch Zuverlässigkeit und Leistung insgesamt verbessert werden.

Die `ip-ranges.json`-Datei kann nicht nur für Firewallregeln verwendet werden, sondern auch zur Konfiguration ausgeklügelter Filter für ausgehende Daten in Ihrer Netzwerkinfrastruktur. Wenn Sie die Ziel-IP-Adressbereiche für verschiedene AWS-Services verstehen, können Sie Routing-Richtlinien einrichten oder fortschrittliche Netzwerksicherheitslösungen nutzen, um ausgehenden Datenverkehr je nach Zielort selektiv zuzulassen oder zu blockieren. Diese Kontrolle des ausgehenden Datenverkehrs ist unerlässlich, um das Risiko von Datenlecks und unbefugtem Zugriff zu minimieren.

Die `ip-ranges.json`-Datei wird regelmäßig aktualisiert. Daher ist es wichtig, eine aktuelle lokale Kopie zu führen, um sicherzustellen, dass Sie über die genauesten und aktuellsten Informationen verfügen. Durch kontinuierliche Nutzung des Inhalts dieser Datei können Sie den Netzwerkzugriff und die Sicherheit Ihrer AWS-basierten Anwendungen effizient verwalten und so Ihre allgemeine Cloud-Sicherheit stärken.

Die folgenden Beispiele können Ihnen dabei helfen, die AWS-IP-Adressbereiche genau nach Ihren Wünschen zu filtern. Unter Linux können Sie das [jq-Tool](#) herunterladen und nutzen, um eine lokale Kopie der JSON-Datei zu analysieren. Die [AWS Tools for Windows PowerShell](#) enthalten ein Cmdlet ([Get-AWSPublicIpAddressRange](#)) für die Analyse dieser JSON-Datei. Weitere Informationen finden Sie im folgenden Blog: [Abfragen der öffentlichen IP-Adressbereiche für AWS](#).

Informationen zum Abrufen der JSON-Datei finden Sie unter [the section called “Herunterladen”](#). Weitere Informationen zur Syntax der JSON-Datei finden Sie unter [the section called “Syntax”](#).

Beispiele

- [Abrufen des Erstellungsdatums der Datei](#)

- [Abrufen der IP-Adressen für eine bestimmte Region](#)
- [Abrufen aller IPv4-Adressen](#)
- [Abrufen aller IPv4-Adressen für einen bestimmten Service](#)
- [Abrufen aller IPv4-Adressen für einen bestimmten Service in einer bestimmten Region](#)
- [Abrufen aller IPv6-Adressen](#)
- [Abrufen aller IPv6-Adressen für einen bestimmten Service](#)
- [Abrufen aller IP-Adressen für eine bestimmte Grenzgruppe](#)

Abrufen des Erstellungsdatums der Datei

Im folgenden Beispiel wird das Erstellungsdatum für `ip-ranges.json` abgerufen.

jq

```
$ jq .createDate < ip-ranges.json  
  
"2024-08-01-17-22-15"
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -OutputPublicationDate  
  
Thursday, August 1, 2024 9:22:35 PM
```

Abrufen der IP-Adressen für eine bestimmte Region

Im folgenden Beispiel wird die JSON-Datei nach den IP-Adressen für die angegebene Region gefiltert.

jq

```
$ 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"
  },
  ...

```

PowerShell

```
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
...			

Abrufen aller IPv4-Adressen

Im folgenden Beispiel wird die JSON-Datei nach den IPv4-Adressen gefiltert.

jq

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

```

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

```

PowerShell

```
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  
...
```

Abrufen aller IPv4-Adressen für einen bestimmten Service

Im folgenden Beispiel wird die JSON-Datei nach den IPv4-Adressen für den angegebenen Service gefiltert.

jq

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

```
13.248.117.0/24  
15.197.34.0/23  
15.197.36.0/22  
...
```

PowerShell

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

```
IpPrefix  
-----  
13.248.117.0/24  
15.197.34.0/23  
15.197.36.0/22  
...
```

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

Im folgenden Beispiel wird die JSON-Datei nach den IPv4-Adressen für den angegebenen Service in der angegebenen Region gefiltert.

jq

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

```
13.248.124.0/24  
99.82.166.0/24  
99.82.171.0/24  
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange -Region us-east-1 -ServiceKey GLOBALACCELERATOR  
| where {$_.IpAddressFormat -eq "Ipv4"} | select IpPrefix
```

```
IpPrefix  
-----  
13.248.117.0/24  
99.82.166.0/24  
99.82.171.0/24  
...
```

Abrufen aller IPv6-Adressen

Im folgenden Beispiel wird die JSON-Datei nach den IPv6-Adressen gefiltert.

jq

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

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

PowerShell

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

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

Abrufen aller IPv6-Adressen für einen bestimmten Service

Im folgenden Beispiel wird die JSON-Datei nach den IPv6-Adressen für den angegebenen Service gefiltert.

jq

```
$ jq -r '.ipv6_prefixes[] | select(.service=="GLOBALACCELERATOR") | .ipv6_prefix' <  
ip-ranges.json
```

```
2600:1f01:4874::/47  
2600:1f01:4802::/47  
2600:1f01:4860::/47  
2600:9000:a800::/40  
...
```

PowerShell

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

```
IpPrefix  
-----  
2600:1f01:4874::/47  
2600:1f01:4802::/47  
2600:1f01:4860::/47  
2600:9000:a800::/40  
...
```


Abrufen aller IP-Adressen für eine bestimmte Grenzgruppe

Im folgenden Beispiel wird die JSON-Datei nach allen IP-Adressen für die angegebene Grenzgruppe gefiltert.

jq

```
$ jq -r '.prefixes[] | 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  
...
```

PowerShell

```
PS C:\> Get-AWSPublicIpAddressRange | where {$_.NetworkBorderGroup -eq "us-west-2-  
lax-1"} | select IpPrefix  
  
IpPrefix  
-----  
70.224.192.0/18  
52.95.230.0/24  
15.253.0.0/16  
...
```

Syntax für den AWS-IP-Adressbereich in der JSON-Datei

AWS veröffentlicht seine aktuellen IP-Adressbereiche im JSON-Format. Informationen zum Abrufen der JSON-Datei finden Sie unter [the section called “Herunterladen”](#). Die Syntax der JSON-Datei sieht wie folgt aus.

```
{  
  "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: Zeichenkette

Beispiel: "syncToken": "1416435608"

createDate

Datum und Uhrzeit der Veröffentlichung im Format JJ-MM-TT-hh-mm-ss (UTC).

Typ: Zeichenkette

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 AWS einen Präfix in spezifischeren Bereichen ankündigen kann. 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: Zeichenkette

Beispiel: "ip_prefix": "198.51.100.2/24"

ipv6_prefix

Der öffentliche IPv6-Adressbereich, in CIDR-Notation. Beachten Sie, dass AWS einen Präfix in spezifischeren Bereichen ankündigen kann.

Typ: Zeichenkette

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

network_border_group

Der Name der Netzwerkrenzgruppe, bei der es sich um einen eindeutigen Satz von Availability Zones oder Local Zones handelt, aus denen AWS IP-Adressen ankündigt, oder GLOBAL. Der Datenverkehr für GLOBAL-Services kann von mehreren (bis zu allen) Availability Zones oder Local Zones, aus denen AWS IP-Adressen ankündigt, angezogen werden oder aus diesen stammen.

Typ: Zeichenkette

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

region

Die AWS-Region oder GLOBAL. Der Datenverkehr für GLOBAL-Services kann von mehreren (bis zu allen) AWS-Regionen angezogen werden oder aus diesen stammen.

Typ: Zeichenkette

Zulässige Werte: af-south-1 | ap-east-1 | ap-east-2 | 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 | ap-southeast-5 | ap-southeast-6 | ap-southeast-7 | ca-central-1 | ca-west-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 | il-central-1 | mx-central-1 | 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

Teilmenge 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: Zeichenkette

Zulässige Werte: AMAZON | AMAZON_APPFLOW | AMAZON_CONNECT | API_GATEWAY | AURORA_DSQL | CHIME_MEETINGS | CHIME_VOICECONNECTOR | CLOUD9 | CLOUDFRONT | CLOUDFRONT_ORIGIN_FACING | CODEBUILD | DYNAMODB | EBS | EC2 | EC2_INSTANCE_CONNECT | GLOBALACCELERATOR | IVS_LOW_LATENCY | 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.

Weitere Informationen

Dieser Abschnitt enthält Links zu zusätzlichen Informationen für verschiedene Service-Codes.

- 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](#)

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_LOW_LATENCY -Servicecode wurde hinzugefügt.	29. Juli 2025
Der AURORA_DSQL -Servicecode wurde hinzugefügt.	21. Mai 2025
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

Beschreibung	Datum der Veröffentlichung
Der KINESIS_VIDEO_STREAMS -Servicecode wurde hinzugefügt.	19. November 2020
Die CHIME_MEETINGS - und CHIME_VOICECONNECTOR -Dienstcodes wurden hinzugefügt.	19. Juni 2020
Der AMAZON_APPFLOW -Servicecode wurde hinzugefügt.	9. Juni 2020
Fügen Sie Unterstützung für die Netzwerkgruppengruppe hinzu.	7. April 2020
Der WORKSPACES_GATEWAYS -Servicecode wurde hinzugefügt.	30. März 2020
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

Beschreibung	Datum der Veröffentlichung
Der S3-Servicecode wurde hinzugefügt.	28. Februar 2017
Unterstützung für IPv6-Adressbereiche hinzugefügt.	22. August 2016
Erstversion	19. November 2014

AWSBenachrichtigungen für -IP-Adressbereiche

AWS veröffentlicht seine aktuellen IP-Adressbereiche im JSON-Format. Wenn eine Änderung an den IP-Adressbereichen von AWS erfolgt, senden wir entsprechende Benachrichtigungen an die Abonnenten des Amazon SNS-Themas AmazonIpSpaceChanged. Weitere Informationen zur Syntax der JSON-Datei finden Sie unter [the section called "Syntax"](#).

Die Nutzlast der Benachrichtigung 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`. Weitere Informationen finden Sie unter [the section called “Herunterladen”](#).

Sie können Benachrichtigungen wie folgt abonnieren.

So melden Sie sich für Benachrichtigungen für AWS-IP-Adressbereiche an

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.

So melden Sie sich von den Benachrichtigungen für AWS-IP-Adressbereiche ab

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](#).

IPv6-Unterstützung für Ihre VPC

Wenn Sie über eine bestehende VPC verfügen, die nur IPv4 unterstützt, und Ressourcen in Ihrem Subnetz zur ausschließlichen Verwendung von IPv4 vorhanden sind, können Sie die Unterstützung von IPv6 für Ihre VPC und die 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”](#).
- Stellen Sie vor dem Verwenden von IPv6 sicher, dass Sie alle Funktionen der IPv6-Adressierung für eine Amazon VPC kennen: [Vergleich von IPv4 und IPv6](#).

Inhalt

- [Hinzufügen der IPv6-Unterstützung für Ihre VPC](#)
- [Beispiel für eine Dual-Stack-VPC-Konfiguration](#)

Hinzufügen der IPv6-Unterstützung für Ihre VPC

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

Inhalt

- [Schritt 1: Ordnen Sie Ihrer VPC und den Subnetzen einen IPv6-CIDR-Block zu.](#)
- [Schritt 2: Aktualisieren Sie Ihre Routing-Tabellen.](#)
- [Schritt 3: Aktualisieren Sie Ihre Sicherheitsgruppenregeln.](#)
- [Schritt 4: Ihren Instances IPv6-Adressen zuweisen](#)

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	Hinweise
Schritt 4: Ihren Instances IPv6-Adressen zuweisen	Weisen Sie aus dem IPv6-Adressbereich Ihres Subnetzes IPv6-Adressen zu Ihren Instances zu.

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 unter Netzwerkgrengruppe die Gruppe aus, aus der AWS IP-Adressen bereitstellt.
 - 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.

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.

Note

In einer Routing-Tabelle kann nicht dasselbe Ziel (`:::/0`) gleichzeitig auf ein Internet-Gateway und ein Internet-Gateway nur für ausgehenden Datenverkehr verweisen. Wenn Sie bei der Konfiguration eines Internet-Gateways nur für ausgehenden Datenverkehr die Fehlermeldung „Es gibt bereits IPv6-Routen mit dem nächsten Hop als Internet-Gateway“ erhalten, müssen Sie zuerst die bestehende IPv6-Route zum Internet-Gateway entfernen, bevor Sie die Route zum nur für ausgehenden Datenverkehr bestimmten Internet-Gateway ergänzen.

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 [Hinzufügen und Löschen von Regeln](#).

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-Typ](#) im Amazon-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 (zum Beispiel eth0) der Instance zugewiesen. Weitere Informationen dazu finden Sie unter [Zuweisen einer IPv6-Adresse zu einer Instance](#) im Amazon-EC2-Benutzerhandbuch.

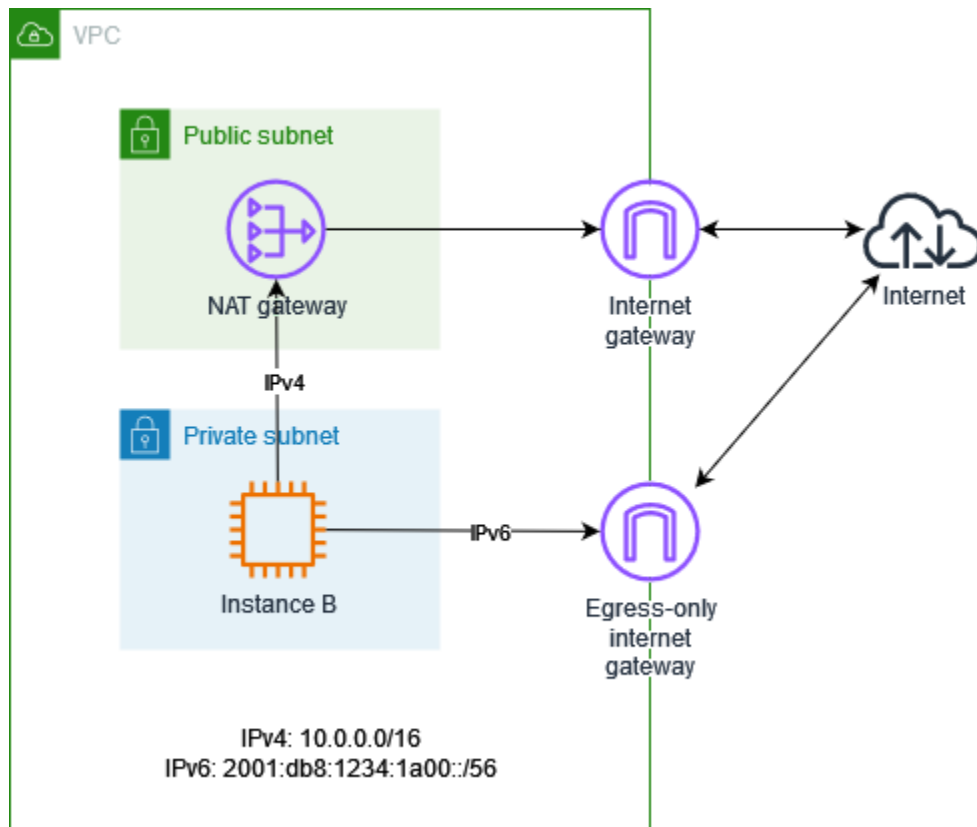
Sie können über ihre IPv6-Adresse eine Verbindung zu einer Instance herstellen. Weitere Informationen finden Sie unter [Herstellen einer Verbindung mit Ihrer Linux-Instance mit einem SSH-Client](#) im Amazon-EC2-Benutzerhandbuch.

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.

Beispiel für eine Dual-Stack-VPC-Konfiguration

Mit einer Dual-Stack-Konfiguration können Sie sowohl IPv4- als auch IPv6-Adressen für die Kommunikation zwischen Ressourcen in Ihrer VPC und Ressourcen über das Internet verwenden.

Das folgende Diagramm zeigt die VPC-Architektur. Ihre VPC hat ein öffentliches und ein privates Subnetz. Die VPC und Subnetze haben sowohl einen IPv4-CIDR-Block als auch einen IPv6-CIDR-Block. Es gibt eine EC2-Instance im privaten Subnetz, die sowohl eine IPv4-Adresse als auch eine IPv6-Adresse hat. Die Instance kann ausgehenden IPv4-Datenverkehr über ein NAT-Gateway an das Internet und ausgehenden IPv6-Datenverkehr über ein Internet-Gateway nur für ausgehenden Datenverkehr an das Internet senden.



Routing-Tabelle für öffentliches Subnetz

Im Folgenden finden Sie eine Routing-Tabelle für das öffentliche Subnetz. Die ersten beiden Einträge sind die lokalen Routen. Der dritte Eintrag sendet sämtlichen IPv4-Datenverkehr zum Internet-Gateway. Beachten Sie, dass der vierte Eintrag nur notwendig ist, wenn Sie planen, EC2-Instances mit IPv6-Adressen im öffentlichen Subnetz zu starten.

Bestimmungsort	Ziel
<i>VPC – IPv4 CIDR</i>	local
<i>VPC – IPv6 CIDR</i>	Lokal
0.0.0.0/0	<i>internet-gateway-id</i>
::/0	<i>internet-gateway-id</i>

Routing-Tabelle für das private Subnetz

Im Folgenden finden Sie eine Routing-Tabelle für das private Subnetz. Die ersten beiden Einträge sind die lokalen Routen. Der dritte Eintrag sendet sämtlichen IPv4-Datenverkehr zum NAT-Gateway. Der letzte Eintrag sendet sämtlichen IPv6-Datenverkehr zum Internet-Gateway für ausgehenden Datenverkehr.

Bestimmungsort	Ziel
<i>VPC – IPv4 CIDR</i>	local
<i>VPC – IPv6 CIDR</i>	Lokal
0.0.0.0/0	<i>nat-gateway-id</i>
::/0	<i>egress-only-gateway-id</i>

AWS Dienste, die unterstützen IPv6

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 gängigste Format für IP-Adressen ist IPv4. Das neue Format für IP-Adressen ist IPv6, welches einen größeren Adressraum bietet als IPv4.

AWS-Services Die Unterstützung für IPv6 umfasst die Unterstützung von Dual-Stack-Konfigurationen (IPv4 und IPv6) oder IPv6 nur 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, bei denen es sich nur um Subnetze, Dual-Stack-Netzwerke oder IPv4 IPv6 nur um Subnetze handelt.

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 Support IPv6 über ihre privaten Endpunkte anbieten, auch wenn sie keinen Support IPv6 über ihre öffentlichen Endpunkte anbieten. Endgeräte, die dies unterstützen, IPv6 können auf DNS-Anfragen mit AAAA-Einträgen antworten.

Dienste, die unterstützen IPv6

In der folgenden Tabelle sind diejenigen aufgeführt AWS-Services , die Dual-Stack-Unterstützung (IPv6nur Support) bieten, und Endgeräte, die dies unterstützen IPv6. Wir werden diese Tabelle

aktualisieren, sobald wir zusätzliche Unterstützung für IPv6 veröffentlichen. Einzelheiten zur Unterstützung IPv6 durch einen Dienst finden Sie in der Dokumentation des Dienstes.

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS Amplify	Ja	Nein	Ja	
Amazon API Gateway	Ja	Nein	Ja	Ja
AWS App Mesh	Ja	Ja	Ja	Nein
AWS App Runner	Ja	Nein	Ja	Ja
AWS AppConfig	Ja	Nein	Ja	Ja
Application Auto Scaling	Nein	Nein	Ja	Ja
AWS Application Discovery Service	Ja	Nein	Ja	Ja
Anwendungswiederherstellungs-Controller (ARC)	Ja	Nein	Ja	
WorkSpaces Amazon-Anwendungen	Ja	Nein	Nein	Nein
AWS AppSync ²	Teilweise	Nein	Teilweise	Ja
Amazon Athena	Ja	Nein	Ja	Ja
AWS Audit Manager	Nein	Nein	Ja	Ja
Amazon Aurora	Ja	Nein	Ja	Nein
Amazon Aurora DSQL	Nein	Nein	Ja	Ja
AWS Auto Scaling	Nein	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS B2B Data Interchange	Ja	Nein	Ja	Ja
AWS Backup	Ja	Nein	Ja	Ja
AWS Batch	Ja	Nein	Ja	Ja
Amazon Bedrock	Nein	Nein	Ja	Ja
AWS Fakturierung und Kostenmanagement Datenexporte	Ja	Nein	Ja	Ja
AWS Fakturierung und Kostenmanagement Preisrechner	Ja	Nein	Ja	Ja
AWS Billing Conductor	Ja	Nein	Ja	Ja
AWS Budgets	Ja	Nein	Ja	
Amazon Braket	Ja	Ja	Ja	Ja
AWS Certificate Manager	Ja	Nein	Ja	Nein
Amazon Chime SDK	Ja	Nein	Ja	
Amazon Comprehend	Ja	Ja	Ja	Ja
AWS Clean Rooms	Ja	Ja	Ja	Ja
AWS Clean Rooms ML	Ja	Ja	Ja	Ja
AWS Cloud9	Ja	Nein	Ja	

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS -Cloud-Control-API	Ja	Nein	Ja	Ja
CloudFormation	Nein	Nein	Ja	Ja
Amazon CloudFront	Ja	Ja	Ja	
AWS CloudHSM	Ja	Nein	Ja	Ja
AWS CloudTrail	Ja	Nein	Ja	Ja
Amazon CloudWatch	Ja	Ja	Ja	Ja
Einblicke in CloudWatch Amazon-Anwendungen	Nein	Nein	Ja	Ja
Amazon CloudWatch Internetmonitor	Nein	Nein	Ja	Ja
CloudWatch Amazon-Protokolle	Ja	Ja	Ja	Ja
Amazon CloudWatch Observability Access Manager	Ja	Ja	Ja	
Amazon CloudWatch Synthetics	Ja	Nein	Ja	Ja
AWS Cloud Map	Ja	Ja	Ja	Ja
AWS Cloud-WAN	Ja	Nein	Ja	Nein
AWS CodeArtifact	Ja	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
Amazon Connect Kundenprofile	Ja	Nein	Ja	Ja
AWS CodeBuild	Nein	Nein	Ja	Ja
AWS CodeCommit	Nein	Nein	Ja	Ja
AWS CodeDeploy	Nein	Nein	Ja	Ja
AWS Compute Optimizer	Nein	Nein	Ja	Ja
Amazon Comprehend Medical	Nein	Nein	Ja	Ja
Amazon CodeGuru Profiler	Ja	Nein	Ja	Ja
Amazon Cognito	Ja	Nein	Ja	
AWS Config	Nein	Nein	Ja	Ja
AWS Control Tower	Nein	Nein	Ja	Ja
AWS Cost Explorer	Ja	Nein	Ja	Ja
AWS Cost Optimization Hub	Ja	Nein	Ja	Ja
AWS Data Exchange	Nein	Nein	Ja	Ja
Amazon Data Firehose	Nein	Nein	Ja	Ja
Amazon Data Lifecycle Manager	Ja	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS Database Migration Service	Ja	Nein	Nein	Ja
AWS DataSync	Ja	Ja	Ja	Ja
Amazon DataZone	Nein	Nein	Ja	Ja
AWS Deadline Cloud	Ja	Nein	Ja	Ja
Amazon Detective	Ja	Ja	Ja	
Direct Connect	Ja	Ja	Nein	Ja
Directory Service	Nein	Nein	Ja	Ja
Amazon EBS direkt APIs	Ja	Nein	Ja	Ja
Amazon EC2	Ja	Ja	Ja	Nein
EC2 Image Builder	Ja	Ja	Ja	Ja
Amazon ECR	Ja	Nein	Ja	Nein
Amazon ECS	Ja	Ja	Ja	Ja
Amazon EFS	Ja	Ja	Ja	Ja
Amazon EKS	Teilweise	Teilweise	Ja	Ja
Amazon EMR	Nein	Nein	Ja	Ja
AWS Elastic Beanstalk	Ja	Nein	Ja	Ja
AWS Elastic Disaster Recovery	Nein	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
ELB	Teilweise	Teilweise	Ja	Nein
Amazon ElastiCache	Ja	Ja	Nein	Ja
AWS Elemental MediaConvert	Nein	Nein	Ja	Ja
AWS Elemental MediaConnect	Ja	Ja	Ja	Teilweise
AWS Social Messaging für Endbenutzer	Ja	Nein	Ja	Nein
AWS Entity Resolution	Ja	Nein	Ja	Ja
Amazon EventBridge	Nein	Nein	Ja	Ja
AWS Fargate	Ja	Nein	Ja	Ja
Amazon FSx	Nein	Nein	Ja	Ja
Amazon GameLift Streams	Ja	Nein	Ja	Ja
AWS Global Accelerator	Ja	Nein	Ja	
AWS Glue	Ja	Nein	Nein	Ja
AWS Glue DataBrew	Nein	Nein	Ja	Ja
Amazon Managed Grafana ³	Ja	Nein	Ja	Ja
AWS Ground Station ⁴	Ja	Nein	Ja	Ja
Amazon GuardDuty	Nein	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS HealthImaging	Nein	Nein	Ja	Ja
AWS HealthLake	Nein	Nein	Ja	Ja
AWS HealthOmics	Nein	Nein	Ja	Ja
AWS Identity and Access Management (ICH BIN)	Ja	Ja	Ja	Nein
AWS IAM-Zugriffsanalyzer	Ja	Nein	Ja	Ja
AWS IAM Identity Center	Nein	Nein	Ja	Ja
AWS IAM-Rollen überall	Nein	Nein	Ja	Ja
Amazon Inspector	Ja	Ja	Ja	Ja
Amazon Interactive Video Service (IVS) ⁵	Ja	Nein	Ja	Ja
AWS IoT Core	Ja	Nein	Ja	Ja
AWS IoT Device Defender	Ja	Nein	Ja	Nein
AWS IoT Device Management	Ja	Nein	Ja	Nein
AWS IoT FleetWise	Ja	Nein	Ja	Ja
AWS IoT Greengrass	Ja	Nein	Ja	Nein
AWS IoT SiteWise	Ja	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS IoT TwinMaker	Ja	Nein	Ja	Ja
AWS IoT Wireless	Ja	Nein	Ja	Ja
Amazon Kendra	Nein	Nein	Ja	Nein
AWS Key Management Service	Ja	Teilweise	Ja	Ja
Amazon Keyspaces	Ja	Ja	Ja	Ja
Amazon Keyspaces CDC streams	Ja	Ja	Ja	Ja
Amazon Kinesis Data Streams	Ja	Nein	Ja	Ja
AWS Lake Formation	Nein	Nein	Nein	Ja
AWS Lambda	Ja	Nein	Ja	Ja
AWS Launch Wizard	Nein	Nein	Ja	Ja
AWS License Manager	Nein	Nein	Ja	Ja
Amazon Lightsail	Ja	Ja	Ja	Ja
Amazon Location Service	Nein	Nein	Ja	Ja
Amazon MQ	Nein	Nein	Ja	Ja
Amazon MWAA	Nein	Nein	Ja	Ja
Amazon Macie	Ja	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS Mainframe Modernization	Ja	Nein	Ja	Ja
Amazon Managed Grafana	Nein	Nein	Ja	Ja
Amazon Managed Service für Prometheus	Ja	Nein	Ja	Ja
AWS Migration Hub Orchestrator	Nein	Nein	Ja	Ja
AWS Network Firewall	Ja	Ja	Nein	Ja
AWS Network Manager	Ja	Nein	Ja	Nein
OpenSearch Amazon-Dienst	Ja	Nein	Ja	
AWS Organizations	Ja	Nein	Ja	Ja
AWS Outposts	Nein	Nein	Ja	Ja
Amazon Personalize	Ja	Nein	Ja	Ja
Amazon Pinpoint	Ja	Nein	Ja	Ja
Amazon Polly	Ja	Nein	Ja	Ja
AWS-Preisliste	Nein	Nein	Ja	Nein
AWS Private Certificate Authority	Ja	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS Private CA Konnektor für Active Directory	Ja	Nein	Ja	Ja
AWS Private CA Konnektor für SCEP	Ja	Nein	Ja	Ja
AWS PrivateLink	Ja	Ja	Ja	
Amazon Q Business	Nein	Nein	Ja	Nein
Amazon RDS	Ja	Nein	Ja	Nein
Amazon RDS Daten-API	Nein	Nein	Ja	Ja
Amazon RDS Performance Insights	Nein	Nein	Ja	Ja
Amazon Redshift	Ja	Nein	Ja	
Amazon Rekognition	Nein	Nein	Ja	Ja
Papierkorb	Ja	Nein	Ja	Ja
AWS re:Post Private	Ja	Nein	Ja	Ja
AWS Resource Access Manager	Ja	Nein	Ja	Ja
AWS Resource Explorer	Ja	Nein	Ja	Nein
AWS -Ressourcengruppen	Ja	Ja	Ja	Ja
AWS Resource Groups Tagging API	Ja	Ja	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
Amazon Route 53	Ja	Ja	Ja	Ja
Amazon S3	Ja	Nein	Ja	Nein
Amazon S3 on Outposts	Nein	Nein	Ja	Nein
Amazon SageMaker	Nein	Nein	Ja	Ja
AWS Secrets Manager	Ja	Nein	Ja	Ja
AWS Security Hub	Nein	Nein	Ja	Ja
Amazon Security Lake	Ja	Nein	Ja	Ja
AWS Security Token Service	Ja	Nein	Ja	Ja
AWS Service Catalog	Nein	Nein	Ja	Ja
AWS Shield	Ja	Ja	Nein	Ja
Amazon Simple Email Service	Ja	Nein	Ja	Ja
Amazon Simple Notification Service	Ja	Nein	Ja	Ja
Amazon Simple Queue Service	Ja	Nein	Ja	Ja
Amazon Simple Workflow Service	Ja	Nein	Ja	Ja
AWS Site-to-Site VPN	Ja	Nein	Ja	Nein
AWS Snow Family	Nein	Nein	Ja	

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS Step Functions	Ja	Nein	Ja	Ja
AWS Storage Gateway	Ja	Ja	Ja	Ja
AWS Systems Manager	Nein	Nein	Ja	Ja
AWS Systems Manager Incident Manager	Nein	Nein	Ja	Ja
AWS Systems Manager für SAP	Nein	Nein	Ja	Ja
Amazon Textract	Nein	Nein	Ja	Ja
Amazon Timestream	Nein	Nein	Ja	Ja
Amazon Transcribe	Ja	Ja	Ja	Ja
AWS Transfer Family ⁶	Ja	Nein	Ja	Ja
AWS Transit Gateway	Ja	Nein	Ja	Nein
Amazon Translate	Ja	Ja	Ja	Ja
AWS Trusted Advisor	Nein	Nein	Ja	Ja
AWS-Benutzerbenachrichtigungen	Nein	Nein	Ja	Ja
Amazon Verified Permissions	Ja	Nein	Ja	Ja
VMware Cloud an AWS	Nein	Nein	Ja	Ja
Amazon VPC	Ja	Ja	Ja	Nein
Amazon VPC Lattice	Nein	Nein	Ja	Ja

Service-Name	Unterstützung von Dual-Stack	IPv6 nur Unterstützung	Unterstützung für öffentliche Endgeräte IPv6	Private Endgeräte unterstützen 1 IPv6
AWS WAF	Ja	Ja	Nein	
AWS WAFV2	Nein	Nein	Ja	Ja
AWS Well-Architected Tool	Nein	Nein	Ja	Ja
Amazon WorkMail	Nein	Nein	Ja	Ja
Amazon WorkSpaces	Ja	Nein	Ja	Ja
AWS X-Ray	Ja	Nein	Ja	Ja

¹ Eine leere Zelle weist darauf hin, dass der Service nicht [in AWS PrivateLink integriert ist](#).

² Dieser Eintrag stellt die IPv6 Unterstützung von AWS AppSync GraphQL- und Event-API-Konfigurationsoperationen über die [AWS AppSync SDK-API](#) dar. IPv6 wird für Client-Verbindungen zu kundenverwaltetem AWS AppSync GraphQL und Event APIs nicht unterstützt.

³ Dieser Eintrag stellt die IPv6 Unterstützung für Grafana-Workspace-Verwaltungsvorgänge dar, z. B. das Aktualisieren von Arbeitsbereichen und Arbeitsbereichsberechtigungen. Allgemeine Grafana-Workspace-Operationen wie das Erstellen und Bearbeiten von Dashboards oder das Abfragen von Datenquellen werden nicht IPv6 unterstützt.

⁴ [Dieser Eintrag steht für die IPv6 Unterstützung von Operationen auf der AWS Ground Station Steuerungsebene, wie z. B. das Aufrufen der API.](#) [AWS Ground Station](#) IPv6 wird von der AWS Ground Station Datenebene nicht unterstützt. Stellen Sie daher sicher, dass auf die Ressourcen, an die Sie Daten liefern (z. B. EC2 Amazon-Instances), zugegriffen werden kann IPv4.

⁵ Dieser Eintrag steht für die IPv6 Unterstützung von Operationen auf der Amazon IVS-Steuerebene, z. B. das Anrufen eines [IVS-Endpunkts](#).

⁶ [Weitere Informationen zum IPv6 Support finden Sie unter AWS Transfer Family IPv6 Einschränkungen.](#)

Zusätzliche IPv6 Unterstützung

Datenverarbeitung

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

Entwicklung von Spielen

- Amazon GameLift Streams unterstützt das Streamen IPv6 auf der Microsoft Windows Server 2022 Base-Runtime.

Netzwerk und Bereitstellung von Inhalten

- Amazon VPC unterstützt die Erstellung von IPv6 Nur-Unternetzen.
- Amazon VPC unterstützt IPv6 AWS Ressourcen bei der Kommunikation mit IPv4 Ressourcen, indem es Ihre Subnetze und Ihre NAT64 NAT-Gateways unterstützt DNS64 .

Sicherheit, Identität und Compliance

- Amazon Detective unterstützt IPv6 Adressen in seinen netzwerkbezogenen Ergebnissen und Entitätsprofilen.
- AWS Identity and Access Management (IAM) unterstützt IPv6 Adressen in identitätsbasierten IAM-Richtlinien.
- Amazon Macie unterstützt IPv6 Adressen in personenbezogenen Daten (PII).
- Amazon Security Lake unterstützt IPv6 Adressen für alle Vorgänge in Protokollquellen und Abonnenten.

Verwaltung und Governance

- AWS CloudTrail Datensätze enthalten IPv6 Quellinformationen.
- AWS CLI Version 2 unterstützt das Herunterladen über IPv6 Verbindungen IPv6 nur für Clients.

Weitere Informationen

- [IPv6 nein AWS](#)
- Amazon [IPv6VPC-Referenzarchitekturen mit zwei Stacks und nur für Amazon VPC](#) (PDF)

Konfigurieren einer Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (VPC) ist ein grundlegender Baustein, mit dem Sie ein logisch isoliertes virtuelles Netzwerk innerhalb der AWS Cloud bereitstellen können. Durch die Erstellung Ihrer eigenen VPC erhalten Sie die volle Kontrolle über die Netzwerkkumgebung, einschließlich der Möglichkeit, IP-Adressbereiche, Subnetze, Routing-Tabellen und Konnektivitätsoptionen zu definieren.

Ihr AWS-Konto enthält eine Standard-VPC für jede AWS-Region. Diese Standard-VPC ist mit Einstellungen vorkonfiguriert, die sie zu einer bequemen Option für den schnellen Start von Ressourcen machen. Die Standard-VPC entspricht jedoch möglicherweise nicht immer Ihren langfristigen Netzwerkanforderungen. Hier kann die Erstellung zusätzlicher VPCs von Vorteil sein.

Das Erstellen zusätzlicher VPCs bietet mehrere Vorteile gegenüber der Verwendung der Standard-VPC, die mit jedem neuen AWS-Konto bereitgestellt wird. Mit einer selbstverwalteten VPC können Sie die Netzwerktopologie so gestalten, dass sie genau auf Ihre spezifischen Anforderungen zugeschnitten ist, unabhängig davon, ob es sich um die Implementierung einer mehrstufigen Anwendung, die Verbindung zu On-Premises-Ressourcen oder die Trennung von Workloads nach Abteilung oder Geschäftseinheit handelt.

Zudem kann die Einrichtung mehrerer VPCs für mehr Sicherheit und Isolierung zwischen Ihren verschiedenen Anwendungen oder Geschäftsbereichen sorgen. Jede VPC fungiert als separates, virtuelles Netzwerk, sodass Sie unterschiedliche Sicherheitsrichtlinien, Zugriffskontrollen und Routing-Konfigurationen anwenden können, die auf jede Umgebung zugeschnitten sind.

Letztlich sollte die Entscheidung, entweder die Standard-VPC zu verwenden oder eine (oder mehrere) benutzerdefinierte VPCs zu erstellen, auf Ihren spezifischen Anwendungsanforderungen, Sicherheitsanforderungen und langfristigen Skalierbarkeitszielen basieren. Wenn Sie Zeit investieren, um Ihre VPC-Infrastruktur sorgfältig zu entwerfen, kann sich das in Form einer robusten, sicheren und anpassungsfähigen Cloud-Netzwerkgrundlage auszahlen.

Inhalt

- [VPC-Grundlagen](#)
- [VPC-Konfigurationsoptionen](#)
- [Standard VPCs](#)
- [Erstellen einer VPC](#)
- [Visualisierung der Ressourcen in Ihrer VPC](#)

- [Hinzufügen oder Entfernen eines IPv4-CIDR-Blocks zu bzw. aus Ihrer VPC](#)
- [DHCP-Optionssätze in Amazon VPC](#)
- [DNS-Attribute für Ihre VPC](#)
- [Network Address Usage für Ihre VPC](#)
- [Freigeben Ihrer VPC-Subnetze für andere Konten](#)
- [Erweitern einer VPC auf eine lokale Zone, eine Wavelength-Zone oder einen Outpost](#)
- [Löschen der VPC](#)
- [Generieren von Infrastructure as Code aus Ihren VPC-Konsolenaktionen mit Console-to-Code](#)

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](#)
- [VPC-Diagramm](#)
- [VPC-Ressourcen](#)

IP-Adressbereich der VPC

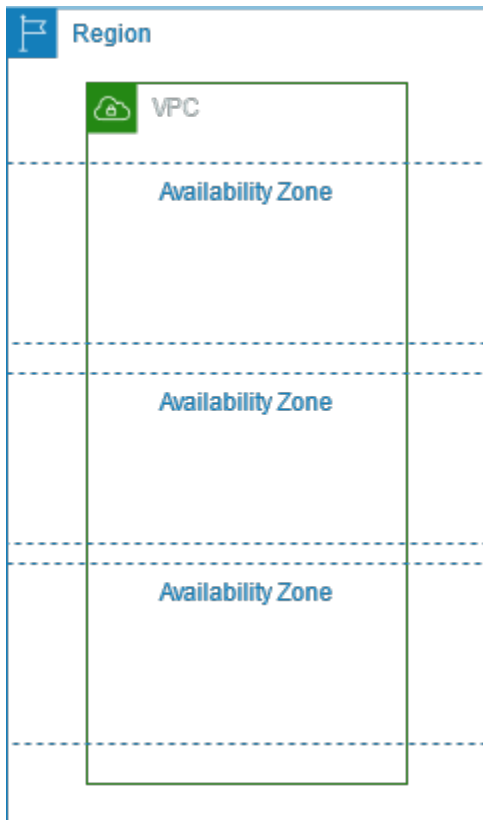
Wenn Sie eine VPC erstellen, legen Sie die IP-Adressen wie folgt fest:

- 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. Beispielfiguren 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 \(NAT-Gateways\)](#)

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 z. B. EC2-Instances, in Ihre 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 für die Tenancy der VPC Default auswählen, nutzen EC2-Instances, die in dieser VPC gestartet werden, das beim Starten der Instance angegebene Tenancy-Attribut. Weitere Informationen finden Sie unter [Starten einer Instance mit definierten Parametern](#) im Amazon-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. Beim Einsatz von AWS Outposts benötigt der Outpost private Konnektivität; Sie müssen die Tenancy Default verwenden.

Standard VPCs

Wenn Sie Amazon VPC verwenden, haben Sie in jeder AWS Region eine Standard-VPC. Eine Standard-VPC umfasst ein öffentliches Subnetz in jeder Availability Zone, ein Internet-Gateway und Einstellungen zum Aktivieren der DNS-Auflösung. Daher können Sie sofort damit beginnen, EC2 Amazon-Instances in einer Standard-VPC VPC. Sie können auch Dienste wie ELB, 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](#)
- [Arbeiten mit Ihrer Standard-VPC und Standard-Subnetzen](#)

Komponenten von Standard-VPCs

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

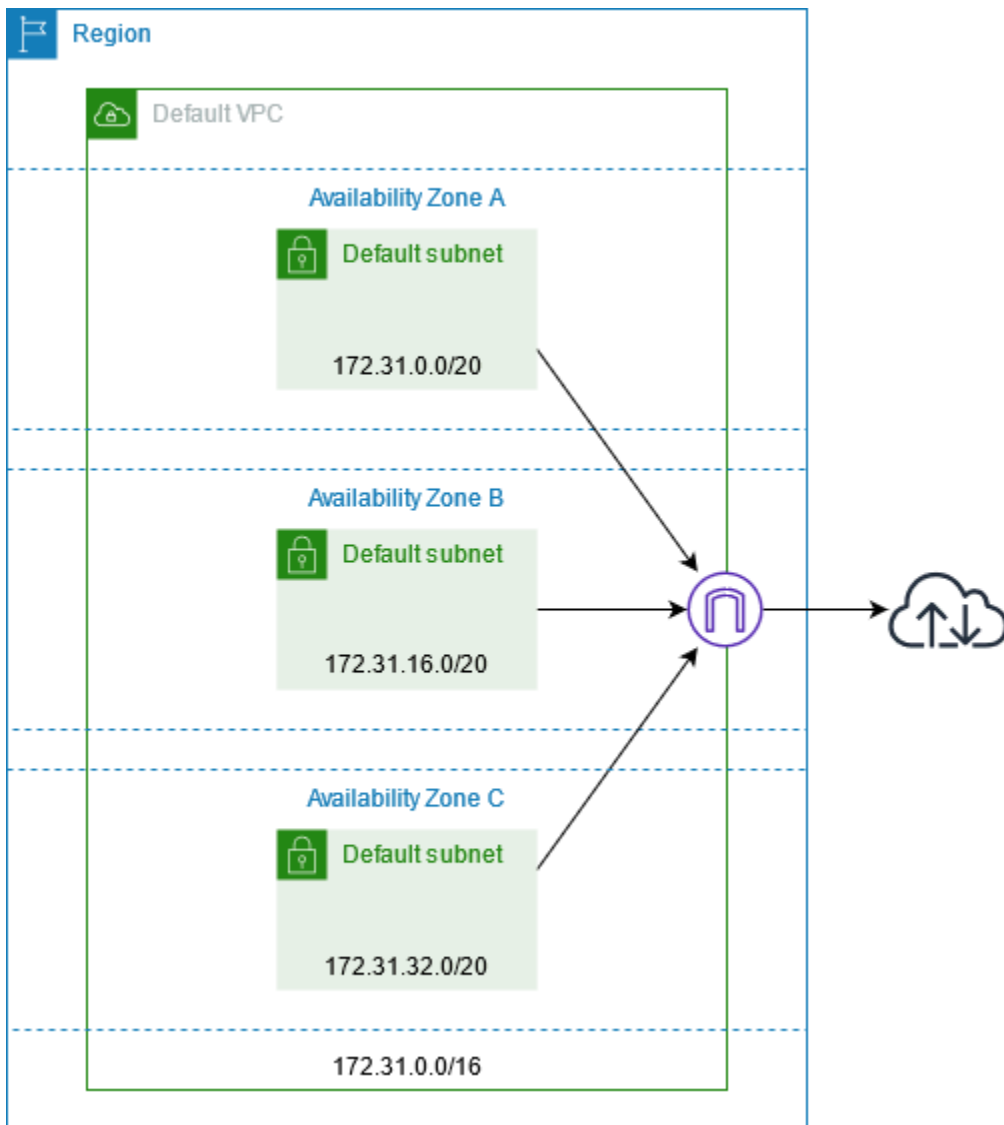
- Erstellen Sie eine VPC mit einer Größe des /16 IPv4 CIDR-Blocks ($172.31.0.0/16$). Dies bietet bis zu 65.536 private Adressen. IPv4
- Erstellen eines Standardsubnetzes der Größe /20 in jeder Availability Zone. Damit stehen bis zu 4.096 Adressen pro Subnetz zur Verfügung, von denen ein paar für die Nutzung durch uns reserviert sind.
- Erstellen eines [Internet-Gateways](#) und Herstellen einer Verbindung mit der Standard-VPC
- Fügen Sie der Haupt-Routintabelle 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

- Ordnen Sie die für Ihr AWS Konto festgelegten Standard-DHCP-Optionen Ihrer Standard-VPC zu.

 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 eine IAM-Richtlinie haben, die die Möglichkeit zum Anrufen verweigert `CreateInternetGateway`, und Sie dann anrufen, wird das Internet-Gateway in der Standard-VPC trotzdem erstellt. `CreateDefaultVpc` Um zu verhindern, dass Amazon ein Internet-Gateway erstellt, müssten Sie `CreateDefaultVpc` und ablehnen `CreateInternetGateway`.
- Informationen zum Blockieren des gesamten Datenverkehrs zu und von den Internet-Gateways in Ihrem Konto finden Sie unter [Sperren Sie den öffentlichen Zugriff VPCs auf Subnetze](#).

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.

Bestimmungsort	Ziel
172.31.0.0/16	Lokal
0.0.0.0/0	<i>internet_gateway_id</i>

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.
- AWS Site-to-Site VPN Verbindungen hinzufügen.
- Fügen Sie weitere IPv4 CIDR-Blöcke hinzu.
- Zugriff VPCs in einer abgelegenen Region mithilfe eines Direct Connect-Gateways. Weitere Informationen zu Direct Connect-Gateways finden Sie unter [Direct Connect-Gateways](#) im AWS Direct Connect -Benutzerhandbuch.

Sie können ein Standardsubnetz wie jedes andere Subnetz verwenden. Fügen Sie benutzerdefinierte Routing-Tabellen hinzu und legen Sie das Netzwerk fest. ACLs Sie können auch ein bestimmtes Standardsubnetz angeben, wenn Sie eine Instance starten. EC2

Sie können Ihrer Standard-VPC optional einen IPv6 CIDR-Block zuordnen.

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 dies tun, kann jedoch keine EC2 Instance, die in diesem Subnetz ausgeführt wird, auf das Internet zugreifen.

Instances, die Sie in einem Standardsubnetz starten, erhalten sowohl eine öffentliche IPv4 als auch eine private IPv4 Adresse und sowohl öffentliche als auch private DNS-Hostnamen. Instances, die Sie in einer Standard-VPC in einem nicht standardmäßigen Subnetz starten, erhalten weder eine öffentliche IPv4 Adresse noch einen DNS-Hostnamen. Sie können das Standardverhalten für die öffentliche IP-Adressierung Ihres Subnetzes ändern. Weitere Informationen finden Sie unter [Ändern der IP-Adressierungsattribute Ihres Subnetzes](#).

Von Zeit zu Zeit AWS kann einer Region eine neue Availability Zone hinzugefügt werden. 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 benötigen, können Sie dieses selbst erstellen. Weitere Informationen finden Sie unter [Erstellen eines Standardsubnetzes](#).

Arbeiten mit Ihrer Standard-VPC und Standard-Subnetzen

In diesem Abschnitt wird beschrieben, wie Sie mit Standard VPCs - und Standardsubnetzen arbeiten.

Inhalt

- [Anzeigen Ihrer Standard-VPC und Standardsubnetze](#)
- [Erstellen einer Standard-VPC](#)
- [Erstellen eines Standardsubnetzes](#)
- [Löschen Ihrer Standardsubnetze und der Standard-VPC](#)

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 Ihr 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 Sie die [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)
- Benutze die [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 Ihr aus VPCs.
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-vpc](#) AWS 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 den PowerShell Befehl [New-EC2DefaultVpcTools](#) für Windows oder die [CreateDefaultVpc](#) Amazon EC2 API-Aktion verwenden.

Erstellen eines Standardsubnetzes

Note

Sie können kein Standard-Subnetz mit der AWS-Managementkonsole erstellen.

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

Wenn Sie ein Standardsubnetz erstellen, wird es mit einem /20 IPv4 CIDR-Block der Größe im nächsten verfügbaren zusammenhängenden Bereich in Ihrer Standard-VPC erstellt. Die folgenden Regeln gelten:

- Sie können den CIDR-Block nicht selbst festlegen.
- Sie können ein zuvor gelöscht 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 Standardsubnetz nicht automatisch einen IPv6 CIDR-Block. Stattdessen können Sie dem Standardsubnetz einen IPv6 CIDR-Block zuordnen, nachdem Sie ihn erstellt haben. Weitere Informationen finden Sie unter [Hinzufügen oder Entfernen eines IPv6-CIDR-Blocks aus Ihrem Subnetz](#).

Um ein Standardsubnetz mit dem zu erstellen AWS CLI

Verwenden Sie den [create-default-subnet](#) AWS CLI Befehl 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 von finden Sie im [AWS Command Line Interface Benutzerhandbuch](#). AWS CLI

Alternativ können Sie den PowerShell Befehl [New-EC2DefaultSubnet](#) Tools für Windows oder die [CreateDefaultSubnet](#) Amazon EC2 API-Aktion 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 VPCs beim Starten von Instances explizit ein Subnetz in einem Ihrer Subnetze 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 der IP-Adressierungsattribute Ihres Subnetzes](#). Sie können nur ein Standardsubnetz pro Availability Zone haben. Sie können kein Standardsubnetz 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

- [Erstellen Sie eine VPC und andere VPC-Ressourcen](#)
- [Ausschließliches Erstellen einer VPC](#)
- [Erstellen einer VPC mithilfe der AWS CLI](#)

Informationen zum Ändern einer VPC finden Sie unter [the section called “CIDR-Block hinzufügen oder entfernen”](#).

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 Resources to create (Zu erstellende Ressourcen) die Option VPC and more (VPC und mehr) aus.
4. Lassen Sie die automatische Generierung von Namenstags aktiviert, um Namenstags für die VPC-Ressourcen zu erstellen, oder deaktivieren Sie sie, 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 Default als Tenancy der VPC auswählen, nutzen EC2-Instances, die in dieser VPC gestartet werden, das beim Starten der Instance angegebene Tenancy-Attribut. Weitere Informationen finden Sie unter [Starten einer Instance mit bestimmten Parametern](#) im Amazon-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. Beim Einsatz von AWS Outposts benötigt der Outpost private Konnektivität; Sie müssen die Tenancy Default verwenden.
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 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 AWS für Sie 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 für NAT-Gateways](#).

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-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 ein VPC-Feature, das 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. Wenn Sie den von IPAM zugewiesenen IPv6-CIDR-Block verwenden, um IPv6-CIDRs für VPCs bereitzustellen, können Sie bei der VPC-Erstellung zusammenhängende IPv6-CIDRs nutzen. Zusammenhängend zugewiesene CIDRs sind sequenziell zugewiesen. Sie ermöglichen Ihnen, Ihre Sicherheits- und Netzwerkregeln zu vereinfachen. Die IPv6-CIDRs können in einem einzigen Eintrag für Netzwerk- und Sicherheitskonstrukte wie Zugriffskontrolllisten, Routing-Tabellen, Sicherheitsgruppen und Firewalls zusammengefasst werden.

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 unter Network Border Gruppe (Netzwerkrandgruppe) die Gruppe aus, aus der AWS IP-Adressen bereitstellt. 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. Informationen zum Einbinden eigener IP-Adressbereiche in AWS finden Sie unter [Bring Your Own IP Addresses \(BYOIP\)](#) im Amazon-EC2-Benutzerhandbuch. 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 für die Tenancy der VPC Default auswählen, nutzen EC2-Instances, die in dieser VPC gestartet werden, das beim Starten der Instance angegebene Tenancy-Attribut. Weitere Informationen finden Sie unter [Starten einer Instance mit definierten Parametern](#) im Amazon-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. Beim Einsatz von AWS Outposts benötigt der Outpost private Konnektivität; Sie müssen die Tenancy Default verwenden.
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 einer VPC mithilfe der AWS CLI

Das folgende Verfahren enthält AWS CLI-Beispielbefehle zum Erstellen einer VPC sowie der 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 den AWS CLI konfigurieren, werden Sie zur Eingabe von AWS-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 und andere VPC-Ressourcen mit der 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, um 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:
- 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
```

- 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
```

- Erstellen Sie mit dem folgenden Befehl [create-route-table](#) eine benutzerdefinierte Routing-Tabelle für die VPC. Der Befehl gibt die ID der neuen Routing-Tabelle zurück.

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

- 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 Routing-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 privaten 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:
- 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
```

- Erstellen Sie das NAT-Gateway im öffentlichen Subnetz mithilfe des folgenden Befehls [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
```

- (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 Routing-Tabelle zurück.

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

- 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
```

- (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 privaten 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
```

Visualisierung der Ressourcen in Ihrer VPC

In diesem Abschnitt wird beschrieben, wie Sie eine visuelle Darstellung der Ressourcen in Ihrer VPC mithilfe der Registerkarte Ressourcenkarte anzeigen können. 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 ein Gateway-Endpunkt vorhanden ist, gibt es eine Gateway-Endpunktresource mit dem Namen des AWS-Services (Amazon S3 oder Amazon DynamoDB), mit dem 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 oder Entfernen eines IPv4-CIDR-Blocks zu bzw. aus Ihrer VPC

In diesem Abschnitt wird beschrieben, wie Sie IPv4- und IPv6-CIDR-Blöcke zu einer VPC hinzufügen oder daraus entfernen.

 Important

- Sie können Ihrer VPC standardmäßig bis zu fünf IPv4-CIDR-Blöcke und bis zu IPv6-CIDR-Blöcke hinzufügen, aber das Limit ist einstellbar. Weitere Informationen finden Sie unter [Amazon VPC-Kontingente](#). Informationen zu Einschränkungen für CIDR-Blöcke für eine VPC finden Sie unter [VPC-CIDR-Blöcke](#).
- Wenn Ihrer VPC mehrere IPv4-CIDR-Blöcke zugeordnet sind, können Sie einen IPv4-CIDR-Block von der VPC entfernen. Es ist nicht möglich, den primären IPv4-CIDR-Block zu entfernen. Sie können nur einen vollständigen CIDR-Block 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.
- 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-Block entfernen.
- Um den IPv6-Block 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.

So können Sie einen CIDR-Block einer VPC mithilfe der Konsole hinzufügen oder daraus 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 dann unter Actions (Aktionen) die Option Edit CIDRs (CIDRs bearbeiten) aus.
4. Um ein CIDR zu entfernen, wählen Sie Entfernen neben dem CIDR aus.
5. Wählen Sie Neuen IPv4-CIDR hinzufügen oder Neuen IPv6-CIDR hinzufügen aus, um einen CIDR hinzuzufügen.
6. Führen Sie für IPv4-CIDR-Block einen der folgenden Schritte aus, um einen CIDR hinzuzufügen:

- 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.
 - Wählen Sie Speichern.
7. Gehen Sie wie folgt vor, um einen CIDR für IPv6-CIDR-Block hinzuzufügen:
- 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 unter Network Border Gruppe (Netzwerkrandgruppe) die Gruppe aus, aus der AWS IP-Adressen bereitstellt. 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 finden Sie unter [Bring your own](#)

[IP addresses \(BYOIP\) to Amazon EC2](#) im Amazon-EC2-Benutzerhandbuch. 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.
- Klicken Sie auf CIDR auswählen, wenn Sie fertig sind.

8. Klicken Sie auf Schließen.

9. Wenn Sie Ihrer VPC einen CIDR-Block hinzugefügt haben, können Sie Subnetze erstellen, die den neuen CIDR-Block verwenden. Weitere Informationen finden Sie unter [Erstellen eines Subnetzes](#).

So können Sie einen CIDR-Block einer VPC mithilfe der AWS CLI zuordnen oder die Zuordnung aufheben

Verwenden Sie die Befehle [associate-vpc-cidr-block](#) und [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?](#)
- [DHCP-Optionssatzkonzepte](#)
- [Arbeiten mit DHCP-Optionslisten](#)

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 Domännennamen 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 Domännennamen 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 „AmazonProvidedDNS“ ausdrücklich im DHCP-Optionssatz angegeben ist. Wenn „AmazonProvidedDNS“ im Optionssatz fehlt, gibt der IPv4-DHCP-Server keine Adresse zurück, unabhängig davon, ob andere IPv4-Nameserver im Optionssatz angegeben werden oder nicht.

Die Amazon-DHCP-Server können auch ein ganzes IPv4- oder IPv6-Präfix für eine Netzwerkschnittstelle in Ihrer VPC mithilfe der Präfixdelegation bereitstellen (siehe [Zuweisen von Präfixen zu Amazon-EC2-Netzwerkschnittstellen](#) im Amazon-EC2-Benutzerhandbuch). Die IPv4-Präfix-Delegation ist in DHCP-Antworten nicht vorgesehen. Der Schnittstelle zugewiesene IPv4-Präfixe können mit IMDS abgerufen werden (siehe [Instance-Metadatenkategorien](#) im Amazon 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:

- Für [auf dem Nitro-System basierende EC2-Instances](#) konfiguriert AWS 169.254.169.253 als Standard-Domain-Nameserver.
- Für [EC2-Instances, die auf Xen basieren](#), werden keine Domain-Nameserver konfiguriert. Und weil Instances in der VPC keinen Zugriff auf einen DNS-Server haben, können sie auch nicht das Internet aufrufen.

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](#)
- [Benutzerdefinierter DHCP-Optionssatz](#)

Standardmäßiger DHCP-Optionssatz

Der Standard-DHCP-Optionssatz enthält die folgenden Einstellungen:

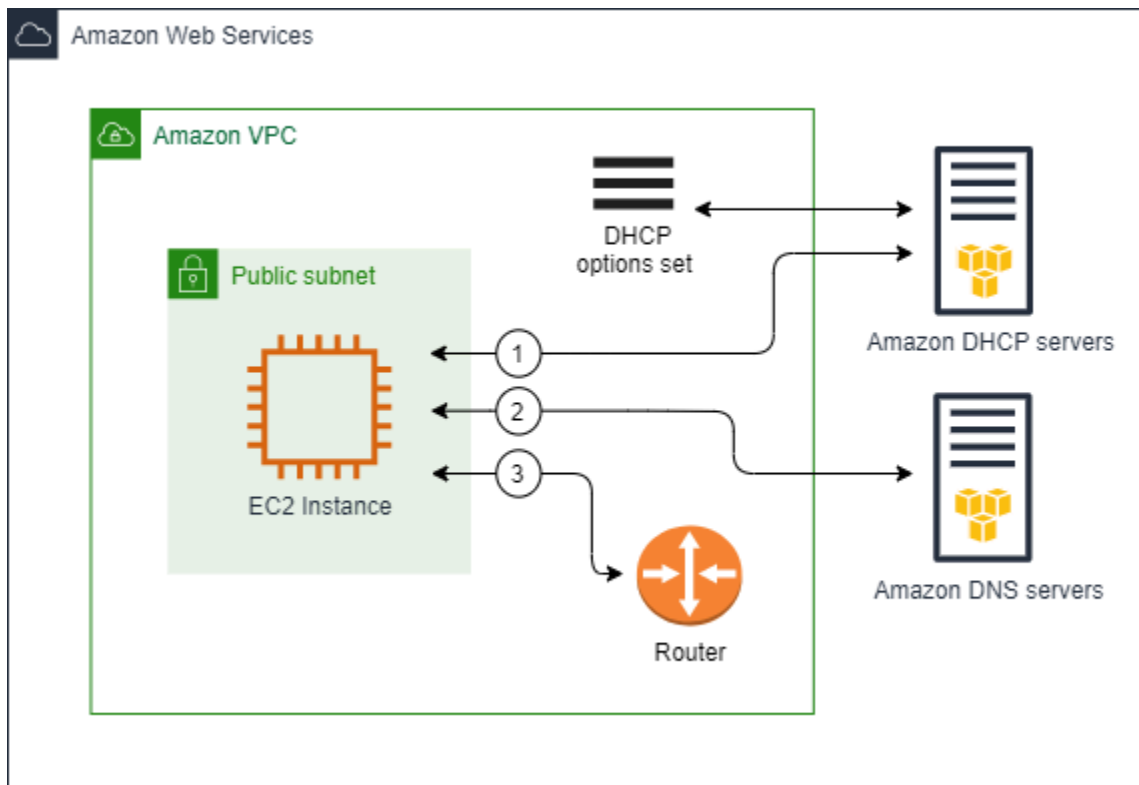
- Domain-Nameserver: Die DNS-Server, die die Netzwerkschnittstellen zur Auflösung von Domain-Namen verwenden. Für einen standardmäßigen DHCP-Optionssatz ist dies immer AmazonProvidedDNS. Weitere Informationen finden Sie unter [Amazon DNS-Server](#).
- Domain-Name: Der Domain-Name, den ein Client beim 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](#).

- **Bevorzugte IPv6-Lease-Zeit:** Sie können jetzt wählen, wie oft eine laufende Instance, der ein IPv6 zugewiesen ist, eine DHCPv6-Lease-Verlängerung durchläuft. Die Standard-Lease-Zeit beträgt 140 Sekunden. Die Lease-Verlängerung erfolgt in der Regel, wenn die Hälfte der Lease-Zeit 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 abzurufen.
- **NetBIOS-Namenserver:** Bei EC2-Instances, die Windows ausführen, ist der NetBIOS-Computernamen ein Anzeigenamen, 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 jederzeit mit dem Amazon-DHCP-Server interagieren, um die temporär zugeteilte IP-Adresse und die zusätzlichen Netzwerkeinstellungen zu erhalten.



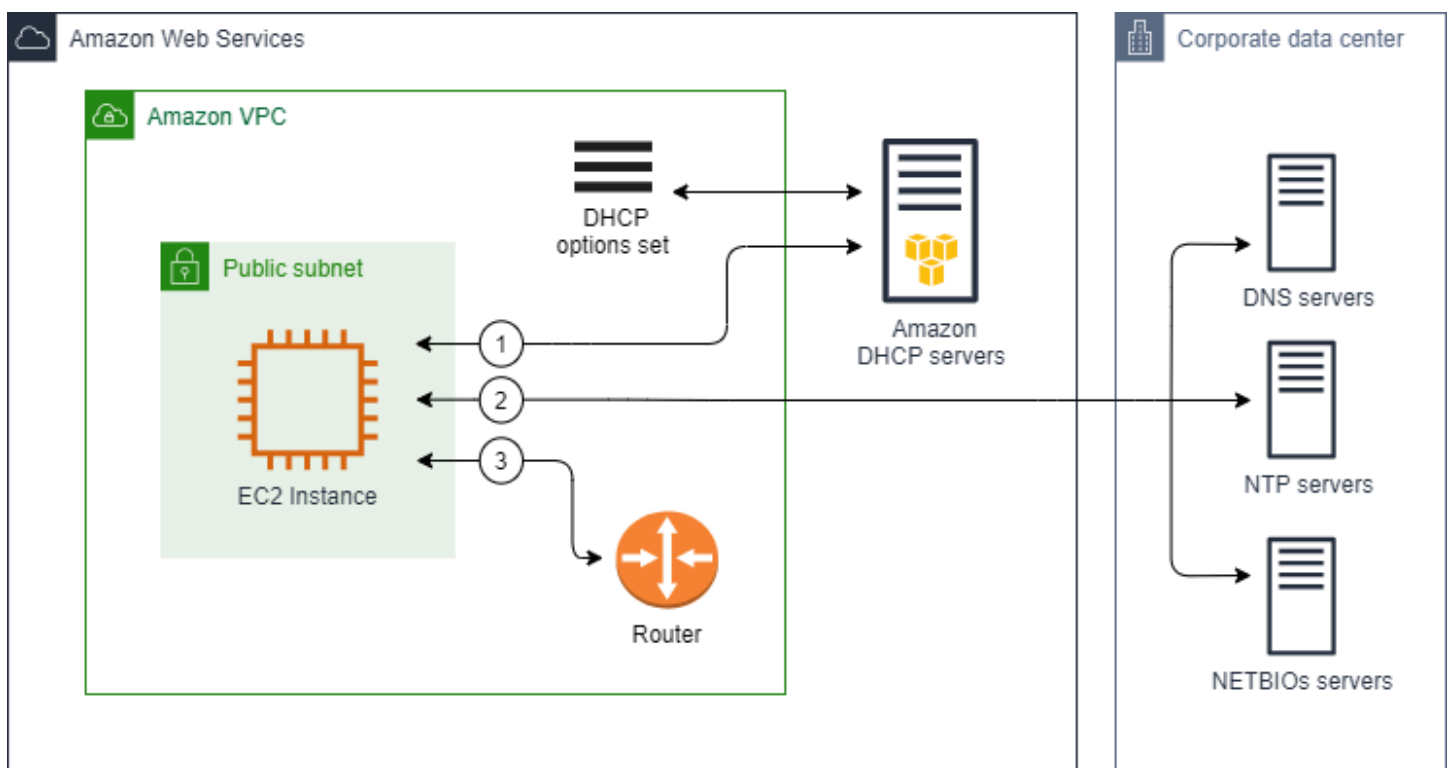
Benutzerdefinierter DHCP-Optionssatz

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

- **Domain-Namensserver:** 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-Namensserver:** Bei EC2-Instances, die Windows ausführen, ist der NetBIOS-Computernamen ein Anzeigename, der der Instance zur Identifizierung im Netzwerk zugewiesen wird. Ein NetBIOS-Namensserver 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) dafür, wie häufig eine laufende Instance, der eine IPv6 zugewiesen ist, eine DHCPv6-Lease-

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

- [Erstellen eines DHCP-Optionssatzes](#)
- [Ändern Sie den Optionssatz, der einer VPC zugeordnet ist](#)
- [Löschen eines DHCP-Optionssatzes](#)

Erstellen eines DHCP-Optionssatzes

Ein benutzerdefinierter DHCP-Optionssatz ermöglicht es Ihnen, Ihre VPC u. a. mit einem eigenen DNS-Server und einem eigenen Domännennamen 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-Optionssatz erstellt.
5. Geben Sie für DHCP-Optionen die benötigten Konfigurationseinstellungen an.
 - Domänenname (optional): Geben Sie den Domännennamen ein, den ein Client beim Auflösen von Hostnamen über DNS verwenden sollte. Wenn Sie AmazonProvidedDNS

nicht verwenden, müssen Ihre benutzerdefinierten Domännennamenserver den Hostnamen entsprechend auflösen. Wenn Sie eine private gehostete Zone von Amazon Route 53 verwenden, können Sie AmazonProvidedDNS verwenden. Weitere Informationen finden Sie unter [DNS-Attribute für Ihre VPC](#).

 Note

Verwenden Sie nur Domännennamen, die Sie vollständig kontrollieren.

Einige Linux-Betriebssysteme akzeptieren mehrere Domännennamen, die durch Leerzeichen getrennt sind. Windows- und andere Linux-Betriebssysteme behandeln den Wert jedoch wie eine einzelne Domäne, was zu unerwartetem Verhalten führen kann. Wenn Ihr DHCP-Optionssatz einer VPC zugeordnet ist, die Instances mit Betriebssystemen enthält, die den Wert als einzelne Domain behandeln, geben Sie nur einen Domain-Namen an.

- Domain name servers (Domännennamenserver) (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 Domännennamenserver eingeben. Wenn Sie beides verwenden, kann es zu unerwartetem Verhalten kommen. Sie können die IP-Adressen von bis zu vier IPv4-Domännennamenservern (oder bis zu drei IPv4-Domännennamenservern und **AmazonProvidedDNS**) und von bis zu vier IPv6-Domännennamenservern eingeben, jeweils getrennt durch Kommata. Obwohl Sie bis zu acht Domännennamenserver angeben können, können einige Betriebssysteme niedrigere Grenzwerte festlegen. Weitere Informationen über AmazonProvidedDNS und den Amazon DNS-Server finden Sie im [Amazon DNS-Server](#).

 Important

Wenn Ihre VPC über ein Internet-Gateway verfügt, stellen Sie sicher, dass Sie Ihren eigenen DNS-Server oder den Amazon DNS-Server (AmazonProvidedDNS) für den Wert der Domain-Namenserver 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 [Einstellen der Zeit für Ihre Instance](#) im Amazon-EC2-Benutzerhandbuch.

- NetBIOS name servers (NetBIOS-Namensserver) (optional): Geben Sie die IP-Adressen von bis zu vier NetBIOS-Namensservern ein.

Bei EC2-Instances, die ein Windows Betriebssystem ausführen, ist der NetBIOS-Computernamen ein Anzeigename, der der Instance zur Identifizierung im Netzwerk zugewiesen wird. Der NetBIOS-Namensserver 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, **2** anzugeben (Punkt-zu-Punkt oder P-Knoten). 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.

- Bevorzugte IPv6-Lease-Zeit (optional): Ein Wert (in Sekunden, Minuten, Stunden oder Jahren) dafür, wie häufig eine laufende Instance, der eine IPv6 zugewiesen ist, eine DHCPv6-Lease-Erneuerung durchläuft. Zulässige Werte liegen zwischen 140 und 2147483647 Sekunden (ungefähr 68 Jahre). Wenn kein Wert eingegeben wird, ist die Standard-Lease-Zeit 140 Sekunden. Wenn Sie die langfristige Adressierung für EC2-Instances verwenden, können Sie die Lease-Dauer verlängern und häufige Anfragen zur Lease-Verlängerung vermeiden. Die Lease-Verlängerung erfolgt in der Regel, wenn die Hälfte der Lease-Zeit 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

- [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

- [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

- [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

- [Grundlagen von Amazon DNS](#)
- [Anzeigen von DNS-Hostnamen für EC2-Instances](#)
- [Anzeigen und Aktualisieren von DNS-Attributen für Ihre VPC](#)

Grundlagen von Amazon DNS

Als AWS-Architekt oder -Administrator ist der Amazon-DNS-Server, auch bekannt als Route 53 Resolver, eine der grundlegenden Netzwerkkomponenten, auf die Sie stoßen werden. Dieser DNS-Resolver-Service ist nativ in jede Availability Zone in Ihrer AWS-Region integriert und bietet eine zuverlässige und skalierbare Lösung für die Auflösung von Domain-Namen in Ihrer Virtual Private Cloud (VPC). In diesem Abschnitt erfahren Sie mehr über die IP-Adressen des Amazon DNS-Servers, die privaten DNS-Hostnamen, die er auflösen kann, und die Regeln für seine Verwendung.

Inhalt

- [Amazon DNS-Server](#)
- [Regeln und Überlegungen](#)
- [DNS-Hostnamen für EC2-Instances](#)
- [DNS-Attribute für Ihre VPC](#)
- [DNS-Kontingente](#)
- [Private gehostete Zonen](#)

Amazon DNS-Server

Der Route 53 Resolver (auch „Amazon-DNS-Server“ oder „AmazonProvidedDNS“ genannt) ist ein DNS-Resolver-Service, der in jede Availability Zone innerhalb 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 2001:db8::/32 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 [verbindungslokale Adresse](#) 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 verbindungslokale IPv4-Adresse (169.254.169.253) immer noch erreichbar, solange „AmazonProvidedDNS“ der Nameserver im DHCP-Optionssatz ist.

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 von DNS-Hostnamen finden Sie unter [Hostnamentypen für Amazon-EC2-Instances](#) im Amazon EC2-Benutzerhandbuch.

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 für EC2-Instances

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 für Ihre VPC](#).

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

Privater IPv4-DNS-Name

Der private IPv4-DNS-Hostname einer Instance wird zu ihrer privaten IPv4-Adresse aufgelöst. Sie können den Hostnamen für den privaten IPv4-DNS-Namen zur Kommunikation zwischen Instances im selben VPC oder in verbundenen VPCs verwenden. Weitere Informationen finden Sie unter [Private IPv4-Adressen](#) im Amazon-EC2-Benutzerhandbuch.

Öffentlicher IPv4-DNS-Name

Der öffentliche IPv4-DNS-Hostname einer Instance wird zu ihrer öffentlichen IPv4-Adresse (außerhalb des Netzwerks der Instance) oder ihrer privaten IPv4-Adresse (innerhalb des Netzwerks der Instance) aufgelöst. Weitere Informationen finden Sie unter [Öffentliche IPv4-Adressen](#) im Amazon-EC2-Benutzerhandbuch.

Um öffentliche IPv4-DNS-Namen über eine VPC-Peering-Verbindung in private IPv4-Adressen aufzulösen, müssen Sie die DNS-Auflösung für die Peering-Verbindung aktivieren. Weitere Informationen finden Sie unter [Aktivieren einer DNS-Auflösung für eine VPC-Peering-Verbindung](#).

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 über RBN finden Sie unter [Hostnamentypen für Amazon-EC2-Instances](#) im Amazon-EC2-Benutzerhandbuch.

DNS-Attribute für Ihre 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
<code>enableDnsHostnames</code>	Bestimmt, ob die VPC das Zuweisen öffentlicher DNS-Hostnamen zu Instances mit öffentlichen IP-Adressen unterstützt. Der Standardwert für dieses Attribut ist <code>false</code>, es sei denn, die VPC ist eine Standard-VPC. Beachten Sie die Regeln und Überlegungen unten für dieses Attribut.
<code>enableDnsSupport</code>	Bestimmt, ob die VPC die DNS-Auflösung über den von Amazon bereitgestellten DNS-Server unterstützt. Wenn dieses Attribut <code>true</code> 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 <code>true</code>. Beachten Sie die Regeln und Überlegungen unten für dieses Attribut.

Regeln und Überlegungen

- Wenn beide Attribute `true` sind, geschieht Folgendes:
 - Instances mit öffentlichen IP-Adressen erhalten entsprechende öffentliche DNS-Hostnamen.
 - Der 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.
 - Der Route 53 Resolver kann von Amazon bereitgestellte private DNS-Hostnamen nicht auflösen.
 - Instances erhalten benutzerdefinierte private DNS-Hostnamen, wenn die [DHCP-Optionsliste](#) einen benutzerdefinierten Domain-Namen enthält. Wenn Sie den Route 53 Resolver-Server nicht verwenden, müssen Ihre benutzerdefinierten Domänennamensserver 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.
- Der Route 53 Resolver kann private DNS-Hostnamen für alle Adressräume zu privaten IPv4-Adressen auflösen. Dies gilt auch für IPv4-Adressbereiche einer VPC, die außerhalb des durch [RFC 1918](#) festgelegten privaten IPv4-Adressbereichs liegen. Falls Sie Ihre VPC jedoch vor Oktober 2016 erstellt haben, löst der 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 [Support](#).

DNS-Kontingente

Für Services, die [verbindungslokale Adressen](#) verwenden, gilt eine Obergrenze von 1 024 Paketen pro Sekunde (PPS). Dieses Limit umfasst die Summe von Route 53 Resolver-DNS-Abfragen, [Instance Metadata Service \(IMDS\)](#)-Anfragen, [Amazon Time Service Network Time Protocol \(NTP\)](#)-Anfragen und [Windows Licensing Service-Anfragen \(für Microsoft Windows-basierte Instances\)](#). 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](#). Anweisungen zum Abrufen von Instance-Metadaten finden Sie unter [Instance-Metadaten abrufen](#) im Amazon EC2-Benutzerhandbuch.

Private gehostete Zonen

Wenn Sie anstelle der privaten IPv4-Adressen oder der von AWS bereitgestellten privaten DNS-Domain-Namen über benutzerdefinierte DNS-Domainnamen wie `example.com` auf die Ressourcen in Ihrer VPC zugreifen möchten, können Sie eine privat 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.

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. Es ist wichtig, diese Hostnamen zu kennen, um eine Verbindung zu Ihren Ressourcen herzustellen.

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 für Ihre 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

- [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

- [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. Mit diesen Einstellungen wird gesteuert, ob Ihre Instances öffentliche DNS-Hostnamen erhalten und ob der Amazon-DNS-Server Ihre privaten DNS-Namen auflösen kann. Die korrekte

Konfiguration dieser Attribute ist für eine reibungslose Kommunikation innerhalb Ihrer VPC von entscheidender Bedeutung.

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.

Details	CIDRs	Flow logs	Tags
Details			
VPC ID  vpc-e03dd489	State  Available	DNS hostnames Enabled	DNS resolution Enabled

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

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

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

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

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 maximale 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, damit sie nicht über die NAU-Kontingentgrenzen hinauswächst. 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
Alle privaten oder öffentlichen IPv4-Adressen und alle IPv6-Adressen, die einer Netzwerkschnittstelle für eine EC2-Instance in der VPC zugewiesen sind	1
An Instances angefügte, zusätzliche EC2-Netzwerkschnittstellen	1
Der Netzwerkschnittstelle zugewiesenes Präfix	1
Network Load Balancer pro AZ	6
Gateway Load Balancer pro AZ	6
VPC-Endpunkt pro AZ	6
Transit-Gateway-Anhang	6
Lambda-Funktion	6
NAT-Gateway	6
EFS-Mounting-Ziel	6
EFA-Schnittstelle (EFA mit einem ENA-Gerät) oder eine reine EFA-Schnittstelle	1
Amazon-EKS-Pod	1

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
- Standard-NAU-Kontingent pro VPC: 64 000 Einheiten

Freigeben Ihrer VPC-Subnetze für andere Konten

Durch die Freigabe des VPC-Subnetzes können mehrere AWS-Konten ihre Anwendungsressourcen wie Amazon-EC2-Instances und Amazon-RDS-Datenbanken (Relational Database Service), Amazon-Redshift-Cluster und AWS Lambda-Funktionen in freigegebenen, zentral verwalteten Virtual Private Clouds (VPCs) erstellen. In diesem Modell gibt das Konto, das die VPC besitzt (Eigentümer), ein oder mehrere Subnetze für andere Konten (Teilnehmer) frei, die zu derselben Organisation von gehöre 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 VPC-Subnetze freigeben, 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 weiter vereinfachen, indem Sie freigegebene Amazon VPC-Subnetze über Konnektivitätsfeatures wie AWS PrivateLink, Transit-Gateways und VPC Peering miteinander verbinden. Weitere Informationen zu den Vorteilen der VPC-Subnetz-Freigabe finden Sie unter [VPC-Freigabe: Ein neuer Ansatz für mehrere Konten und für die VPC-Verwaltung](#).

Es gibt Quoten für die VPC-Subnetz-Freigabe. Weitere Informationen finden Sie unter [VPC-Subnetz-Freigabe](#).

Inhalt

- [Voraussetzungen für die Arbeit mit freigegebenen Subnetzen](#)
- [Arbeiten mit freigegebenen Subnetzen](#)
- [Fakturierung und Messung für den Eigentümer und Teilnehmer](#)
- [Verantwortlichkeiten und Berechtigungen für Besitzer und Teilnehmer](#)
- [AWS-Ressourcen und freigegebene VPC-Subnetze](#)

Voraussetzungen für die Arbeit mit freigegebenen Subnetzen

Dieser Abschnitt enthält die Voraussetzungen für die Arbeit mit freigegebenen Subnetzen:

- Die Konten für den VPC-Eigentümer und -Teilnehmer müssen von AWS Organizations verwaltet werden.

- Sie müssen die Ressourcenfreigabe in der AWS RAM-Konsole über das Hauptkonto Ihrer Organisation ermöglichen. Weitere Informationen finden Sie unter [Ressourcenfreigabe für AWS Organizations aktivieren](#) im AWS RAM-Benutzerhandbuch.
- Sie müssen eine Ressourcenfreigabe erstellen. Sie können bei der Erstellung der Ressourcenfreigabe angeben, welche Subnetze freigegeben werden sollen, oder Sie können später mithilfe des Verfahrens im nächsten Abschnitt die Subnetze zur Ressourcenfreigabe hinzufügen. Weitere Informationen finden Sie unter [Erstellen einer Ressourcenfreigabe](#) im AWS RAM-Benutzerhandbuch.

Arbeiten mit freigegebenen Subnetzen

In diesem Abschnitt wird beschrieben, wie freigegebene Subnetze in der AWS-Konsole und AWS CLI verwendet werden.

Inhalt

- [Freigeben eines Subnetzes](#)
- [Freigeben eines freigegebenen Subnetzes rückgängig machen](#)
- [Identifizieren des Eigentümers eines freigegebenen Subnetzes](#)

Freigeben eines Subnetzes

Sie können Nichtstandard-Subnetze für andere Konten innerhalb Ihrer Organisation wie folgt freigeben. Darüber hinaus können Sie Sicherheitsgruppen unternehmensweit über AWS Organizations hinweg freigeben. Weitere Informationen finden Sie unter [Sicherheitsgruppen mit AWS Organizations teilen](#).

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.

Ein Subnetz unter Verwendung der freigebe AWS CLI

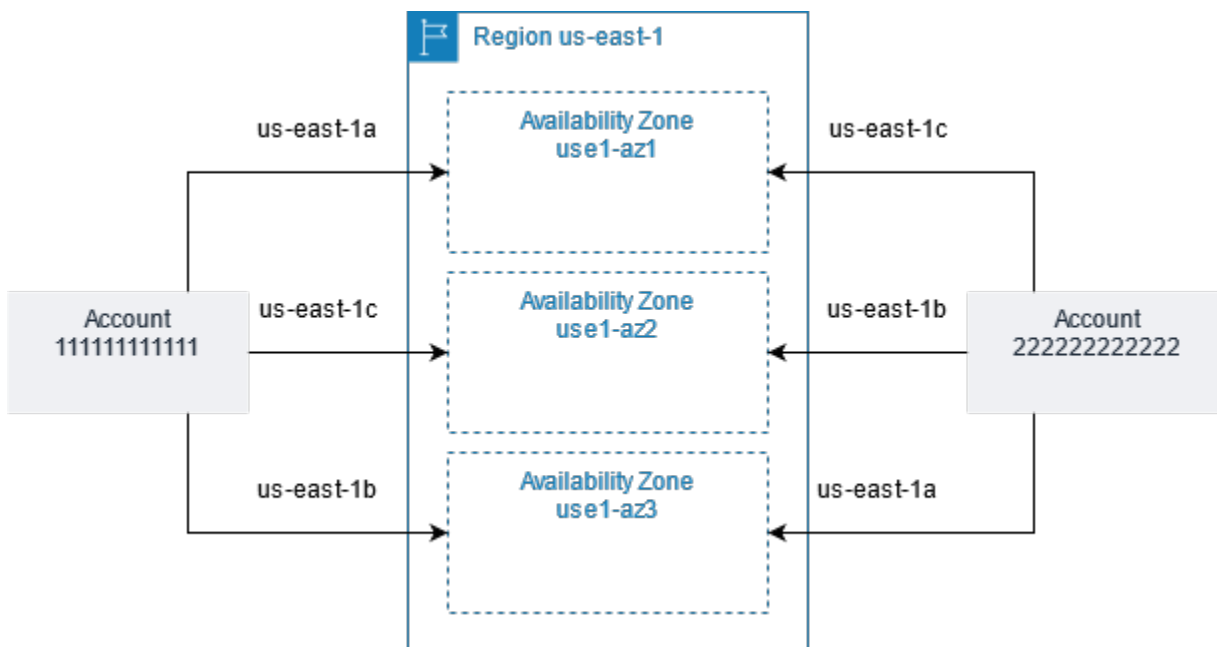
Verwenden Sie die Befehle [create-resource-share](#) und [associate-resource-share](#).

Zuweisung von Subnetzen über Availability Zones hinweg

Um sicherzustellen, dass Ressourcen auf die Availability Zones einer Region verteilt sind, ordnen wir Availability Zones einzelnen Namen für jedes Konto zu. So befindet sich die Availability Zone us-east-1a für Ihr AWS-Konto möglicherweise nicht im selben Ort 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:

- Vorhandene Teilnehmerressourcen werden weiterhin im nicht länger freigegebenen Subnetz ausgeführt. AWS Managed Services (z. B. Elastic Load Balancing) mit automatisierten/verwalteten

Workflows (wie Auto Scaling oder Ersetzen von Knoten) 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.

Die Freigabe eines Subnetzes unter Verwendung der aufhebe AWS CLI

Verwenden Sie den Befehl [disassociate-resource-share](#).

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.

Identifizieren des Eigentümers eines Subnetzes mithilfe der AWS CLI

Verwenden Sie die Befehle [describe-subnets](#) und [describe-vpcs](#), in deren Ausgabe die ID des Besitzers enthalten ist.

Fakturierung und Messung für den Eigentümer und Teilnehmer

Dieser Abschnitt enthält Fakturierungs- und Nutzungsdetails für diejenigen, denen das freigegebene Subnetz gehört, und für diejenigen, die mit dem freigegebenen Subnetz arbeiten:

- In einer gemeinsam genutzten VPC bezahlt jeder Teilnehmer seine Anwendungsressourcen, einschließlich Amazon EC2-Instances, Amazon Relational Database Service-Datenbanken, Amazon Redshift-Clustern und AWS Lambda-Funktionen. Teilnehmer zahlen darüber hinaus Datenübertragungskosten für Datenübertragungen zwischen Availability Zones sowie für Datenübertragungen über VPC-Peering-Verbindungen, Internet-Gateways und AWS Direct Connect-Gateways.
- VPC-Eigentümer zahlen Stundennutzungsgebühren (wenn zutreffend), Gebühren für die Datenverarbeitung und die Datenübertragung über NAT-Gateways, Virtual Private Gateways, Transit-Gateways, AWS PrivateLink- und VPC-Endpunkte. Zudem werden öffentliche IPv4-Adressen, die in freigegebenen VPCs verwendet werden, den VPC-Eigentümern in Rechnung gestellt. Weitere Informationen zur Preisgestaltung für öffentliche IPv4-Adressen finden Sie auf der Registerkarte Öffentliche IPv4-Adresse auf der Seite [Preise für Amazon VPC](#).
- 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

Dieser Abschnitt enthält detaillierte Informationen zu den Verantwortlichkeiten und Berechtigungen für diejenigen, denen das freigegebene Subnetz gehört (Eigentümer), und für diejenigen, die das freigegebene Subnetz verwenden (Teilnehmer).

Besitzer-Ressourcen

Eigentümer sind für die VPC-Ressourcen verantwortlich, die sie besitzen. 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, Route-53-Resolver-Endpunkte, Internet-Gateways, NAT-Gateways, Virtual Private Gateways und Transit Gateway-Anhänge.

Teilnehmer-Ressourcen

Teilnehmer sind für die VPC-Ressourcen verantwortlich, die sie besitzen. 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-Subnetz-Freigabe](#).

VPC-Ressourcen

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

Flow-Protokolle

- Teilnehmer können Flow-Protokolle für Netzwerkschnittstellen, deren Eigentümer sie sind, in einem freigegebenen VPC-Subnetz erstellen, löschen und beschreiben.
- Teilnehmer können Flow-Protokolle für Netzwerkschnittstellen, deren Eigentümer sie nicht sind, in einem freigegebenen VPC-Subnetz nicht erstellen, löschen oder beschreiben.
- Teilnehmer können für ein freigegebenes VPC-Subnetz keine Flow-Protokolle erstellen, löschen oder beschreiben.
- VPC-Eigentümer können Flow-Protokolle für Netzwerkschnittstellen, deren Eigentümer sie nicht sind, in einem freigegebenen VPC-Subnetz erstellen, löschen und beschreiben.
- VPC-Eigentümer können Flow-Protokolle für ein freigegebenes VPC-Subnetz erstellen, löschen und beschreiben.
- VPC-Eigentümer können von einem Teilnehmer erstellte Flow-Protokolle 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. Teilnehmer können Internet-Gateways in einem freigegebenen VPC-Subnetz beschreiben. Teilnehmer können Internet-Gateways für ausgehenden Verkehr in einem freigegebenen VPC-Subnetz nicht beschreiben.

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-Eigentümer können Netzwerkschnittstellen beschreiben, die Teilnehmern in einem freigegebenen VPC-Subnetz gehören. VPC-Eigentümer können nicht auf andere Weise mit Netzwerkschnittstellen arbeiten, die den Teilnehmern gehören, z. B. Anhängen, Trennen oder Ändern der Netzwerkschnittstellen, die den Teilnehmern in einem freigegebenen 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

- Teilnehmer können Regeln für eingehenden und ausgehenden Datenverkehr für eigene Sicherheitsgruppen in einem freigegebenen VPC-Subnetz erstellen, löschen, beschreiben oder

ändern. Teilnehmer können mit Sicherheitsgruppen arbeiten, die von VPC-Besitzern erstellt wurden, wenn [der VPC-Besitzer die Sicherheitsgruppe für den Teilnehmer freigegeben hat](#).

- Teilnehmer können Regeln in den Sicherheitsgruppen erstellen, deren Besitzer sie sind und die auf Sicherheitsgruppen, die anderen Teilnehmern oder dem VPC-Besitzer gehören, wie folgt verweisen: account-number/security-group-id
- Teilnehmer können keine Instances mit der Standard-Sicherheitsgruppe für die VPC starten, da diese dem Besitzer gehört.
- Teilnehmer können keine Instances mit Nicht-Sicherheitsgruppen starten, die anderen Teilnehmern oder dem VPC-Besitzer gehören, sofern die Sicherheitsgruppe [für sie freigegeben ist](#).
- VPC-Besitzer können Sicherheitsgruppen beschreiben, die von Teilnehmern in einem gemeinsam genutzten VPC-Subnetz erstellt wurden. VPC-Besitzer können auf keine 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 für andere Konten oder Organisationseinheiten in derselben Organisation von AWS Organizations freigeben. 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.

- Teilnehmer können ihre eigenen Sicherheitsgruppen mit einer freigegebenen VPC verknüpfen. Auf diese Weise kann der Teilnehmer die Sicherheitsgruppe mit Elastic Network-Schnittstellen verwenden, die er in der freigegebenen VPC besitzt.

AWS-Ressourcen und freigegebene VPC-Subnetze

Die folgenden AWS-Services unterstützen Ressourcen in freigegebenen VPC-Subnetzen. Weitere Informationen finden Sie unter den Links zur entsprechenden Servicedokumentation.

- [Amazon Aurora](#)
- [AWS Database Migration Service](#)
- [Amazon-EC2](#)
- [Amazon ECS](#)
- Amazon ElastiCache (Redis OSS)
- [Amazon EFS](#)
- [Amazon Elastic Kubernetes Service](#)
- Elastic Load Balancing
 - [Application Load Balancer](#)
 - [Gateway Load Balancers](#)
 - [Network Load Balancers](#)
- [Amazon EMR](#)
- [AWS Glue](#)
- AWS Lambda
- Amazon MQ mit Apache MQ (nicht Rabbit MQ)
- Amazon MSK
- AWS Network Manager
 - [AWS Cloud-WAN](#)
 - [Network Access Analyzer](#)
 - [Reachability Analyzer](#)
- Amazon OpenSearch Service
- [AWS PrivateLink[†]](#)

- [Amazon Relational Database Service \(RDS\)](#)
- [Amazon Redshift](#)
- [Amazon Route 53](#)
- [Amazon SageMaker Unified Studio](#)
- [AWS Transit Gateway](#)
- [AWS Verified Access](#)
- Amazon VPC
 - [Peering](#)
 - [Datenverkehrsspiegelung](#)
- [Amazon VPC Lattice](#)

† Über einen VPC-Endpunkt in einer freigegebenen VPC können Sie eine Verbindung zu allen AWS-Services herstellen, die PrivateLink unterstützen. Eine Liste der Services, die PrivateLink unterstützen, finden Sie unter [AWS-Services, die sich mit AWS PrivateLink integrieren lassen](#) im Handbuch von AWS PrivateLink.

In dieser Liste sollen alle Services aufgeführt werden, die das Starten von Ressourcen in freigegebenen VPC-Subnetzen unterstützen. Trotz unserer besten Bemühungen gibt es möglicherweise Services, die das Starten von Ressourcen in freigegebenen VPC-Subnetzen unterstützen und hier nicht aufgeführt sind. Wenn Sie Fragen haben, können Sie gern Feedback zu Dokumentationen senden.

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 lokale 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.

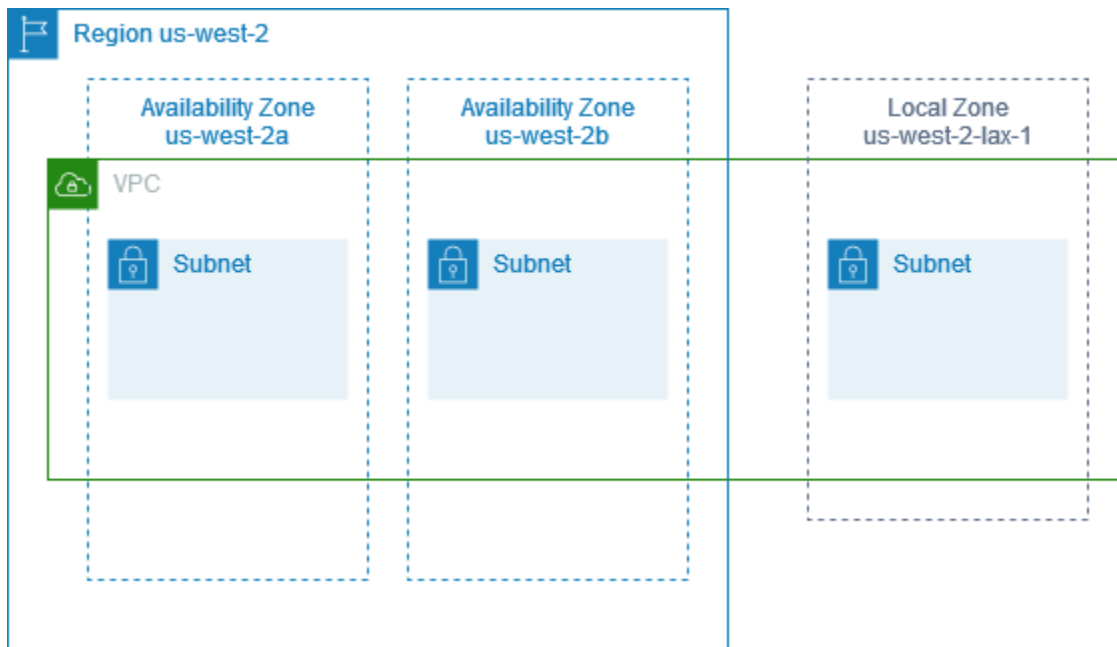
Subnetze in AWS Local Zones

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 Netzwerkgranzgruppe für die Adressen festlegen, die die Adressen auf die Gruppe beschränkt. Wenn Sie eine Netzwerkgranzgruppe festlegen, können die IP-Adressen nicht zwischen Netzwerkgranzgruppen 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 Netzwerkgranzgruppe, 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 Netzwerkgranzgruppe 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 Netzwerkgranzgruppe 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 Direct Connect-Standort in einer Region. Das On-Premises-Rechenzentrum hat eine Direct Connect-Verbindung zum Direct Connect-Standort.

Note

Datenverkehr, 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 Subnetzdetaill in der Amazon-VPC-Konsole anzeigen oder den Befehl [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 Direct Connect-Benutzerhandbuch.

- Ein Direct Connect-Gateway Informationen zum Erstellen eines Direct Connect-Gateways finden Sie unter [Erstellen eines Direct Connect Gateway](#) im 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 Direct Connect-Benutzerhandbuch.
- Eine private virtuelle Schnittstelle für die Verbindung vom 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 Direct Connect-Benutzerhandbuch.

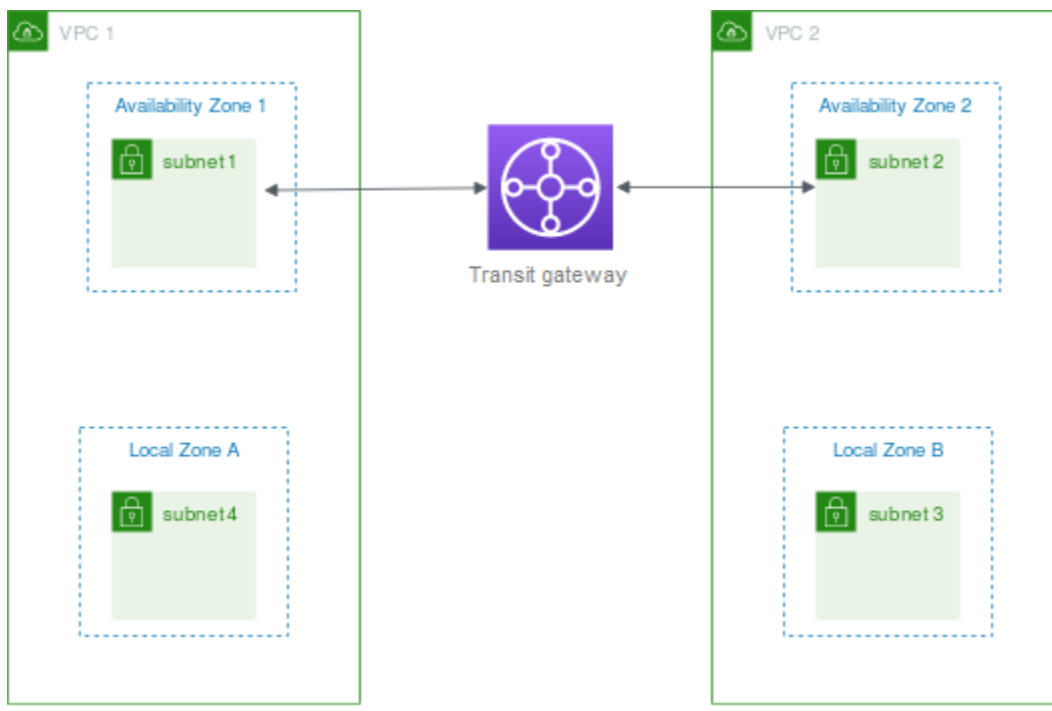
Verbinden von Subnetzen der Local Zone mit einem Transit-Gateway

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 den Subnetz-Routing-Tabellen der Local Zone-Subnetze 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.

Bestimmungsort	Ziel
<i>VPC 1 CIDR</i>	<i>Lokal</i>
<i>VPC 2 CIDR</i>	<i>vpc1-attachment-network-interface-id</i>

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

Bestimmungsort	Ziel
<i>VPC 2 CIDR</i>	<i>Lokal</i>
<i>VPC 1 CIDR</i>	<i>vpc2-attachment-network-interface-id</i>

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
<i>VPC 1 CIDR</i>	<i>Anhang für VPC 1</i>	verbreitet

CIDR	Attachment	Routing-Typ
<i>VPC 2 CIDR</i>	<i>Anhang für VPC 2</i>	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 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 den Befehl [describe-availability-zones](#), um die übergeordnete Zone zu suchen.
- 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.

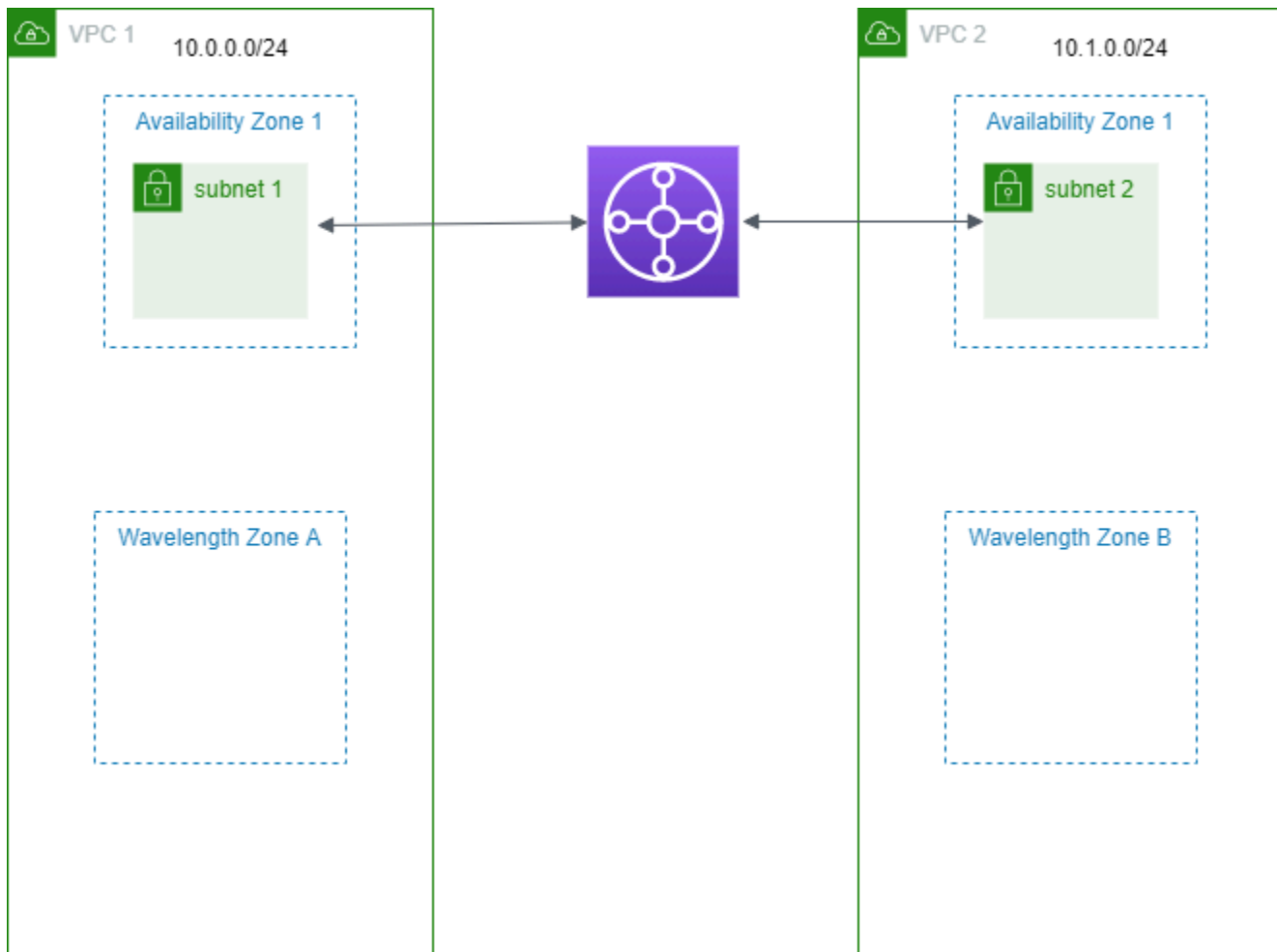
- Einträge für jede VPC in der Routingtabelle des Transit-Gateways. Informationen zum Erstellen von Transit Gateway-Routen finden Sie unter [Transit Gateway-Routing-Tabellen](#) im Amazon VPC Transit Gateways-Handbuch.
- Für jede VPC ein Eintrag in der VPC-Routing-Tabelle, der das andere VPC-CIDR als 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-222222222222222222

Die Routingtabelle für VPC 2 hat den folgenden Eintrag:

Zielbereich	Ziel
10.0.0.0/24	tgw-222222222222222222



Subnetze in AWS Outposts

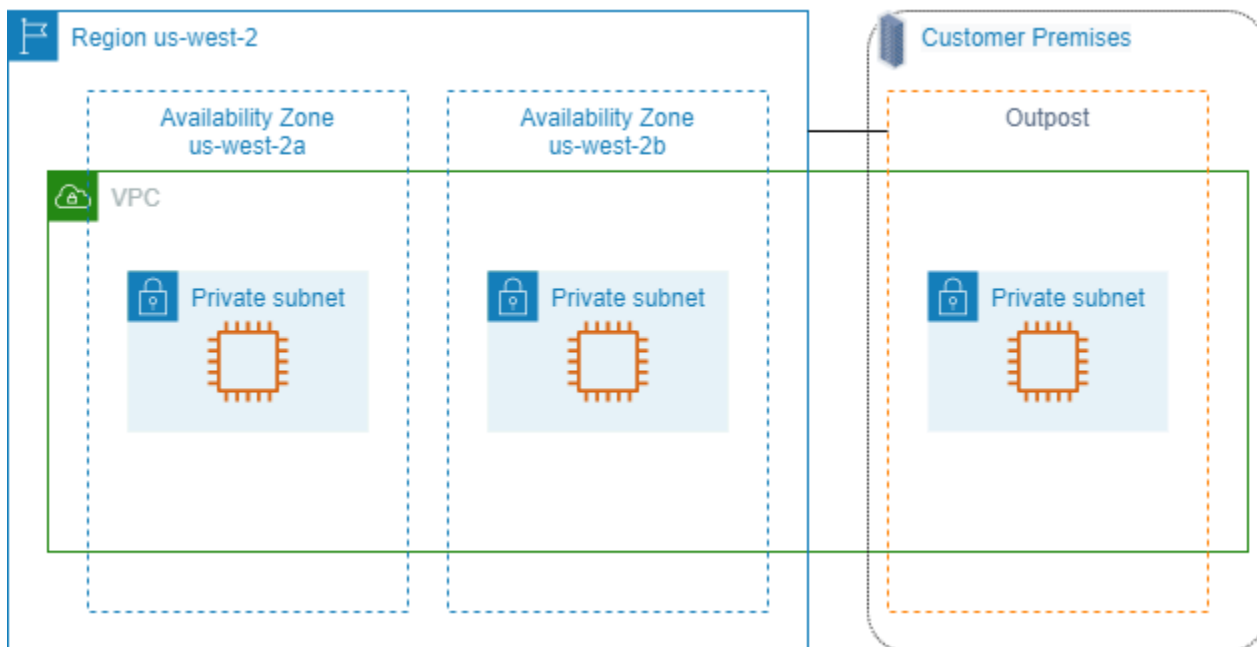
AWS Outposts bietet Ihnen die gleiche AWS-Hardwareinfrastruktur, Services, APIs und Tools zum Erstellen und Ausführen Ihrer Anwendungen On-Premises und in der Cloud. AWS Outposts ist ideal für Workloads geeignet, die einen Zugriff mit niedriger Latenz auf On-Premises-Anwendungen oder -Systeme benötigen, 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.

Note

Wenn Sie ein [Flow-Protokoll](#) für die VPC erstellt haben, die Sie löschen, beachten Sie, dass Flow-Protokolle für gelöschte VPCs irgendwann automatisch entfernt werden.

Inhalt

- [Löschen einer VPC mithilfe der Konsole](#)
- [Eine VPC mithilfe einer Befehlszeile löschen](#)

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 [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 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 mithilfe der 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
```

Generieren von Infrastructure as Code aus Ihren VPC-Konsolenaktionen mit Console-to-Code

Die Konsole bietet eine Anleitung zum Erstellen von Ressourcen und zum Testen von Prototypen. Wenn Sie dieselben Ressourcen in großem Umfang erstellen möchten, benötigen Sie Automatisierungscode. Console-to-Code ist ein Feature von Amazon Q Developer, die Ihnen den Einstieg in Automatisierungscode erleichtern kann. Console-to-Code zeichnet Ihre Konsolenaktionen auf, einschließlich Standardwerten und kompatiblen Parametern. Anschließend wird mithilfe generativer KI Code in Ihrem bevorzugten Infrastructure as Code (IaC)-Format für die gewünschten Aktionen vorgeschlagen. Da der Konsolen-Workflow sicherstellt, dass die von Ihnen angegebenen Parameterwerte zusammen gültig sind, hat der mithilfe von Console-to-Code generierte Code

kompatible Parameterwerte. Sie können den Code als Ausgangspunkt verwenden und ihn dann so anpassen, dass er für Ihren speziellen Anwendungsfall produktionsbereit ist.

Mit Console-to-Code können Sie sich z. B. selbst aufzeichnen, indem Sie die VPC-Konsole verwenden, um Subnetze, Sicherheitsgruppen, NACLs, eine benutzerdefinierte Routing-Tabelle und ein Internet-Gateway zu erstellen und Code im JSON-Format zu generieren. CloudFormation Anschließend können Sie diesen Code kopieren und für die Verwendung in Ihrer CloudFormation-Vorlage anpassen.

Console-to-Code kann derzeit Infrastructure as Code (IaC) in den folgenden Sprachen und Formaten generieren:

- CDK Java
- CDK Python
- CDK TypeScript
- CloudFormation JSON
- CloudFormation YAML

Weitere Informationen und Anweisungen zur Verwendung von Console-to-Code finden Sie unter [Automatisieren von AWS-Services mit Console-to-Code von Amazon Q Developer](#) im Amazon-Q-Developer-Benutzerhandbuch.

Subnetze für Ihre VPC

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

Inhalt

- [Subnetze-Grundlagen](#)
- [Subnetzsicherheit](#)
- [Erstellen eines Subnetzes](#)
- [Hinzufügen oder Entfernen eines IPv6-CIDR-Blocks aus Ihrem Subnetz](#)
- [Ändern der IP-Adressierungsattribute Ihres Subnetzes](#)
- [Subnetz-CIDR-Reservierungen](#)
- [Konfigurieren von Routing-Tabellen](#)
- [Middlebox-Routing-Assistent](#)
- [Löschen eines Subnetzes](#)

Subnetze-Grundlagen

Jedes Subnetz muss sich vollständig innerhalb einer Availability Zone befinden und darf nicht mehrere Zonen umfassen. Weil AWS-Ressourcen in separaten Availability Zones gestartet werden, können Sie Ihre Anwendungen vor den Fehlern einer einzelnen Zone schützen.

Inhalt

- [Subnetz-IP-Adressbereiche](#)
- [Subnetz-Typen](#)
- [Subnetzdiagramm](#)
- [Subnetz-Routing](#)
- [Subnetz-Einstellungen](#)

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 Services verwendet, die nur in der VPC verfügbar sind. Beispiele finden Sie unter [Verbindungslokale Adressen](#) im Amazon-EC2-Benutzerhandbuch.

Weitere Informationen finden Sie unter [IP-Adressierung für Ihre VPCs und Subnetze](#).

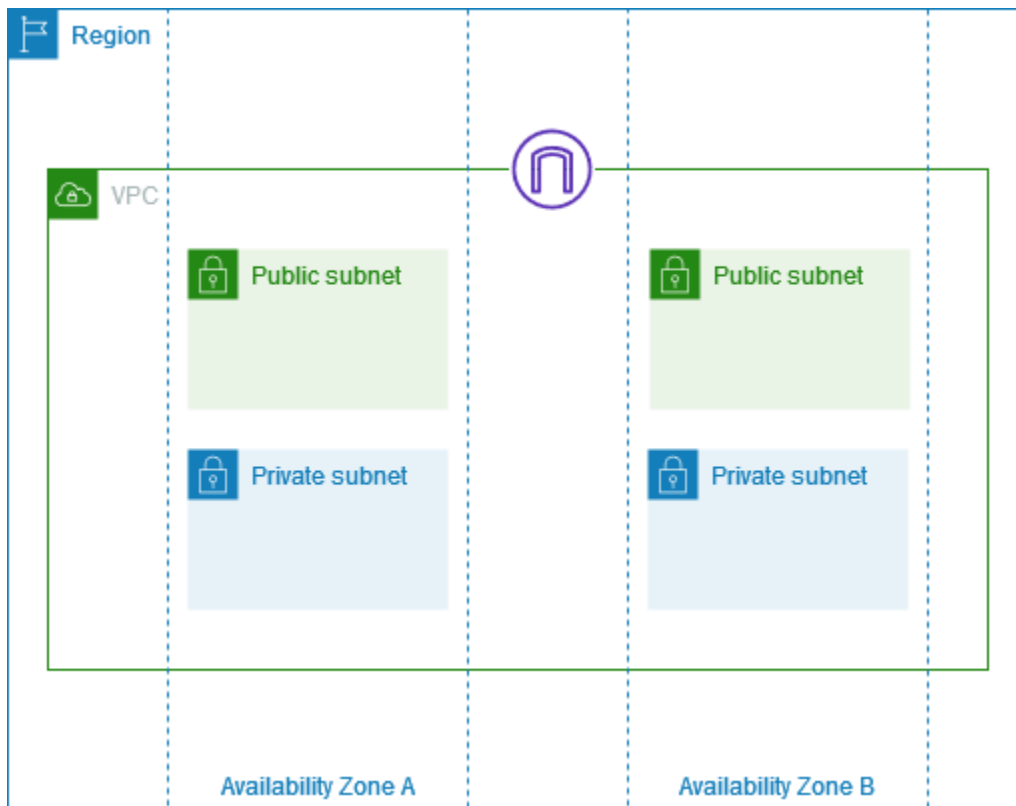
Subnetz-Typen

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

- 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.
- EVS-Subnetz: Dieser Subnetztyp wird mit Amazon EVS erstellt. Weitere Informationen finden Sie unter [VLAN-Subnetz](#) im Benutzerhandbuch für Amazon EVS.

Subnetzdiagramm

Das folgende Diagramm zeigt eine VPC mit Subnetzen in zwei Availability Zones und einem Internet-Gateway. Jede Availability Zone hat ein öffentliches Subnetz und ein privates Subnetz.



Diagramme, die Subnetze in Local Zones und Wavelength Zones zeigen, finden Sie unter [Funktionsweise von AWS Local Zones](#) und [Funktionsweise von AWS Wavelength](#).

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 festgelegt wird, ob eine in einem Subnetz erstellte Netzwerkschnittstelle einer öffentlichen IPv4-Adresse, und falls zutreffend, einer IPv6-Adresse zugeordnet ist. Dazu zählt auch die primäre Netzwerkschnittstelle (z. B. 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-Instances](#) im Amazon-EC2-Benutzerhandbuch.

Subnetzsicherheit

Um Ihre AWS-Ressourcen zu schützen, empfehlen wir, 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 stellt Funktionen bereit, mit denen Sie die Sicherheit für die Ressourcen in Ihrer VPC steigern 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 Sie 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 [Steuerung des Datenverkehrs in Subnetzen mithilfe von Zugriffskontrolllisten für Netzwerke](#).

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. Unter Availability Zone können Sie eine Zone für das Subnetz auswählen. Alternativ können Sie die Standardeinstellung No Preference (Keine Präferenz) beibehalten, damit AWS eine Zone für Sie auswählt.

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 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.
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.

Wie Sie ein Subnetzes zu Ihrer VPC unter Verwendung der AWS CLI hinzufügen

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 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 [Ändern der IP-Adressierungsattribute Ihres Subnetzes](#).
- 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 [Steuerung des Datenverkehrs in Subnetzen mithilfe von Zugriffskontrolllisten für Netzwerke](#).
- Geben Sie das Subnetz für andere Konten frei. Weitere Informationen finden Sie unter [???](#).

Hinzufügen oder Entfernen eines IPv6-CIDR-Blocks aus 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.

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-Block 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.

So können Sie einen IPv6-CIDR-Block zu einem Subnetz hinzufügen oder daraus 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. Um eine CIDR hinzuzufügen, wählen Sie Add IPv6 CIDR aus, wählen Sie einen VPC-CIDR-Block aus, geben Sie einen Subnetz-CIDR-Block ein, und wählen Sie eine Netzmaskenlänge, die der Netzmaskenlänge der 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.
5. Um eine CIDR zu entfernen, suchen Sie den IPv6-CIDR-Block und wählen Sie Entfernen.

6. Wählen Sie Speichern.

Zuordnen eines IPv6-CIDR-Blocks einem Subnetz mit Hilfe der AWS CLI

Verwenden Sie den Befehl [associate-subnet-cidr-block](#).

So heben Sie die Zuordnung eines IPv6-CIDR-Blocks von einem Subnetz mit Hilfe der AWS CLI auf

Verwenden Sie den Befehl [disassociate-subnet-cidr-block](#).

Ändern der IP-Adressierungsattribute 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 `false`. Sie können dieses Attribut mit der Amazon VPC-Konsole ändern.

Standardmäßig ist das IPv6-Adressierungsattribut aller Subnetze auf `false` eingestellt. 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.

So ändern Sie das IP-Adressierungsverhalten 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.
5. 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.

So ändern Sie ein Subnetzattribut mit der AWS CLI

Verwenden Sie den Befehl [modify-subnet-attribute](#).

Subnetz-CIDR-Reservierungen

Eine Subnetz-CIDR-Reservierung ist ein Bereich von IPv4- oder IPv6-Adressen, den Sie beiseite legen, damit AWS sie nicht Ihren Netzwerkschnittstellen zuweist. 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: Ermöglicht Ihnen, einer einzelnen Netzwerkschnittstelle ein Präfix zuzuweisen. Weitere Informationen finden Sie unter [Zuweisen von Präfixen zu Amazon-EC2-Netzwerkschnittstellen](#) im Amazon-EC2-Benutzerhandbuch.
- Explizit: Ermöglicht Ihnen, eine individuelle IP-Adresse einer einzelnen Netzwerkschnittstelle manuell zuzuweisen.

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 überschneiden.
- 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, stehen die ungenutzten IP-Adressen für AWS zur Zuweisung an Ihre Netzwerkschnittstellen zur Verfügung. Durch das Löschen einer Subnetzreservierung wird die Zuweisung der verwendeten IP-Adressen nicht aufgehoben.
- Der Reservierungstyp wirkt sich auf die Anzahl der verfügbaren IP-Adressen für das Subnetz aus. Wenn Sie eine Präfix-Reservierung erstellen, nimmt die Anzahl sofort ab. Wenn Sie eine explizite Präfix-Reservierung erstellen, nimmt die Anzahl ab, wenn die IP-Adressen zugewiesen werden.

Weitere Informationen zur CIDR-Notation (Classless Inter-Domain Routing) finden Sie unter [IP-Adressierung](#).

Inhalt

- [Arbeiten mit Subnetz-CIDR-Reservierungen mithilfe der Konsole](#)
- [Arbeiten mit Subnetz-CIDR-Reservierungen mithilfe von AWS CLI](#)

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 mit Subnetz-CIDR-Reservierungen mithilfe von AWS CLI

Sie können die AWS CLI verwenden, um Subnetz-CIDR-Reservierungen 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 dient als Datenverkehrs-Controller für Ihre Virtual Private Cloud (VPC). Jede Routing-Tabelle enthält Regeln, sogenannte Routen, die festlegen, wohin der Netzwerkverkehr von Ihrem Subnetz oder Gateway geleitet wird. Wenn Sie eine VPC erstellen, erstellen wir auch die Haupt-Routing-Tabelle für die VPC. Sie können zusätzliche Routing-Tabellen für Ihre VPC erstellen, damit Sie die Netzwerkpfade für Ihre VPC genauer steuern können.

Über Routing-Tabellen können Sie angeben, mit welchen Netzwerken Ihre VPC kommunizieren darf, z. B. mit anderen VPCs oder On-Premises-Netzwerken. Für jede Route wird eine Zieladresse (CIDR-Block- oder Präfixliste) und ein Ziel (z. B. ein Internet-Gateway, ein NAT-Gateway, eine VPC-Peering-Verbindung oder eine VPN-Verbindung) angegeben. Der Datenverkehr wird auf der Grundlage der Ziel-IP-Adresse an Ziele weitergeleitet. Mit Routing-Tabellen können Sie komplexe Netzwerkarchitekturen erstellen, die öffentliche Subnetze, private Subnetze, reine VPN-Subnetze und isolierte Subnetze umfassen.

Inhalt

- [Routing-Tabellen-Konzepte](#)
- [Subnetz-Routingtabellen](#)
- [Gateway-Routing-Tabellen](#)
- [Funktionsweise der Routenpriorität](#)

- [Beispiele für Routing-Optionen](#)
- [Erstellen einer Routing-Tabelle für Ihre VPC](#)
- [Verwalten von Subnetz-Routing-Tabellen](#)
- [So ersetzen Sie die Routing-Haupttabelle](#)
- [Kontrollieren des eingehenden Datenverkehrs in Ihre VPC mit einer Gateway-Routing-Tabelle](#)
- [Ersetzen oder Wiederherstellen des Ziels für eine lokale Route](#)
- [Erweitertes Routing in Ihrer VPC](#)
- [Beheben von Problemen mit der Erreichbarkeit in Ihrer VPC](#)

Routing-Tabellen-Konzepte

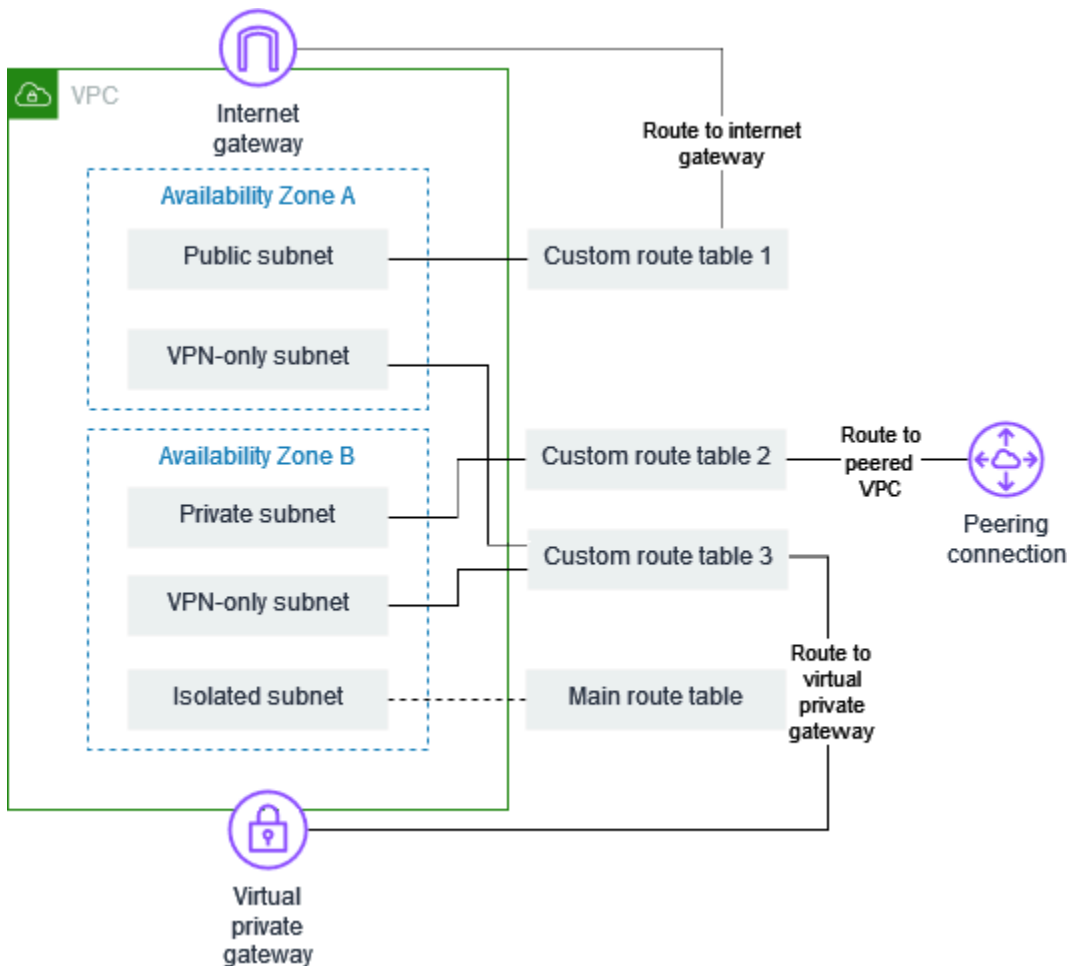
Im Folgenden sind die wichtigsten Konzepte für Routing-Tabellen aufgeführt:

- 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 -CIDR 172.16.0.0/12.
- Ziel – Das Gateway, die Netzwerkschnittstelle oder die Verbindung, über die der Zieldatenverkehr gesendet werden soll, z. B. ein Internet-Gateway.
- Lokale Route – Eine Standardroute für die Kommunikation innerhalb der VPC. Wenn die VPC IPv4- und IPv6-Adressen hat, gibt es eine lokale Route für IPv4 und eine lokale Route für IPv6.
- 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.
- 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.

Beispiel-VPC mit Routing-Tabellen

Das folgende Diagramm zeigt eine VPC mit fünf Subnetzen, einer Haupt-Routing-Tabelle und drei benutzerdefinierten Routing-Tabellen. Alle vier Routing-Tabellen haben lokale Routen. Die benutzerdefinierte Routing-Tabelle 1 hat eine Route zu einem Internet-Gateway und ist dem öffentlichen Subnetz in Availability Zone A zugeordnet. Die benutzerdefinierte Routing-Tabelle 2 hat eine Route zu einer per Peering verbundenen VPC und ist dem privaten Subnetz in Availability Zone B zugeordnet. Die benutzerdefinierte Routing-Tabelle 3 hat eine Route zu einem virtuellen privaten Gateway und ist den reinen VPN-Subnetzen in beiden Availability Zones zugeordnet.



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](#)
- [Haupt-Routing-Tabelle](#)
- [Benutzerdefinierte Routing-Tabellen](#)
- [Zuordnung der Subnetz-Routing-Tabelle](#)

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	<i>igw-id</i>

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 verbindungslokalen Adressraums und ist für AWS-Services 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 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 befindet sich innerhalb des ULA-Raums (Unique Local Address) und ist für AWS-Services 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-aabbccdde1122334

- 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.

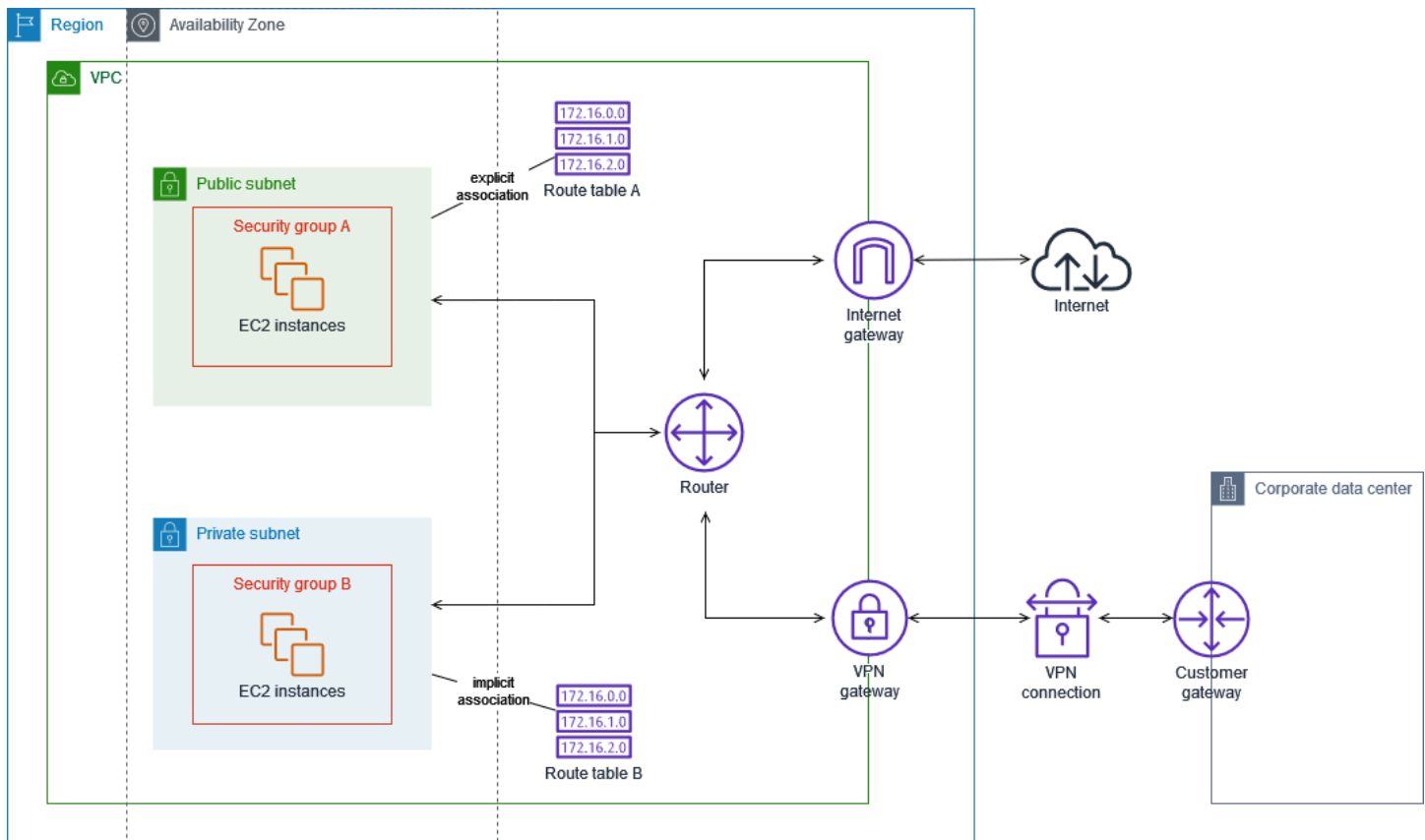
Zuordnung der Subnetz-Routing-Tabelle

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 der expliziten Zuordnungen](#).

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
<i>VPC-CIDR</i>	Local
0.0.0.0/0	<i>igw-id</i>

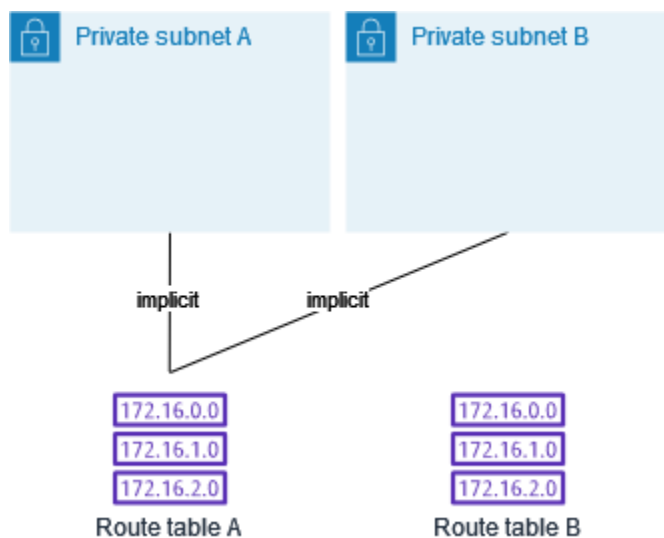
Routing-Tabelle B ist die Haupt-Routing-Tabelle. Es besteht implizit eine Zuordnung zum dem privaten Subnetz. Darin enthalten ist eine Route, die den gesamten Datenverkehr an das virtuelle private Gateway sendet, aber keine Route zum Internet-Gateway, was das Subnetz zu einem reinen VPN-Subnetz macht. 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
<i>VPC-CIDR</i>	Local
0.0.0.0/0	<i>vgw-id</i>

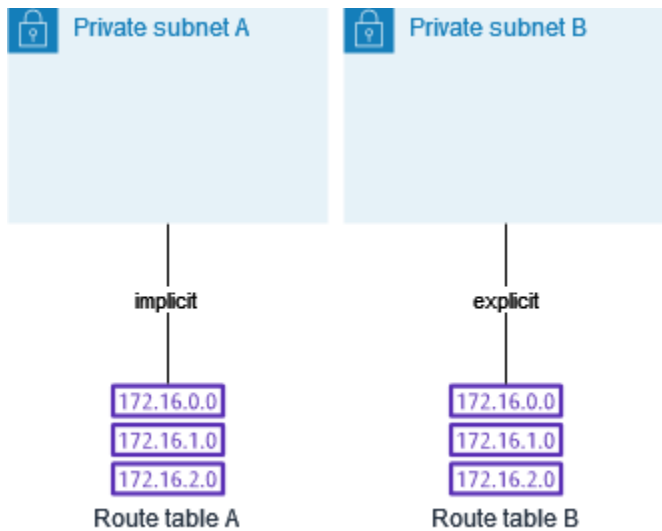
Beispiel 2: Ersetzen der Haupt-Router-Tabelle

Möglicherweise möchten Sie Änderungen an der Haupt-Router-Tabelle vornehmen. Um Störungen des Datenverkehrs zu vermeiden, empfehlen wir, zuerst die Routenänderungen mithilfe einer benutzerdefinierten Router-Tabelle zu testen. Wenn Sie mit dem Ergebnis des Tests zufrieden sind, können Sie die Haupt-Router-Tabelle durch die neue benutzerdefinierte Tabelle ersetzen.

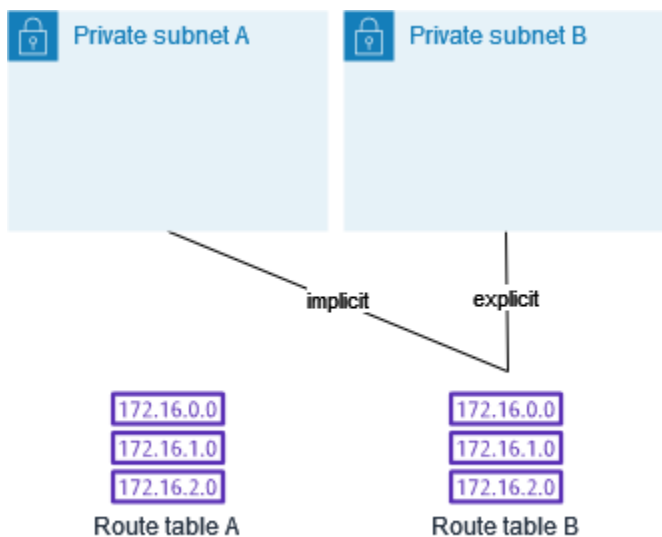
Das folgende Diagramm zeigt zwei Subnetze und zwei Router-Tabellen. Subnetz A ist implizit der Router-Tabelle A, der Haupt-Router-Tabelle, zugeordnet. Subnetz B ist implizit der Router-Tabelle A zugeordnet. Die Router-Tabelle B, eine benutzerdefinierte Router-Tabelle, ist keinem der Subnetze zugeordnet.



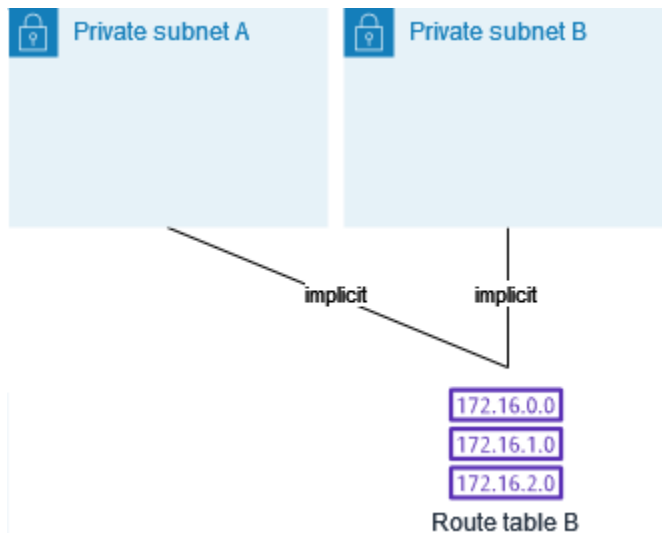
Um die Haupt-Router-Tabelle zu ersetzen, erstellen Sie zunächst eine explizite Zuordnung zwischen Subnetz B und Router-Tabelle B. Testen Sie die Router-Tabelle B.



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-Tabelle bezeichnet. Sie können eine Gateway-Routing-Tabelle erstellen, um den Routing-Pfad des Datenverkehrs in Ihrer 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](#)
- [Regeln und Überlegungen](#)

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	<i>eni-id</i>

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	<i>eni-id</i>

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.

Funktionsweise der 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.

Die folgende Liste enthält eine Zusammenfassung der Routenpriorität mit Links zu den folgenden Abschnitten, die detailliertere Informationen und Beispiele enthalten:

1. [Längstes Präfix](#) (zum Beispiel hat 10.10.2.15/32 Priorität gegenüber 10.10.2.0/24)
2. [Statische Routen](#) (wie VPC-Peering und Internet-Gateway-Verbindungen)
3. [Präfixlisten-Routen](#)
4. [Propagierte Routen](#)
 - a. Direct-Connect-BGP-Routen (dynamische Routen)
 - b. Statische VPN-Routen
 - c. VPN-BGP-Routen (dynamische Routen) (z. B. virtuelle private Gateways)

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 für statisch und dynamisch 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 das Ziel einer propagierten Route identisch mit dem Ziel einer statischen Route ist, hat die statische Route Priorität. Die folgenden Ressourcen verwenden statische Routen:

- 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 für Präfixlisten

Wenn Ihre Routing-Tabelle auf eine Präfixliste verweist, gelten die folgenden Regeln:

- 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.

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](#)
- [Routing zu einem NAT-Gerät](#)
- [Routing zu einem Virtual Private Gateway](#)
- [Routing an ein lokales AWS Outposts-Gateway](#)
- [Routing an eine VPC-Peering-Verbindung](#)
- [Routing zu einem Gateway-VPC-Endpunkt](#)
- [Routing zu einem Egress-Only-Internet-Gateway](#)
- [Routing für ein Transit-Gateway](#)
- [Routing für eine Middlebox-Appliance](#)
- [Routing unter Verwendung einer Präfixliste](#)
- [Routing zu einem Gateway Load Balancer-Endpunkt](#)

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-xxxxxxxxxxxxxxxxxx`) als Ziel hinzu.

Ziel	Ziel
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

Weitere Informationen finden Sie unter [Aktivieren des Internetzugangs für eine VPC mithilfe eines Internet-Gateways](#).

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	<i>nat-gateway-id</i>

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-xxxxxxx, 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	<i>nat-gateway-id</i>
pl-xxxxxxx	<i>vpce-id</i>
10.25.0.0/16	<i>pcx-id</i>

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 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-xxxxxxxxxxxxxxxxxxxx).

Ziel	Ziel
10.0.0.0/16	<i>vgw-id</i>

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 Direct Connect-Verbindung über ein Virtual Private Gateway. Weitere Informationen finden Sie im [Direct Connect-Benutzerhandbuch](#).

Routing an ein lokales AWS Outposts-Gateway

In diesem Abschnitt werden Routing-Tabellenkonfigurationen für das Routing zu einem lokalen AWS Outposts-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

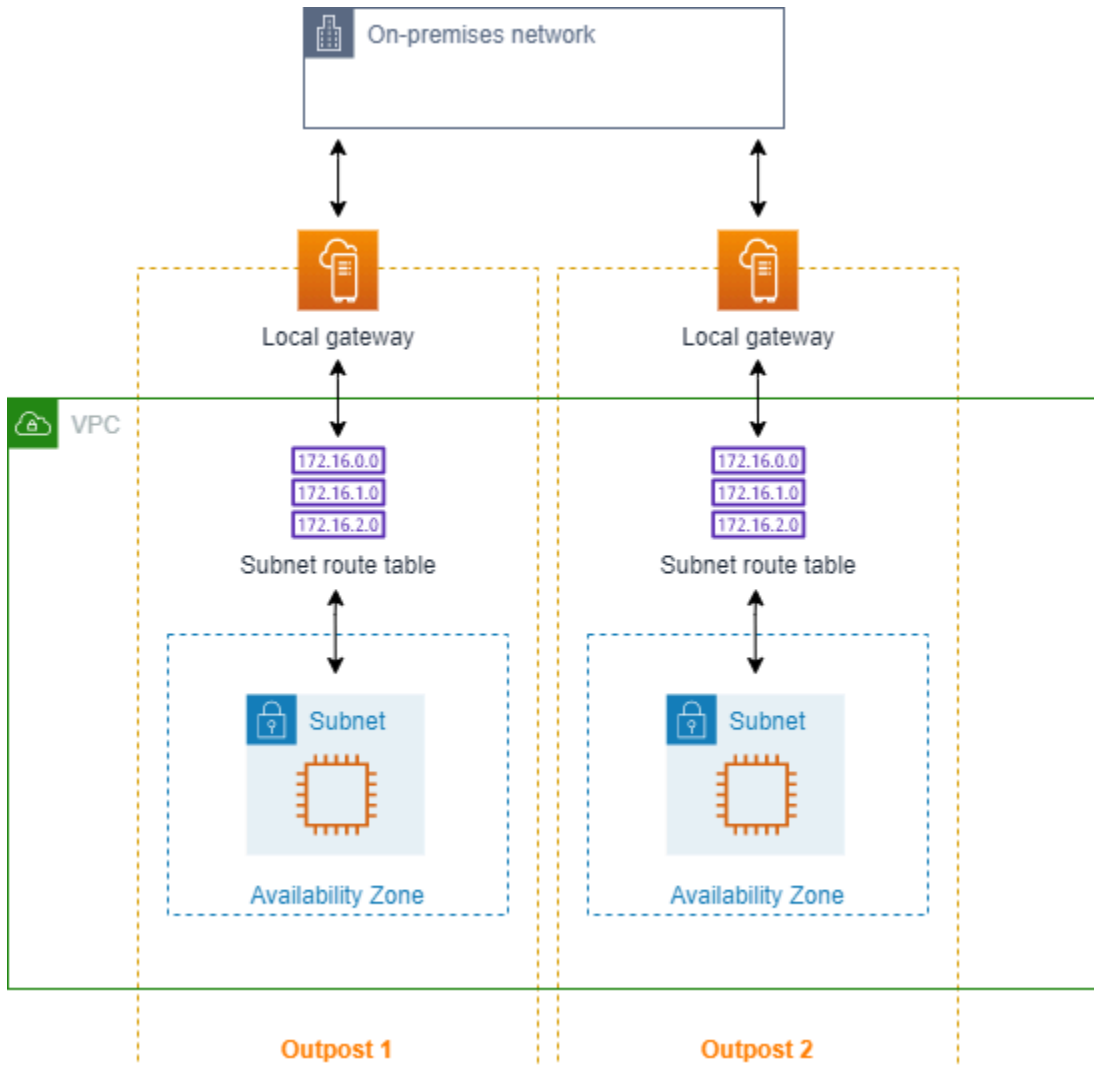
Subnetze, die sich in VPCs befinden, die mit AWS Outposts verknüpft sind, können einen zusätzlichen Zieltyp eines lokalen Gateways haben. Betrachten Sie den Fall, in dem der lokale Gateway-Routenverkehr mit der Zieladresse 192.168.10.0/24 an das Kundennetzwerk gesendet werden soll. Fügen Sie dazu die folgende Route mit dem Zielnetzwerk und einem Ziel des lokalen Gateways () hi (lgw-xxxx).

Ziel	Ziel
192.168.10.0/24	<i>lgw-id</i>

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	<i>lgw-1-id</i>

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	<i>lgw-2-id</i>

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

Mithilfe eines Gateway-VPC-Endpunkts können Sie eine private Verbindung zwischen Ihrer VPC und einem anderen AWS-Service erstellen. 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 (p1-**xxxxxxxx**) als Zielbereich und der Endpunkt-ID (vpce-**xxxxxxxxxxxxxxxxxxxx**) 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	<i>eigw-id</i>

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-111111111111111111
- VPC B: 10.2.0.0/16, Anfügungs-ID tgw-attach-222222222222222222

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	<i>tgw-id</i>

Folgendes ist ein Beispiel für die Transit-Gateway-Routing-Tabellen-Einträge für die VPC-Anfügungen.

Ziel	Ziel
10.1.0.0/16	tgw-attach-111111111111111111
10.2.0.0/16	tgw-attach-222222222222222222

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, damit AWS automatisch die entsprechenden Routing-Tabellen für Ihr Gateway, Ihre Middlebox und Ihr Ziel-Subnetz konfiguriert. 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 Datenverkehr korrekt weitergeleitet wird und dass es keine unbeabsichtigten Folgen gibt, wenn Sie die Routing-Verbreitung aktivieren oder deaktivieren (z. B. ist die Routing-Verbreitung für eine 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](#)
- [Routing des Datenverkehrs zwischen einem Gateway und einer Appliance](#)
- [Routing-Intersubnetzdatenverkehr an eine Appliance](#)

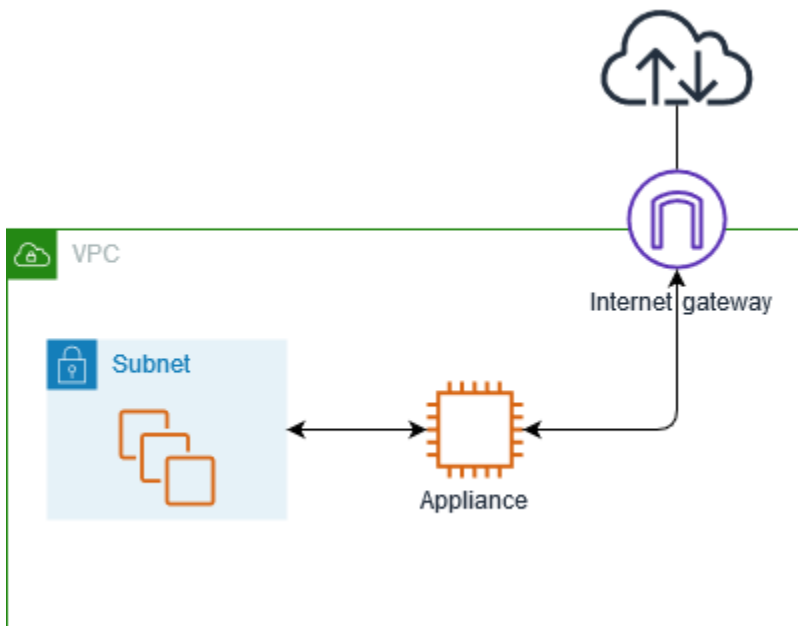
Überlegungen zu Appliances

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-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.

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
<i>VPC-CIDR</i>	Local
<i>Subnetz-CIDR</i>	<i>Appliance-Netzwerkschnittstellen-ID</i>

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
<i>VPC-CIDR</i>	<i>Appliance-Netzwerkschnittstellen-ID</i>

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.

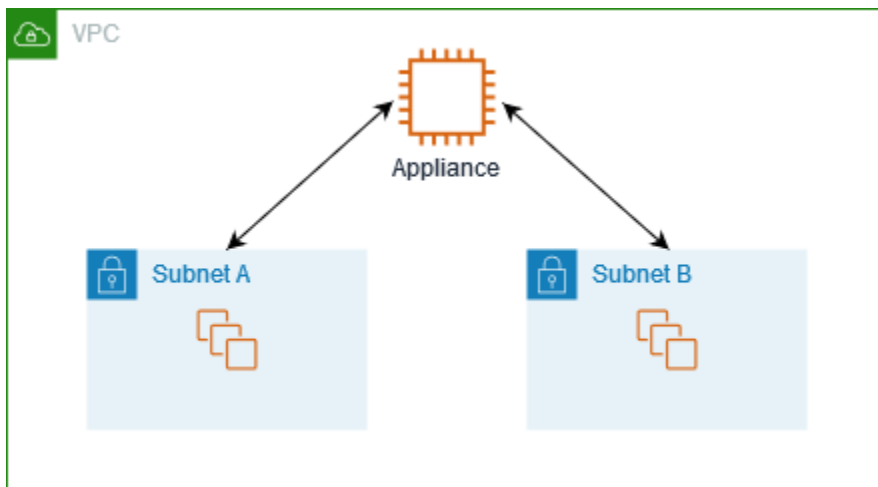
Ziel	Ziel
<i>VPC-CIDR</i>	Local
0.0.0.0/0	<i>Appliance-Netzwerkschnittstellen-ID</i>

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
<i>VPC-CIDR</i>	Local
0.0.0.0/0	<i>igw-id</i>

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
<i>VPC-CIDR</i>	Local
<i>Subnetz-B-CIDR</i>	<i>Appliance-Netzwerkschnittstellen-ID</i>

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
<i>VPC-CIDR</i>	Local
<i>Subnetz-A-CIDR</i>	<i>Appliance-Netzwerkschnittstellen-ID</i>

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
<i>VPC-CIDR</i>	<i>Appliance-Netzwerkschnittstellen-ID</i>

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	<i>tgw-id</i>

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 einen Gateway Load Balancer erstellen, einen [Endpunktservice für einen Gateway Load Balancer](#) konfigurieren und dann einen [Gateway-Load-Balancer-Endpunkt](#) in Ihrer VPC erstellen, um ihn 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	<i>vpc-endpoint-id</i>

Wenn Sie einen Gateway-Load-Balancer-Endpunkt als Ziel verwenden, können Sie keine Präfixliste als Zieladresse angeben. Wenn Sie versuchen, eine Route mit einer Präfixliste, die einen VPC-Endpunkt als Ziel hat, zu erstellen oder zu ersetzen, erhalten Sie diese Fehlermeldung: „Eine Route mit einer Präfixliste, die einen VPC-Endpunkt als Ziel hat, kann nicht erstellt oder ersetzt werden.“

Weitere Informationen finden Sie unter [Gateway Load Balancer](#).

Erstellen einer Routing-Tabelle für Ihre VPC

Führen Sie die folgenden Aufgaben aus, um eine benutzerdefinierte Routing-Tabelle für Ihre VPC zu erstellen und zu konfigurieren. Eine neue Routing-Tabelle enthält standardmäßig lokale Routen für die Kommunikation innerhalb der VPC. Sie können Routen hinzufügen, um den Netzwerkverkehr auf Basis des Ziel-IP-Adressbereichs an bestimmte Ziele weiterzuleiten.

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.

Sie können die Zuordnung eines Subnetzes zu einer Routing-Tabelle aufheben. Sofern Sie ein Subnetz nicht explizit einer anderen Routing-Tabelle zuordnen, ist das Subnetz implizit der Haupt-Routing-Tabelle zugeordnet.

Note

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](#).

Aufgaben

- [Erstellen der Routing-Tabelle](#)
- [Hinzufügen von Routen zur Routing-Tabelle](#)
- [Zuordnen eines Subnetzes zu der Routing-Tabelle](#)

Erstellen der Routing-Tabelle

Erstellen einer -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).

Erstellen einer -Routing-Tabelle mithilfe der AWS CLI

Verwenden Sie den Befehl [create-route-table](#).

Hinzufügen von Routen zur Routing-Tabelle

Über die Konsole fügen Sie einer Routing-Tabelle Routen wie folgt hinzu:

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 Aktionen und dann Routen bearbeiten.
4. Wählen Sie Route hinzufügen aus.
5. Geben Sie unter Zieladresse einen der folgenden Werte ein:
 - einen IP-Adressbereich – z. B. 192.168.0.0/16
 - eine einzelne IP-Adresse – z. B. 192.168.10.1/32
 - die ID einer Präfixliste – z. B. pl-0abcdef1234567890
6. Wählen Sie unter Ziel einen Ressourcentyp aus (z. B. eine Netzwerkschnittstelle) und geben Sie dann die ID der Ressource ein (z. B. eni-11223344556677889).
7. Wählen Sie Änderungen speichern aus.

Über die AWS CLI fügen Sie einer Routing-Tabelle Routen wie folgt hinzu:

Verwenden Sie den Befehl [create-route](#).

Zuordnen eines Subnetzes zu der Routing-Tabelle

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).

Über die AWS CLI ordnen Sie ein Subnetz einer Routing-Tabelle wie folgt zu oder heben die Zuordnung auf:

- [associate-route-table](#)
- [disassociate-route-table](#)

Verwalten von Subnetz-Routing-Tabellen

Verwenden Sie die folgenden Verfahren, um das VPC-Routing mithilfe von Routing-Tabellen zu verwalten.

Aufgaben

- [Festlegen der Routing-Tabelle für ein Subnetz](#)
- [Bestimmen der expliziten Zuordnungen](#)
- [Hinzufügen, Ändern und Entfernen von Routen](#)
- [Aktivieren oder Deaktivieren der Routing-Verbreitung](#)
- [Bearbeiten der Routing-Tabelle für ein Subnetz](#)

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.

Über die Konsole legen Sie die Routing-Tabelle für ein Subnetz wie folgt fest:

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 der expliziten Zuordnungen](#).

Bestimmen der expliziten Zuordnungen

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 (Hauptttabelle), 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.

Über die AWS CLI beschreiben Sie eine oder mehrere Routing-Tabellen und zeigen ihre Zuordnungen wie folgt an:

Verwenden Sie den Befehl [describe-route-tables](#).

Hinzufügen, Ändern und Entfernen von Routen

Sie können Routen für Ihre Routing-Tabellen hinzufügen, ändern oder löschen.

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.

Überlegungen

- Sie können nur selbst erstellte Routen verändern.
- Wenn Sie eine Route ändern oder löschen, wirkt sich dies auf bestehende Verbindungen aus, die diese Routen verwenden. Verbindungen, die andere Routen verwenden, sind nicht betroffen.
- Es gibt ein Kontingent für die Anzahl der Routen, die Sie pro Routing-Tabelle hinzufügen können. Weitere Informationen finden Sie unter [Amazon VPC-Kontingente](#).

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 Zieladresse einen IP-Adressbereich, eine einzelne IP-Adresse oder die ID einer Präfixliste ein. Wählen Sie unter Ziel den Ressourcentyp aus und geben Sie dann die ID der Ressource ein.
5. Zum Ändern einer Route geben Sie den neuen CIDR-Block oder die neue Präfixlisten-ID ein und wählen Sie ein Ziel aus.
6. Zum Entfernen einer Route wählen Sie Remove (Entfernen) aus.

7. Wählen Sie Änderungen speichern aus.

Über die AWS CLI aktualisieren Sie die Routen für eine Routing-Tabelle wie folgt:

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`.

- [create-route](#)
- [replace-route](#)
- [delete-route](#)

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.

Über die Konsole aktivieren oder deaktivieren Sie die Routing-Verbreitung wie folgt:

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 oder deaktivieren Sie das Kontrollkästchen Aktivieren neben dem Virtual Private Gateway.
5. Wählen Sie Speichern.

Über die AWS CLI aktivieren oder deaktivieren Sie die Routing-Verbreitung wie folgt:

- [enable-vgw-route-propagation](#)

- [disable-vgw-route-propagation](#)

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.

Über die AWS CLI ändern Sie die einem Subnetz zugeordnete Routing-Tabelle wie folgt:

Verwenden Sie den Befehl [replace-route-table-association](#).

So ersetzen Sie die Routing-Haupttabelle

In diesem Abschnitt wird beschrieben, wie Sie die Haupt-Routing-Tabelle für Ihre VPC ändern können.

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.

Über die AWS CLI ersetzen Sie die Haupt-Routing-Tabelle wie folgt:

- Verwenden Sie den Befehl [replace-route-table-association](#).

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).

Kontrollieren des eingehenden Datenverkehrs in Ihre VPC mit einer Gateway-Routing-Tabelle

Um den in Ihre VPC eingehenden Datenverkehr mit einer Gateway-Routing-Tabelle zu kontrollieren, können Sie ein Internet-Gateway oder ein Virtual Private Gateway einer Routing-Tabelle zuordnen oder die Zuordnung aufheben. Weitere Informationen finden Sie unter [Gateway-Routing-Tabellen](#).

So ordnen Sie einem Gateway eine Routing-Tabelle über die Konsole zu oder heben die Zuordnung 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 Edge Associations (Edge-Zuordnungen) die Option Edit edge associations (Edge-Zuordnungen bearbeiten) aus.
4. Aktivieren oder deaktivieren Sie das Kontrollkästchen für das Gateway.
5. Wählen Sie Änderungen speichern aus.

So ordnen Sie einem Gateway mit der eine Routing-Tabelle zu AWS CLI

Verwenden Sie den Befehl [associate-route-table](#). Im folgenden Beispiel wird die angegebene Routing-Tabelle dem ausgewählten Internet-Gateway zugeordnet.

```
aws ec2 associate-route-table
  --route-table-id rtb-01234567890123456 \
  --gateway-id igw-11aa22bb33cc44dd1
```

Über die AWS CLI heben Sie die Zuordnung einer Routing-Tabelle von einem Gateway wie folgt auf:

Verwenden Sie den Befehl [disassociate-route-table](#). Geben Sie die ID der Zuordnung zwischen der Routing-Tabelle und dem Gateway an.

```
aws ec2 disassociate-route-table \
  --association-id rtbassoc-0abcdef1234567890
```

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.

Über die Konsole ersetzen Sie die lokale Route wie folgt:

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.

So ersetzen Sie das Ziel für eine lokale Route mit der AWS CLI

Verwenden Sie den Befehl [replace-route](#). Im folgenden Beispiel wird das Ziel der lokalen Route durch die angegebene Netzwerkschnittstelle ersetzt.

```
aws ec2 replace-route \  
  --route-table-id rtb-01234567890123456 \  
  --destination-cidr-block 10.0.0.0/16 \  
  --network-interface-id eni-11223344556677889
```

So stellen Sie das Ziel für eine lokale Route mithilfe der wieder her AWS CLI

Im folgenden Beispiel wird das lokale Ziel für die angegebene Routing-Tabelle wiederhergestellt.

```
aws ec2 replace-route \  
  --route-table-id rtb-01234567890123456 \  
  --destination-cidr-block 10.0.0.0/16 \  
  --local-target
```

Erweitertes Routing in Ihrer VPC

Konfigurieren Sie erweiterte Routing-Szenarien für Ihre VPC. In diesem Abschnitt werden sowohl statische als auch dynamische Routing-Ansätze zur Verwaltung des Verkehrsflusses behandelt:

- Statisches Ingress-Routing: Konfigurieren Sie statische Routen, um eingehenden Internetverkehr, der für Ihre BYOIP-Adresspools (Bring Your Own IP) bestimmt ist, an bestimmte Netzwerkschnittstellen innerhalb Ihrer VPC weiterzuleiten.
- Dynamisches Routing mit VPC-Routenserver: Verwenden Sie BGP-basiertes dynamisches Routing, um VPC- und Internet-Gateway-Routing-Tabellen automatisch zu aktualisieren und so Fehlertoleranz und automatisches Failover für Ihre Workloads zu gewährleisten.

Inhalt

- [Weiterleiten des Internetverkehrs an eine einzige Netzwerkschnittstelle](#)

- [Dynamisches Routing in Ihrer VPC mit VPC Route Server](#)

Weiterleiten des Internetverkehrs an eine einzige Netzwerkschnittstelle

Sie können eingehenden Internetverkehr für große Pools öffentlicher IP-Adressen an eine einzige Elastic-Network-Schnittstelle (ENI) in Ihrer VPC weiterleiten.

Bisher akzeptierten Internet-Gateways Datenverkehr für öffentliche IP-Adressen nur dann, wenn diese direkt mit Netzwerkschnittstellen in der VPC verknüpft waren. Bei Instance-Typen ist die Anzahl der IP-Adressen begrenzt, die Netzwerkschnittstellen zugeordnet werden können. Das sorgt für Herausforderungen in der Telekommunikation und für das Internet der Dinge (IoT), da der Datenverkehr für IP-Pools in diesen Bereichen die Limits überschreitet.

Durch dieses Routing entfällt die komplexe Adressübersetzung bei eingehenden Internetverbindungen. Sie können eigene öffentliche IP-Pools (BYOIP) verwenden und Ihr VPC-Internet-Gateway so konfigurieren, dass der Datenverkehr für den gesamten Pool akzeptiert und an eine einzige Netzwerkschnittstelle weitergeleitet wird. Dieses Feature ist besonders nützlich für:

- Telekommunikation: Verwalten großer Subscriber-IP-Pools ohne Mehraufwand bei der Adressübersetzung
- IoT-Anwendungen: Konsolidieren des Datenverkehrs von Tausenden Geräte-IP-Adressen
- Beliebiges Szenario: Erzwingen des Datenverkehr-Routings über ENI-Zuordnungslimits hinaus

Sie können dieses Routing in VPC Route Server integrieren, um in Failover-Szenarien dynamische Routenaktualisierungen zu ermöglichen.

Wichtigste Vorteile

Diese Routing-Methode bietet folgende Vorteile:

- Keine Adressübersetzung erforderlich: direktes Routing reduziert die NAT-Komplexität
- ENI-Limits umgehen: Verarbeitung von IP-Pools, die die Limits für die Instance-Zuweisung überschreiten
- Branchenoptimiert: für Telekommunikations- und IoT-Anforderungen entwickelt
- Dynamisches Failover: Integration in Route Server für automatische Updates

Verfügbarkeit

Sie können dieses Feature in allen kommerziellen AWS-Regionen, AWS-Regionen in China und AWS-GovCloud-Regionen verwenden.

Inhalt

- [Bevor Sie beginnen](#)
- [Funktionsweise](#)
- [Schritt 1: Erstellen einer VPC](#)
- [Schritt 2: Erstellen und Zuordnen eines Internet-Gateways](#)
- [Schritt 3: Erstellen eines Subnetzes für die Ziel-Instance](#)
- [Schritt 4: Erstellen einer Routing-Tabelle für das Subnetz](#)
- [Schritt 5: Erstellen einer Sicherheitsgruppe für die Ziel-Instance](#)
- [Schritt 6: Starten einer Ziel-EC2-Instance](#)
- [Schritt 7: Erstellen der Routing-Tabelle für das Internet-Gateway](#)
- [Schritt 8: Zuordnen der Routing-Tabelle zum Internet-Gateway](#)
- [Schritt 9: Zuordnen Ihres BYOIP-Pools zum Internet-Gateway](#)
- [Schritt 10: Hinzufügen einer statischen Route mit Ihrer Instance als Ziel](#)
- [Schritt 11: Konfigurieren der Ziel-Instance](#)
- [Schritt 12: Konfigurieren der Instance für die Verarbeitung des Datenverkehrs](#)
- [Schritt 13: Testen der Verbindung](#)
- [Fehlerbehebung](#)
- [Erweiterte Option: Route-Server-Integration für dynamisches Routing](#)
- [Bereinigen](#)

Bevor Sie beginnen

Voraussetzungen für dieses Tutorial:

1. Ein BYOIP-Pool: Sie müssen Ihren eigenen IP-Adressbereich in AWS hinzugefügt haben. Führen Sie die Schritte unter [Eigene IP-Adressen mitbringen \(BYOIP\) in Amazon EC2](#) aus.
2. Überprüfen Sie Ihren BYOIP-Pool: Vergewissern Sie sich mit dem folgenden Befehl, dass Ihr Pool bereit ist:

```
aws ec2 describe-public-ipv4-pools --region us-east-1
```

Suchen Sie in der Ausgabe nach Ihrem Pool und stellen Sie sicher, dass `PoolAddressRanges` die `Available` Adressen anzeigt.

3. Entsprechende Berechtigungen: Stellen Sie sicher, dass Ihr AWS-Konto Berechtigungen zum Erstellen von VPC-Ressourcen und EC2-Instances und zum Verwalten von BYOIP-Pools hat.

Funktionsweise

In diesem Abschnitt werden die technischen Konzepte des Internet-Gateway-Ingress-Routings erläutert. Außerdem wird beschrieben, wie der Datenverkehr vom Internet zu Ihrer Ziel-Instance gelangt.

Gründe zur Verwendung des Internet-Gateway-Ingress-Routings

Bisher mussten Sie aufgrund von ENI-Zuordnungslimits eine Adressübersetzung durchführen, um den Datenverkehr für eine große Anzahl von IP-Adressen zu konsolidieren. Diese Erweiterung beseitigt diese Komplexität, da sie das direkte Routing von BYOIP-Pools an Ziel-Instances ermöglicht.

Funktionsweise der Weiterleitung

Dieses Feature funktioniert nur mit den öffentlichen IP-CIDRs, die Sie gemäß dem BYOIP-Prozess zu AWS mitbringen. Der BYOIP-Prozess stellt sicher, dass das öffentliche IP-CIDR Teil Ihres Kontos ist. Wenn das öffentliche BYOIP-CIDR bereit ist:

1. Ordnen Sie diesem öffentlichen IP-Adresspool eine Internet-Gateway-Routing-Tabelle zu. Das Internet-Gateway muss bereits einer VPC zugeordnet sein. Diese Zuordnung ermöglicht der VPC, Datenverkehr zu akzeptieren, der für das IP-CIDR bestimmt ist. Stellen Sie sicher, dass das Internet-Gateway eine dedizierte Routing-Tabelle hat, die nicht von einem Subnetz mitgenutzt wird.
2. Nachdem Sie den BYOIP-Pool der Internet-Gateway-Routing-Tabelle zugeordnet haben, können Sie in die Routing-Tabelle eine Route mit einem Ziel eingeben, das dem IP-CIDR oder einem Teil davon entspricht. Das Ziel dieser Route wäre die ENI, an die Sie Ihren Datenverkehr weiterleiten möchten.
3. Wenn Ihr Datenverkehr für Ihren BYOIP-CIDR bei AWS eingeht, prüft AWS die Internet-Gateway-Routing-Tabelle und leitet den Datenverkehr an die entsprechende VPC weiter.
4. Innerhalb der VPC leitet das Internet-Gateway den Datenverkehr an die Ziel-ENI weiter.

5. Das Ziel (eine Elastic-Network-Schnittstelle, die Ihrer Workload zugeordnet ist) verarbeitet den Datenverkehr.

Bewährte Methoden für

- Halten Sie die Routing-Tabellen getrennt: Die Internet-Gateway-Routing-Tabelle darf nur für das Internet-Gateway genutzt werden. Ordnen Sie diese Routing-Tabelle nicht VPC-Subnetzen zu. Verwenden Sie separate Routing-Tabellen für das Subnetz-Routing.
- Weisen Sie BYOIP-IPs nicht direkt zu: Ordnen Sie öffentliche IP-Adressen aus Ihrem BYOIP-Pool nicht direkt EC2-Instances oder Netzwerkschnittstellen zu. Die Ingress-Routing-Funktion des Internet-Gateways leitet den Datenverkehr ohne direkte IP-Zuordnung an Instances weiter.

Important

Wenn Sie [VPC Block Public Access \(BPA\)](#) verwenden und BPA aktiviert ist, wird der Datenverkehr an Subnetze mithilfe von Ingress-Routing blockiert, auch wenn Sie einen BPA-Ausschluss auf Subnetzebene eingerichtet haben. Ausschlüsse auf Subnetzebene funktionieren nicht für das Ingress-Routing. Sie können Ingress-Routing-Datenverkehr mit aktiviertem BPA wie folgt zulassen:

- BPA vollständig deaktivieren oder
- Ausschluss auf VPC-Ebene verwenden

Schritt 1: Erstellen einer VPC

Führen Sie diesen Schritt aus, um eine VPC zu erstellen, die Ihre Ziel-Instance und Ihr Internet-Gateway hostet.

Note

Achten Sie darauf, dass Sie das VPC-Kontingentlimit noch nicht erreicht haben. Weitere Informationen finden Sie unter [Amazon VPC-Kontingente](#).

AWS Konsole

1. Öffnen Sie die [Amazon VPC-Konsole](#).

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. Geben Sie unter Namens-Tag einen Namen für Ihre VPC ein (beispielsweise **IGW-Ingress-VPC**).
5. Geben Sie unter IPv4-CIDR-Block einen gültigen CIDR-Block ein (beispielsweise **10.0.0.0/16**).
6. Wählen Sie VPC erstellen aus.

AWS CLI

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications  
'ResourceType=vpc,Tags=[{Key=Name,Value=IGW-Ingress-VPC}]' --region us-east-1
```

Schritt 2: Erstellen und Zuordnen eines Internet-Gateways

Führen Sie diesen Schritt aus, um ein Internet-Gateway zu erstellen und an Ihre VPC anzufügen und dadurch die Internetverbindung zu aktivieren.

AWS Konsole

1. Öffnen Sie die [Amazon VPC-Konsole](#).
2. Wählen Sie in der VPC-Konsole die Option Internet-Gateways aus.
3. Wählen Sie Create internet gateway (Internet-Gateway erstellen) aus.
4. Geben Sie unter Namens-Tag einen Namen für Ihr Internet-Gateway ein (beispielsweise **IGW-Ingress-Gateway**).
5. Wählen Sie Create internet gateway (Internet-Gateway erstellen) aus.
6. Wählen Sie Ihr Internet-Gateway und dann Aktionen, An VPC anfügen aus.
7. Wählen Sie Ihre VPC und dann Internet-Gateway anfügen aus.

AWS CLI

```
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-  
gateway,Tags=[{Key=Name,Value=IGW-Ingress-Gateway}]' --region us-east-1  
  
aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id  
vpc-0123456789abcdef0 --region us-east-1
```

Hinweis: Ersetzen Sie die Ressourcen-IDs durch Ihre tatsächlichen IDs aus dem vorherigen Schritt.

Schritt 3: Erstellen eines Subnetzes für die Ziel-Instance

Schließen Sie diesen Schritt ab, um ein Subnetz für Ihre Ziel-Instance zu erstellen.

AWS Konsole

1. Wählen Sie im Navigationsbereich der VPC-Konsole Subnets (Subnetze).
2. Wählen Sie Subnetz erstellen.
3. Wählen Sie unter VPC-ID Ihre VPC aus.
4. Geben Sie unter Subnetzname einen Namen ein (z. B. **Target-Subnet**).
5. Unter Availability Zone können Sie eine Zone für das Subnetz auswählen. Alternativ können Sie die Standardeinstellung No Preference (Keine Präferenz) beibehalten, damit AWS eine Zone für Sie auswählt.
6. Wählen Sie für IPv4-CIDR-Block die Option Manuelle Eingabe aus und geben Sie einen CIDR-Block ein (beispielsweise **10.0.1.0/24**).
7. Wählen Sie Subnetz erstellen.

AWS CLI

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.1.0/24 \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Target-Subnet}]' \
  --region us-east-1
```

Schritt 4: Erstellen einer Routing-Tabelle für das Subnetz

Führen Sie diesen Schritt aus, um eine Routing-Tabelle für Ihr Subnetz zu erstellen und dem Subnetz zuzuordnen.

AWS Konsole

1. Wählen Sie im Navigationsbereich der VPC-Konsole Routing-Tabellen aus.
2. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).
3. Geben Sie unter Name einen Namen für Ihre Routing-Tabelle ein (beispielsweise **Target-Subnet-Route-Table**).

4. Wählen Sie unter VPC Ihre VPC aus.
5. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).
6. Wählen Sie die Routing-Tabelle aus und klicken Sie auf Aktionen, Subnetzzuordnungen bearbeiten.
7. Wählen Sie Ihr Subnetz und dann Zuweisungen speichern aus.

AWS CLI

```
aws ec2 create-route-table \
  --vpc-id vpc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Target-Subnet-Route-Table}]' \
  --region us-east-1

aws ec2 associate-route-table \
  --route-table-id rtb-0987654321fedcba0 \
  --subnet-id subnet-0123456789abcdef0 \
  --region us-east-1
```

Schritt 5: Erstellen einer Sicherheitsgruppe für die Ziel-Instance

Schließen Sie diesen Schritt ab, um eine Sicherheitsgruppe zu erstellen, die den Netzwerkzugriff auf Ihre Ziel-Instance steuert.

AWS Konsole

1. Wählen Sie im Navigationsbereich der VPC-Konsole Sicherheitsgruppen aus.
2. Wählen Sie Sicherheitsgruppe erstellen aus.
3. Geben Sie unter Name der Sicherheitsgruppe einen Namen ein (z. B. **IGW-Target-SG**).
4. Geben Sie für Beschreibung den Text **Security group for IGW ingress routing target instance** ein.
5. Wählen Sie im Feld VPC Ihre VPC aus.
6. Um Regeln für eingehenden Datenverkehr hinzuzufügen, wählen Sie Eingehende Regeln aus. Wählen Sie für jede Regel Regel hinzufügen aus und geben Sie Folgendes an:
 - Typ: Alle ICMP – IPv4, Quelle: 0.0.0.0/0 (für Ping-Tests).
 - Typ: SSH, Port: 22, Quelle: 0.0.0.0/0 (für EC2 Instance Connect).

 Note

Diese Sicherheitsgruppe öffnet für dieses Tutorial SSH-Ports für den gesamten Internetverkehr. Das Tutorial ist nur für Informationszwecke bestimmt und sollte nicht für Produktionsumgebungen konfiguriert werden. In der Produktion sollten Sie den SSH-Zugriff auf ausgewählte IP-Bereiche beschränken.

- Wählen Sie Sicherheitsgruppe erstellen aus.

AWS CLI

```
aws ec2 create-security-group \  
  --group-name IGW-Target-SG \  
  --description "Security group for IGW ingress routing target instance" \  
  --vpc-id vpc-0123456789abcdef0 \  
  --region us-east-1  
  
aws ec2 authorize-security-group-ingress \  
  --group-id sg-0123456789abcdef0 \  
  --protocol icmp \  
  --port -1 \  
  --cidr 0.0.0.0/0 \  
  --region us-east-1  
  
aws ec2 authorize-security-group-ingress \  
  --group-id sg-0123456789abcdef0 \  
  --protocol tcp \  
  --port 22 \  
  --cidr 0.0.0.0/0 \  
  --region us-east-1
```

Schritt 6: Starten einer Ziel-EC2-Instance

Führen Sie diesen Schritt aus, um die EC2-Instance zu starten, die den Datenverkehr von Ihrem BYOIP-Pool empfängt.

AWS Konsole

1. Öffnen Sie die [Amazon EC2-Konsole](#).
2. Wählen Sie Launch Instance (Instance starten) aus.

3. Geben Sie unter Name einen Namen für Ihre Instance ein (beispielsweise **IGW-Target-Instance**).
4. Wählen Sie für Anwendungs- und Betriebssystem-Images (Amazon Machine Image) die Option Amazon-Linux-2023-AMI aus.
5. Wählen Sie für Instance-Typ die Option t2.micro aus (für das kostenlose Kontingent qualifiziert).
6. Wählen Sie für Schlüsselpaar (Anmeldung) ein bestehendes Schlüsselpaar aus oder erstellen Sie ein neues.
7. Wählen Sie für Netzwerkeinstellungen die Option Bearbeiten aus und konfigurieren Sie Folgendes:
 - VPC: Wählen Sie Ihre VPC aus.
 - Subnetz: Wählen Sie Ihr Subnetz aus.
 - Öffentliche IP-Adresse automatisch zuweisen: Aktiviert
 - Firewall (Sicherheitsgruppen): Klicken Sie auf „Vorhandene Sicherheitsgruppe auswählen“ und wählen Sie Ihrer Sicherheitsgruppe aus.
8. Wählen Sie Launch Instance (Instance starten) aus.
9. Wichtig: Rufen Sie nach dem Start die Instance-Details auf und notieren Sie sich die Netzwerkschnittstellen-ID (beginnt mit „eni-“). Diese benötigen Sie für Schritt 10.

AWS CLI

```
aws ec2 run-instances \  
  --image-id ami-0abcdef1234567890 \  
  --count 1 \  
  --instance-type t2.micro \  
  --key-name your-key-pair \  
  --security-group-ids sg-0123456789abcdef0 \  
  --subnet-id subnet-0123456789abcdef0 \  
  --associate-public-ip-address \  
  --tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=IGW-Target-Instance}]' \  
  --region us-east-1
```

Finden Sie die ENI-ID in der Konsole wie folgt:

1. Wählen Sie in der EC2-Konsole Ihre Instance aus.
2. Gehen Sie zur Registerkarte Netzwerk.

3. Notieren Sie sich die Netzwerkschnittstellen-ID (z. B. `eni-0abcdef1234567890`).

Finden Sie die ENI-ID mit der AWS CLI wie folgt:

```
aws ec2 describe-instances --instance-ids i-0123456789abcdef0 --query  
'Reservations[0].Instances[0].NetworkInterfaces[0].NetworkInterfaceId' --output text  
--region us-east-1
```

Schritt 7: Erstellen der Routing-Tabelle für das Internet-Gateway

Führen Sie diesen Schritt aus, um eine dedizierte Routing-Tabelle für das Internet-Gateway zu erstellen, das das Ingress-Routing verarbeitet.

AWS Konsole

1. Wählen Sie in der VPC-Konsole Routing-Tabellen aus.
2. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).
3. Geben Sie unter Name einen Namen für Ihre Routing-Tabelle ein (beispielsweise **IGW-Ingress-Route-Table**).
4. Wählen Sie unter VPC Ihre VPC aus.
5. Klicken Sie auf Create Route Table (Routing-Tabelle erstellen).
6. Wählen Sie die Routing-Tabelle aus und klicken Sie auf die Registerkarte Edge-Zuordnungen.
7. Wählen Sie Edge-Zuordnungen bearbeiten aus.
8. Wählen Sie Ihr Internet-Gateway und dann Änderungen speichern aus.

AWS CLI

```
aws ec2 create-route-table \  
  --vpc-id vpc-0123456789abcdef0 \  
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=IGW-Ingress-  
Route-Table}]' \  
  --region us-east-1
```

Schritt 8: Zuordnen der Routing-Tabelle zum Internet-Gateway

Führen Sie diesen Schritt aus, um Ihre Routing-Tabelle dem Internet-Gateway zuzuordnen und die Ingress-Routing-Funktionalität zu aktivieren.

AWS Konsole

1. Klicken Sie im Navigationsbereich der VPC-Konsole auf Routing-Tabellen und wählen Sie die erstellte Routing-Tabelle aus.
2. Wählen Sie auf der Registerkarte Edge Associations (Edge-Zuordnungen) die Option Edit edge associations (Edge-Zuordnungen bearbeiten) aus.
3. Aktivieren Sie das Kontrollkästchen für das Internet-Gateway.
4. Wählen Sie Änderungen speichern aus.

AWS CLI

```
aws ec2 associate-route-table \  
  --route-table-id rtb-0123456789abcdef0 \  
  --gateway-id igw-0123456789abcdef0 \  
  --region us-east-1
```

Schritt 9: Zuordnen Ihres BYOIP-Pools zum Internet-Gateway

Führen Sie diesen Schritt aus, um Ihren BYOIP-Pool der Routing-Tabelle für das Internet-Gateway zuzuordnen, sodass die VPC Datenverkehr für Ihren IP-Bereich akzeptieren kann.

AWS Konsole

1. Klicken Sie im Navigationsbereich der VPC-Konsole auf Routing-Tabellen und wählen Sie die erstellte Routing-Tabelle für das Internet-Gateway aus.
2. Klicken Sie auf die Registerkarte IPv4-Pool-Zuordnungen.
3. Klicken Sie auf die Schaltfläche Zuordnungen bearbeiten.
4. Wählen Sie Ihren BYOIP-Pool aus (z. B. pool-12345678901234567).
5. Klicken Sie auf die Schaltfläche Zuordnungen speichern.

AWS CLI

```
aws ec2 associate-route-table \  
  --route-table-id rtb-0123456789abcdef0 \  
  --public-ipv4-pool pool-12345678901234567 \  
  --region us-east-1
```

Hinweis: Ersetzen Sie `rtb-0123456789abcdef0` durch die ID der Internet-Gateway-Routing-Tabelle und `pool-12345678901234567` durch Ihre BYOIP-Pool-ID.

Schritt 10: Hinzufügen einer statischen Route mit Ihrer Instance als Ziel

Schließen Sie diesen Schritt ab, um eine Route hinzuzufügen, die den Datenverkehr von Ihrem BYOIP-Bereich zur Netzwerkschnittstelle Ihrer Ziel-Instance weiterleitet.

AWS Konsole

1. Klicken Sie im Navigationsbereich der VPC-Konsole auf Routing-Tabellen und wählen Sie die erstellte Routing-Tabelle für das Internet-Gateway aus.
2. Wählen Sie Aktionen und dann Routen bearbeiten.
3. Wählen Sie Route hinzufügen aus.
4. Geben Sie als Ziel Ihren BYOIP-CIDR oder eine Teilmenge ein (z. B. **203.0.113.0/24**). Der Präfix muss zwischen /23 und /28 liegen.
5. Wählen Sie für Ziel die Option Netzwerkschnittstelle aus und geben Sie die ENI-ID Ihrer Instance ein (z. B. `eni-0abcdef1234567890`).
6. Wählen Sie Änderungen speichern aus.

AWS CLI

```
aws ec2 create-route \
  --route-table-id rtb-0123456789abcdef0 \
  --destination-cidr-block 203.0.113.0/24 \
  --network-interface-id eni-0abcdef1234567890 \
  --region us-east-1
```

Schritt 11: Konfigurieren der Ziel-Instance

Führen Sie diesen Schritt aus, um Ihre Ziel-Instance zu konfigurieren, sodass der für BYOIP-Adressen bestimmte Datenverkehr ordnungsgemäß verarbeitet wird.

Wichtig: Schließen Sie die Instance-Konfiguration ab, bevor Sie die Konnektivität testen (Schritt 12). Damit das Ingress-Routing funktioniert, muss die Instance dafür konfiguriert sein, auf BYOIP-Adressen zu reagieren.

AWS Konsole

1. Stellen Sie mit EC2 Instance Connect eine Verbindung zu Ihrer Ziel-Instance her:

- Wählen Sie in der EC2-Konsole Ihre Instance aus.
- Wählen Sie Aktionen > Verbinden aus.
- Wählen Sie die Registerkarte EC2 Instance Connect aus.
- Wählen Sie Connect aus.

2. Fügen Sie Ihrer Instance-Schnittstelle eine BYOIP-IP-Adresse hinzu:

Suchen Sie zunächst nach dem Namen Ihrer Netzwerkschnittstelle:

```
ip link show
```

Fügen Sie dann die IP-Adresse hinzu (ersetzen Sie `203.0.113.10` durch eine IP aus Ihrem BYOIP-Bereich):

```
sudo ip addr add 203.0.113.10/32 dev eth0
```

Hinweis: Ersetzen Sie `203.0.113.10` durch eine beliebige IP-Adresse aus dem BYOIP-Bereich, den Sie testen möchten. Der Schnittstellenname kann je nach Instance-Typ `eth0`, `ens5` oder ähnlich lauten.

3. Deaktivieren Sie in der EC2-Konsole die Quell-/Zielprüfung:

- Wählen Sie Ihre Instance aus.
- Gehen Sie zur Registerkarte Netzwerk und klicken Sie auf die Netzwerkschnittstelle.
- Wählen Sie Aktionen, Quell-/Zielprüfung ändern, Deaktivieren aus.

AWS CLI

```
aws ec2 modify-network-interface-attribute \  
  --network-interface-id eni-0abcdef1234567890 \  
  --no-source-dest-check \  
  --region us-east-1
```

Schritt 12: Konfigurieren der Instance für die Verarbeitung des Datenverkehrs

Führen Sie diesen Schritt aus, um Ihrer Instance BYOIP-Adressen hinzuzufügen und die Quell-/Zielprüfung zu deaktivieren. Das ermöglicht die ordnungsgemäße Verarbeitung des Datenverkehrs.

AWS Konsole

1. Stellen Sie mit EC2 Instance Connect eine Verbindung zu Ihrer Ziel-Instance her:

- Wählen Sie in der EC2-Konsole Ihre Instance aus.
- Wählen Sie Aktionen > Verbinden aus.
- Wählen Sie die Registerkarte EC2 Instance Connect aus.
- Wählen Sie Connect aus.

2. Fügen Sie Ihrer Instance-Schnittstelle eine BYOIP-IP-Adresse hinzu:

Suchen Sie zunächst nach dem Namen Ihrer Netzwerkschnittstelle:

```
ip link show
```

Fügen Sie dann die IP-Adresse hinzu (ersetzen Sie ens5 durch den tatsächlichen Schnittstellennamen):

```
sudo ip addr add 203.0.113.10/32 dev ens5
```

Hinweis: Ersetzen Sie `203.0.113.10` durch eine beliebige IP-Adresse aus dem BYOIP-Bereich, den Sie testen möchten. Der Schnittstellename kann je nach Instance-Typ `eth0`, `ens5` oder ähnlich lauten.

3. Deaktivieren Sie in der EC2-Konsole die Quell-/Zielprüfung:

- Wählen Sie Ihre Instance aus.
- Gehen Sie zur Registerkarte Netzwerk und klicken Sie auf die Netzwerkschnittstelle.
- Wählen Sie Aktionen, Quell-/Zielprüfung ändern, Deaktivieren aus.

AWS CLI

```
aws ec2 modify-network-interface-attribute \  
  --network-interface-id eni-0abcdef1234567890 \  
  --no-source-dest-check \  
  --region us-east-1
```

Schritt 13: Testen der Verbindung

Führen Sie diesen Schritt aus, um zu überprüfen, ob der Internetverkehr ordnungsgemäß über die BYOIP-Adressen an Ihre Ziel-Instance weitergeleitet wird.

1. Überwachen Sie den eingehenden Datenverkehr auf Ihrer Ziel-Instance mithilfe von tcpdump:

```
sudo tcpdump -i any icmp
```

2. Testen Sie an einem anderen Terminal oder Computer die Konnektivität zu Ihrer BYOIP-IP-Adresse:

```
ping 203.0.113.10
```

3. Erwartete Ergebnisse:

- Der Ping-Befehl sollte erfolgreich sein und Antworten von Ihrer BYOIP-IP-Adresse zeigen.
- tcpdump sollte eingehende Pakete für die BYOIP-Adresse anzeigen, etwa so:

```
12:34:56.789012 IP 203.0.113.100 > 203.0.113.10: ICMP echo request, id 1234, seq 1, length 64
12:34:56.789123 IP 203.0.113.10 > 203.0.113.100: ICMP echo reply, id 1234, seq 1, length 64
```

- Der Datenverkehr sollte so aussehen, als stamme er von externen IP-Adressen. Das beweist, dass das Ingress-Routing des Internet-Gateways den Internetverkehr an Ihre Instance weiterleitet.

Fehlerbehebung

Verwenden Sie diesen Abschnitt, um häufig auftretende Probleme zu lösen, die bei der Einrichtung des Internet-Gateway-Ingress-Routings auftreten können.

Datenverkehr kommt nicht bei der Instance an

- Prüfen Sie, ob die richtige ENI-ID als Ziel für die Routing-Tabelle angegeben ist.
- Stellen Sie sicher, dass der BYOIP-Pool zur Routing-Tabelle für das Internet-Gateway zugeordnet ist.
- Vergewissern Sie sich, dass die Quell-/Zielprüfung für die Instance deaktiviert ist.
- Stellen Sie sicher, dass Sicherheitsgruppen den Datenverkehrstyp zulassen, den Sie testen.

Erstellung der Route schlägt fehl

- Stellen Sie sicher, dass der BYOIP-Pool der Routing-Tabelle ordnungsgemäß zugeordnet ist.
- Vergewissern Sie sich, dass der Ziel-CIDR innerhalb Ihres BYOIP-Bereichs liegt.
- Prüfen Sie, ob die Ziel-ENI vorhanden ist und an eine laufende Instance angefügt ist.
- Stellen Sie sicher, dass Ihr BYOIP-Präfix zwischen /23 und /28 liegt (Präfixe außerhalb dieses Bereichs werden nicht unterstützt).

Ping/Konnektivität schlägt fehl

- Stellen Sie sicher, dass die IP-Adressen der Instance-Schnittstelle hinzugefügt wurden.
- Prüfen Sie, ob Sicherheitsgruppen ICMP (für Ping) oder relevante Ports zulassen.
- Vergewissern Sie sich, dass sich die Instance im aktiven Zustand befindet.
- Führen Sie den Test von mehreren externen Standorten durch.

Erweiterte Option: Route-Server-Integration für dynamisches Routing

Für Umgebungen, die ein automatisches Failover erfordern, kann diese Funktion in VPC Route Server integriert werden. Das ermöglicht Folgendes:

- Dynamische Routen-Aktualisierung bei Instance-Ausfällen
- Keine manuellen Eingriffe bei der Routenverwaltung
- Verfügbarkeit auf Unternehmensniveau für kritische Workloads

Dies ist besonders wichtig für Telekommunikations- und IoT-Anwendungsfälle, in denen eine hohe Verfügbarkeit unerlässlich ist.

Note

Bei der Verwendung von Route Server mit mehreren BGP-Peers sollten Sie beachten, dass maximal 32 BGP-Peers dasselbe Präfix für dieselbe Routing-Tabelle ankündigen können.

Für Umgebungen, die dynamisches Routing, automatisches Failover und die Lastverteilung auf mehrere Instances erfordern, sollten Sie die Integration in AWS Route Server in Betracht ziehen. Route Server ermöglicht BGP-basiertes dynamisches Routing anstelle von statischen Routen. Das bietet folgende Vorteile:

- Dynamische Routenankündigung von Instances über BGP
- Automatisches Failover zwischen mehreren Ziel-Instances
- Lastverteilung auf mehrere Endpunkte
- Zentralisiertes Routenmanagement über BGP-Protokolle

Dies ist ein wichtiger Anwendungsfall für Bereitstellungen im Unternehmen, die hohe Verfügbarkeit und dynamische Routing-Funktionen erfordern. Detaillierte Anweisungen zur Einrichtung von Route Server finden Sie in der [Dokumentation für AWS Route Server](#).

Bereinigen

Um laufende Gebühren zu vermeiden, sollten Sie die Ressourcen löschen, die Sie für dieses Tutorial erstellt haben:

Schritt 1: Beenden der EC2-Instance

Schließen Sie diesen Schritt ab, um die EC2-Instance zu beenden, damit keine weiteren Gebühren für Rechenressourcen anfallen.

AWS Konsole

1. Öffnen Sie die [Amazon EC2-Konsole](#).
2. Wählen Sie im Navigationsbereich der EC2-Konsole die Option Instances aus.
3. Wählen Sie die Instance und dann Instance-Status, Instance beenden aus.
4. Wählen Sie zur Bestätigung Beenden aus.

AWS CLI

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 --region us-east-1
```

Schritt 2: Trennen eines Internet-Gateways von einer VPC

Führen Sie diesen Schritt aus, um das Internet-Gateway von Ihrer VPC zu trennen und zu löschen.

AWS Konsole

1. Öffnen Sie die [Amazon VPC-Konsole](#).

2. Wählen Sie im Navigationsbereich der VPC-Konsole die Option Internet-Gateways aus.
3. Wählen Sie das Internet-Gateway und dann Aktionen, Von VPC trennen aus.
4. Wählen Sie Internet-Gateway trennen aus.
5. Wählen Sie anschließend Aktionen, Internet-Gateway löschen aus.
6. Wählen Sie Internet-Gateway löschen aus.

AWS CLI

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id vpc-0123456789abcdef0 --region us-east-1

aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --region us-east-1
```

Schritt 3: Löschen der VPC

Führen Sie diesen Schritt aus, um die VPC und alle zugehörigen Ressourcen zu löschen und damit die Bereinigung abzuschließen.

AWS Konsole

1. Wählen Sie in der VPC-Konsole Ihre VPCs aus.
2. Wählen Sie die VPC aus und klicken Sie auf Aktionen, VPC löschen.
3. Geben Sie zur Bestätigung **delete** ein und wählen Sie Löschen aus.

AWS CLI

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0 --region us-east-1
```

Note

Durch das Löschen der VPC werden auch die zugehörigen Subnetze, Routing-Tabellen und Sicherheitsgruppen gelöscht.

 Note

Ihr BYOIP-Pool bleibt für die zukünftige Verwendung verfügbar und wird im Rahmen dieser Bereinigung nicht gelöscht.

Dynamisches Routing in Ihrer VPC mit VPC Route Server

Amazon VPC Route Server vereinfacht das Routing des Datenverkehrs zwischen Workloads, die innerhalb einer VPC bereitgestellt werden, und ihren Internet-Gateways. Mit dieser Funktion aktualisiert der VPC-Routenserver VPC- und Internet-Gateway-Routentabellen dynamisch mit Ihren bevorzugten IPv4 IPv6 OD-Routen, um die Routing-Fehlertoleranz für diese Workloads zu erreichen. Auf diese Weise können Sie den Datenverkehr innerhalb einer VPC automatisch umleiten, was die Verwaltbarkeit des VPC-Routings und die Interoperabilität mit Workloads von Drittanbietern verbessert.

Der Route Server unterstützt die folgenden Routing-Tabellentypen:

- VPC-Routing-Tabellen, die nicht mit Subnetzen verknüpft sind
- Subnetz-Routingtabellen
- Routing-Tabellen für das Internet-Gateway

Der Route Server unterstützt keine Routing-Tabellen, die virtuellen privaten Gateways zugeordnet sind. Verwenden Sie [Transit Gateway Connect](#), um Routen in eine Transit-Gateway-Routing-Tabelle zu übertragen.

Kontingente

Informationen zu den mit Amazon VPC Route Server verbundenen Kontingenten finden Sie unter [Routenserver-Kontingente](#).

Preise

Informationen zu den Kosten im Zusammenhang mit Amazon VPC Route Server finden Sie auf der Amazon-VPC-Preisseite unter der Registerkarte [VPC Route Server](#).

Inhalt

- [Terminologie](#)
- [Funktionsweise von Amazon VPC Route Server](#)

- [Peer-Protokollierung des Route Servers](#)
- [Erste-Schritte-Tutorial](#)

Terminologie

Die folgenden Begriffe werden in dieser Anleitung verwendet:

- FIB: Die [Forwarding Information Base \(FIB\)](#) dient als Weiterleitungstabelle für die Routen, die der Route Server nach Auswertung aller verfügbaren Routing-Informationen und Richtlinien als die besten Routen in der RIB ermittelt hat. Die FIB-Routen, die in den Routing-Tabellen installiert sind. Die FIB wird bei jeder Änderung der RIB neu berechnet.
- RIB: Die [Routing Information Base \(RIB\)](#) dient als Datenbank, in der alle Routing-Informationen und Netzwerktopologiedaten gespeichert werden, die von einem Router oder Routing-System gesammelt wurden, z. B. Routen, die von BGP-Peers abgerufen wurden. Die RIB wird ständig aktualisiert, wenn neue Routing-Informationen eingehen oder sich bestehende Routen ändern. Dadurch wird sichergestellt, dass der Route Server immer den aktuellsten Überblick über die Netzwerktopologie hat und optimale Routing-Entscheidungen treffen kann.
- Routenserver: Die Routenserver-Komponente aktualisiert Ihre VPC- und Internet-Gateway-Routentabellen mit den IPv4 oder IPv6 -Routen in Ihrer Forwarding Information Base (FIB). Der Route Server stellt eine einzige FIB und Routing Information Base (RIB) dar.
- Routenserver-Zuordnung: Eine Routenserver-Zuordnung ist die Verbindung, die zwischen einem Route Server und einer VPC hergestellt wird.
- Routenserver-Endpunkt: Ein Routenserver-Endpunkt ist eine AWS verwaltete Komponente innerhalb eines Subnetzes, die [BGP-Verbindungen \(Border Gateway Protocol\)](#) zwischen Ihrem Routenserver und Ihren BGP-Peers ermöglicht.
- Route-Server-Peer: Ein Route-Server-Peer ist eine Sitzung zwischen einem Route-Server-Endpunkt und dem Gerät, auf dem das Gerät installiert ist AWS (z. B. eine Firewall-Appliance oder eine andere Netzwerksicherheitsfunktion, die auf einer Instanz ausgeführt wird). EC2 Das Gerät muss die folgenden Anforderungen erfüllen:
 - Über eine Elastic-Network-Schnittstelle in der VPC verfügen
 - BGP (Border Gateway Protocol) unterstützen
 - BGP-Sitzungen initiieren können
- Routenserver-Verbreitung: Wenn diese Option aktiviert ist, installiert Routenserver-Verbreitung die Routen in der FIB in der von Ihnen angegebenen Routing-Tabelle. Route-Server unterstützt IPv4 und leitet IPv6 die Ausbreitung weiter.

Funktionsweise von Amazon VPC Route Server

In diesem Abschnitt wird erklärt, wie Amazon VPC Route Server funktioniert und wie er die Routing-Fehlertoleranz für Ihre in Subnetzen ausgeführten Workloads erreicht.

Inhalt

- [-Übersicht](#)
- [Diagramme](#)

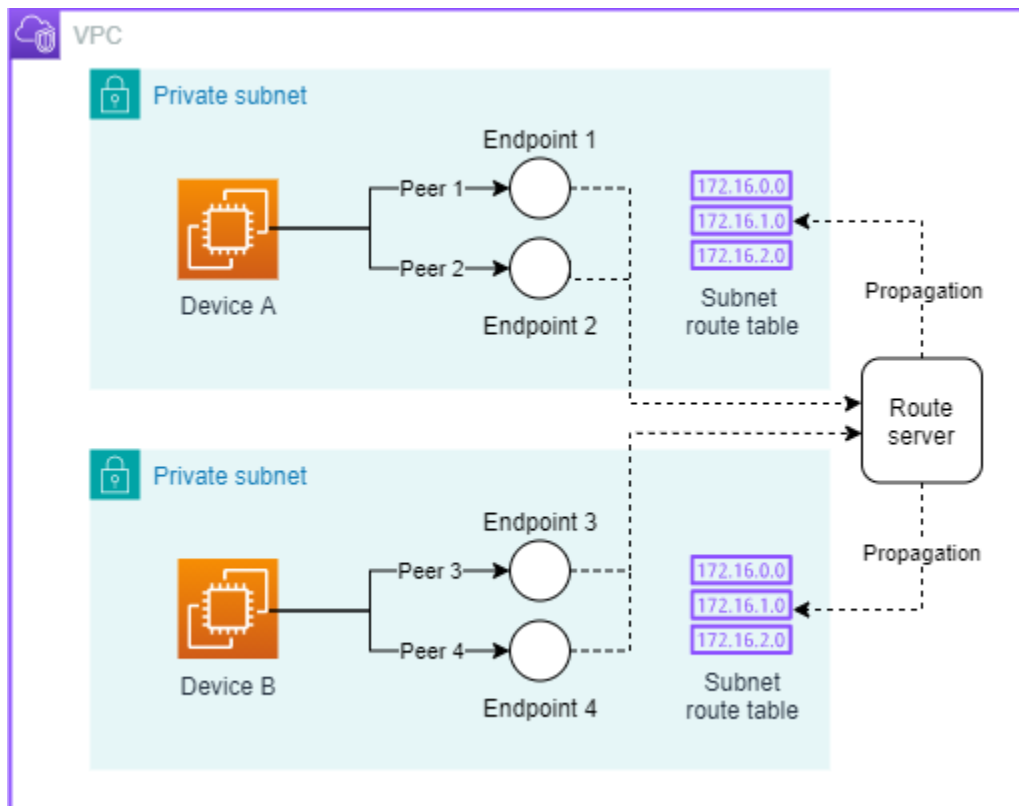
-Übersicht

Funktionsweise von Amazon VPC Route Server:

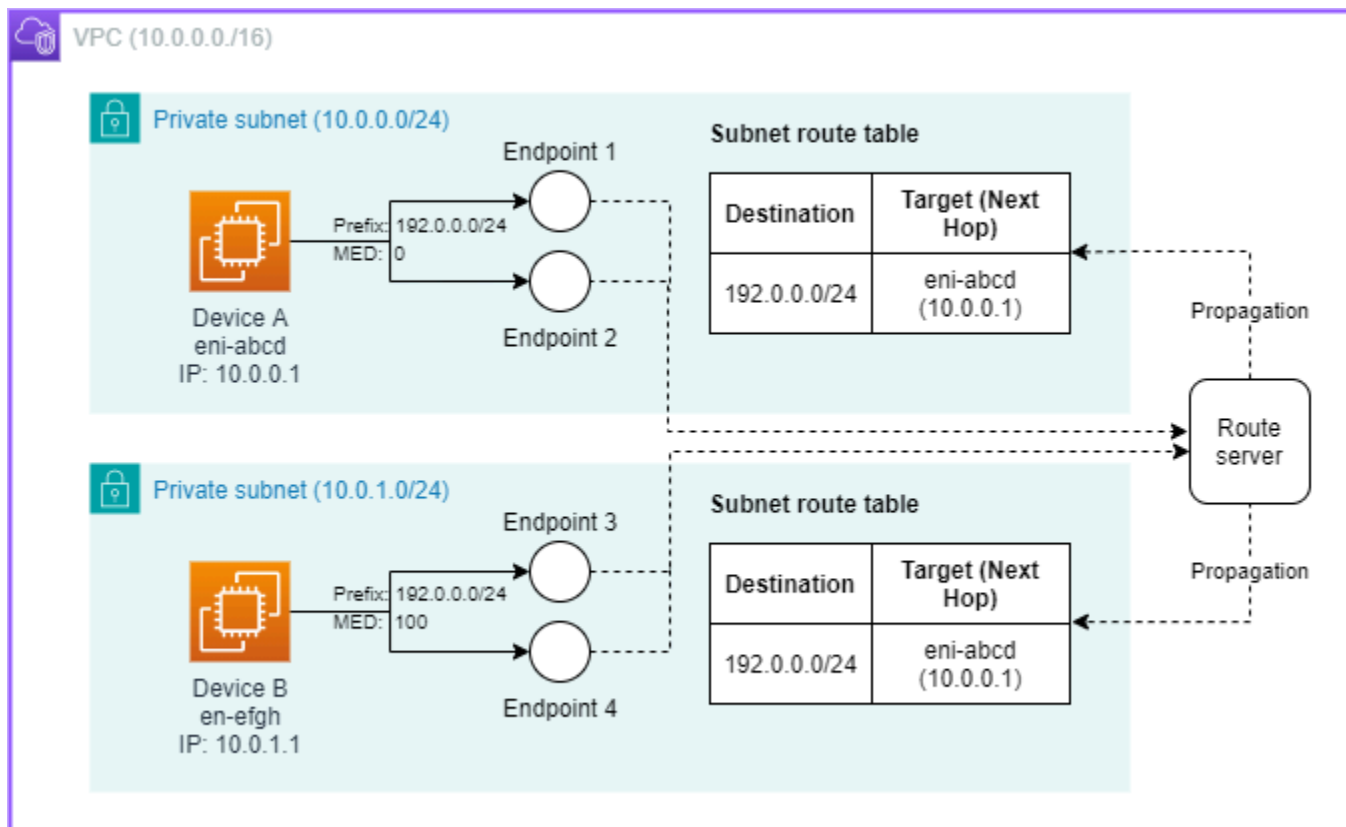
1. Sie konfigurieren ein Netzwerkgerät (wie eine Firewall, die auf einer EC2 Instance in der VPC ausgeführt wird) für die Verwendung von Amazon VPC Route Server.
2. Das Netzwerkgerät fällt aus.
3. Die Routenserver-Endpunkte erkennen den Fehler über [BFD \(Bidirectional Forwarding Detection\)](#), das auf dem Routenserver-Peer konfiguriert ist.
4. Die Routenserver-Endpunkte aktualisieren den Route Server so, dass er Routen in einer [Routing Information Base \(RIB\)](#) zurückzieht, in der das ausgefallene Gerät der nächste Hop ist.
5. Der Route Server berechnet aus der RIB eine [Forwarding Information Base \(FIB\)](#) und wählt dabei die besten verfügbaren Routen aus.
6. Der Route Server aktualisiert die konfigurierten Routing-Tabellen mit den Routen von der FIB.
7. Der gesamte neue Verkehr wird an das Standby-Gerät weitergeleitet.

Diagramme

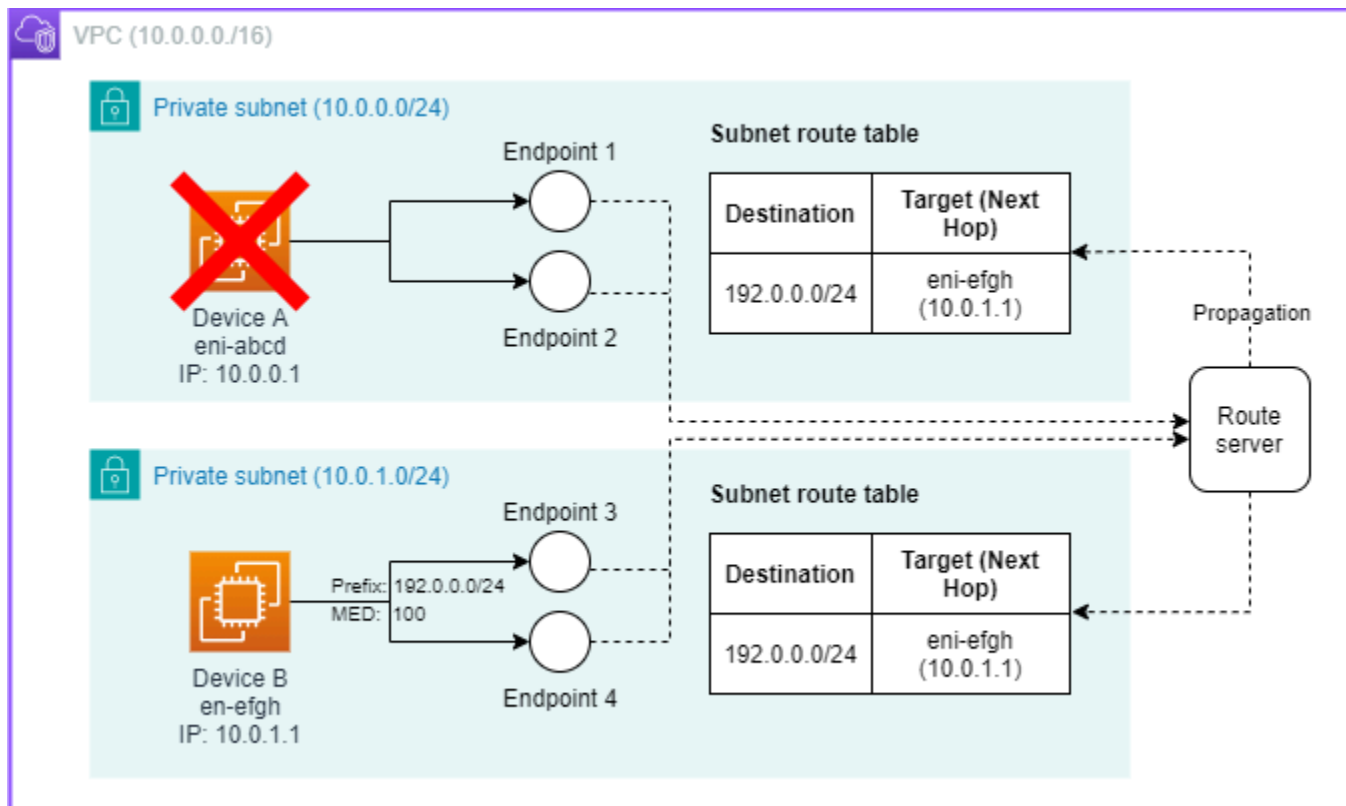
Im Folgenden finden Sie ein Beispieldiagramm eines VPC-Routenservers mit Routenserver-Endpunkten, die für Geräte in zwei Subnetzen konfiguriert sind.



Ausgehend vom obigen Beispiel als Baseline zeigt das folgende Beispiel ein detaillierteres Design, bei dem sowohl Gerät A als auch Gerät B über BGP angeben, dass sie beliebigen Verkehr mit einer Ziel-IP im Bereich von 192.0.0.0/24 (von 192.0.0.0 bis 192.0.0.255) annehmen können. Das Multi-Exit Diskriminator (MED)-Attribut von 0 teilt dem Routenserver mit, dass Gerät A Gerät B vorzuziehen ist. Der Routenserver empfängt die Route und das MED-Attribut von Gerät A und installiert diese Route in den Subnetz-Routing-Tabellen mit der Netzwerkschnittstelle von Gerät A als „nächster Hop“. Infolgedessen wird jeglicher Verkehr innerhalb des Subnetzes mit einer Ziel-IP im Bereich 192.0.0.0/24 an Gerät A gesendet. Gerät A verarbeitet den Verkehr dann und sendet ihn weiter. Der Datenverkehr innerhalb eines Subnetzes (10.0.0.0/24 oder 10.0.1.0/24), der an 192.0.0.0/24 gebunden ist, wird als nächster Hop an Gerät A eni-abcd (10.0.0.1) weitergeleitet.



Das letzte Beispiel unten zeigt, wie der Route Server mit dem Failover umgeht. Das höhere MED-Attribut teilt dem Route Server zwar mit, dass Gerät B weniger bevorzugt ist als Gerät A, aber wenn Gerät A eni-abcd (10.0.0.1) ausfällt, aktualisiert der Route Server die Subnetz-Routing-Tabellen und der Verkehr zu 192.0.0.0/24 wird als nächster Hop an Gerät B eni-efgh (10.0.1.1) weitergeleitet.



Peer-Protokollierung des Route Servers

Verwenden Sie die VPC-Routenserver-Peer-Protokollierung für Folgendes:

- Überwachen des Zustands von BGP- und BFD-Sitzungen
- Fehlerbehebung bei Verbindungsproblemen
- Überprüfen historischer Sitzungsänderungen
- Verfolgen des Netzwerkstatus

Preisgestaltung

- CloudWatch: Wenn Sie Route-Server-Peer-Logs in Logs veröffentlichen, fallen Gebühren für Datenaufnahme und Archivierung für verkaufte Logs an. CloudWatch
- S3: Für die Datenerfassung und Archivierung fallen Gebühren für angebotene Protokolle an, wenn Sie Routenserver-Peer-Protokolle in Amazon S3 veröffentlichen.
- Data Firehose: Es fallen die üblichen Kosten für Erfassung und Lieferung an.

Verkaufte Logs sind Logs von bestimmten AWS Services, die zu volumenabhängigen Preisen erhältlich sind und an CloudWatch Logs, Amazon S3 oder Amazon Data Firehose geliefert werden. Weitere Informationen finden Sie unter [Amazon CloudWatch Pricing](#), wählen Sie Logs aus und suchen Sie nach Vending Logs.

Beispielprotokollformat

```
{
  "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
  "event_timestamp": 1746643505367,
  "type": "RouteStatus",
  "status": "ADVERTISED",
  "message": {
    "prefix": "10.24.34.0/32",
    "asPath": "65000",
    "med": 100,
    "nextHopIp": "10.24.34.1"
  }
}

{
  "resource_arn": "arn:aws:ec2:us-east-1:111122223333:route-server-peer/
rsp-1234567890abcdef0",
  "event_timestamp": 1746643490000,
  "type": "BGPStatus",
  "status": "UP",
  "message": null
}
```

Wobei Folgendes gilt:

- Das `resource_arn` ist der ARN für den Routenserver-Peer.
- Das `event_timestamp` ist der Zeitstempel des Ereignisses.
- Der `type` der von uns erzeugten Protokollereignisse (RouteStatus, BGPStatus, BFDStatus).
- Das `status`-Feld ist das Status-Update.
 - Für Nachrichten vom Typ RouteStatus
 - ADVERTISED (Die Route wurde vom Peer angekündigt)
 - UPDATED (Die bestehende Route wurde vom Peer aktualisiert)
 - WITHDRAWN (Die Route wurde vom Peer zurückgezogen)

- Für BFDStatus- und BGPStatus-Updates
 - UP, DOWN.
- Das message Feld wird derzeit nur für Routenattribute für den RouteStatus Nachrichtentyp verwendet, kann aber mit relevanten Informationen für jeden Typ gefüllt werden.

AWS Management Console

So erstellen Sie Peer-Protokolle für Routenserver:

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Route Server.
3. Wählen Sie auf der Seite Route Server die Option Routenserver-Peers aus.
4. Wählen Sie die Registerkarte Protokollzustellung.
5. Wählen Sie Protokollzustellung hinzufügen.
6. Wählen Sie ein Ziel und konfigurieren Sie die Einstellungen:
 - CloudWatch Amazon-Protokolle
 - Protokolltyp: Arten von Protokollen, die zugestellt werden sollen. Der einzige unterstützte Protokolltyp ist EVENT_LOGS.
 - Zielprotokollgruppe: Die CloudWatch Protokollgruppe, in die Protokolle gesendet werden. Sie können eine bestehende Protokollgruppe auswählen oder eine neue erstellen (Beispiel:/aws/vpc/route-server-peers).
 - Feldauswahl: Datenfelder, die in Ihre Protokolle aufgenommen werden sollen.
 - Ausgabeformat: So werden Protokolle formatiert:
 - JSON: Strukturiertes Format für die Computerverarbeitung
 - Text: Klartextformat
 - Feldtrennzeichen: Bei Verwendung des Textformats ist dies das Zeichen, das Felder voneinander trennt (Beispiel: Komma, Tabulator, Leerzeichen).
 - Amazon S3
 - Kontoübergreifend — Logs an verschiedene Konten senden AWS
 - Protokolltyp: Arten von Protokollen, die zugestellt werden sollen. Der einzige unterstützte Protokolltyp ist EVENT_LOGS.

- **Lieferziel-ARN:** Der Amazon-Ressourcenname des S3-Buckets in einem anderen AWS Konto, an das Protokolle gesendet werden.
- **Feldauswahl:** Datenfelder, die in Ihre Protokolle aufgenommen werden sollen.
- **Suffix:** Die den Namen der Protokolldateien hinzugefügte Endung (Beispiel: .log, .txt).
- **Hive-kompatibel:** Wenn diese Option aktiviert ist, werden Protokolle in einer Ordnerstruktur organisiert, die Hive-basierte Tools nutzt, um die Suche mit Services wie Amazon Athena zu vereinfachen.
- **Feldtrennzeichen:** Bei Verwendung des Textformats ist dies das Zeichen, das Felder voneinander trennt.
- **Im aktuellen Konto**
 - **Protokolltyp:** Arten von Protokollen, die zugestellt werden sollen. Der einzige unterstützte Protokolltyp ist `EVENT_LOGS`.
 - **Ziel-S3-Bucket:** Der S3-Bucket in Ihrem Konto, in den Protokolle gesendet werden. Sie können einen Unterordnerpfad angeben.
 - **Feldauswahl:** Datenfelder, die in Ihre Protokolle aufgenommen werden sollen.
 - **Suffix:** Die den Namen der Protokolldateien hinzugefügte Endung (Beispiel: .log, .txt).
 - **Hive-kompatibel:** Wenn diese Option aktiviert ist, werden Protokolle in einer Ordnerstruktur organisiert, die Hive-basierte Tools nutzt, um die Suche zu vereinfachen.
 - **Feldtrennzeichen:** Bei Verwendung des Textformats ist dies das Zeichen, das Felder voneinander trennt.
- **Amazon Data Firehose**
 - **Kontoübergreifend**
 - **Protokolltyp:** Arten von Protokollen, die zugestellt werden sollen. Der einzige unterstützte Protokolltyp ist `EVENT_LOGS`.
 - **Lieferziel-ARN:** Der Amazon-Ressourcenname des Firehose-Lieferstreams in einem anderen AWS Konto.
 - **Feldauswahl:** Datenfelder, die in Ihre Protokolle aufgenommen werden sollen.
 - **Feldtrennzeichen:** Bei Verwendung des Textformats ist dies das Zeichen, das Felder voneinander trennt.
 - **Im aktuellen Konto**

- **Protokolltyp:** Arten von Protokollen, die zugestellt werden sollen. Der einzige unterstützte Protokolltyp ist `EVENT_LOGS`.
- **Zielstream für die Lieferung:** Der Firehose-Lieferstream in Ihrem Konto, an den Protokolle gesendet werden. Der Stream muss den Quelltyp „Direct Put“ verwenden.
- **Feldauswahl:** Datenfelder, die in Ihre Protokolle aufgenommen werden sollen.
- **Ausgabeformat:** So werden Protokolle formatiert:
 - **JSON:** Strukturiertes Format für die Computerverarbeitung
 - **Text:** Klartextformat
- **Feldtrennzeichen:** Bei Verwendung des Textformats ist dies das Zeichen, das Felder voneinander trennt.

Command line

Die Befehle in diesem Abschnitt sind mit der AWS CLI -Befehlsreferenz verknüpft. Die Dokumentation enthält detaillierte Beschreibungen der Optionen, die Sie beim Ausführen der Befehle verwenden können.

So erstellen Sie Peer-Protokolle für Route Server:

1. Verwenden Sie den Befehl [put-delivery-source](#).

- **Beispielanforderung**

```
aws logs put-delivery-source --name "source-rsp-1234567890abcdef0" --  
resource-arn "arn:aws:ec2:us-east-1:111122223333:route-server-peer/  
rsp-1234567890abcdef0" --log-type "EVENT_LOGS"
```

- **Beispielantwort**

```
{  
  "deliverySource": {  
    "name": "source-rsp-1234567890abcdef0",  
    "arn": "arn:aws:logs:us-east-1:111122223333:delivery-source:source-  
rsp-1234567890abcdef0",  
    "resourceArns": [  
      "arn:aws:ec2:us-east-1:111122223333:route-server-peer/  
rsp-1234567890abcdef0"  
    ],  
    "service": "ec2",  
  },  
}
```

```
    "logType": "EVENT_LOGS"
  }
}
```

2. Verwenden Sie den Befehl [put-delivery-destination](#).

- Das folgende AWS CLI-Beispiel erstellt ein Routenserver-Protokoll. Die Protokolle werden an die angegebene Protokollgruppe übermittelt.
- Beispielanforderung

```
aws logs put-delivery-destination --name "destination-rsp-abcdef01234567890"
--destination-resource-arn "arn:aws:logs:us-east-1:111122223333:log-group:/
aws/vendedlogs/ec2/route-server-peer/EVENT_LOGS/rsp-abcdef01234567890"
```

- Beispielantwort

```
{
  "deliveryDestination": {
    "name": "destination-rsp-abcdef01234567890",
    "arn": "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890",
    "deliveryDestinationType": "CWL",
    "deliveryDestinationConfiguration": {
      "destinationResourceArn": "arn:aws:logs:us-
east-1:111122223333:log-group:/aws/vendedlogs/ec2/route-server-peer/
EVENT_LOGS/rsp-abcdef01234567890"
    }
  }
}
```

3. Verwenden Sie den Befehl [create-delivery](#).

- Beispielanforderung

```
aws logs create-delivery --delivery-source-name "source-rsp-1234567890abcdef0"
--delivery-destination-arn "arn:aws:logs:us-east-1:111122223333:delivery-
destination:destination-rsp-abcdef01234567890"
```

- Beispielantwort

```
{
  "delivery": {
```

```
    "id": "1234567890abcdef0",
    "arn": "arn:aws:logs:us-
east-1:111122223333:delivery:1234567890abcdef0",
    "deliverySourceName": "source-rsp-1234567890abcdef0",
    "deliveryDestinationArn": "arn:aws:logs:us-
east-1:111122223333:delivery-destination:destination-rsp-abcdef01234567890",
    "deliveryDestinationType": "CWL",
    "recordFields": [
        "resource_arn",
        "event_timestamp",
        "type",
        "status",
        "message"
    ]
}
```

Erste-Schritte-Tutorial

Dieses Tutorial erläutert den Prozess zum Einrichten und Konfigurieren des VPC-Routenservers, um dynamisches Routing in Ihrer VPC zu aktivieren. Sie erfahren, wie Sie alle erforderlichen Komponenten erstellen und konfigurieren, das BGP-Peering einrichten und den ordnungsgemäßen Betrieb überprüfen. Das Tutorial deckt alles ab, von der ersten IAM-Einrichtung über Tests bis hin zur Bereinigung.

Bevor Sie mit diesem Tutorial beginnen, stellen Sie sicher, dass Sie über Folgendes verfügen:

- Administrativer Zugriff auf Ihr AWS Konto
- eine VPC mit mindestens zwei Subnetzen, in denen Sie dynamisches Routing aktivieren möchten
- Netzwerkgeräte (wie Firewalls, die auf EC2 Instanzen ausgeführt werden), die BGP unterstützen und als Route-Server-Peer-Geräte dienen können
- Grundkenntnisse in BGP-Konzepten und Netzwerken AWS

Die Schritte können entweder über die AWS Management Console oder ausgeführt werden. AWS CLI Beide Methoden sind für jeden Schritt verfügbar.

Geschätzte Zeit bis zum Abschluss des Vorgangs: 15–30 Minuten

Schritte

- [Schritt 1: Die erforderlichen Berechtigungen für die IAM-Rolle konfigurieren](#)
- [Schritt 2: Einen Route Server erstellen](#)
- [Schritt 3: Einen Route Server zu einer VPC zuweisen](#)
- [Schritt 4: Routenserver-Endpunkte erstellen](#)
- [Schritt 5: Routenserver-Verbreitung aktivieren](#)
- [Schritt 6: Einen Routenserver-Peer erstellen](#)
- [Schritt 7: BGP-Sitzungen von den Geräten aus initiieren](#)
- [Schritt 8: Bereinigen](#)

Schritt 1: Die erforderlichen Berechtigungen für die IAM-Rolle konfigurieren

Stellen Sie zur Verwendung von VPC Route Server sicher, dass der IAM-Benutzer oder die verwendete Rolle über die erforderlichen IAM-Berechtigungen verfügt. Im Folgenden finden Sie eine Anleitung, welche Berechtigungen für jede API erforderlich sind:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateRouteServer",
      "Effect": "Allow",
      "Action": [
        "sns:CreateTopic"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DeleteRouteServer",
      "Effect": "Allow",
      "Action": [
        "sns:DeleteTopic"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CreateRouteServerEndpoint",
      "Effect": "Allow",
```

```

        "Action": [
            "ec2:CreateNetworkInterface",
            "ec2:CreateNetworkInterfacePermission",
            "ec2:CreateSecurityGroup",
            "ec2:DescribeSecurityGroups",
            "ec2:AuthorizeSecurityGroupIngress",
            "ec2:CreateTags",
            "ec2>DeleteTags"
        ],
        "Resource": "*"
    },
    {
        "Sid": "DeleteRouteServerEndpoint",
        "Effect": "Allow",
        "Action": [
            "ec2>DeleteNetworkInterface",
            "ec2>DeleteSecurityGroup",
            "ec2:RevokeSecurityGroupIngress",
            "ec2:CreateTags",
            "ec2>DeleteTags"
        ],
        "Resource": "*"
    },
    {
        "Sid": "CreateRouteServerPeer",
        "Effect": "Allow",
        "Action": [
            "ec2:AuthorizeSecurityGroupIngress"
        ],
        "Resource": "*"
    },
    {
        "Sid": "DeleteRouteServerPeer",
        "Effect": "Allow",
        "Action": [
            "ec2:RevokeSecurityGroupIngress"
        ],
        "Resource": "*"
    }
}

```


Schritt 2: Einen Route Server erstellen

Führen Sie die Schritte in diesem Abschnitt durch, um einen Route Server zu erstellen.

Die Routenserver-Komponente aktualisiert Ihre VPC- und Internet-Gateway-Routentabellen mit den IPv4 oder IPv6 -Routen in Ihrer Forwarding Information Base (FIB). Der Route Server stellt eine einzige FIB und Routing Information Base (RIB) dar.

AWS Management Console

So erstellen Sie einen Route Server

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Route Server.
3. Wählen Sie auf der Seite Route Server die Option Route Server erstellen aus.
4. Konfigurieren Sie auf der Seite Route Server erstellen die folgenden Einstellungen:
 - Geben Sie unter Name einen Namen für Ihren Routenserver ein (z. B. "my-route-server-01"). Der Name darf maximal 255 Zeichen lang sein.
 - Geben Sie für Amazon Side ASN einen BGP-ASN-Wert ein. Der Wert muss im Bereich von 1–4294967295 liegen. Wir empfehlen die Verwendung einer privaten ASN im Bereich von 64512 bis 65534 (16-Bit-ASN) oder 4200000000 bis 4294967294 (32-Bit-ASN).
 - Wählen Sie für Dauerhafte Routen entweder Aktivieren oder Deaktivieren aus. Diese Option bestimmt, ob Routen beibehalten werden sollen, nachdem alle BGP-Sitzungen beendet wurden:
 - Falls aktiviert: Routen werden in der Routing-Datenbank des Route Servers beibehalten, auch wenn alle BGP-Sitzungen enden
 - Falls deaktiviert: Routen werden aus der Routing-Datenbank entfernt, wenn alle BGP-Sitzungen enden
 - Wenn Sie dauerhafte Routen aktiviert haben, geben Sie für Dauer einen Wert zwischen 1 und 5 Minuten ein. Diese Dauer gibt an, wie lange der Route Server nach der Wiederherstellung von BGP wartet, um die Fortdauer der Routen aufzuheben. Wenn Sie sie beispielsweise auf 1 Minute festlegen, hat Ihr Gerät nach der Wiederherstellung von BGP eine Minute Zeit, um die Routen neu zu lernen und anzukündigen, bevor der Route Server wieder normal funktioniert. Während 1 Minute normalerweise ausreichend ist, können Sie bis zu 5 Minuten festlegen, wenn Ihr BGP-Netzwerk mehr Zeit benötigt, um alle Routen vollständig wiederherzustellen und neu zu lernen.

- (Optional) Um SNS-Benachrichtigungen für BGP-Statusänderungen zu aktivieren, schalten Sie den Schalter SNS-Benachrichtigungen aktivieren um. Durch die Aktivierung von SNS-Benachrichtigungen werden Änderungen des BGP- oder BFD-Sitzungsstatus auf Routenserver-Peers und Wartungsbenachrichtigungen für Routenserver-Endpunkte an ein von AWS bereitgestelltes SNS-Thema beibehalten. Einzelheiten zu diesen Benachrichtigungen finden Sie in der Tabelle mit den Details zu den SNS-Benachrichtigungen unten.
5. (Optional) Um Ihrem Route Server Tags hinzuzufügen, scrollen Sie nach unten zum Abschnitt Tags – optional und wählen Sie Neues Tag hinzufügen aus. Geben Sie einen Schlüssel und einen optionalen Wert für jedes Tag ein. Sie können bis zu 50 Tags hinzufügen.
 6. Überprüfen Sie die Einstellungen und klicken Sie auf Route Server erstellen.
 7. Warten Sie, bis der Route Server erstellt wurde. Sobald der Vorgang abgeschlossen ist, werden Sie zur Seite Route Server weitergeleitet, auf der Ihr neuer Route Server mit dem Status Verfügbar aufgeführt wird.

Command line

Gehen Sie wie folgt vor, um einen neuen Route Server zu erstellen, um dynamisches Routing in einer VPC zu verwalten.

Geben Sie für `--amazon-side-asn` einen BGP-ASN-Wert ein. Der Wert muss im Bereich von 1-4294967295 liegen. Wir empfehlen die Verwendung einer privaten ASN im Bereich von 64512 bis 65534 (16-Bit-ASN) oder 4200000000 bis 4294967294 (32-Bit-ASN).

1. Befehl:

```
aws ec2 create-route-server --amazon-side-asn 65000
```

Antwort:

```
{
  "RouteServer": {
    "RouteServerId": "rs-1",
    "AmazonSideAsn": 65000,
    "State": "pending"
  }
}
```

2. Warten Sie, bis der Route Server verfügbar ist.

Befehl:

```
aws ec2 describe-route-servers
```

Antwort:

```
{
  "RouteServer": {
    "RouteServerId": "rs-1",
    "AmazonSideAsn": 65000,
    "State": "available"
  }
}
```

Details zur SNS-Benachrichtigung

Die folgende Tabelle enthält Details zu den Nachrichten, die Amazon VPC Route Server mithilfe von Amazon SNS sendet:

Standardfelder		Nachrichtenattribute (Metadaten)			
Fehlermeldung	Wann sie gesendet wird	timestamp	eventCode	routeServerEndpointId	affectedRouteServerPeerIds
Der Router-Endpoint [ENDPOINT ID] wird derzeit gewartet. BFD- und BGP-Sitzungen	Wartung der Endpunkte des Route Servers	Format: 2025-02-17T15:55:00Z	ROUTE_SERVER_ENDPOINT_MAINTENANCE	Betroffene Endpunkt-ID	Liste der betroffenen Kollegen IDs

Standardfelder		Nachrichtenattribute (Metadaten)			
Welche Routen können betroffen sein.					
Fehlermeldung	Wann sie gesendet wird	timestamp	eventCode	routeServerPeerId	newBgpStatus
BGP für Routenserver-Peer [PEER ID] ist jetzt [UP/DOWN].	Änderung des BGP-Status des Routenserver-Peers	Format: 2025-02-17T15:55:00Z	ROUTE_SERVER_PEER_BGP_STATUS_CHANGE	Betroffene Peer-ID	NACH OBEN oder NACH UNTEN
Fehlermeldung	Wann sie gesendet wird	timestamp	eventCode	routeServerPeerId	newBfdStatus
BFD für Routenserver-Peer [PEER ID] ist jetzt [UP/DOWN].	Änderung des BFD-Status des Routenserver-Peers	Format: 2025-02-17T15:55:00Z	ROUTE_SERVER_PEER_BFD_STATUS_CHANGE	Betroffene Peer-ID	NACH OBEN oder NACH UNTEN

Schritt 3: Einen Route Server zu einer VPC zuweisen

Führen Sie die Schritte in diesem Abschnitt durch, um den Routen Server einer VPC zuzuweisen.

Eine Routenserver-Zuordnung ist die Verbindung, die zwischen einem Route Server und einer VPC hergestellt wird. Dies ist ein grundlegender Konfigurationsschritt, der es dem Route Server ermöglicht, mit Appliances in Ihrer VPC zu arbeiten.

Wenn Sie eine Routenserver-Zuordnung erstellen:

- Sie verbindet den Route Server mit einer bestimmten VPC.
- Sie ermöglicht dem Route Server, mit Routing-Tabellen in den Subnetzen der VPC zu interagieren.
- Sie ermöglicht dem Route Server, Routen innerhalb der zugehörigen VPC zu empfangen und zu verbreiten.
- Sie legt den Bereich fest, in dem der Route Server betrieben werden kann.

Hauptaspekte einer Routenserver-Zuordnung:

- Jeder Route Server kann einer VPC zugeordnet werden. Jede VPC kann standardmäßig bis zu 5 separate Routenserver-Zuordnungen haben. Weitere Informationen zu Kontingenten finden Sie unter [Route-Service-Kontingente](#).
- Die Zuordnung muss erstellt werden, bevor der Route Server Routen verwalten kann.
- Die Zuordnung kann überwacht werden, um ihren Status nachzuverfolgen (z. B. zuordnen und zugeordnet).
- Die Zuordnung kann entfernt (getrennt) werden, wenn Sie nicht mehr möchten, dass der Route Server in dieser VPC betrieben wird.

AWS Management Console

Einen Route Server einer VPC zuordnen

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Route Server.
3. Wählen Sie den Route Server aus, den Sie einer VPC zuordnen möchten.
4. Wählen Sie auf der Registerkarte Zuordnung die Option Route Server zuordnen aus.
5. Im Dialogfeld Routenserver zuordnen:
 - Das Feld Routenserver-ID wird automatisch mit Ihrem ausgewählten Route Server aufgefüllt
 - Wählen Sie für VPC-ID in der Drop-down-Liste die VPC aus, die Sie zuordnen möchten.
6. Wählen Sie Route Server zuordnen aus.
7. Warten Sie, bis die Zuweisung abgeschlossen ist. Sobald der Vorgang abgeschlossen ist, wird der Status auf der Registerkarte Zuordnung als Zugeordnet angezeigt.

Command line

Verwenden Sie das folgende Verfahren, um einem Route Server eine VPC zuzuordnen.

1. Befehl:

```
aws ec2 associate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

Antwort:

```
{
  "RouteServerAssociation": {
    "RouteServerId": "rs-1",
    "VpcId": "vpc-1",
    "State": "associating"
  }
}
```

2. Warten Sie, bis die Zuweisung abgeschlossen ist.

Befehl:

```
aws ec2 get-route-server-associations --route-server-id rs-1
```

Antwort:

```
{
  "RouteServerAssociation": {
    "RouteServerId": "rs-1",
    "VpcId": "vpc-1",
    "State": "associated"
  }
}
```

Schritt 4: Routenserver-Endpunkte erstellen

Führen Sie die Schritte in diesem Abschnitt durch, um Routenserver-Endpunkte zu erstellen. Erstellen Sie aus Redundanzgründen zwei Endpunkte pro Subnetz.

Ein Routenserver-Endpunkt ist eine AWS verwaltete Komponente innerhalb eines Subnetzes, die [BGP-Verbindungen \(Border Gateway Protocol\)](#) zwischen Ihrem Routenserver und Ihren BGP-Peers ermöglicht.

Routenserver-Endpunkte sind die „Kontaktpunkte“, an denen Ihre Netzwerkgeräte BGP-Sitzungen mit dem Route Server einrichten. Sie sind die Komponenten, die die BGP-Verbindungen tatsächlich verarbeiten, während der Route Server selbst die Routing-Entscheidungen und die Routenverbreitung verwaltet.

 Note

Für Routenserver-Endpunkte werden 0,75 USD pro Stunde berechnet.

AWS Management Console

So erstellen Sie Routenserver-Endpunkte

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsmenü unter Virtual Private Cloud die Option Route Server.
3. Wählen Sie den Route Server aus, für den Sie Endpunkte erstellen möchten.
4. Klicken Sie im unteren Bereich auf die Registerkarte Routenserver-Endpunkte.
5. Wählen Sie Routenserver-Endpunkt erstellen aus.
6. Konfigurieren Sie auf der Seite Routenserver-Endpunkt erstellen die folgenden Einstellungen:
 - Geben Sie unter Name einen beschreibenden Namen für Ihren Endpunkt ein.
 - Vergewissern Sie sich, dass für Route Server der richtige Route Server ausgewählt ist.
 - Wählen Sie für Subnetz das Subnetz aus, in dem der Endpunkt erstellt werden soll.
7. (Optional) Um Ihrem Routenserver-Endpunkt Tags hinzuzufügen, scrollen Sie nach unten zum Abschnitt Tags – optional und wählen Sie Neues Tag hinzufügen aus. Geben Sie einen Schlüssel und einen optionalen Wert für jedes Tag ein.
8. Überprüfen Sie die Einstellungen und wählen Sie dann Routenserver-Endpunkt erstellen.
9. Warten Sie, bis der Endpunkt erstellt wurde. Sobald der Vorgang abgeschlossen ist, wird eine Erfolgsmeldung angezeigt.
10. Wiederholen Sie die Schritte 5–9, um einen zweiten Endpunkt im selben Subnetz mit einem anderen Namen zu erstellen.

11. Wiederholen Sie die Schritte 5–10 für jedes Subnetz, in dem Sie Routenserver-Endpunkte benötigen.
12. Nachdem Sie die Endpunkte erstellt haben, kehren Sie zur Registerkarte Routenserver-Endpunkte für Ihren Route Server zurück.
13. Vergewissern Sie sich, dass für jedes Subnetz zwei Endpunkte aufgeführt sind.
14. Vergewissern Sie sich, dass der Status für jeden Endpunkt Verfügbar ist.

Command line

Gehen Sie wie folgt vor, um einen Routenserver-Endpunkt zu erstellen.

1. Befehl:

```
aws ec2 create-route-server-endpoint --route-server-id rs-1 --subnet-id subnet-1
```

Antwort:

```
{
  "RouteServerEndpoint": {
    "RouteServerId": "rs-1",
    "RouteServerEndpointId": "rse-1",
    "VpcId": "vpc-1",
    "SubnetId": "subnet-1",
    "State": "pending"
  }
}
```

2. Möglicherweise dauert es einige Minuten, bis die Endpunkte nach der Erstellung vollständig verfügbar sind.

Befehl:

```
aws ec2 describe-route-server-endpoints
```

Antwort:

```
{
  "RouteServerEndpoint": {
    "RouteServerId": "rs-1",
```



```
    "RouteServerEndpointId": "rse-1",  
    "VpcId": "vpc-1",  
    "SubnetId": "subnet-1",  
    "EniId": "eni-123",  
    "EniAddress": "10.1.2.3",  
    "State": "available"  
  }  
}
```

Wiederholen Sie die Schritte, um einen zweiten Endpunkt im selben Subnetz mit einem anderen Namen zu erstellen, und erstellen Sie Endpunkte für jedes Subnetz, das Routenserver-Endpunkte benötigt.

Schritt 5: Routenserver-Verbreitung aktivieren

Schließen Sie diesen Schritt ab, um die Routenserver-Verbreitung zu aktivieren.

Wenn diese Option aktiviert ist, installiert die Routenserver-Verbreitung die Routen in der FIB in der von Ihnen angegebenen Routing-Tabelle. Der Routenserver unterstützt IPv4 und leitet die Weiterleitung weiter. IPv6

Die Routenserver-Verbreitung ist der Mechanismus, der Routing-Tabellen automatisiert. Anstatt Routing-Tabellen manuell zu aktualisieren, gibt der Route Server automatisch die entsprechenden Routen mit Routen von der FIB an die konfigurierten Routing-Tabellen weiter.

Hauptaspekte der Routenserver-Verbreitung:

- Konfiguration
 - Verbindet einen Route Server mit bestimmten Routing-Tabellen
 - Legt fest, welche Routing-Tabellen dynamische Routenaktualisierungen erhalten
 - Kann pro Routing-Tabelle aktiviert oder deaktiviert werden
- Funktionalität
 - Aktualisiert Routing-Tabellen automatisch mit Routen, die von BGP-Peers gelernt wurden
 - Propagiert die besten verfügbaren Routen auf der Grundlage von BGP-Attributen
 - Behält die Routenkonsistenz in allen angegebenen Routing-Tabellen bei
 - Aktualisiert Routen dynamisch, wenn sich die Netzwerkbedingungen ändern
- Zustände

- Kann aktiviert werden (Routen werden weitergegeben)
- Kann deaktiviert werden (Routen werden nicht weitergegeben)

AWS Management Console

So aktivieren Sie die Routenserver-Verbreitung

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie den Route Server aus, für den Sie die Verbreitung aktivieren möchten.
3. Wählen Sie im Bereich mit den Routenserver-Details die Registerkarte Verbreitungen aus.
4. Wählen Sie Verbreitung aktivieren aus.
5. Im Dialogfeld Verbreitung aktivieren:
 - Wird die Routenserver-ID vorab ausgefüllt.
 - Wählen Sie unter Routing-Tabelle die Ziel-Routing-Tabelle aus dem Dropdownmenü für neu übertragene Routen aus.
6. Wählen Sie zur Bestätigung Verbreitung aktivieren aus.
7. Warten Sie, bis sich der Verbreitungsstatus in der Liste der Verbreitungen zu Verfügbar ändert.
8. Stellen Sie sicher, dass die ausgewählte Routing-Tabelle in der Liste der Verbreitungen mit dem Status Verfügbar angezeigt wird.

Command line

Gehen Sie wie folgt vor, um die Routenserver-Verbreitung zu aktivieren.

1. Befehl:

```
aws ec2 enable-route-server-propagation --route-table-id rtb-1 --route-server-id rs-1
```

Antwort:

```
{
  "RouteServerRoutePropagation": {
    "RouteServerId": "rs-1",
```

```
        "RouteTableId": "rtb-1",  
        "State": "pending"  
    }  
}
```

2. Warten Sie, bis sich der Verbreitungsstatus auf verfügbar ändert.

Befehl:

```
aws ec2 get-route-server-propagations --route-server-id rs-1
```

Antwort:

```
{  
  "RouteServerRoutePropagation": {  
    "RouteServerId": "rs-1",  
    "RouteTableId": "rtb-1",  
    "State": "available"  
  }  
}
```

Schritt 6: Einen Routenserver-Peer erstellen

Ein Route-Server-Peer ist eine Sitzung zwischen einem Routenserver-Endpunkt und dem Gerät, auf dem das Gerät installiert ist AWS (z. B. eine Firewall-Appliance oder eine andere Netzwerksicherheitsfunktion, die auf einer EC2 Instanz ausgeführt wird). Das Gerät muss die folgenden Anforderungen erfüllen:

- Über eine Elastic-Network-Schnittstelle in der VPC verfügen
- BGP (Border Gateway Protocol) unterstützen
- BGP-Sitzungen initiieren können

Note

Aus Redundanzgründen empfehlen wir, einen Routenserver-Peer pro Routenserver-Endpunkt zu erstellen.

AWS Management Console

So erstellen Sie einen Routenserver-Peer

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationspfad VPC > Routenserver-Peers > Routenserver-Peer erstellen aus.
3. Konfigurieren Sie unter Details Folgendes:
 - Name: Geben Sie einen Namen für Ihren Routenserver-Peer ein (bis zu 255 Zeichen).
Beispiel: my-route-server-peer -01
 - Routenserver-Endpunkt-ID: Wählen Sie einen Routenserver-Endpunkt aus der Dropdownliste aus. Wählen Sie optional Einen Routenserver-Endpunkt erstellen aus, um einen neuen zu erstellen.
 - Peer-Adresse: Geben Sie die IPv4 Adresse des Peers ein. Muss eine gültige IP-Adresse sein. Die Peer-Adresse muss vom Routenserver-Endpunkt aus erreichbar sein.
 - Peer-ASN: Geben Sie die ASN (Autonomous System Number) für den BGP-Peer ein. Der Wert muss im Bereich von 1-4294967295 liegen. Die ASN sollte normalerweise private Bereiche verwenden (64512-65534 für 16-Bit oder 4200000000-4294967294 für 32-Bit)
 - Peer-Aktivitätserkennung:
 - BGP-Keepalive (Standard): Standardmäßiger BGP-Keepalive-Mechanismus
 - BFD: Bidirectional Forwarding Detection für schnelleres Failover
 - (Optional) Wählen Sie unter Tags die Option Neues Tag hinzufügen aus, um Schlüssel-Wert-Paar-Tags hinzuzufügen. Mithilfe von Tags können AWS Ressourcen identifiziert und nachverfolgt werden.
4. Überprüfen Sie Ihre Einstellungen und wählen Sie Routenserver-Peer erstellen.

Command line

Erstellen Sie einen Routing-Server-Peer wie folgt.

1. Befehl:

```
aws ec2 create-route-server-peer --route-server-endpoint-id rse-1 --peer-address 10.0.2.3 --bgp-options PeerAsn=65001,PeerLivenessDetection=bfd
```

Antwort:

In der Antwort können die Statuswerte `pending` | `available` | `deleting` | `deleted` sein.

```
{
  "RouteServerPeer": {
    "RouteServerPeerId": "rsp-1",
    "RouteServerId": "rs-1",
    "VpcId": "vpc-1",
    "SubnetId": "subnet-1",
    "State": "pending",
    "EndpointEniId": "eni-2",
    "EndpointEniAddress": "10.0.2.4",
    "PeerEniId": "eni-1",
    "PeerAddress": "10.0.2.3",
    "BgpOptions": {
      "PeerAsn": 65001,
    },
    "PeerLivenessDetection": "bfd",
    "BgpStatus": {
      "Status": "Up"
    }
  }
}
```

2. Warten Sie, bis sich der Verbreitungsstatus auf verfügbar ändert.

Befehl:

```
aws ec2 describe-route-server-peers
```

Antwort:

```
{
  "RouteServerPeer": {
    "RouteServerPeerId": "rsp-1",
    "RouteServerId": "rs-1",
    "VpcId": "vpc-1",
    "SubnetId": "subnet-1",
    "State": "available",
    "EndpointEniId": "eni-2",
    "EndpointEniAddress": "10.0.2.4",
```

```
    "PeerEniId": "eni-1",
    "PeerAddress": "10.0.2.3",
    "BgpOptions": {
        "PeerAsn": 65001,
        "PeerLivenessDetection": "bfd"
    },
    "BgpStatus": {
        "Status": "down"
    }
}
```

Schritt 7: BGP-Sitzungen von den Geräten aus initiieren

Wenn der Status des Routenserver-Peers verfügbar ist, konfigurieren Sie Ihren Workload so, dass die BGP-Sitzung mit dem Routenserver-Endpunkt initiiert wird.

Das Initiieren einer BGP-Sitzung von den Geräten in Ihren Subnetzen aus wird in diesem Handbuch jedoch nicht behandelt. Der Routenserver-Endpunkt initiiert die BGP-Sitzung nicht.

Sie können überprüfen, ob das VPC-Routenserver-Feature funktioniert, indem Sie überprüfen, ob die Routing-Tabelle die besten vom Route Server weitergeleiteten Routen enthält.

Schritt 8: Bereinigen

Der Teil des Tutorials über das Erstellen ist abgeschlossen. Führen Sie die Schritte in diesem Abschnitt durch, um die von Ihnen erstellten VPC-Routenserver-Komponenten zu entfernen.

7.1: BGP-Werbung auf den Geräten zurückziehen

Das Zurückziehen von BGP-Werbung auf den Geräten in Ihren Subnetzen wird in diesem Handbuch jedoch nicht behandelt. Erkundigen Sie sich bei Bedarf bei Ihrem Drittanbieter nach Ihren BGP-Konfigurationen.

7.2: Die Routenserver-Verbreitung deaktivieren

Gehen Sie wie folgt vor, um die Routenserver-Verbreitung zu deaktivieren.

AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie den Route Server aus, für den Sie die Verbreitung deaktivieren möchten.

3. Wählen Sie Aktionen > Route Server ändern.
4. Wählen Sie im Bereich mit den Routenserver-Details die Registerkarte Verbreitungen aus.
5. Wählen Sie die Verbreitung aus, die Sie deaktivieren möchten, und wählen Sie dann Verbreitung deaktivieren.
6. Wählen Sie im Dialogfeld Routenserver-Verbreitung deaktivieren aus.

Command line

1. Verbreitung deaktivieren:

```
aws ec2 disable-route-server-route-propagation --route-table-id rtb-1 --route-server-id rs-1
```

2. Vergewissern Sie sich, dass die Verbreitung gelöscht wurde:

```
aws ec2 get-route-server-route-propagations --route-server-id rs-1 [--route-table-id rtb-1]
```

7.3: Routenserver-Peers löschen

Gehen Sie wie folgt vor, um Routenserver-Peers zu löschen.

AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationspfad Route Server > Routenserver-Peers aus.
3. Wählen Sie einen Routenserver-Peer aus.
4. Wählen Sie Aktionen > Routenserver-Peer löschen.

Command line

1. Peers löschen:

```
aws ec2 delete-route-server-peer --route-server-peer-id rsp-1
```

2. Das Löschen bestätigen:

```
aws ec2 describe-route-server-peers [--route-server-peer-ids rsp-1] [--filters  
Key=RouteServerId|RouteServerEndpointId|VpcId]
```

7.4: Routenserver-Endpunkte löschen

Gehen Sie wie folgt vor, um Routenserver-Endpunkte zu löschen.

AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie den Route Server aus, für den Sie Endpunkte löschen möchten.
3. Wählen Sie Routenserver-Endpunkte aus.
4. Wählen Sie den Endpunkt aus und wählen Sie Aktionen > Routenserver-Endpunkt löschen.
5. Geben Sie Löschen ein und wählen Sie Löschen aus.

Command line

1. Beschreiben Sie die Endpunkte:

```
aws ec2 describe-route-server-endpoints
```

2. Löschen Sie die Routenserver-Endpunkte:

```
aws ec2 delete-route-server-endpoint --route-server-endpoint-id rse-1
```

3. Gehen Sie sicher, dass die Endpunkte gelöscht wurden:

```
aws ec2 describe-route-server-endpoints [--route-server-endpoint-ids rsp-1] [--  
filters Key=RouteServerId|VpcId|SubnetId]
```

7.5: Routenserver von VPC trennen

Gehen Sie wie folgt vor, um die Zuordnung des Route Servers zur VPC aufzuheben.

AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie den Route Server aus, für den Sie die Zuordnung aufheben möchten.
3. Wählen Sie Zuordnung.
4. Wählen Sie Route Server trennen.
5. Bestätigen Sie die vorzunehmenden Änderungen und wählen Sie Route Server trennen.

Command line

1. Trennen Sie den Route Server von der VPC:

```
aws ec2 disassociate-route-server --route-server-id rs-1 --vpc-id vpc-1
```

2. Bestätigen Sie die Trennung:

```
aws ec2 get-route-server-associations --route-server-id rs-1
```

7.6 Route Server löschen

Gehen Sie wie folgt vor, um den Route Server zu löschen.

AWS Management Console

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie den Route Server aus, der gelöscht werden soll.
3. Wählen Sie Aktionen > Route Server löschen aus.
4. Geben Sie Löschen ein und wählen Sie Löschen aus.

Command line

1. Route Server löschen:

```
aws ec2 delete-route-server --route-server-id rs-1
```

2. Das Löschen bestätigen:

```
aws ec2 describe-route-servers [--route-server-ids rs-1] [--filters Key=VpcId]
```

Das Tutorial zum Amazon VPC Route Server ist abgeschlossen.

Beheben von Problemen mit der Erreichbarkeit in Ihrer VPC

Reachability Analyzer ist ein Tool zur statischen Konfigurationsanalyse. Mit Reachability Analyzer können Sie die Netzwerkerreichbarkeit zwischen zwei Ressourcen in Ihrer VPC analysieren und debuggen. Reachability Analyzer erstellt Hop-by-Hop-Details des virtuellen Pfads zwischen diesen Ressourcen, wenn sie erreichbar sind, und identifiziert andernfalls die blockierende Komponente. Das Tool kann beispielsweise fehlende oder falsch konfigurierte Routen in Routing-Tabellen identifizieren.

Weitere Informationen finden Sie im [Leitfaden Reachability Analyzer](#).

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](#)

- [Weiterleiten des VPC-Datenverkehrs an eine Sicherheits-Appliance](#)
- [Überlegungen des Middlebox-Routing-Assistenten](#)
- [Middlebox-Szenarien](#)

Voraussetzungen für Middlebox-Routing-Assistent

Prüfen [the section called “Überlegungen des Middlebox-Routing-Assistenten”](#). 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

Weiterleiten des VPC-Datenverkehrs an eine Sicherheits-Appliance

Der Middlebox-Routing-Assistent ist in der Amazon-VPC-Konsole verfügbar.

Inhalt

- [1. Erstellen von Routen mit dem Middlebox-Routing-Assistenten](#)
- [2. Ändern von Middlebox-Routen](#)
- [3. Löschen der Konfiguration des Middlebox-Routing-Assistenten](#)

1. 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.

2. 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.

3. 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.

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.

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-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.

- Wenn Sie Middlebox-Routing zur Weiterleitung über eine Sicherheits-Appliance verwenden, wird die [Referenzierung von Sicherheitsgruppen](#) zwischen der Quelle und dem endgültigen Ziel nach der Überprüfung nicht unterstützt.

Middlebox-Szenarien

Amazon Virtual Private Cloud (VPC) bietet ein breites Spektrum von Netzwerkfunktionen, mit denen Sie das Routing des Datenverkehrs in Ihrem virtuellen Netzwerk anpassen und steuern können. Eine solche Funktion ist der Middlebox-Routing-Assistent, der eine detaillierte Kontrolle über den Routing-Pfad des Datenverkehrs ermöglicht, der in Ihre VPC eintritt oder Ihre VPC verlässt.

Wenn Sie den Datenverkehr zu Inspektions-, Überwachungs- oder Optimierungszwecken an eine Sicherheits-Appliance, einen Load Balancer oder ein anderes Netzwerkgerät umleiten müssen, kann der Middlebox-Routing-Assistent den Vorgang vereinfachen. Dieser Assistent erstellt automatisch die erforderlichen Routing-Tabellen und Routen (Hops), um den angegebenen Datenverkehr nach Bedarf umzuleiten. Dadurch entfällt der manuelle Aufwand, der für die Einrichtung komplexer Routing-Konfigurationen erforderlich ist.

Der Middlebox-Routing-Assistent unterstützt mehrere verschiedene Szenarien. Sie können damit beispielsweise den Datenverkehr für ein bestimmtes Subnetz untersuchen, das Routing und die Inspektion des Middlebox-Datenverkehrs in Ihrer gesamten VPC konfigurieren oder den Datenverkehr zwischen bestimmten Subnetzen selektiv untersuchen. Diese detaillierte Kontrolle des Datenverkehrs ermöglicht es Ihnen, erweiterte Sicherheitsrichtlinien zu implementieren, eine zentrale Netzwerküberwachung einzurichten oder die Leistung Ihrer Cloud-basierten Anwendungen zu optimieren.

Die folgenden Beispiele beschreiben Szenarien für den Middlebox-Routing-Assistenten.

Inhalt

- [Überprüfen des Datenverkehrs, der für ein Subnetz bestimmt ist](#)
- [Konfigurieren des Routings und der Inspektion des Middlebox-Datenverkehrs in einer VPC](#)
- [Überprüfen des Datenverkehrs zwischen Subnetzen](#)

Überprüfen des Datenverkehrs, der für ein Subnetz bestimmt ist

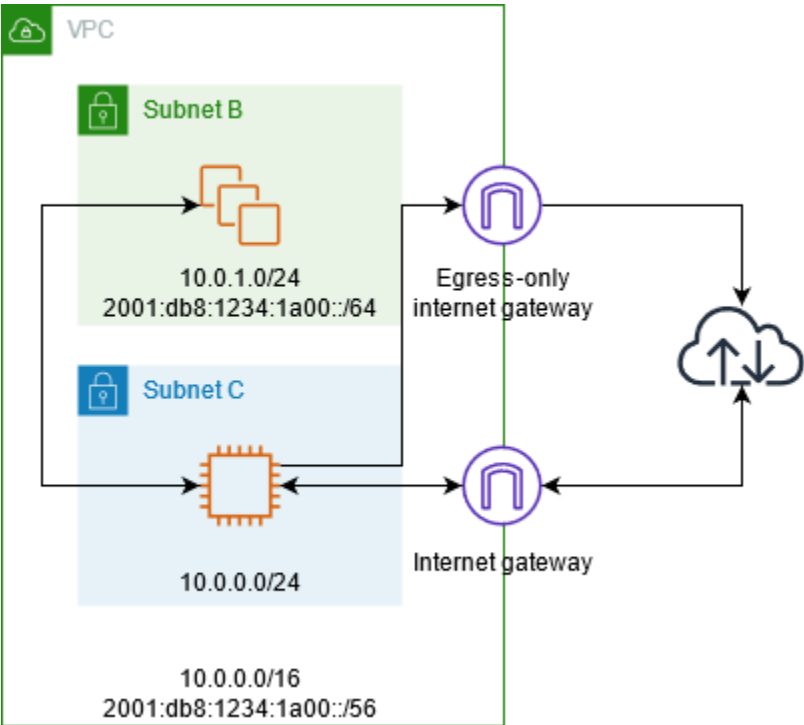
Stellen Sie sich das Szenario vor, in dem Datenverkehr über ein Internet-Gateway in die VPC eingeht und Sie den gesamten Datenverkehr, der für ein Subnetz, z. B. Subnetz B, bestimmt ist, mithilfe einer auf einer EC2-Instance installierten Firewall-Appliance überprüfen möchten. Die Firewall-Appliance 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.

Bestimmungsort	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).

Bestimmungsort	Ziel	Zweck
<i>10.0.0.0/16</i>	Local	Lokale Route für IPv4
0.0.0.0/0	<i>appliance-eni</i>	Weiterleiten des IPv4-Datenverkehrs für das Internet an die Middlebox
<i>2001:db8:1234:1a00::/56</i>	Local	Lokale Route für IPv6
::/0	<i>appliance-eni</i>	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).

Bestimmungsort	Ziel	Zweck
<i>10.0.0.0/16</i>	Local	Lokale Route für IPv4
0.0.0.0/0	<i>igw-id</i>	IPv4-Datenverkehr an das Internet-Gateway weiterleiten
<i>2001:db8:1234:1a00::/56</i>	Local	Lokale Route für IPv6
::/0	<i>eigw-id</i>	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“)

Konfigurieren des Routings und der Inspektion des Middlebox-Datenverkehrs in einer VPC

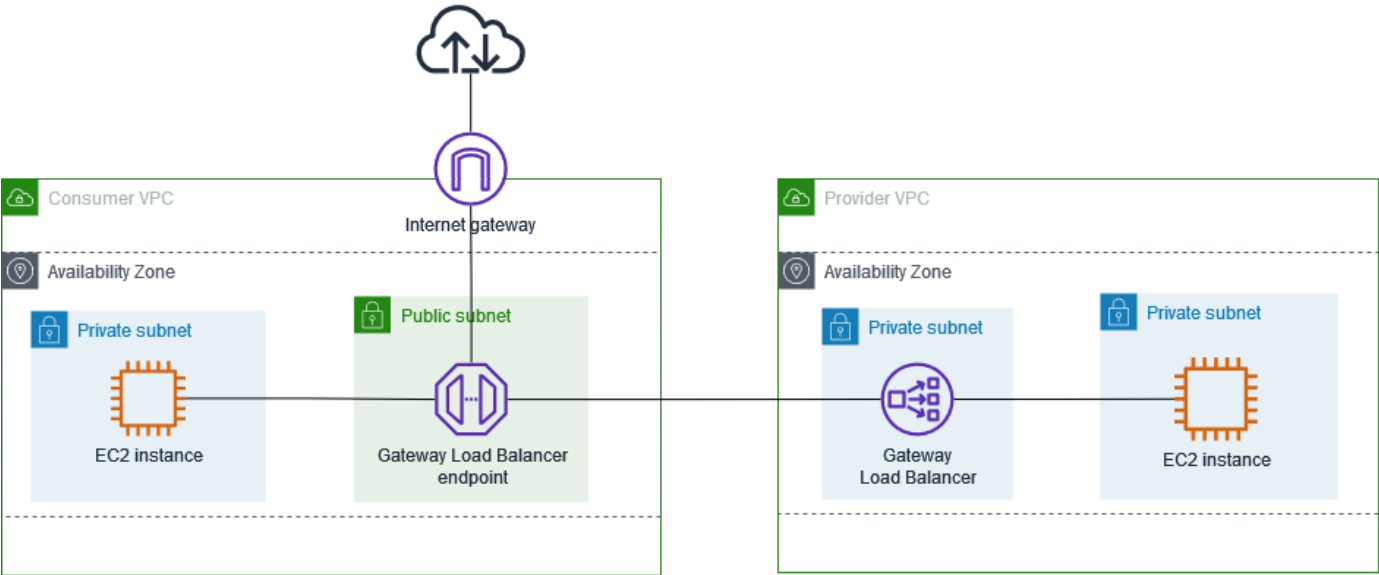
Im folgenden Beispiel möchten Sie den Datenverkehr untersuchen, der vom Internet-Gateway aus in eine VPC gelangt und für ein Subnetz bestimmt ist. Verwenden Sie dazu eine Flotte von Sicherheits-Appliances, die hinter einem Gateway Load Balancer in der Sicherheits-VPC konfiguriert sind. Der Besitzer der 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 an 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.

Bestimmungsort	Ziel	Zweck
VPC-CIDR des Verbrauchers	Local	Lokale Route

Bestimmungsort	Ziel	Zweck
<i>CIDR des Anwendungs-Subnetzes</i>	<i>endpunkt-ID</i>	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.

Bestimmungsort	Ziel	Zweck
<i>VPC-CIDR des Verbrauchers</i>	Local	Lokale Route
0.0.0.0/0	<i>endpunkt-ID</i>	Leiten Sie den Datenverkehr von den Anwendungsservern 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.

Bestimmungsort	Ziel	Zweck
<i>VPC-CIDR des Anbieters</i>	Local	Lokale Route. Stellt sicher, dass der aus dem Internet stammende Datenverkehr an die Anwendungsserver weitergeleitet wird.
0.0.0.0/0	<i>igw-id</i>	Leitet den gesamten Datenverkehr an das Internet-Gateway

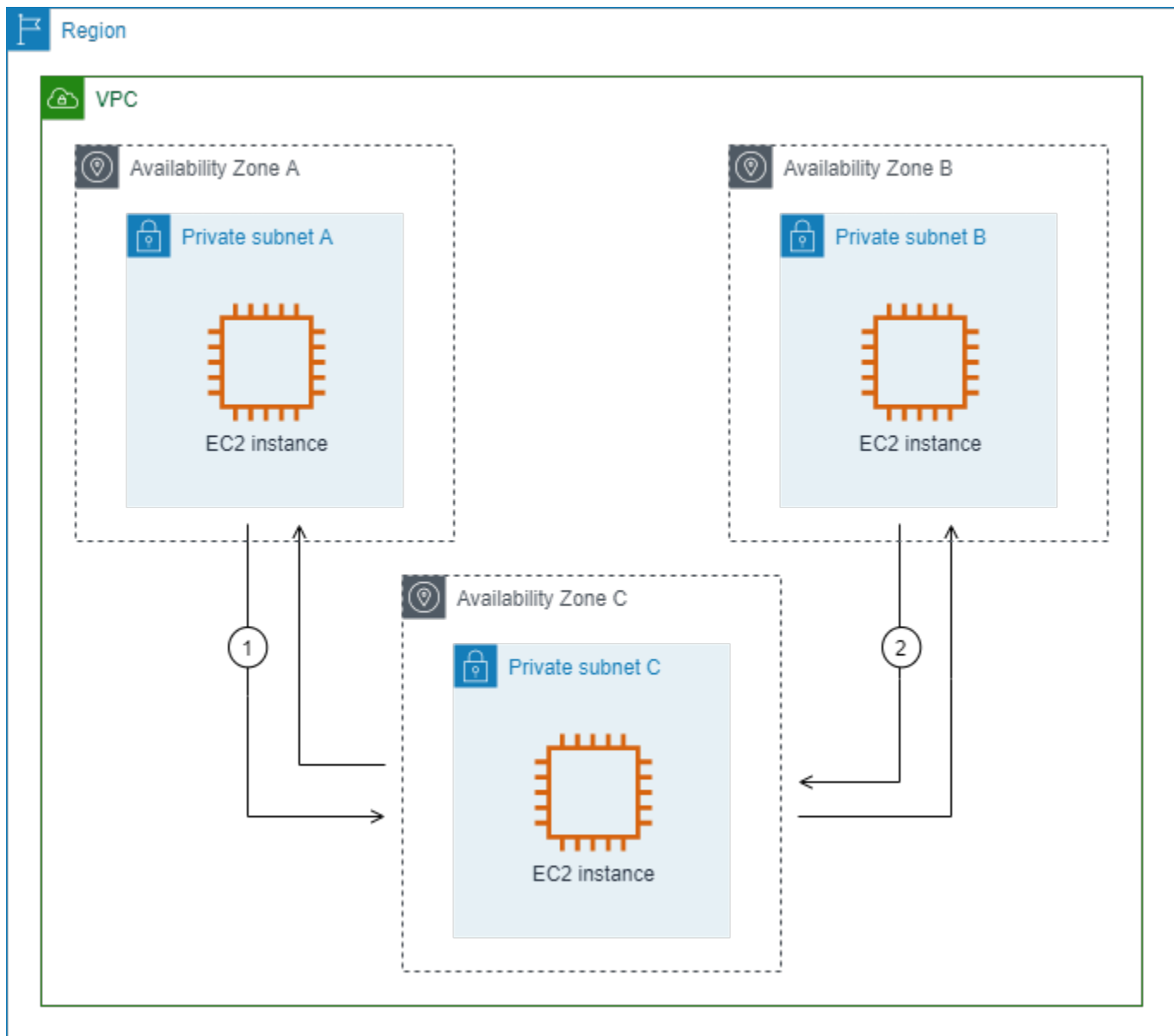
Wenn Sie den Middlebox-Routing-Assistenten verwenden, werden die folgenden Tags der Routing-Tabelle zugeordnet:

- 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.

Bestimmungsort	Ziel	Zweck
<i>VPC-CIDR</i>	Local	Lokale Route
<i>Subnetz-B-CIDR</i>	<i>appliance-eni</i>	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.

Bestimmungsort	Ziel	Zweck
<i>VPC-CIDR</i>	Local	Lokale Route

Bestimmungsort	Ziel	Zweck
<i>Subnetz-A-CIDR</i>	<i>appliance-eni</i>	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.

Bestimmungsort	Ziel	Zweck
<i>VPC-CIDR</i>	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.

Wenn Sie ein Subnetz löschen, wird der diesem Subnetz zugeordnete CIDR-Block an den verfügbaren IP-Adresspool der VPC zurückgegeben. Das bedeutet, dass die IP-Adressen innerhalb

des CIDR-Bereichs des Subnetzes anderen Subnetzen oder Ressourcen innerhalb derselben VPC neu zugewiesen werden können.

Es ist wichtig zu beachten, dass durch das Löschen eines Subnetzes nicht automatisch die darin enthaltenen Ressourcen gelöscht werden. Sie müssen zuerst alle EC2-Instances beenden, alle Netzwerkschnittstellen löschen und alle anderen mit dem Subnetz verknüpften Ressourcen entfernen, bevor Sie mit dem Löschen des Subnetzes fortfahren können.

Wie Sie ein Subnetz mit Hilfe der Konsole löschen

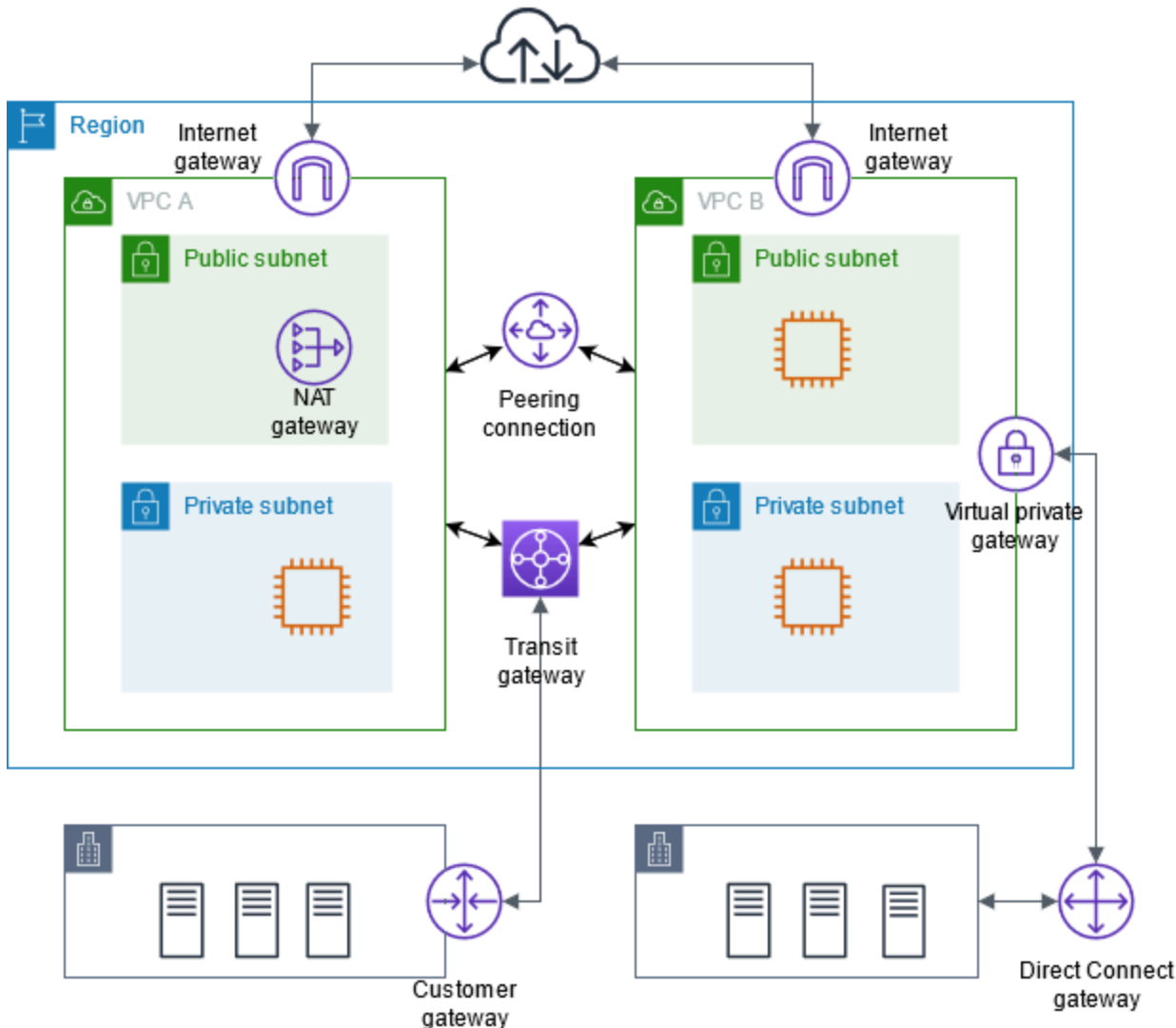
1. Öffnen Sie die Amazon EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Dazu müssen Sie zunächst alle Instances im Subnetz beenden. Weitere Informationen finden Sie unter [Beenden Ihrer Instance](#) im Amazon-EC2-Benutzerhandbuch.
3. Öffnen Sie die Amazon VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
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

Sie können Ihre Virtual Private Cloud (VPC) mit anderen Netzwerken verbinden, zum Beispiel mit anderen VPCs, mit dem Internet oder mit Ihrem On-Premises-Netzwerk.



Sie können Ihre Virtual Private Cloud (VPC) mit anderen Netzwerken verbinden, zum Beispiel mit anderen VPCs, mit dem Internet oder mit Ihrem On-Premises-Netzwerk.

Das Diagramm veranschaulicht einige dieser Verbindungsoptionen. VPC A ist über ein Internet-Gateway mit dem Internet verbunden. Die EC2-Instanz im privaten Subnetz kann über ein NAT-Gateway im öffentlichen Subnetz eine Internetverbindung herstellen. VPC B ist ebenfalls mit dem Internet verbunden, jedoch über ein direktes Internet-Gateway, sodass die EC2-Instanz im öffentlichen Subnetz auf das Internet zugreifen kann.

Zudem sind VPC A und VPC B über eine VPC-Peering-Verbindung und ein Transit-Gateway miteinander verbunden. Das Transit-Gateway ist per VPN-Anhang an ein Rechenzentrum angeschlossen und VPC B ist über eine Direct Connect-Verbindung an dasselbe Rechenzentrum angeschlossen. Diese Interkonnektivität ermöglicht es Organisationen, ihre Cloud-Ressourcen in die On-Premises-Infrastruktur zu integrieren und so eine Hybrid-Cloud-Umgebung zu schaffen.

Die Verbindung von VPCs mit anderen Netzwerken ist ein wichtiger Aspekt beim Aufbau einer Cloud-Infrastruktur innerhalb von AWS. Es bietet Organisationen Flexibilität und Kontrolle über ihre Netzwerkkonfigurationen und ermöglicht es ihnen, VPC-Architekturen zu entwerfen, die ihren Geschäfts- und Sicherheitsanforderungen entsprechen. Diese Konnektivitätsoptionen ermöglichen einen effizienten Datenfluss zwischen verschiedenen Komponenten einer verteilten IT-Landschaft, unabhängig davon, ob sie sich in der Cloud oder in einer On-Premises-Umgebung befinden.

AWS bietet eine Reihe von Tools und Funktionen zur Aktivierung dieser VPC-Verbindungen, darunter Internet-Gateways, NAT-Gateways, VPC-Peering, Transit-Gateways und Direct Connect. Durch die Nutzung dieser Funktionen können Organisationen sichere und integrierte Cloud-Umgebungen erstellen, die sich nahtlos in ihre bestehende IT-Infrastruktur integrieren lassen.

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.

Weitere Informationen finden Sie unter [Verbindungsoptionen für Amazon Virtual Private Cloud](#).

Inhalt

- [Aktivieren des Internetzugangs für eine VPC mithilfe eines Internet-Gateways](#)
- [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](#)
- [Zuordnen von elastischen IP-Adressen zu Ressourcen in Ihrer VPC](#)
- [Verbinden Ihrer VPC mit anderen VPCs und Netzwerken über ein Transit-Gateway](#)
- [Verbinden Ihrer VPC mit Remote-Netzwerken über AWS Virtual Private Network](#)
- [Verbinden von VPCs mit VPC-Peering](#)

Aktivieren des Internetzugangs für eine VPC mithilfe eines Internet-Gateways

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 auf Ihrem lokalen Computer eine Verbindung zu einer EC2-Instance in 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. Weitere Informationen finden Sie unter [IP-Adressen und NAT](#).

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](#).

Inhalt

- [Grundlagen zu Internet-Gateways](#)
- [Hinzufügen eines Internetzugriffs zu einem Subnetz](#)
- [Löschen eines Internet-Gateways](#)

Grundlagen zu Internet-Gateways

Um ein Internet-Gateway zu verwenden, müssen Sie es einer VPC anhängen und Routing konfigurieren.

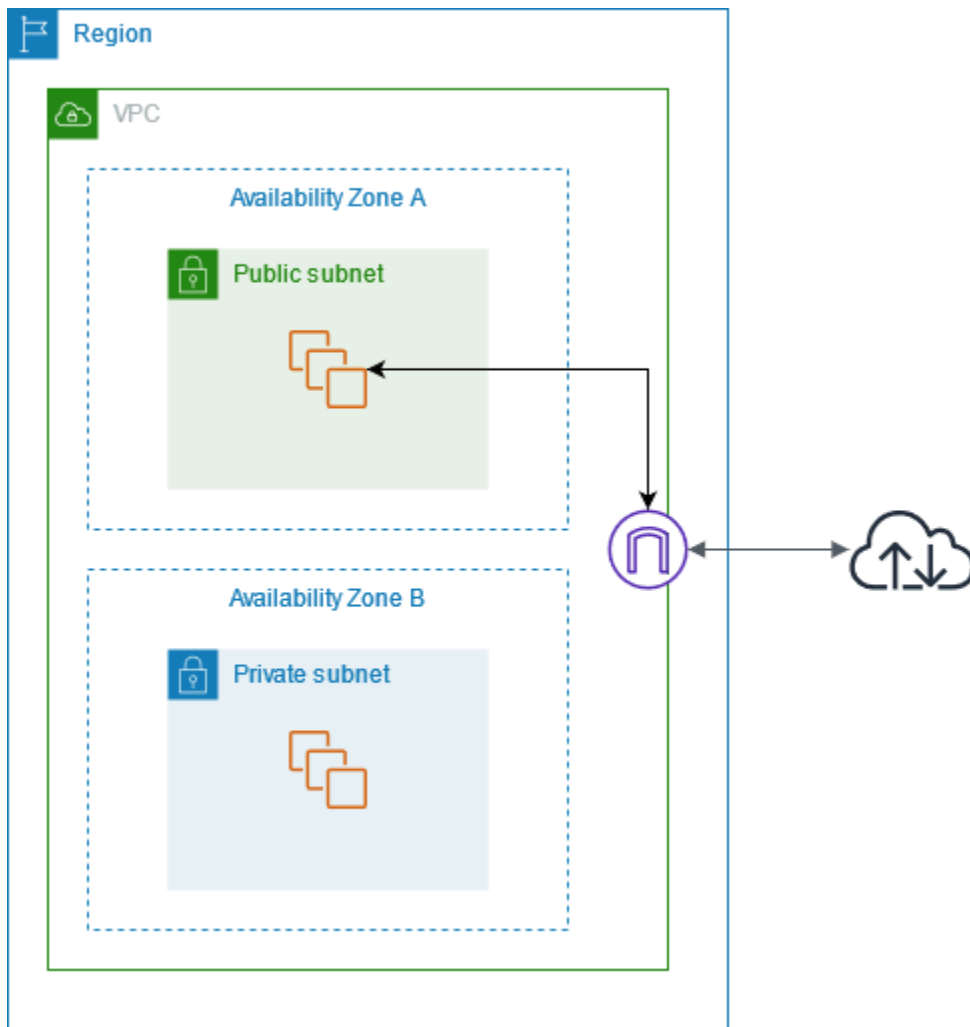
Weiterleitungskonfiguration

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 Subnetz bezeichnet.

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 festlegen, z. B. auf die öffentlichen IPv4-Adressen der öffentlichen Endpunkte Ihres Unternehmens außerhalb von AWS oder auf die Elastic-IP-Adressen anderer Amazon-EC2-Instances außerhalb Ihrer VPC.

Abbildung zu Internet-Gateways

In der folgenden Abbildung ist das Subnetz in Availability Zone A ein öffentliches Subnetz, da seine Routing-Tabelle eine Route hat, 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.



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. Daher stellt das Internet-Gateway auch die 1:1-NAT für Ihre Instance bereit. Verlässt der Datenverkehr nun Ihr VPC-Subnetz, um im Internet angezeigt zu werden, wird im Feld für die Antwortadresse die öffentliche IPv4-Adresse oder die Elastic-IP-Adresse Ihrer Instance angegeben und nicht die 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.

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)

Hinzufügen eines Internetzugriffs zu einem Subnetz

Im Folgenden wird beschrieben, wie Sie den Internetzugriff von einem Subnetz in einer nicht standardmäßigen VPC mit einem Internet-Gateway unterstützen. Sie müssen das Internet-Gateway erstellen, es an die VPC anhängen und Routing für das Subnetz konfigurieren.

Nachdem Sie den Internetzugang für Ihr Subnetz konfiguriert haben, müssen Sie dafür sorgen, dass die Ressourcen im Subnetz auf das Internet zugreifen können. Beispielsweise müssen Ihre EC2-

Instances über eine öffentliche IPv4- oder IPv6-Adresse verfügen, und die Sicherheitsgruppen für Ihre Instances müssen bestimmten Datenverkehr in das und aus dem Internet zulassen.

Um Ihren Instances alternativ Internetzugang zu bieten, ohne ihnen eine öffentliche IP-Adresse zuzuweisen, verwenden Sie stattdessen ein NAT-Gerät. Weitere Informationen finden Sie unter [NAT-Geräte](#).

Um den Internetzugang zu entfernen, können Sie das Internet-Gateway von Ihrer VPC trennen und dann löschen. Weitere Informationen finden Sie unter [the section called "Löschen eines Internet-Gateways"](#).

Aufgaben

- [Schritt 1: Ein Internet-Gateway erstellen](#)
- [Schritt 2: Das Internet-Gateway mit der VPC verknüpfen](#)
- [Schritt 3: Der Subnetz-Routing-Tabelle eine Route hinzufügen](#)

Schritt 1: Ein Internet-Gateway erstellen

Gehen Sie wie folgt vor, um ein Internet-Gateway zu erstellen.

So erstellen Sie ein Internet-Gateway mithilfe der Konsole

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.

So erstellen Sie ein Internet-Gateway mithilfe der Befehlszeile

- [create-internet-gateway](#) (AWS CLI)

- [New-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

Schritt 2: Das Internet-Gateway mit der VPC verknüpfen

Um ein Internet-Gateway zu verwenden, müssen Sie es einer VPC anhängen.

So hängen Sie ein Internet-Gateway mithilfe der Konsole 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. Um es anzuhängen, wählen Sie Aktionen, „An VPC anhängen“, wählen Sie eine verfügbare VPC aus und wählen Sie Internet-Gateway anhängen.
5. Um es zu trennen, wählen Sie Aktionen, Von VPC trennen und dann Internet-Gateway trennen. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Internet-Gateway trennen.

So hängen Sie ein Internet-Gateway mithilfe der Befehlszeile einer VPC an

- [attach-internet-gateway](#) (AWS CLI)
- [Add-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

Schritt 3: Der Subnetz-Routing-Tabelle eine Route hinzufügen

Die Routing-Tabelle für das private Subnetz muss eine Route enthalten, die den Internetdatenverkehr an das Internet-Gateway leitet.

So konfigurieren Sie die Subnetz-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. Wählen Sie die Routing-Tabelle für das Subnetz aus. Standardmäßig nutzt ein Subnetz die Haupt-Routing-Tabelle für die VPC. Alternativ können Sie [eine neue Routing-Tabelle erstellen](#) und dann das [Subnetz mit der neuen Routing-Tabelle verbinden](#).
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 ein und wählen Sie das Internet-Gateway für Ziel aus.

6. Wählen Sie Änderungen speichern aus.

So konfigurieren Sie die Subnetz-Routing-Tabelle mithilfe der Befehlszeile

- [create-route](#) (AWS CLI)
- [New-EC2Route](#) (AWS Tools for Windows PowerShell)

Löschen eines Internet-Gateways

Wenn Sie für eine VPC keinen Internetzugang mehr benötigen, können Sie das Internet-Gateway von der VPC trennen und dann löschen. Sie können ein Internet-Gateway, das noch immer einer VPC zugeordnet ist, nicht löschen. 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 mithilfe der Konsole von einer VPC

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. Um es anzuhängen, wählen Sie Aktionen, „An VPC anhängen“, wählen Sie eine verfügbare VPC aus und wählen Sie Internet-Gateway anhängen.
5. Um es zu trennen, wählen Sie Aktionen, Von VPC trennen und dann Internet-Gateway trennen. Wenn Sie zur Bestätigung aufgefordert werden, wählen Sie Internet-Gateway trennen.

So beschreiben Sie Ihre Internet-Gateways, einschließlich Anlagen, mithilfe der Befehlszeile

- [describe-internet-gateways](#) (AWS CLI)
- [Get-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

So trennen Sie ein Internet-Gateway mithilfe der Befehlszeile von einer VPC

- [detach-internet-gateway](#) (AWS CLI)
- [Dismount-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

So löschen Sie ein Internet-Gateway mithilfe der Konsole

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.

So löschen Sie ein Internet-Gateway mithilfe der Befehlszeile

- [delete-internet-gateway](#) (AWS CLI)
- [Remove-EC2InternetGateway](#) (AWS Tools for Windows PowerShell)

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.

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 \(NAT-Gateways\)](#).

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](#).

Inhalt

- [Grundlagen des Internet-Gateways für ausgehenden Verkehr](#)
- [Hinzufügen eines auf ausgehenden Verkehr beschränkten Internetzugriffs zu einem Subnetz](#)

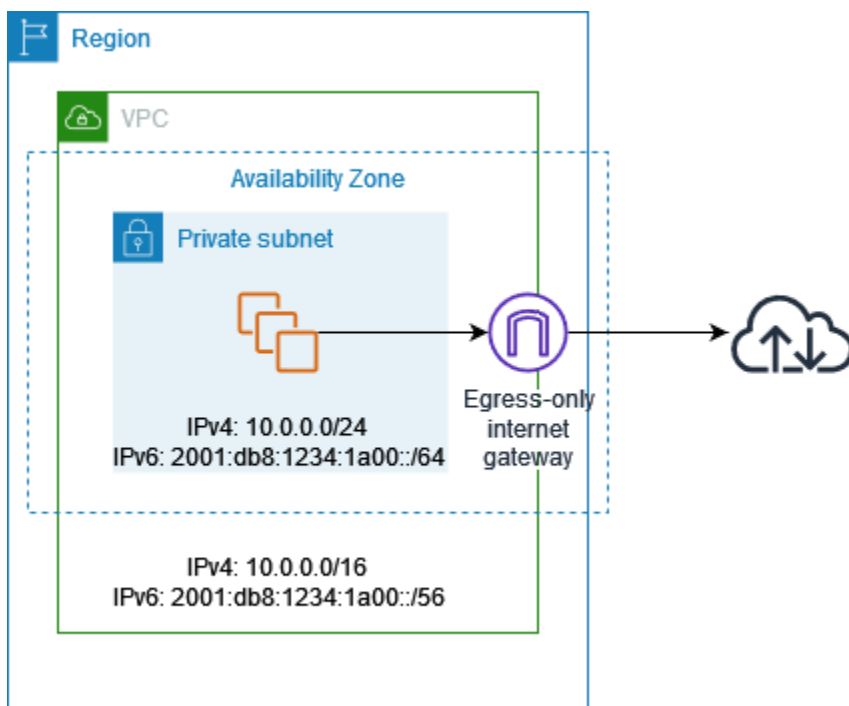
Grundlagen des Internet-Gateways für ausgehenden Verkehr

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.

Das Internet-Gateway nur für ausgehenden Verkehr ist zustandsbehaftet: Es leitet Datenverkehr von den Instances im Subnetz an das Internet oder andere AWS-Services weiter und sendet die Antwort dann zurück an die Instances.

Sie können eine Sicherheitsgruppe nicht mit einem Internet-Gateway nur für ausgehenden Datenverkehr verknüpfen, um den Datenverkehr zu kontrollieren, der das Internet-Gateway nur für ausgehenden Datenverkehr erreichen oder verlassen darf. 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	<i>eigw-id</i>

Hinzufügen eines auf ausgehenden Verkehr beschränkten Internetzugriffs zu einem Subnetz

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

- [1. Erstellen eines Internet-Gateways nur für ausgehenden Verkehr](#)
- [2. Erstellen einer benutzerdefinierten Routing-Tabelle](#)
- [3. Löschen eines Internet-Gateways nur für ausgehenden Verkehr](#)
- [Befehlszeilenübersicht](#)

1. 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 entfernen] Wählen Sie Remove (Entfernen) rechts neben dem Schlüssel und dem Wert des Tags.

5. Wählen Sie die VPC aus, in der Sie das Internet-Gateway für ausgehenden Verkehr erstellen möchten.
6. Wählen Sie Erstellen aus.

2. 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 Save (Speichern) aus.

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](#).

3. 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 gelöscht 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.

Befehlszeilenübersicht

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile ausführen.

Erstellen eines Internet-Gateways nur für ausgehenden Verkehr

- [create-egress-only-internet-gateway](#) (AWS CLI)
- [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)

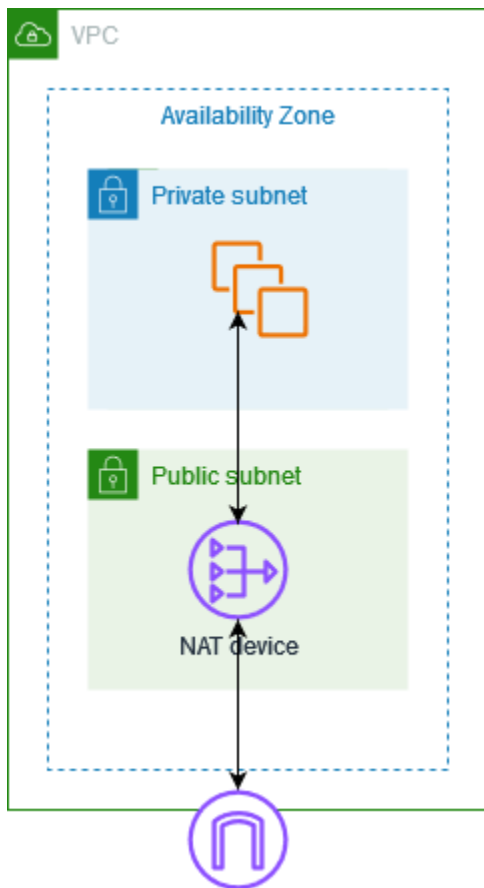
Löschen eines Internet-Gateways nur für ausgehenden Verkehr

- [delete-egress-only-internet-gateway](#) (AWS CLI)
- [Remove-EC2EgressOnlyInternetGateway](#) (AWS Tools for Windows PowerShell)

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 z. B. ein NAT-Gerät in einem öffentlichen Subnetz, das es EC2-Instances in einem privaten Subnetz ermöglicht, sich über ein Internet-Gateway 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 von AWS angebotenes verwaltetes NAT-Gerät verwenden, das als NAT-Gateway bezeichnet wird, oder Sie können Ihr eigenes NAT-Gerät auf einer EC2-Instance erstellen, die als NAT-Instance bezeichnet wird. Es wird empfohlen, NAT-Gateways zu verwenden, da sie eine bessere Verfügbarkeit und Bandbreite bieten und weniger Administrationsaufwand erfordern.

Inhalt

- [NAT gateways \(NAT-Gateways\)](#)
- [NAT-Instances](#)
- [Vergleich zwischen NAT-Gateways und NAT-Instances](#)

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 die Instances keine unerwünschten eingehenden Verbindungen aus dem Internet empfangen. Sie erstellen ein öffentliches NAT-Gateway in einem öffentlichen Subnetz und müssen beim Erstellen einer Elastic-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 einem anderen VPCs oder Ihrem lokalen 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 zu einem anderen VPCs oder Ihrem lokalen Netzwerk herstellen, aber die Instances können keine unaufgeforderten eingehenden Verbindungen von dem anderen oder dem lokalen Netzwerk empfangen. VPCs Sie können den Datenverkehr vom NAT-Gateway über ein Transit Gateway oder ein Virtual Private Gateway weiterleiten. Sie können einem privaten NAT-Gateway keine Elastic-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.

Ein NAT-Gateway ist für die Verwendung mit IPv4 oder Traffic (über) vorgesehen. IPv6 [DNS64 und NAT64](#) Eine weitere Option zur Aktivierung der reinen ausgehenden Internetkommunikation über IPv6 ist die Verwendung eines Internet-Gateways für ausgehenden Datenverkehr.

Sowohl private als auch öffentliche NAT-Gateways ordnen die private IPv4 Quelladresse 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.

Überlegungen

- Verbindungen müssen immer ausgehend von der VPC initiiert werden, die das NAT-Gateway enthält.
- 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. Das öffentliche NAT-Gateway nutzt die Elastic-IP-Adresse nur dann als IP-Quelladresse, wenn es zusammen mit einem Internet-Gateway in derselben VPC verwendet wird.

Inhalt

- [Grundlagen zu NAT-Gateways](#)
- [Arbeiten mit NAT-Gateways](#)
- [Regionale NAT-Gateways für automatische Multi-AZ-Erweiterung](#)
- [Anwendungsfälle für NAT-Gateway](#)
- [DNS64 und NAT64](#)
- [Überprüfen Sie den Verkehr von NAT-Gateways](#)
- [Überwachen von NAT-Gateways mit Amazon CloudWatch](#)
- [Problembehandlung bei NAT-Gateways](#)
- [Preisgestaltung für NAT-Gateways](#)

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 [Gateways](#).

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 unseren Datenverkehr IPv4 unterstützt. IPv6 Für den IPv6 Datenverkehr ist das NAT-Gateway zuständig. NAT64 Wenn Sie dies in Verbindung mit DNS64 (auf dem Route 53 Resolver verfügbar) verwenden, können Ihre IPv6 Workloads in einem Subnetz in Amazon VPC mit Ressourcen kommunizieren. IPv4 Diese IPv4 Dienste können in derselben VPC (in einem separaten Subnetz) oder einer anderen VPC, in Ihrer lokalen Umgebung oder im Internet vorhanden 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 zuordnen (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](#).
- Wenn Sie ein NAT-Gateway erstellen, können Sie die primäre private IPv4 Adresse auswählen, die dem NAT-Gateway zugewiesen werden soll. Andernfalls wählen wir in Ihrem Namen eine aus dem IPv4 Adressbereich des Subnetzes aus. Sie können die primäre IPv4 Privatadresse nicht ändern oder entfernen. Sie können nach Bedarf sekundäre IPv4 Privatadressen hinzufügen.
- Sie können einer Sicherheitsgruppe kein NAT-Gateway zuordnen. Sie können Ihren Instances Sicherheitsgruppen zuordnen, um den ein- und ausgehenden Datenverkehr zu steuern.
- Wir erstellen eine vom Anforderer verwaltete Netzwerkschnittstelle für Ihr NAT-Gateway. Sie können diese Netzwerkschnittstelle mit der EC2 Amazon-Konsole anzeigen. Suchen Sie nach der ID des NAT-Gateways in der Beschreibung. Sie können zur Netzwerkschnittstelle Tags ergänzen, aber Sie können andere Eigenschaften dieser Netzwerkschnittstelle nicht ändern.

- 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 [Netzwerk ACLs](#).
- Es ist nicht möglich, Datenverkehr über eine VPC-Peering-Verbindung an ein NAT-Gateway weiterzuleiten. Der Datenverkehr von einem NAT-Gateway über VPC-Peering zu Zielen im Peering VPCs unterstützt jedoch das „Return to Sender“-Verhalten — Rückverkehr wird automatisch zurück zum ursprünglichen NAT-Gateway geleitet, auch wenn in der Ziel-VPC keine Rückrouten konfiguriert sind. Dieses Verhalten ist spezifisch für NAT-Gateways und gilt nicht für Standardinstanzen. EC2 Um dies zu verhindern, verwenden Sie, NACLs um den Rückverkehr zu blockieren.

Nicht unterstützt:

Client # Peering # NAT # Internet

Unterstützt:

Client # NAT # Peering # Destination

- Sie können den Datenverkehr nicht von Site-to-Site VPN oder Direct Connect über ein virtuelles privates Gateway an ein NAT-Gateway weiterleiten. Sie können den Datenverkehr von Site-to-Site VPN oder Direct Connect an ein NAT-Gateway weiterleiten, wenn Sie ein Transit-Gateway anstelle eines virtuellen privaten Gateways verwenden.
- NAT-Gateways unterstützen Datenverkehr mit einer maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) von 8 500, es ist jedoch wichtig, Folgendes zu beachten:
 - Die MTU einer Netzwerkverbindung ist die Größe (in Byte) des größten zulässigen Datenpakets, das über die Verbindung übergeben werden kann. Je größer die MTU einer Verbindung, desto mehr Daten können in einem einzelnen Paket übergeben werden.
 - Pakete mit mehr als 8 500 Byte, die am NAT-Gateway eingehen, werden verworfen (oder fragmentiert, falls zutreffend).
 - 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 zur Überprüfung und Einstellung der MTU für eine Instance finden Sie unter [Netzwerk-MTU für Ihre EC2 Instance](#) im EC2 Amazon-Benutzerhandbuch.

- NAT-Gateways unterstützen Path MTU Discovery (PMTUD) über ICMPv4 FRAG_NEEDED-Pakete und Packet Too Big-Pakete (PTB). ICMPv6
- NAT-Gateways erzwingen das Klemmen der maximalen Segmentgröße (MSS) für alle Pakete. Weitere Informationen finden Sie unter [RFC879](#).

Arbeiten mit NAT-Gateways

Sie können die Amazon VPC-Konsole verwenden, um Ihre NAT-Gateways zu erstellen und zu verwalten.

Aufgaben

- [Kontrollieren Sie die Verwendung von NAT-Gateways](#)
- [Erstellen eines NAT-Gateways](#)
- [Bearbeiten sekundärer IP-Adresszuweisungen](#)
- [Markieren eines NAT-Gateways](#)
- [Löschen eines NAT-Gateways](#)
- [Befehlszeilenübersicht](#)

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](#).

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 Elastic-IP-Adressen ausgeschöpft haben. Weitere Informationen 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 Elastic-IP-Adresse zuzuweisen, oder wählen Sie Elastic-IP zuweisen aus, um dem öffentlichen NAT-Gateway automatisch eine 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 Elastic-IP-Adresse zuweisen, muss die Netzwerkgranzgruppe der EIP mit der Netzwerkgranzgruppe 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 Netzwerkgranzgruppe für die AZ des Subnetzes anhand der Details des Subnetzes sehen. In ähnlicher Weise können Sie die Netzwerkgranzgruppe eines EIP anzeigen,

indem Sie sich die Details der EIP-Adresse ansehen. Weitere Informationen finden Sie unter [1. Zuweisen einer Elastic-IP-Adresse](#).

2. (Optional) Wählen Sie Zusätzliche Einstellungen 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 nach dem Zufallsprinzip eine private IPv4 Adresse aus dem Subnetz zugewiesen, in dem sich Ihr NAT-Gateway befindet.
3. Fahren Sie mit Schritt 11 fort.
8. Wenn Sie Privat ausgewählt haben, wählen Sie für Zusätzliche Einstellungen, Methode zur Zuweisung privater IPv4 Adressen eine der folgenden Optionen:
 - Automatisch zuweisen: 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 IPv4 Privatadresse die primäre private IPv4 Adresse für das NAT-Gateway aus. Für sekundäre IPv4 Privatadressen können Sie optional bis zu 7 sekundäre IPv4 Privatadressen 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 NAT-Gateway AWS zuweisen möchten. Sie können bis zu 7 IPv4 Adressen auswählen.

 Note

Sekundäre IPv4 Adressen sind optional und sollten zugewiesen oder zugewiesen werden, wenn Ihre Workloads, die ein NAT-Gateway verwenden, 55.000 gleichzeitige Verbindungen zu einem einzigen Ziel (dieselbe Ziel-IP, denselben Zielport und dasselbe Protokoll) überschreiten. Sekundäre IPv4 Adressen erhöhen die Anzahl der verfügbaren Ports und erhöhen daher die Obergrenze für die Anzahl gleichzeitiger 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 IPv4 Privatadresse eine private IPv4 Adresse ein.

2. Geben Sie unter Sekundäre IPv4 Privatadresse bis zu 7 sekundäre IPv4 Privatadressen 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 zuordnen (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 anhand der [CloudWatchErrorPortAllocationNAT-Gateway-Metriken](#) feststellen PacketsDropCount, 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 mit dem Verfahren in diesem Abschnitt erstellt haben. Sie können Elastic-IP-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 sein (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](#).

Um sekundäre IPv4 Adresszuordnungen zu bearbeiten

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 Adresszuordnungen Sie bearbeiten möchten.
4. Wählen Sie Aktionen und dann Bearbeiten sekundärer IP-Adresszuweisungen aus.
5. Wenn Sie die sekundären IPv4 Adresszuordnungen eines privaten NAT-Gateways bearbeiten, wählen Sie unter Aktion die Option Neue IPv4 Adressen zuweisen oder Vorhandene IPv4 Adressen aufheben aus. Wenn Sie die sekundären IPv4 Adresszuordnungen eines öffentlichen NAT-Gateways bearbeiten, wählen Sie unter Aktion die Option Neue IPv4 Adressen zuordnen oder Vorhandene IPv4 Adressen trennen 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 die Methode zur Zuweisung IPv4 von Privatadressen:
 - Automatisch zuweisen: Wählt AWS automatisch eine primäre IPv4 Privatadresse aus und Sie entscheiden, ob Sie AWS dem NAT-Gateway bis zu 7 sekundäre IPv4 Privatadressen 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 Allocation ID eine Elastic IP-Adresse aus, die Sie mit einer sekundären IPv4 Adresse hinzufügen möchten. Dieser Schritt ist erforderlich. Sie müssen eine Elastic IP-Adresse zusammen mit einer privaten IPv4 Adresse auswählen. Wenn Sie für die Zuweisungsmethode Private IP-Adressen Benutzerdefiniert ausgewählt haben, müssen Sie außerdem für jede Elastic IP-Adresse, die Sie hinzufügen, eine private IPv4 Adresse eingeben.

 Important

Wenn Sie einem öffentlichen NAT-Gateway eine sekundäre EIP zuweisen, muss die Netzwerkgranzgruppe der EIP mit der Netzwerkgranzgruppe 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 Netzwerkgranzgruppe für die AZ des Subnetzes anhand der Details des Subnetzes sehen. In ähnlicher Weise können Sie die Netzwerkgranzgruppe eines EIP anzeigen, indem Sie sich die Details der EIP-Adresse ansehen. Weitere Informationen finden Sie unter [1. 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 Elastic-IP-Adressen pro Region. Weitere Informationen finden Sie unter [Elastic-IP-Adressen](#).

- Wenn Sie die Zuweisung neuer Adressen aufheben oder die 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 zum Arbeiten mit Tags finden Sie unter [Taggen Ihrer EC2 Amazon-Ressourcen](#) im EC2 Amazon-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 Stichwörter 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 diesen 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 Aktionen, 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 [5. Freigeben einer Elastic-IP-Adresse](#).

Befehlszeilenübersicht

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile ausführen.

Weisen Sie einem privaten NAT-Gateway eine private IPv4 Adresse zu

- [assign-private-nat-gateway-Adresse](#) (AWS CLI)
- [Register-EC2PrivateNatGatewayAddress](#) (AWS Tools for Windows PowerShell)

Ordnen Sie Elastic IP-Adressen und private IPv4 Adressen einem öffentlichen NAT-Gateway zu

- [associate-nat-gateway-address](#) (AWS CLI)
- [Register-EC2NatGatewayAddress](#) (AWS Tools for Windows PowerShell)

Erstellen eines NAT-Gateways

- [create-nat-gateway](#) (AWS CLI)
- [New-EC2NatGateway](#) (AWS Tools for Windows PowerShell)

Löschen eines NAT-Gateways

- [delete-nat-gateway](#) (AWS CLI)
- [Remove-EC2NatGateway](#) (AWS Tools for Windows PowerShell)

Beschreiben eines NAT-Gateways

- [describe-nat-gateways](#) (AWS CLI)
- [Get-EC2NatGateway](#) (AWS Tools for Windows PowerShell)

Aufheben der Zuordnung von sekundären Elastic-IP-Adressen von einem öffentlichen NAT-Gateway

- [disassociate-nat-gateway-address](#) (AWS CLI)
- [Unregister-EC2NatGatewayAddress](#) (AWS Tools for Windows PowerShell)

Markieren eines NAT-Gateways

- [create-tags](#) (AWS CLI)

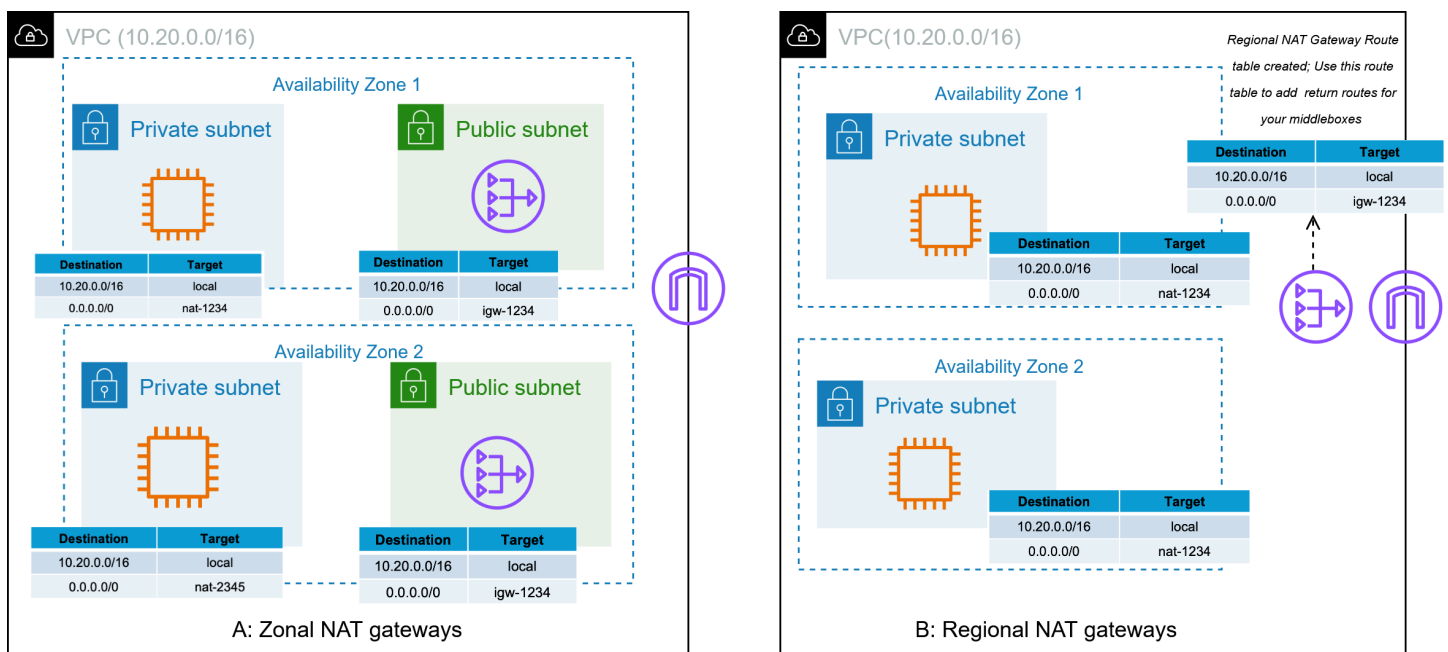
- [New-EC2Tag](#) (AWS Tools for Windows PowerShell)

Heben Sie die Zuweisung sekundärer IPv4 Adressen zu einem privaten NAT-Gateway auf

- [unassign-private-nat-gateway-Adresse](#) (AWS CLI)
- [Unregister-EC2PrivateNatGatewayAddress](#) (AWS Tools for Windows PowerShell)

Regionale NAT-Gateways für automatische Multi-AZ-Erweiterung

Verwenden Sie regionale NAT-Gateways, wenn Sie Ihre Netzwerkarchitektur vereinfachen, Ihre Sicherheitslage verbessern und standardmäßig Hochverfügbarkeit konfigurieren möchten. Ein regionales NAT-Gateway erweitert sich automatisch auf die Availability Zones, je nachdem, wo Ihre Workloads vorhanden sind. Im Gegensatz zu Standard-NAT-Gateways (als zonale NAT-Gateways bezeichnet), die in einer einzigen Availability Zone betrieben werden, folgen regionale NAT-Gateways Ihren Workloads und sorgen so für automatische Hochverfügbarkeit.



Das Diagramm A auf der linken Seite stellt die aktuelle Konfiguration mit dem zonalen NAT-Gateway dar. Sie erstellen zunächst zonale NAT-Gateways pro Availability Zone und hosten Ihre NATs in öffentlichen Subnetzen. Anschließend konfigurieren Sie separate Routen pro Availability Zone von Ihren privaten Subnetzen zum NAT in dieser Availability Zone. Sie wiederholen diesen Schritt jedes Mal, wenn Ihre Workloads auf eine neue Availability Zone erweitert werden, um eine hohe Verfügbarkeit zu gewährleisten. Darüber hinaus müssen Sie in der Routentabelle Ihres NAT-Subnetzes pro Availability Zone Routen für das Internet-Gateway hinzufügen.

Andererseits müssen Sie bei einem regionalen NAT-Gateway kein öffentliches Subnetz einrichten, um es zu hosten. Sie müssen auch nicht jedes Mal, wenn Ihre Workloads auf neue Availability Zones erweitert werden, NAT-Gateways erstellen und löschen und Ihre Routing-Tabellen bearbeiten. Stattdessen erstellen Sie einfach ein NAT-Gateway mit regionalem Modus, wählen Ihre VPC aus und diese wird automatisch erweitert und verkleinert, AZs je nachdem, wie Ihre Workload vorhanden ist, um eine hohe Verfügbarkeit zu gewährleisten. Wie in Abbildung B dargestellt, können Sie den Datenverkehr von Ihren Ressourcen in einem privaten Subnetz über alle Ressourcen AZs zu dieser einzigen regionalen NAT-Gateway-ID weiterleiten oder dieselbe Routing-Tabelle für die Subnetze in Ihrer AZ verwenden, um die Netzwerkadressübersetzung durchzuführen. Sobald Sie Ihr regionales NAT-Gateway erstellt haben, erstellt es AWS automatisch eine Routing-Tabelle, die eine vorkonfigurierte Route zum Internet-Gateway enthält. Sie können diese Routentabelle verwenden, um Ihren Middleboxes Rückrouten hinzuzufügen.

Vorteile

Regionale NAT-Gateways bieten die folgenden Vorteile:

- Vereinfachte Einrichtung — Verwenden Sie eine einzige NAT-ID für alle Availability Zones, die über Netzwerkschnittstellen verfügen, sodass Sie denselben Routeneintrag für Subnetze in verschiedenen Availability Zones verwenden können.
- Verbesserte Sicherheit — Keine öffentlichen Subnetze erforderlich. Ein regionales NAT-Gateway ist eine eigenständige Ressource mit eigener Routing-Tabelle. Sie benötigen kein öffentliches Subnetz in Ihrer VPC, um ein regionales NAT-Gateway zu hosten, wodurch die Wahrscheinlichkeit einer Fehlkonfiguration privater Ressourcen in Subnetzen mit öffentlicher Konnektivität verringert wird.
- Automatische Hochverfügbarkeit — Wird automatisch an Ihren Workloadbedarf erweitert und verkleinert, um die zonale Affinität aufrechtzuerhalten, die standardmäßig für hohe Verfügbarkeit sorgt.
- Höhere Port- und IP-Grenzwerte — Ihre regionalen NAT-Gateways unterstützen bis zu 32 IP-Adressen pro Availability Zone (im Vergleich zu 8 bei zonalen NAT-Gateways). Jede IP-Adresse erhöht das Limit für gleichzeitige Verbindungen zu einem beliebigen Ziel (identifiziert durch eine eindeutige Kombination aus Ziel-IP, Zielport und Protokoll) um 55.000.

Wann sollten regionale NAT-Gateways verwendet werden

Erwägen Sie die Verwendung regionaler NAT-Gateways für alle Anwendungsfälle, außer für solche, die private Konnektivität erfordern. Regionale NAT-Gateways bieten keine private

Konnektivität und wir empfehlen, Ihre NAT-Gateways für private NAT-Anwendungsfälle im zonalen Verfügbarkeitsmodus zu verwenden.

So funktionieren regionale NAT-Gateways

Wenn Sie Ressourcen in einer neuen Availability Zone starten, erkennt das regionale NAT-Gateway das Vorhandensein einer Netzwerkschnittstelle (ENI) in dieser Availability Zone und dehnt sich automatisch auf diese Zone aus. In ähnlicher Weise werden Verträge für das NAT-Gateway von der Availability Zone aus abgeschlossen, in der es keine aktiven Workloads gibt.

Es kann bis zu 60 Minuten dauern, bis Ihr regionales NAT-Gateway auf eine neue Availability Zone erweitert wird, nachdem dort eine Ressource instanziiert wurde. Bis diese Erweiterung abgeschlossen ist, wird der relevante Datenverkehr von dieser Ressource zonenübergreifend von Ihrem regionalen NAT-Gateway in einer der vorhandenen Availability Zones verarbeitet.

Regionale NAT-Gateways unterstützen zwei Modi:

- **Automatischer Modus** — In diesem Modus werden IP-Adressen und die Erweiterung der Availability Zone AWS automatisch verwaltet (empfohlen). Wenn Sie in diesem Modus Ihre eigenen IP-Adressen verwenden möchten und Amazon VPC IPAM verwenden, finden Sie weitere Informationen unter [Definieren einer öffentlichen IPv4 Zuweisungsstrategie mit IPAM-Richtlinien](#) im Amazon VPC IPAM-Benutzerhandbuch.
- **Manueller Modus** — In diesem Modus verwalten Sie manuell IP-Adressen und steuern die Netzwerkadressübersetzung für jede Availability Zone. Im manuellen Modus sind Sie dafür verantwortlich, Ihr NAT-Gateway in allen Availability Zones zu erweitern und zu nutzen.

Preisgestaltung

Preisinformationen finden Sie unter [Amazon VPC-Preise](#).

Erstellen Sie ein regionales NAT-Gateway

Verwenden der Konsole

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. Wählen Sie für den Verfügbarkeitsmodus die Option Regional aus. Sie müssen keine Subnetze angeben, wenn Sie die regionale Verfügbarkeit wählen

5. Wählen Sie eine VPC aus.
6. Schließen Sie die verbleibende Konfiguration ab und wählen Sie Create NAT Gateway aus.

Verwenden der AWS CLI

Erstellen Sie ein regionales NAT-Gateway

```
aws ec2 create-nat-gateway --vpc-id vpc-12345678 --availability-mode regional
```

Details zum NAT-Gateway anzeigen

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-12345678
```

IP-Adressen hinzufügen (manueller Modus)

```
aws ec2 associate-nat-gateway-address --nat-gateway-id nat-12345678 --availability-zone us-east-1b --allocation-ids eipalloc-12345678
```

IP-Adressen entfernen

```
aws ec2 disassociate-nat-gateway-address --nat-gateway-id nat-12345678 --association-ids eipassoc-12345678
```

Löschen Sie ein regionales NAT-Gateway

```
aws ec2 delete-nat-gateway --nat-gateway-id nat-12345678
```

Von zonalen zu regionalen NAT-Gateways konvertieren

Important

Dadurch werden Ihre bestehenden Verbindungen zurückgesetzt. Wir empfehlen Ihnen, diese Schritte in Ihrem Wartungsfenster durchzuführen.

Sie können vorhandene zonale NAT-Gateways mit einem von zwei Ansätzen in ein regionales NAT-Gateway umwandeln:

Wenn Sie mit der Verwendung regionaler NAT-Gateways mit neuen IP-Adressen einverstanden sind:

1. Erstellen Sie ein neues regionales NAT-Gateway
2. Aktualisieren Sie die Routentabellen so, dass sie auf das regionale NAT-Gateway verweisen
3. Löschen Sie die alten zonalen NAT-Gateways

Dieser Ansatz verwendet neue IP-Adressen und setzt bestehende Verbindungen zurück, wenn Routen aktualisiert werden.

Wenn Sie vorhandene IP-Adressen mit regionalen NAT-Gateways wiederverwenden möchten:

1. Löschen Sie vorhandene zonale NAT-Gateways, um ihre IP-Adressen freizugeben
2. Erstellen Sie ein regionales NAT-Gateway mit den freigegebenen IP-Adressen
3. Aktualisieren Sie die Routentabellen so, dass sie auf das regionale NAT-Gateway verweisen

Bei diesem Ansatz bleiben IP-Adressen erhalten, es ist jedoch ein Wartungsfenster erforderlich, da der Datenverkehr während des Übergangs unterbrochen wird.

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

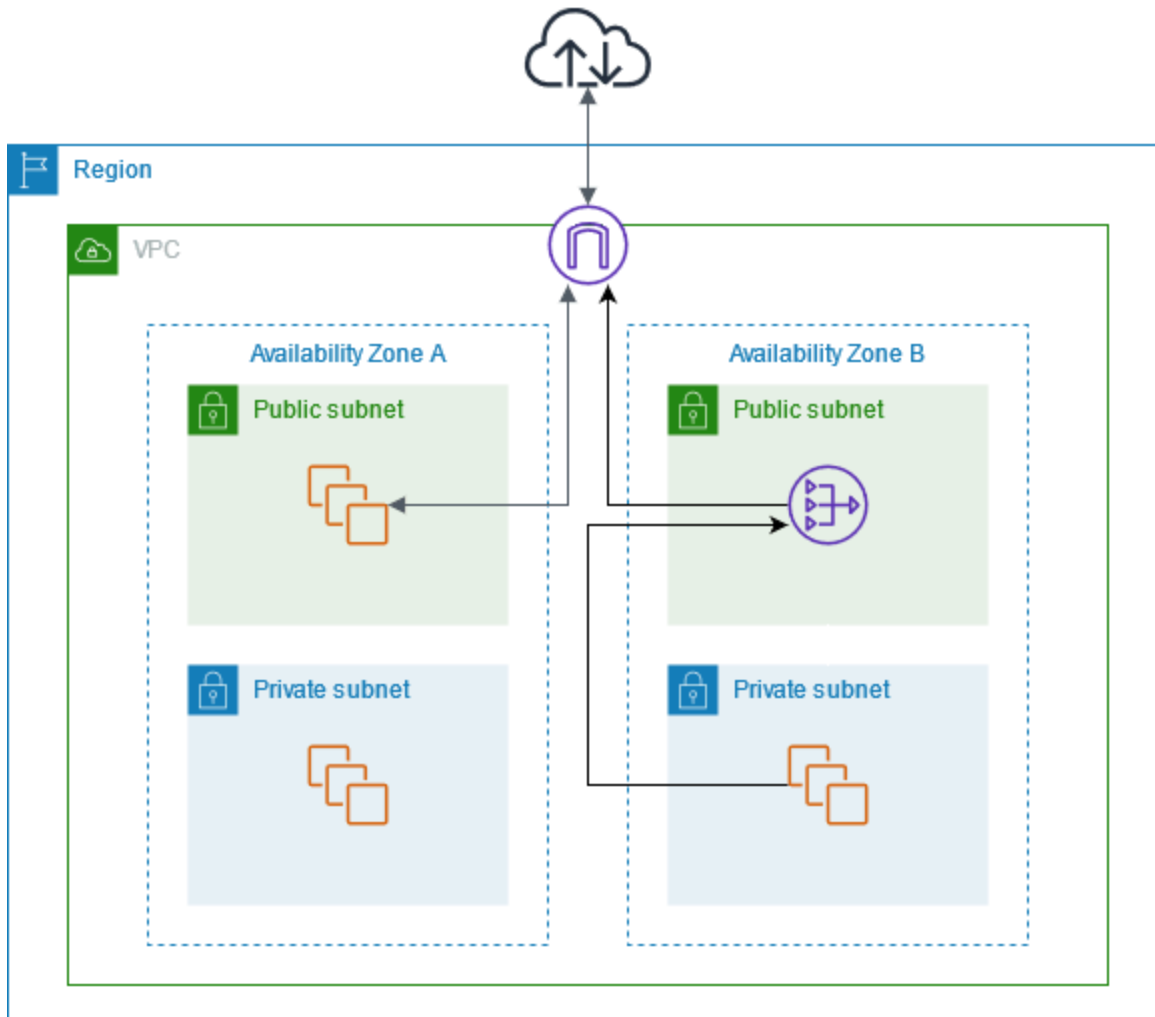
Sie können ein öffentliches NAT-Gateway verwenden, um es Instances in einem privaten Subnetz zu ermöglichen, ausgehenden Datenverkehr an das Internet zu senden, ohne dass das Internet Verbindungen zu den Instances herstellen kann.

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 Quelladresse 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
<i>VPC CIDR</i>	Lokal
0.0.0.0/0	<i>internet-gateway-id</i>

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
<i>VPC CIDR</i>	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
<i>VPC CIDR</i>	Lokal
0.0.0.0/0	<i>internet-gateway-id</i>

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
<i>VPC CIDR</i>	Lokal
0.0.0.0/0	<i>nat-gateway-id</i>

Weitere Informationen finden Sie unter [the section called “Verwalten von Subnetz-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 Elastic-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 mithilfe von PuTTYgen](#) im EC2 Amazon-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 [Verbinden mit Ihrer Linux-Instance mithilfe von PuTTY](#). 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 abubrechen. 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 im EC2 Amazon-Benutzerhandbuch unter [Ihre Instance beenden.](#)

Zugriff auf Ihr Netzwerk mit bereits aufgeführten IP-Adressen

Sie können ein privates NAT-Gateway verwenden, um die Kommunikation von Ihrem Netzwerk VPCs zu Ihrem lokalen Netzwerk mithilfe eines Pools von Adressen auf der Zulassungsliste 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.

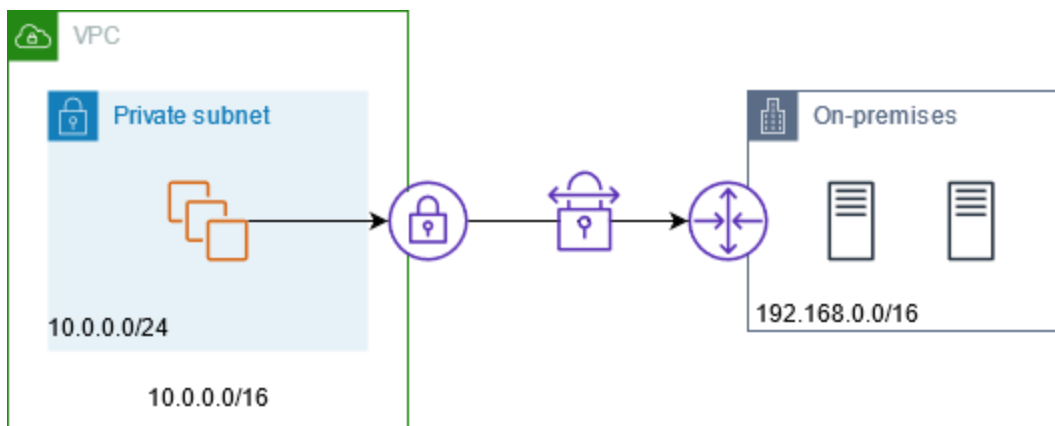
Inhalt

- [-Übersicht](#)

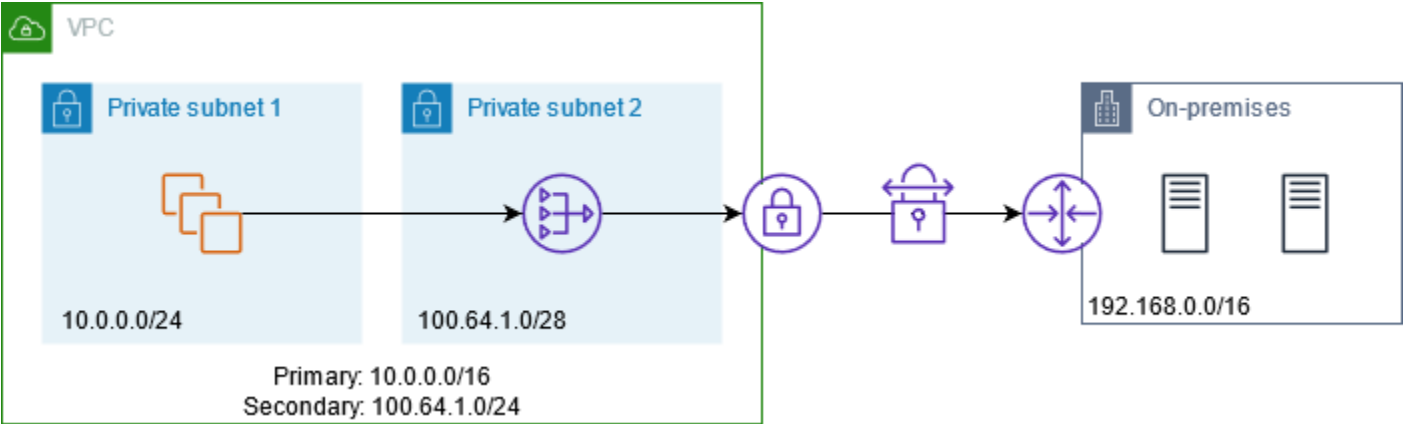
- [Ressourcen](#)
- [Routing](#)

-Übersicht

Das folgende Diagramm zeigt, wie Instances über auf lokale Ressourcen zugreifen können. Site-to-Site 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.

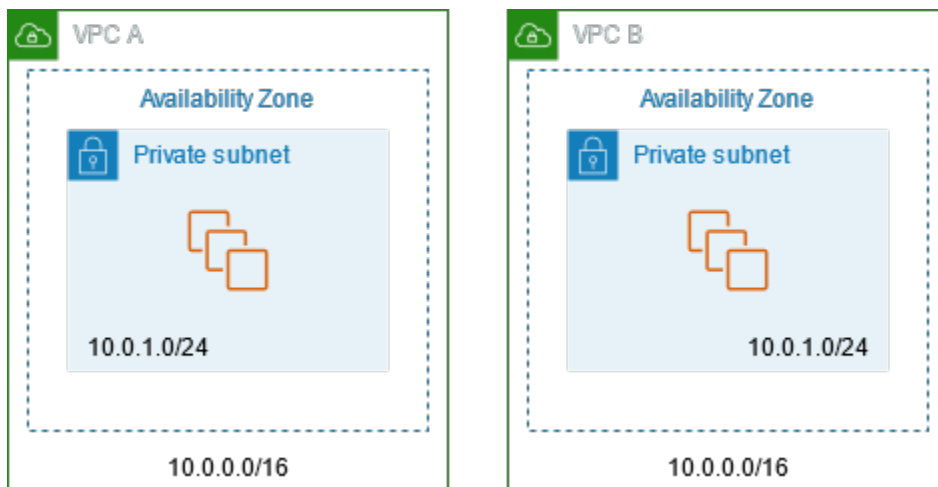
Bestimmungsort	Ziel
10.0.0.0/16	Local
100.64.1.0/24	local
192.168.0.0/16	nat-gateway-id

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
<i>10.0.0.0/16</i>	Local
<i>100.64.1.0/24</i>	local
<i>192.168.0.0/16</i>	<i>vgw-id</i>

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

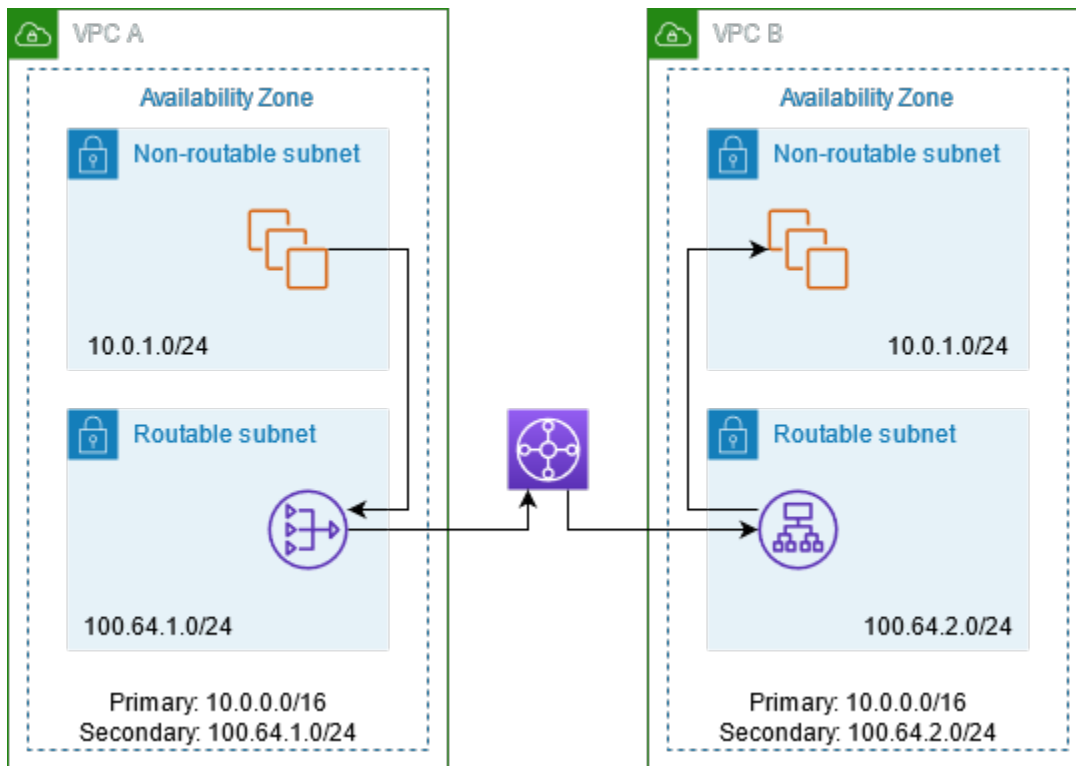
- [-Übersicht](#)
- [Ressourcen](#)
- [Routing](#)

-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 routbaren IP-Adressbereiche den jeweiligen Bereichen zu. VPCs
- 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 ein Transit-Gateway, um eine Verbindung herzustellen. VPCs 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
<i>10.0.0.0/16</i>	Local
<i>100.64.1.0/24</i>	local
<i>100.64.2.0/24</i>	<i>nat-gateway-id</i>

Dies ist die Routing-Tabelle für das routbare Subnetz in VPC A:

Bestimmungsort	Ziel
<i>10.0.0.0/16</i>	Local
<i>100.64.1.0/24</i>	local
<i>100.64.2.0/24</i>	<i>transit-gateway-id</i>

Dies ist die Routing-Tabelle für das nicht routbare Subnetz in VPC B:

Bestimmungsort	Ziel
<i>10.0.0.0/16</i>	Local
<i>100.64.2.0/24</i>	local

Dies ist die Routing-Tabelle für das routbare Subnetz in VPC B:

Bestimmungsort	Ziel
<i>10.0.0.0/16</i>	Local
<i>100.64.2.0/24</i>	local
<i>100.64.1.0/24</i>	<i>transit-gateway-id</i>

Es folgt ein Beispiel für die Routing-Tabelle des Transit-Gateways.

CIDR	Attachment	Routing-Typ
<i>100.64.1.0/24</i>	<i>Attachment for VPC A</i>	Statisch
<i>100.64.2.0/24</i>	<i>Attachment for VPC B</i>	Statisch

DNS64 und NAT64

Ein NAT-Gateway unterstützt die Netzwerkadressübersetzung von IPv6 nach IPv4, im Volksmund auch bekannt als. NAT64 NAT64 unterstützt Ihre IPv6 AWS Ressourcen bei der Kommunikation mit IPv4 Ressourcen in derselben VPC oder einer anderen VPC, in Ihrem lokalen Netzwerk oder über das Internet. Sie können den Resolver NAT64 mit DNS64 Amazon Route 53 verwenden oder Ihren eigenen DNS64 Server verwenden.

Inhalt

- [Was ist DNS64?](#)
- [Was ist? NAT64](#)
- [Konfigurieren und DNS64 NAT64](#)

Was ist DNS64?

Ihre Workloads, die IPv6 nur in ausgeführt werden, VPCs können nur IPv6 Netzwerkpakete senden und empfangen. DNS64Andernfalls wird bei einer DNS-Abfrage für einen Dienst, der IPv4 nur für den Dienst verwendet wird, als Antwort eine IPv4 Zieladresse zurückgegeben, und Ihr IPv6 Nur-Dienst kann nicht mit der Zieladresse kommunizieren. Um diese Kommunikationslücke zu schließen, können Sie die Option DNS64 für ein Subnetz aktivieren. Sie gilt dann für alle AWS Ressourcen innerhalb

dieses Subnetzes. Mit DNS64 sucht der Amazon Route 53 Resolver nach dem DNS-Eintrag für den Service, nach dem Sie gefragt haben, und führt einen der folgenden Schritte aus:

- Wenn der Datensatz eine IPv6 Adresse enthält, wird der ursprüngliche Datensatz zurückgegeben und die Verbindung wird ohne Übersetzung hergestellt. IPv6
- Wenn dem Ziel im DNS-Eintrag keine IPv6 Adresse zugeordnet ist, synthetisiert der Route 53 Resolver eine, indem er der IPv4 Adresse im Datensatz das in RFC6 052 (64 : ff9b : : /96) definierte bekannte /96 Präfix voranstellt. Ihr IPv6 Only-Dienst sendet Netzwerkpakete an die synthetisierte Adresse. IPv6 Sie müssen diesen Datenverkehr dann über das NAT-Gateway weiterleiten, das die erforderliche Übersetzung des Datenverkehrs durchführt, damit IPv6 Dienste in Ihrem Subnetz auf IPv4 Dienste außerhalb dieses Subnetzes zugreifen können.

Sie können die Aktivierung oder Deaktivierung DNS64 in einem Subnetz [modify-subnet-attribute](#) mithilfe der AWS CLI oder mit der VPC-Konsole vornehmen, indem Sie ein Subnetz auswählen und Aktionen > Subnetzeinstellungen bearbeiten wählen.

Was ist? NAT64

NAT64 ermöglicht es Ihren IPv6 Nur-Diensten in Amazon VPCs , mit IPv4 Nur-Diensten innerhalb derselben VPC (in verschiedenen Subnetzen) oder verbunden VPCs, in Ihren lokalen Netzwerken oder über das Internet zu kommunizieren.

NAT64 ist automatisch auf Ihren vorhandenen NAT-Gateways oder auf allen neuen NAT-Gateways, die Sie erstellen, verfügbar. 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 es funktioniert. NAT64

Wenn Ihr IPv6 Only-Dienst nach der Aktivierung DNS64 Netzwerkpakete über das NAT-Gateway an eine synthetisierte IPv6 Adresse sendet, passiert Folgendes:

- Anhand des 64 : ff9b : : /96 Präfixes erkennt das NAT-Gateway, dass es sich um IPv4 das ursprüngliche Ziel handelt, IPv4 und übersetzt die IPv6 Pakete durch Ersetzung in:
 - Quelle IPv6 mit eigener privater IP, die vom Internet-Gateway in Elastic IP-Adresse übersetzt wird.
 - Ziel IPv6 zu, IPv4 indem das Präfix gekürzt wird 64 : ff9b : : /96.
- Das NAT-Gateway sendet die übersetzten IPv4 Pakete über das Internet-Gateway, das Virtual Private Gateway oder das Transit-Gateway an das Ziel und initiiert eine Verbindung.

- Der IPv4 Only-Host sendet IPv4 Antwortpakete zurück. Nachdem eine Verbindung hergestellt wurde, akzeptiert das NAT-Gateway die IPv4 Antwortpakete von den externen Hosts.
- Die IPv4 Antwortpakete sind für das NAT-Gateway bestimmt, das die Pakete empfängt und NATs sie degeneriert, indem es seine IP (Ziel-IP) durch die IPv6 Adresse des Hosts ersetzt und der IPv4 Quelladresse wieder `64:ff9b::/96` vorangestellt. Das Paket fließt dann in der lokalen Route zum Host.

Auf diese Weise ermöglicht das NAT-Gateway Ihren IPv6 Nur-Workloads in einem Subnetz die Kommunikation mit IPv4 Nur-Diensten außerhalb des Subnetzes.

Konfigurieren und DNS64 NAT64

Folgen Sie den Schritten in diesem Abschnitt, um die Kommunikation mit IPv4 reinen Diensten NAT64 zu konfigurieren DNS64 und zu aktivieren.

Inhalt

- [Ermöglichen Sie mit IPv4 der CLI die Kommunikation mit reinen Diensten im Internet AWS](#)
- [Ermöglichen Sie die Kommunikation mit IPv4 reinen Diensten in Ihrer lokalen Umgebung](#)

Ermöglichen Sie mit IPv4 der CLI die Kommunikation mit reinen Diensten im Internet AWS

Wenn Sie über ein Subnetz mit IPv6 reinen Workloads verfügen, das mit IPv4 Nur-Diensten außerhalb des Subnetzes kommunizieren muss, zeigt Ihnen dieses Beispiel, wie Sie diese Nur-Dienste für die Kommunikation mit IPv6 Nur-Diensten im Internet aktivieren. IPv4

Sie sollten zunächst ein NAT-Gateway in einem öffentlichen Subnetz konfigurieren (getrennt von dem Subnetz, das die reinen Workloads enthält). IPv6 Zum Beispiel sollte das Subnetz, das das NAT-Gateway enthält, über eine `0.0.0.0/0`-Route verfügen, die auf das Internet-Gateway gerichtet ist.

Gehen Sie wie folgt vor, damit diese IPv6 Nur-Dienste eine Verbindung zu Nur-Diensten im Internet herstellen können: IPv4

1. Fügen Sie der Routentabelle des Subnetzes, das die reinen Workloads enthält, die folgenden drei Routen hinzu: IPv6
 - IPv4 Route (falls vorhanden), die auf das NAT-Gateway verweist.

- `64:ff9b::/96`-Route, die auf das NAT-Gateway zeigt. Dadurch kann der Datenverkehr von Ihren Workloads, die IPv6 nur für IPv4 -Dienste bestimmt sind, über das NAT-Gateway geleitet werden.
- `IPv6 :::/0`Route, die auf das Internet-Gateway für ausgehenden Datenverkehr (oder das Internet-Gateway) verweist.

Beachten Sie, dass der Verweis `:::/0` auf das Internet-Gateway es externen IPv6 Hosts (außerhalb der VPC) ermöglicht, eine Verbindung herzustellen. IPv6

```
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 in dem Subnetz, das die reinen IPv6 Workloads enthält.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-1a2b3c4d --enable-dns64
```

Jetzt können Ressourcen in Ihrem privaten Subnetz statusbehaftete Verbindungen IPv4 sowohl IPv6 mit Diensten im Internet herstellen. Konfigurieren Sie Ihre Sicherheitsgruppe NACLs entsprechend, um ausgehenden und eingehenden Datenverkehr dem Datenverkehr zuzulassen. `64:ff9b::/96`

Ermöglichen Sie die Kommunikation mit IPv4 reinen Diensten in Ihrer lokalen 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 Route 53 Resolver-Endpunkt in einer VPC und weisen ihm die IPv4 Adressen zu, von denen Route 53 Resolver Abfragen weiterleiten soll. Für Ihren lokalen DNS-Resolver sind dies die IP-Adressen, von denen die DNS-Abfragen stammen, und es sollten sich daher um Adressen handeln. IPv4

- 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 geben auch die IPv4 Adressen der lokalen Resolver an.
- Nachdem Sie nun einen ausgehenden Route 53 Resolver-Endpunkt eingerichtet haben, müssen Sie ihn in DNS64 dem Subnetz aktivieren, das IPv6 nur Ihre Workloads enthält, und alle Daten, die für Ihr lokales Netzwerk bestimmt sind, über ein NAT-Gateway weiterleiten.

So DNS64 funktioniert das für reine Ziele in lokalen Netzwerken: IPv4

1. Sie weisen dem ausgehenden Route 53 Resolver-Endpunkt in Ihrer VPC eine IPv4 Adresse zu.
2. Die DNS-Anfrage von Ihrem IPv6 Dienst geht an Route 53 Resolver über IPv6. Route 53 Resolver gleicht die Abfrage mit der Weiterleitungsregel ab und ruft eine IPv4 Adresse für Ihren lokalen 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 steht für eine ENI, die die Anfrage an die lokale IPv4 Adresse Ihres DNS-Resolvers weiterleitet.
4. Der lokale Resolver sendet das Antwortpaket über den ausgehenden Endpunkt IPv4 zurück an den Route 53 Resolver.
5. Unter der Annahme, dass die Abfrage von einem DNS64 -aktivierten Subnetz aus gestellt wurde, führt Route 53 Resolver zwei Dinge aus:
 - a. Überprüft den Inhalt des Antwortpakets. Wenn der Datensatz eine IPv6 Adresse enthält, wird der Inhalt unverändert beibehalten, wenn er jedoch nur einen Datensatz enthält. IPv4 Es synthetisiert auch einen IPv6 Datensatz, indem es der IPv4 Adresse `64:ff9b::/96` vorangestellt wird.
 - b. Verpackt den Inhalt neu und sendet ihn an den Service in Ihrer VPC. IPv6

Überprüfen Sie den Verkehr von NAT-Gateways

Sie können einen Netzwerk-Firewall-Proxy an Ihr NAT-Gateway anhängen, um den Datenverkehr auf Ihrem NAT-Gateway zu überprüfen und zu filtern. Mit dieser Sicherheitskontrolle können Sie Datenlecks außerhalb Ihres vertrauenswürdigen Perimeters verhindern und unerwünschte eingehende Antworten blockieren.

Funktionsweise

Wenn Sie einen Netzwerk-Firewall-Proxy erstellen, müssen Sie ein vorhandenes NAT-Gateway auswählen, an das der Proxy angeschlossen werden soll. Nach der Erstellung hat der Proxy:

- Der Proxy wird mit einem vollqualifizierten Domainnamen geliefert und Sie müssen Ihre Anwendungen so einrichten, dass sie HTTP- und HTTPS-Verbindungsanfragen an den Proxy senden. Der Proxy filtert zunächst den Domainnamen in der Verbindungsanfrage auf der Grundlage der vom Kunden eingegebenen Regeln. Wenn der Kunde dies zulässt, führt der Proxy dann eine DNS-Abfrage durch, um die IP-Adresse der Domain abzurufen. Anschließend wurde eine TCP-Verbindung mit dem Endziel hergestellt. Je nachdem, ob die TLS-Entschlüsselung aktiviert ist, filtert der Proxy dann die TLS-Verbindung anhand der IP-Adresse und der Header-Attribute und stellt nur dann eine TLS-Verbindung mit dem Ziel her, wenn die IP- und Header-Attribute (einschließlich der Header-Aktion und des URL-Pfads) nach den Richtlinien zulässig sind.
- Die Appliance überprüft und filtert den Datenverkehr.
- Zulässiger Verkehr wird bis zum Ziel weitergeführt (im Internet, in der lokalen Umgebung oder in einer anderen VPC).

Appliances anschließen

Appliances werden über die AWS Network Firewall an NAT-Gateways angeschlossen. Anweisungen zum Erstellen und Anhängen von Appliances finden Sie im [Network Firewall Proxy Developer Guide](#).

Angeschlossene Appliances anzeigen

Verwenden Sie den [describe-nat-gateways](#) folgenden Befehl, um Appliances anzuzeigen, die an Ihr NAT-Gateway angeschlossen sind:

```
aws ec2 describe-nat-gateways --nat-gateway-ids nat-1234567890abcdef0
```

Die Antwort enthält ein `AttachedAppliances` Feld mit folgenden Angaben:

- `Typ` — Der Gerätetyp (z. B. `network-firewall-proxy`)
- `ApplianceArn` — Die ARN der angeschlossenen Appliance
- `AttachmentState` — Aktueller Status des Anhangs (`attached`, `detaching`, `detached`, `attach_failed`, `detach_failed`)
- `ModificationState` — Aktueller Änderungsstatus (`modifying`, `completed`, `failed`)

- **VpcEndpointId**— Die VPC-Endpunkt-ID, die verwendet wird, um den Datenverkehr VPCs zur Inspektion und Filterung von der Anwendung zum Proxy weiterzuleiten
- **FailureCode**— Der Fehlercode, wenn der Vorgang zum Anhängen oder Ändern der Appliance fehlgeschlagen ist
- **FailureMessage**— Eine beschreibende Meldung, die den Fehler erklärt, falls der Vorgang zum Anschließen oder Ändern der Appliance fehlgeschlagen ist

Überwachen von NAT-Gateways mit Amazon CloudWatch

Sie können Ihren NAT-Gateway mit CloudWatch überwachen. Dabei werden Informationen von Ihrem NAT-Gateway erfasst und lesbare, nahezu Echtzeitmetriken erstellt. Diese Informationen können Sie für die Überwachung Ihres NAT-Gateways und die Fehlersuche verwenden. Diese Metriken geben Ihnen einen Einblick in den Zustand und die Leistung Ihres NAT-Gateways, damit Sie dessen Betrieb genau überwachen und Probleme schnell beheben können.

Die von CloudWatch gesammelten NAT-Gateway-Metriken umfassen Datenpunkte wie verarbeitete Bytes, Anzahl von Paketen, Verbindungszahlen und Fehlerraten. So können Sie den Datenverkehr, der durch Ihr NAT-Gateway fließt, genau verstehen und etwaige Anomalien oder Engpässe identifizieren. CloudWatch stellt diese Metrikdaten in Intervallen von einer Minute bereit und bietet Ihnen so einen detaillierten, minutengenauen Überblick über das Verhalten Ihres NAT-Gateways.

Zudem speichert CloudWatch diese NAT-Gateway-Metrikdaten für einen längeren Zeitraum von 15 Monaten, sodass Sie Trends und Muster im Laufe der Zeit analysieren können. Sie können diese historischen Daten für die Kapazitätsplanung und zur Leistungsoptimierung verwenden und die langfristige Entwicklung Ihrer NAT-Gateway-Nutzung nachvollziehen.

Um diese leistungsstarken Überwachungsfunktionen zu nutzen, können Sie benutzerdefinierte CloudWatch-Dashboards und -Warnungen erstellen, die auf Ihre spezifischen Anforderungen zugeschnitten sind. Sie könnten beispielsweise Warnmeldungen einrichten, um benachrichtigt zu werden, wenn die ausgehende Datenübertragung Ihres NAT-Gateways einen bestimmten Schwellenwert überschreitet, sodass Sie potenziellen Bandbreitenbeschränkungen proaktiv begegnen können.

Weitere Informationen zu Preisen finden Sie unter [Amazon CloudWatch – Preise](#).

Inhalt

- [Metriken und Dimensionen des NAT-Gateway](#)
- [Anzeigen von NAT-Gateway-CloudWatch-Metriken](#)

- [Erstellen von CloudWatch-Alarmen zur Überwachung eines NAT-Gateways](#)

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-Gateway 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 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.
BytesInFromSource	Anzahl der Bytes, die von dem NAT-Gateway von Clients in Ihrer VPC empfangen wurden. Wenn der Wert für BytesOutToDestination kleiner als der Wert für BytesInFromSource ist, kommt es ggf. bei der Verarbeitung des NAT-Gateways zu einem Datenverlust, oder der Datenverkehr wird vom NAT-Gateway aktiv blockiert.

Metrik	Beschreibung
	omSource 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. Das beinhaltet nur die erste SYN. In einigen Fällen kann ConnectionAttemptCount aufgrund einer erneuten SYN-Übertragung niedriger sein als ConnectionEstablishedCount . 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. Dies schließt SYN- und SYN-Neuübertragungen ebenfalls ein. 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 Leerlaufstatus übergegangen sind. Wenn der Wert für IdleTimeoutCount zunimmt, kann dies darauf hindeuten, dass Clients hinter dem NAT-Gateway ältere Verbindungen wiederverwenden. Einheit: Anzahl Statistiken: Die nützlichste Statistik ist Sum.

Metrik	Beschreibung
PacketsDropCount	Anzahl der Pakete, die vom NAT-Gateway verworfen wurden. Um die Anzahl der verworfenen Pakete als Prozentsatz des gesamten Paket-Datenverkehrs zu berechnen, verwenden Sie diese Formel: $\text{PacketsDropCount} / (\text{PacketsInFromSource} + \text{PacketsInFromDestination}) * 100$. Wenn dieser Wert 0,01 Prozent des Gesamtdatenverkehrs auf dem NAT-Gateway überschreitet, liegt möglicherweise ein Problem mit dem Amazon VPC-Service vor. Verwenden Sie das AWS Service Health Dashboard, um Probleme mit dem Service zu erkennen, die dazu führen könnten, dass NAT-Gateways Pakete verwerfen. 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 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.

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 Paketrage (pro Sekunde verarbeitete Pakete) und meldet dann das Maximum der sechs Raten (die höchste durchschnittliche Paketrage). 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-Metrikdaten werden in Intervallen von 1 Minute an CloudWatch gesandt. Metriken werden zuerst nach dem Service-Namespaces 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 a 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, sobald 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 Metrik BytesOutToDestination für das NAT-Gateway und wählen Sie dann Select metric (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 Metrik ErrorPortAllocation für das NAT-Gateway und wählen Sie dann Select metric (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 angezeigt `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-	Prüfen Sie auf der Seite Subnets (Subnetze) der Amazon VPC-Konsole, wie

Angezeigter Fehler	Ursache	Lösung
	Gateway ist eine Netzwerkschnittstelle mit einer privaten IP-Adresse aus dem IP-Adressbereich des Subnetzes erforderlich.	viele IP-Adressen in Ihrem Subnetz verfügbar sind. 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-xxxxx-xxx 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 Hinzufügen eines Internetzugriffs zu einem Subnetz .

Angezeigter Fehler	Ursache	Lösung
Die Elastic-IP-Adresse eipalloc-xxxxxxx 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 Erste Schritte zum Verwenden von 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 angezeigt: `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 erläutert [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 Zielpunkt 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 für NAT-Gateways

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 von Amazon Linux AMI, 2018.03, die am 31. Dezember 2020 das Ende des Standardsupports erreicht hat. Die Wartungsunterstützung endet am 31. Dezember 2023. Weitere Informationen finden Sie im folgenden Blogbeitrag: [Amazon Linux AMI End of Life](#).

Wenn Sie ein vorhandenes NAT-AMI verwenden, empfiehlt AWS 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 als NAT-Gateways zu Ihrem Anwendungsfall passen, können Sie Ihr eigenes NAT-AMI aus einer aktuellen Version von Amazon Linux erstellen, wie in [the section called “3. Erstellen eines NAT-AMI”](#) beschrieben.

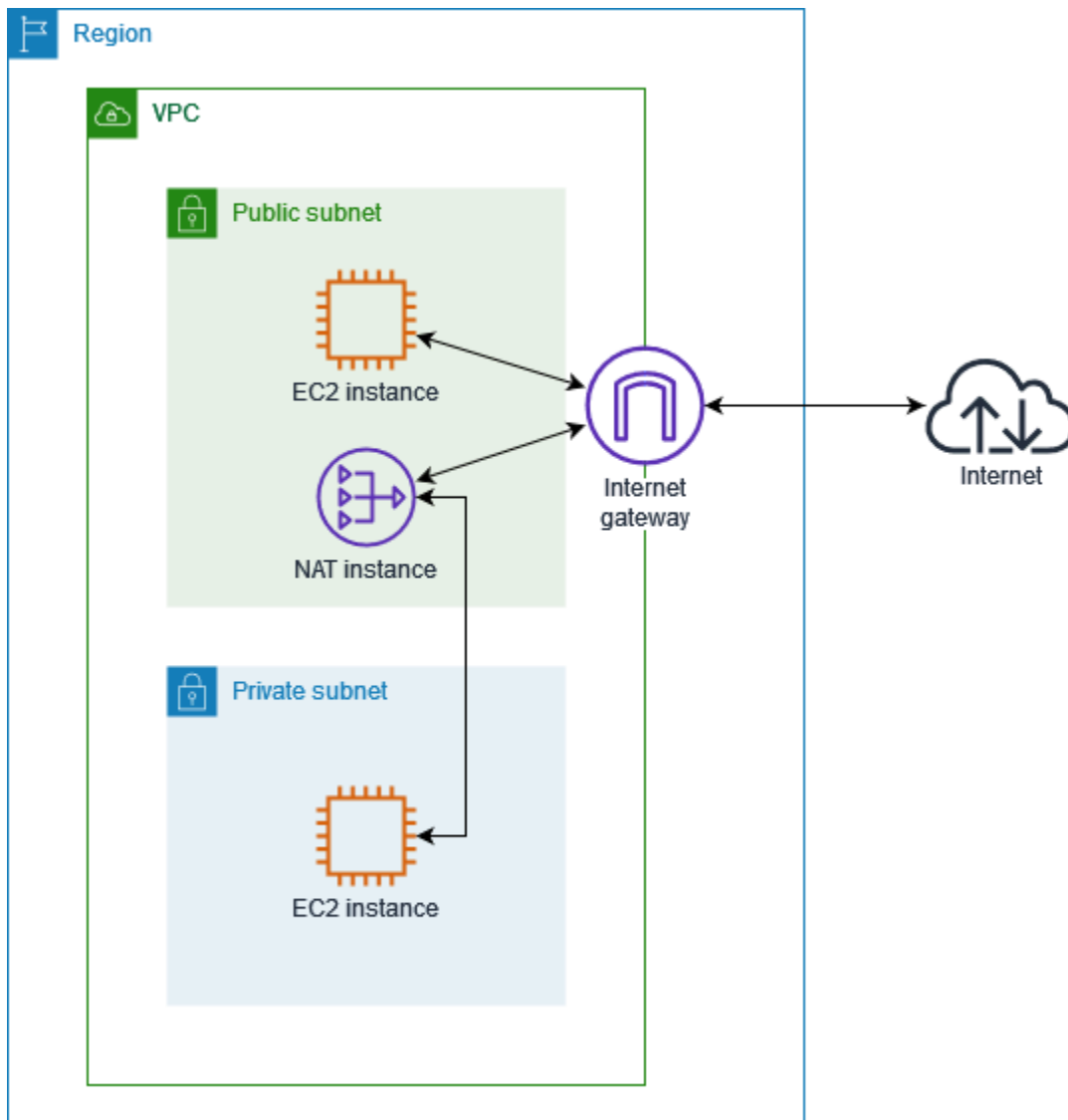
Inhalt

- [Grundlagen zu NAT-Instances](#)
- [Ermöglichen der Kommunikation außerhalb der VPC für private Ressourcen](#)

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.

Ermöglichen der Kommunikation außerhalb der VPC für private Ressourcen

In diesem Abschnitt wird beschrieben, wie Sie NAT-Instances erstellen und mit ihnen arbeiten, um Ressourcen in einem privaten Subnetz die Kommunikation außerhalb der Virtual Private Cloud zu ermöglichen.

Aufgaben

- [1. Erstellen einer VPC für die NAT-Instance](#)
- [2. Erstellen einer Sicherheitsgruppe für Ihre NAT-Instance](#)
- [3. Erstellen eines NAT-AMI](#)
- [4. Starten einer NAT-Instance](#)
- [5. Deaktivieren der Quell-/Zielprüfungen](#)
- [6. Aktualisieren der Routing-Tabelle](#)
- [7. Testen Ihrer NAT-Instance](#)

1. 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.

2. 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 für eingehenden Datenverkehr aufgeführt.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentare
<i>CIDR für privates Subnetz</i>	TCP	80	Erlauben Sie eingehenden HTTP-Datenverkehr von Servern zum privaten Subnetz.
<i>CIDR für privates Subnetz</i>	TCP	443	Erlauben Sie eingehenden HTTPS-Datenverkehr von Servern zum privaten Subnetz.
<i>Öffentlicher IP-Adressbereich Ihres Netzwerks</i>	TCP	22	Lässt eingehenden SSH-Zugriff auf die NAT-Instance von Ihrem Netzwerk zu (über das Internet-Gateway)

Im Folgenden sind die empfohlenen Regeln für ausgehenden Datenverkehr aufgeführt.

Bestimmungsort	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](#).

3. 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

- 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
```

- Erstellen Sie aus der EC2-Instance ein NAT-AMI. Weitere Informationen finden Sie unter [Erstellen eines Linux-AMI aus einer Instance](#) im Amazon-EC2-Benutzerhandbuch.

4. 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

- Öffnen Sie die Amazon EC2-Konsole unter <https://console.aws.amazon.com/ec2/>.
- Wählen Sie auf dem Dashboard Launch Instance (Instance starten) aus.
- Geben Sie unter Name einen Namen für Ihre NAT-Instance ein.
- Wählen Sie für Anwendungs- und Betriebssystemabbilder Ihr NAT-AMI aus (wählen Sie Weitere AMIs durchsuchen, Meine AMIs).
- Wählen Sie für Instance-Typ einen Instance-Typ aus, der die Anforderungen Ihrer NAT-Instance an Rechenleistung, Arbeitsspeicher und Speicherplatz erfüllt.
- Wählen Sie unter Schlüsselpaar ein vorhandenes Schlüsselpaar aus oder Erstellen Sie ein neues Schlüsselpaar.
- Führen Sie unter Network settings (Netzwerkeinstellungen) die folgenden Schritte aus:
 - 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 (Öffentliche 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 [5. Deaktivieren der Quell-/Zielprüfungen](#)).
 10. Aktualisieren Sie die Routing-Tabelle, um Datenverkehr an die NAT-Instance zu senden (siehe [6. Aktualisieren der Routing-Tabelle](#)).

5. 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.

6. 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](#).

7. 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 Edit inbound rules (Regeln für eingehenden Datenverkehr bearbeiten) aus.
5. Wählen Sie Add rule. 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 Add rule. 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 Add rule. 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 Ihres privaten Schlüssels mit PuTTYgen](#).

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 abubrechen. 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 abubrechen.

```
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 [5. Deaktivieren der Quell-/Zielprüfungen](#).
- Stellen Sie sicher, dass Ihre Routing-Tabellen korrekt konfiguriert sind. Weitere Informationen finden Sie unter [6. 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 die 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 das NAT-Gateway .	Anzeigen von CloudWatch-Metriken für die Instance.
Timeout-Verhalten	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

Eine Elastic IP-Adresse ist eine statische, öffentliche IPv4 Adresse, die speziell für die dynamische Natur des Cloud Computing entwickelt wurde. Mit dieser Funktion können Sie eine Elastic IP-Adresse mit einer beliebigen Instanz oder Netzwerkschnittstelle innerhalb einer beliebigen Virtual Private Cloud (VPC) in Ihrem AWS Konto verknüpfen. Durch die Nutzung von Elastic-IP-Adressen können Sie eine Vielzahl von Vorteilen nutzen, die die Verwaltung und Stabilität Ihrer cloudbasierten Infrastruktur vereinfachen.

Einer der Hauptvorteile von Elastic-IP-Adressen ist ihre Fähigkeit, den Ausfall einer Instanz zu maskieren. Sollte es bei einer Instance zu einem unerwarteten Ausfall kommen oder eine Instance ersetzt werden müssen, können Sie die zugehörige Elastic-IP-Adresse einer anderen Instance in

Ihrer VPC neu zuordnen. Dieser Failover-Prozess stellt sicher, dass Ihre Anwendungen und Services über einen konsistenten und zuverlässigen öffentlichen Endpunkt verfügen, wodurch Ausfallzeiten minimiert und ein hervorragendes Benutzererlebnis ermöglicht wird.

Zudem bieten Elastic-IP-Adressen Flexibilität bei der Verwaltung Ihrer Netzwerkressourcen. Sie können diese Adressen je nach Bedarf programmgesteuert zuordnen und trennen, sodass Sie den Datenverkehr je nach Ihren sich ändernden Geschäftsanforderungen an verschiedene Instances weiterleiten können. Diese dynamische Zuweisung öffentlicher IP-Adressen ermöglicht es Ihnen, sich an veränderte Anforderungen anzupassen, Ihre Infrastruktur zu skalieren und innovative Architekturen ohne die Einschränkungen statischer IP-Zuweisungen zu implementieren.

Elastic-IP-Adressen können nicht nur als Failover verwendet werden, sondern auch als stabile IDs für Ihre cloudbasierten Ressourcen dienen. Dies kann nützlich sein, wenn Sie externe Dienste wie DNS-Einträge oder Firewall-Regeln für die Kommunikation mit Ihren von Ihnen AWS gehosteten Anwendungen konfigurieren. Durch die Zuweisung einer persistenten öffentlichen IP-Adresse können Sie Ihre Netzwerkkonfigurationen zukunftsicher gestalten und vermeiden, dass externe Referenzen aktualisiert werden müssen, wenn zugrunde liegende Instances ersetzt oder skaliert werden.

Inhalt

- [Elastic-IP-Adresskonzepte und -Regeln](#)
- [Erste Schritte zum Verwenden von Elastic-IP-Adressen](#)

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 EC2 Amazon-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 der primären Netzwerkschnittstelle Ihrer Instance eine Elastic IP-Adresse zuordnen, wird deren aktuelle öffentliche IPv4 Adresse (falls vorhanden) für den öffentlichen IP-Adresspool freigegeben. Wenn Sie die Elastic IP-Adresse trennen, wird der primären Netzwerkschnittstelle innerhalb weniger Minuten automatisch 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](#).
- Elastische 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 Netzwerkgranzgruppe zuordnen. Dies ist der Ort, von dem aus wir den CIDR-Block bewerben. Durch Festlegen der Netzwerkgranzgruppe 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 EC2 Amazon-Benutzerhandbuch.
- Öffentliche IPv4 Adressen unterstützen Tags zur Kostenzuweisung. Wenn Sie Tags auf Elastic IP-Adressen anwenden, können Sie diese Tags verwenden, um die Kosten für öffentliche IPv4 Adressen in zu verfolgen AWS Cost Explorer.

Bevor Sie Tags als Kostenzuweisungs-Tags verwenden können, müssen Sie die Tags aktivieren. Weitere Informationen finden Sie unter [Activating user-defined cost allocation tags](#) (Benutzerdefinierte Kostenzuordnungs-Tags aktivieren) im AWS Billing -Benutzerhandbuch. Hinweis: Nachdem Sie benutzerdefinierte Tags erstellt und auf Ihre Ressourcen angewendet

haben, kann es bis zu 24 Stunden dauern, bis die Tag-Schlüssel auf der Seite für Kostenzuordnungs-Tags zur Aktivierung angezeigt werden.

Sobald die Kostenzuordnung-Tags aktiviert sind...

- Für alle öffentlichen IPv4 Adressen (einschließlich öffentlicher IPv4 Adressen, die EC2 Instances zugewiesen sind, und Elastic IP-Adressen), die mit einer elastic network interface verknüpft sind, können Sie die mit öffentlichen IPv4 Adressen verbundenen Kosten im Cost Explorer anzeigen, indem Sie Nutzungstyp > Öffentlich IPv4 InUseAddress (Stunden) wählen.
- Wenn eine markierte Elastic IP-Adresse keiner ENI oder einer gestoppten Ressource (wie einer gestoppten EC2 Instance) zugeordnet ist, wird sie als inaktive IPv4 Adresse betrachtet. Sie können die mit inaktiven IPv4 Adressen verbundenen Kosten im Cost Explorer anzeigen, indem Sie Verwendungsart > Öffentlich IPv4 IdleAddress (Stunden) wählen.

Weitere Informationen zum Cost Explorer finden Sie unter [Analysieren Ihrer Kosten mit AWS Cost Explorer](#) im AWS Billing -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.

Weitere Informationen zu den Preisen für Elastic IP-Adressen finden Sie unter Öffentliche IPv4 Adresse in der [Amazon VPC-Preisgestaltung](#).

Erste Schritte zum Verwenden von Elastic-IP-Adressen

In den folgenden Abschnitten werden die ersten Schritte zum Verwenden von Elastic-IP-Adressen beschrieben.

Aufgaben

- [1. Zuweisen einer Elastic-IP-Adresse](#)
- [2. So ordnen Sie eine Elastic-IP-Adresse zu](#)
- [3. Aufheben der Zuordnung einer Elastic-IP-Adresse](#)
- [4. Übertragen von Elastic-IP-Adressen](#)
- [5. Freigeben einer Elastic-IP-Adresse](#)
- [6. Wiederherstellen einer Elastic-IP-Adresse](#)
- [Befehlszeilenübersicht](#)

1. 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 aus.
3. Wählen Sie Elastic-IP-Adresse zuweisen aus.
4. (Optional) Wenn Sie eine Elastic IP-Adresse (EIP) zuweisen, wählen Sie die Netzwerkgranzgruppe aus, der die EIP zugewiesen werden soll. Eine Netzwerkgranzgruppe 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 Netzwerkgranzgruppen als die AZs in einer Region haben, 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 Netzwerkgranzgruppe zuordnen wie die AWS Ressource, die der EIP zugeordnet wird. Eine EIP in einer Netzwerkgranzgruppe kann nur in Zonen dieser Netzwerkgranzgruppe angekündigt werden und nicht in anderen Zonen, die durch andere Netzwerkgranzgruppen repräsentiert werden.

Wenn Sie Local Zones oder Wellenlängenzonen aktiviert haben (weitere Informationen finden Sie unter [Aktivieren einer lokalen Zone](#) oder [Aktivieren von Wellenlängenzonen](#)), können Sie eine Netzwerkgranzgruppe für AZs, Local Zones oder Wellenlängenzonen auswählen. Wählen Sie die Netzwerkgranzgruppe sorgfältig aus, da sich die EIP und die AWS Ressource, der sie zugeordnet ist, in derselben Netzwerkgranzgruppe befinden müssen. Sie können die EC2 Konsole verwenden, um die Netzwerkgranzgruppe 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 Netzwerkgranzgruppe an, wohingegen Local Zones oder Wavelength Zones zu ihren eigenen separaten Netzwerkgranzgruppen gehören.

Wenn Sie Local Zones oder Wavelength Zones nicht aktiviert haben, ist bei der Zuweisung einer EIP die Netzwerkgranzgruppe, 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 Netzwerkgranzgruppe zuweisen, in der gesamten Region, AZs in der Sie sich befinden, beworben wird.

5. Wählen Sie für den öffentlichen IPv4 Adresspool eine der folgenden Optionen aus:

- Der IP-Adresspool von Amazon — Wenn Sie möchten, dass eine IPv4 Adresse aus dem IP-Adresspool von Amazon zugewiesen wird.
- Mein Pool an öffentlichen 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 IPv4 Adresspool — Wenn Sie eine IPv4 Adresse aus einem Pool, der in Ihrem lokalen Netzwerk erstellt wurde, für die Verwendung mit einem Outpost zuweisen möchten. 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.

2. 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 aus. 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.

3. 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 aus 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).

4. 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 AWS-Konto zum anderen zu verlagern. Sie müssen nicht warten, bis neue Elastic IP-Adressen in Ihren Sicherheitsgruppen zugelassen werden und. NACLs
- Zentralisierte Sicherheitsadministration — Verwenden Sie ein zentrales AWS Sicherheitskonto, um Elastic IP-Adressen zu verfolgen und zu übertragen, die auf Einhaltung der Sicherheitsbestimmungen überprüft wurden.

- Disaster Recovery — Verwenden Sie Elastic IP-Adressübertragungen, um bei Notfällen schnell eine IPs Neuzuweisung für öffentlich zugängliche Internet-Workloads vorzunehmen.

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 [describe-address-transfers](#) AWS CLI Befehls). 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 [describe-address-transfers](#) AWS CLI Befehls) 14 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 aus 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 Konto-ID übertragen IDs die 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 aus IPs.
4. Vergewissern Sie sich IPs, dass Sie in der Ressourcenliste von Elastic die Eigenschaft aktiviert haben, die die Spalte 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 [describe-address-transfers](#) AWS CLI Befehls). 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:

- **AddressLimitExceeded:** 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 EC2 Amazon-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 EC2 Amazon-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 werden. Weitere Informationen finden Sie unter [Trennen einer Elastic IP-Adresse](#) im EC2 Amazon-Benutzerhandbuch.

Für alle anderen Ausnahmen [wenden Sie sich an 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 aus.
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.

5. 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 Gebühren an, auch wenn sie keiner Instance zugeordnet ist. 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 aus 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.

6. 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 die Wiederherstellung dazu führt, dass Sie Ihr Elastic IP-Adresskontingent überschreiten.

Sie können eine Elastic IP-Adresse mithilfe der EC2 Amazon-API oder eines Befehlszeilentools 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
```

Befehlszeilenübersicht

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

- [disable-address-transfer](#) (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)

Übertragung für Elastic-IP-Adressen aktivieren

- [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)

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 Direct Connect-Verbindungen weiterleitet.

Einer der Hauptvorteile der Verwendung eines Transit-Gateways ist die Möglichkeit, die Verwaltung der Konnektivität zwischen Ihren VPCs und On-Premises-Netzwerken zu zentralisieren und zu vereinfachen. Anstatt mehrere VPN-Verbindungen oder Direct-Connect-Verbindungen zu konfigurieren, können Sie das Transit-Gateway als zentralen Integrationspunkt nutzen. Das kann dazu beitragen, die Gesamtkomplexität und den betrieblichen Aufwand Ihrer Netzwerkarchitektur zu reduzieren.

Die Preise für die Nutzung eines Transit-Gateways basieren auf dem Datenvolumen, das über das Gateway übertragen wird. Es gibt eine Gebühr pro GB für die Übertragung von Daten innerhalb und außerhalb des Transit-Gateways sowie eine separate Gebühr pro Stunde für die Transit-Gateway-Ressource selbst. Die spezifischen Preise können je nach AWS-Region variieren und können sich ändern. Daher ist es wichtig, die aktuellsten Informationen auf der Seite mit den aktuellen Preisgestaltung für AWS Transit Gateway zu lesen. Wenn Sie das Preismodell für Transit-Gateways verstehen, können Sie die laufenden Kosten im Zusammenhang mit diesem AWS-Netzwerkservice besser planen und budgetieren. Dies in Kombination mit der betrieblichen Effizienz und den Vorteilen bei der Konnektivität macht Transit-Gateways zu einer überzeugenden Wahl für Unternehmen, die skalierbare und kostengünstige Hybrid-Cloud-Lösungen entwickeln möchten.

In der folgenden Tabelle werden einige gängige Anwendungsfälle für Transit-Gateways beschrieben. Weitere Informationen zu den einzelnen Anwendungsfällen finden Sie unter [Beispiel-Szenarios für Transit-Gateways](#) im Benutzerhandbuch für AWS Transit Gateway.

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.
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.
Isolierte VPCs mit freigegebenen 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.

Weitere Informationen finden Sie unter [AWS Transit Gateway](#).

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.

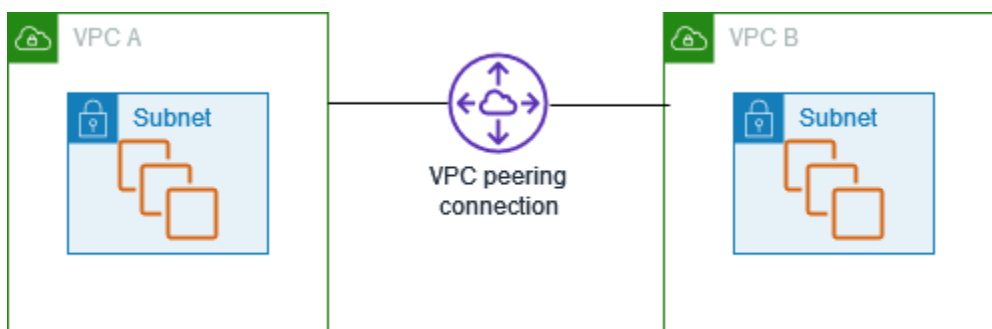
VPN-Konnektivitäts option	Beschreibung
AWS Site-to-Site VPN	Sie können eine IPsec-VPN-Verbindung zwischen Ihrer VPC und Ihrem Remote-Netzwerk einrichten. Auf der AWS-Seite der Site-to-Site VPN-Verbindung stellt ein Virtual Private Gateway bzw. ein Transit-Gateway zwei VPN-Endpunkte (Tunnel) bereit, um 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 ermöglichen. Weitere Informationen finden Sie unter Sichere Kommunikation zwischen Standorten über VPN CloudHub im AWS Site-to-Site VPN-Benutzerhandbuch.

VPN-Konnektivitäts option	Beschreibung
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 ausgeführt 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-Communities angeboten werden, wählen. Hier finden Sie softwarebasierte VPN-Appliances von Drittanbietern AWS Marketplace .

Zudem können mit 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 Direct Connect?](#) im Direct Connect-Benutzerhandbuch.

Verbinden von VPCs mit VPC-Peering

Eine VPC-Peering-Verbindung ist eine Netzwerkfunktion, die eine sichere und direkte Kommunikation zwischen zwei Virtual Private Clouds (VPCs) innerhalb der AWS-Infrastruktur ermöglicht. Diese private Verbindung ermöglicht es den Ressourcen in den Peering-VPCs, miteinander zu interagieren, als ob sie Teil desselben Netzwerks wären. Eine Übertragung über das öffentliche Internet ist dann nicht mehr notwendig.



Beim Erstellen einer VPC-Peering-Verbindung wird die vorhandene VPC-Infrastruktur genutzt, um diese Verbindung herzustellen, ohne dass ein Gateway, AWS Site-to-Site VPN oder zusätzliche physische Hardware erforderlich ist. Dieses Design stellt sicher, dass es keine einzelne Fehlerquelle oder Engpässe bei der Bandbreite gibt.

Einer der Hauptvorteile einer VPC-Peering-Verbindung ist die Möglichkeit, VPCs über verschiedene AWS-Konten oder sogar verschiedene AWS-Regionen hinweg zu verbinden. Diese Flexibilität ermöglicht es Unternehmen, ihre Cloud-Ressourcen nahtlos zu integrieren, unabhängig davon, ob sie sich innerhalb desselben Kontos befinden oder auf mehrere Konten und geografische Standorte verteilt sind. Der private Charakter der Verbindung stellt außerdem sicher, dass der gesamte Datenverkehr zwischen den miteinander verbundenen VPCs innerhalb des AWS-Netzwerks verbleibt, ohne jemals das öffentliche Internet zu durchlaufen.

Die Anwendungsfälle für VPC-Peering-Verbindungen sind breit gefächert. Organisationen können diese Funktion nutzen, um eine sichere Kommunikation zwischen verschiedenen Ebenen einer Anwendung (beispielsweise Webservern und Datenbankservern) zu ermöglichen, die gemeinsame Nutzung von Ressourcen zwischen mehreren Teams oder Geschäftseinheiten zu erleichtern oder sogar Hybrid-Cloud-Architekturen zu errichten, indem sie On-Premises-Netzwerke mit ihren AWS-VPCs verbinden.

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.

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

Sie können VPC Flow Logs verwenden, um detaillierte Informationen über den Datenverkehr zu und von Netzwerkschnittstellen in Ihren VPCs zu erfassen.

Amazon CloudWatch Internetmonitor

Sie können Internet Monitor verwenden, um zu sehen, wie sich Internetprobleme auf die Leistung und Verfügbarkeit zwischen Ihren gehosteten Anwendungen AWS und Ihren Endbenutzern auswirken. Sie können auch nahezu in Echtzeit untersuchen, wie Sie die erwartete Latenz Ihrer Anwendung verbessern können, indem Sie auf andere Dienste umsteigen oder den Datenverkehr über andere AWS-Regionen Dienste auf Ihren Workload umleiten. Weitere Informationen finden Sie unter [Amazon CloudWatch Internet Monitor verwenden](#).

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

Sie können diese Funktion verwenden, um Netzwerkverkehr von einer Netzwerkschnittstelle einer EC2 Amazon-Instance zu kopieren und ihn zur Deep Packet Inspection an out-of-band Sicherheits- und Überwachungs-Appliances zu 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. Nachdem Sie die Quell- und Zielressourcen angegeben haben, erstellt Reachability Analyzer hop-by-hop Details zum virtuellen Pfad zwischen ihnen, wenn sie erreichbar sind, und identifiziert die blockierende Komponente, wenn 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 Logs

AWS CloudTrail protokolliert API-Aufrufe für Amazon VPC, wie zum Beispiel:

- Welche API-Aufrufe getätigt wurden (z. B. Aktionen wie das Erstellen oder Ändern von VPC-Ressourcen)
- Die Quell-IP-Adresse des Aufrufs
- Wer den Aufruf gemacht hat
- Wann der Anruf getätigt wurde

Separate Protokolle werden für CreateVpc-, DeleteVpc- und CreateDefaultVpc-Aktionen erstellt. Diese Protokolle enthalten auch die Standardressourcen (wie alle Standard-Internet-Gateways oder Standardsicherheitsgruppen), die erstellt und mit der VPC verbunden wurden.

Weitere Informationen finden Sie unter [Protokollieren von EC2 Amazon-API-Aufrufen AWS CloudTrail](#) im EC2 Amazon-Benutzerhandbuch.

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. Der konfigurierte Lieferpfad und die Berechtigungen, die das Senden von Netzwerkdatenverkehrsprotokollen an ein Ziel wie CloudWatch Logs oder S3 ermöglichen, werden als Abonnements bezeichnet. 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 des Netzwerkverkehrs mithilfe von Flow-Protokollen für Transit-Gateway](#) im Benutzerhandbuch zu Amazon VPC Transit Gateways.

Inhalt

- [Grundlagen zu Flow-Protokollen](#)
- [Flow-Protokolldatensätze](#)
- [Beispiele für Flow-Protokolldatensätze](#)
- [Einschränkungen von Flow-Protokollen](#)
- [Preisgestaltung](#)
- [Arbeiten mit Flow-Protokollen](#)
- [Veröffentlichen Sie Flow-Logs in CloudWatch Logs](#)
- [Veröffentlichen von Flow-Protokollen auf Amazon S3](#)
- [Veröffentlichen von Flow-Protokollen in Amazon Data Firehose](#)
- [Abfragen von Flow-Protokollen mit Amazon Athena](#)
- [Fehlerbehebung bei VPC Flow Logs](#)

Grundlagen zu Flow-Protokollen

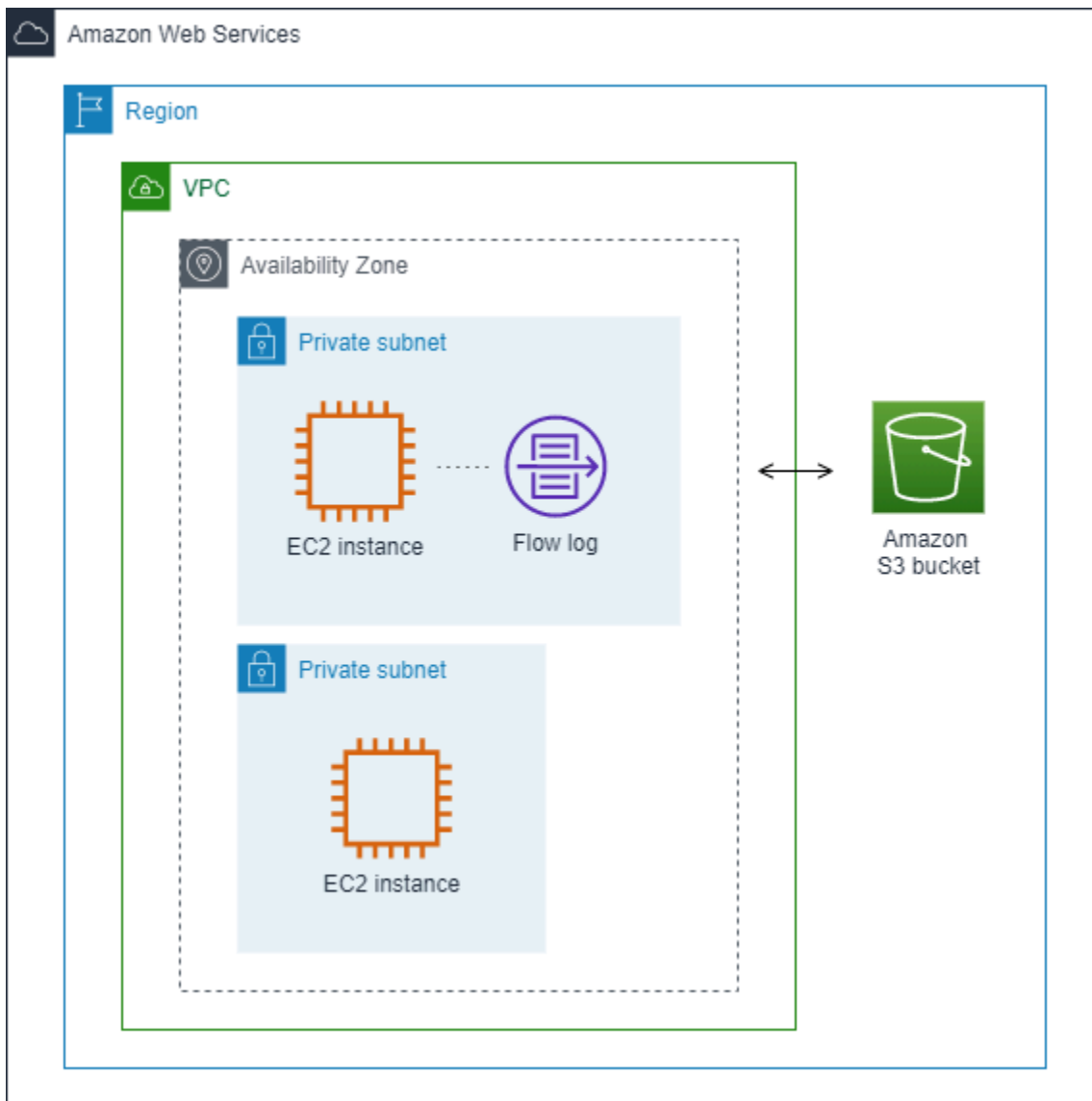
Sie können Flow-Protokolle für VPCs, Subnetze oder Netzwerkschnittstellen erstellen. Wenn Sie ein Flow-Protokoll für ein Subnetz oder eine VPC erstellen, werden alle Netzwerkschnittstellen innerhalb dieses Subnetzes oder der VPC überwacht.

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](#).

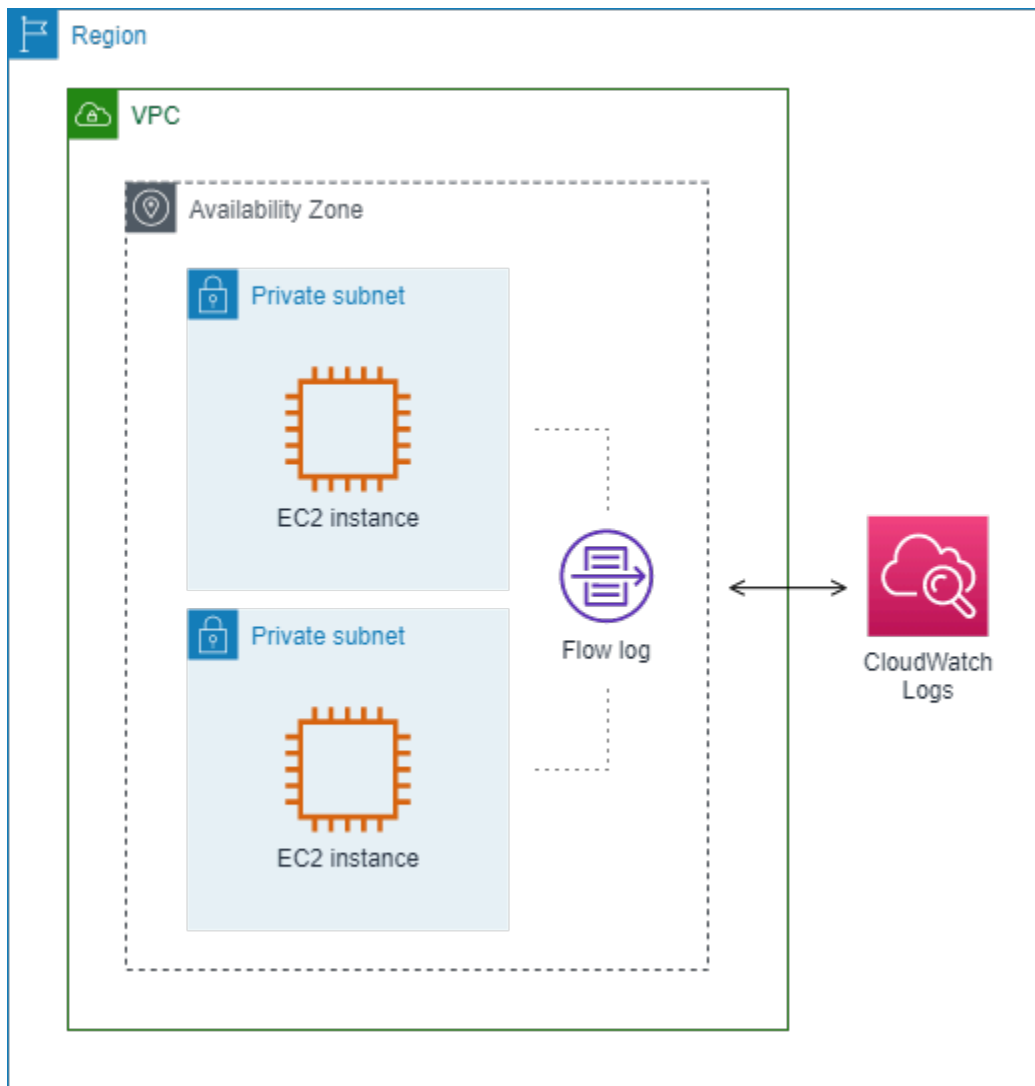
Für die Erstellung eines Flow-Protokolls geben Sie Folgendes an:

- 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 für eine der EC2 Instances in einem privaten Subnetz erfasst und die Flow-Protokolldatensätze in einem Amazon S3 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 [2. 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.:

- ELB

- Amazon RDS
- Amazon ElastiCache
- Amazon Redshift
- Amazon WorkSpaces
- NAT-Gateways
- Transit Gateways

Unabhängig von der Art der Netzwerkschnittstelle müssen Sie die EC2 Amazon-Konsole oder die EC2 Amazon-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 [4. 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

- [Aggregationsintervall](#)

- [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. Gibt ein „-“-Symbol für Datenflüsse zurück, die mit einem regionalen NAT-Gateway verknüpft sind.	2

Feld	Beschreibung	Version
	Parquet-Datentyp: STRING	
srcaddr	Für eingehenden Datenverkehr ist das die IP-Adresse der Datenverkehrsquelle. Für ausgehenden Verkehr ist dies die private IPv4 Adresse oder die IPv6 Adresse der Netzwerkschnittstelle, die den Verkehr sendet. Für ausgehenden Datenverkehr vom regionalen NAT-Gateway ist dies dieselbe Quell-IP-Adresse auf Paketebene wie in. pkt-srcaddr Siehe auch pkt-srcaddr. Parquet-Datentyp: SCHNUR	2
dstaddr	Die Zieladresse für ausgehenden Verkehr IPv4 oder die IPv6 Oder-Adresse der Netzwerkschnittstelle für eingehenden Verkehr auf der Netzwerkschnittstelle. Die IPv4 Adresse der Netzwerkschnittstelle ist immer ihre private IPv4 Adresse. Für eingehenden Datenverkehr zum regionalen NAT-Gateway ist dies dieselbe Ziel-IP-Adresse auf Paketebene wie in. pkt-dstaddr Siehe auch 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

Feld	Beschreibung	Version
bytes	Die Anzahl der Bytes, die während des Flows übertragen wurden Parquet-Datentyp: INT_64	2
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 Netzwerkschnittstelle 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 Netzwerkschnittstelle 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 dem Netzwerk nicht zugelassen ACLs, oder Pakete kamen an, nachdem die Verbindung geschlossen wurde. Parquet-Datentyp: STRING	2

Feld	Beschreibung	Version
log-status	Der Protokollstatus des Flow-Protokolls: • OK – Daten werden normal auf den ausgewählten Zielen protokolliert. • 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. Während des Aggregationsintervalls werden einige Flow-Protokolldatensätze möglicherweise übersprungen (siehe log-status in Verfügbare Felder). Dies kann durch eine interne AWS Kapazitätsbeschränkung oder einen internen Fehler verursacht werden. Wenn Sie VPC-Flow-Log-Gebühren anzeigen und einige Flow-Logs während des Flow-Log-Aggregationsintervalls übersprungen AWS Cost Explorer werden, ist die Anzahl der gemeldeten Flow-Logs höher als die Anzahl der von Amazon VPC veröffentlichten Flow-Logs. AWS Cost Explorer Parquet-Datentyp: STRING	2
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. Gibt ein „-“ -Symbol für Flows zurück, die mit dem regionalen NAT-Gateway verknüpft sind. Parquet-Datentyp: STRING	3

Feld	Beschreibung	Version
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 unterstütztes Flag ist und ECE nicht. Wenn die Flag-Kombination aus irgendeinem Grund ungültig ist und der Wert nicht berechnet werden kann, ist 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

Feld	Beschreibung	Version
pkt-src-aws-service	Der Name der Teilmenge von IP-Adressbereichen für das Feld pkt-srcaddr, wenn die Ziel-IP-Adresse für einen AWS -Service ist. Wenn die Quell-IP-Adresse zu einem überlappenden Bereich gehört, pkt-src-aws-service wird nur einer der AWS Dienstcod es angezeigt. Die möglichen Werte sind: AMAZON AMAZON_APPFLOW AMAZON_CONNECT API_GATEWAY AURORA_DS QL CHIME_MEETINGS CHIME_VOICECONNECTOR CLOUD9 CLOUDFRONT CLOUDFRONT_ORIGIN_FACING CODEBUILD DYNAMODB EBS EC2 EC2_INSTANCE_CONNECT GLOBALACCELERATOR IVS_LOW_LATENCY IVS_REALTIME KINESIS_VIDEO_STREAMS MEDIA_PACKAGE_V2 ROUTE53 ROUTE53_HEALTHCHECKS ROUTE53_HEALTHCHECKS_PUBLISHING ROUTE53_RESOLVER S3 WORKSPACES_GATEWAYS Parquet-Datentyp: SCHNUR	5
pkt-dst-aws-service	Der Name der Teilmenge der IP-Adressbereiche für das pkt-dstaddr Feld, wenn die Ziel-IP-Adresse für einen AWS Dienst bestimmt ist. 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

Feld	Beschreibung	Version
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 einer AWS verwalteten Netzwerkschnittstelle oder eines lokalen Outpost-Gateways • 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 eine Local Zone oder eine Wavelength Zone • 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
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-cluster-name	Name des ECS-Clusters, wenn der Datenverkehr von einer ausgeführten ECS-Aufgabe stammt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: aufzurufenListClusters. Parquet-Datentyp: STRING	7

Feld	Beschreibung	Version
ecs-container-instance-arn	ARN der ECS-Container-Instance, wenn der Datenverkehr von einer laufenden ECS-Task auf einer EC2 Instance stammt. Wenn der Kapazitätsanbieter AWS Fargate ist, wird für dieses Feld „-“ angezeigt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters und ecs: aufzurufenListContainerInstances. 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 der Kapazitätsanbieter AWS Fargate ist, wird für dieses Feld „-“ angezeigt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters und ecs: aufzurufenListContainerInstances. Parquet-Datentyp: STRING	7
ecs-container-id	Docker-Laufzeit-ID des Containers, wenn der Datenverkehr von einer ausgeführten ECS-Aufgabe 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: aufzurufenListClusters. Parquet-Datentyp: STRING	7
ecs-second-container-id	Docker-Laufzeit-ID des Containers, wenn der Datenverkehr von einer ausgeführten ECS-Aufgabe stammt. Wenn die ECS-Aufgabe mehr als einen Container enthält, ist dies die Docker-Laufzeit-ID des zweiten Containers. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: aufzurufenListClusters. Parquet-Datentyp: STRING	7

Feld	Beschreibung	Version
ecs-service-name	Name des ECS-Service, wenn der Datenverkehr von einer ausgeführten ECS-Aufgabe stammt und die ECS-Aufgabe von einem ECS-Service gestartet wurde. Wenn die ECS-Aufgabe nicht von einem ECS-Service gestartet wurde, wird in diesem Feld „-“ angezeigt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters und ecs: aufzurufenListServices. Parquet-Datentyp: STRING	7
ecs-task-definition-arn	ARN der ECS-Aufgabendefinition, wenn der Datenverkehr von einer ausgeführten ECS-Aufgabe 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-Aufgabe, wenn der Datenverkehr von einer ausgeführten ECS-Aufgabe 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-Aufgabe, wenn der Datenverkehr von einer ausgeführten ECS-Aufgabe stammt. Um dieses Feld in Ihr Abonnement aufzunehmen, benötigen Sie die Erlaubnis, ecs: ListClusters und ecs: aufzurufenListTasks. Parquet-Datentyp: STRING	7

Feld	Beschreibung	Version
reject-reason	Der Grund, warum der Datenverkehr abgelehnt wurde. Mögliche Werte: BPA, EC. Gibt für jeden anderen Ablehnungsgrund ein „-“ zurück. • BPA — Weitere Informationen zu VPC Block Public Access (BPA) finden Sie unter Sperren Sie den öffentlichen Zugriff VPCs auf Subnetze • EC — Der Flow wird von VPC Endpoint aufgrund von Verschlüsselungskontrollen abgelehnt. Weitere Informationen zu VPC Encryption Controls finden Sie unter VPC-Verschlüsselung bei der Übertragung erzwingen. Parquet-Datentyp: STRING	8
resource-id	Die ID des regionalen NAT-Gateways, das die Netzwerkschnittstelle enthält, für die der Verkehr aufgezeichnet wird. Gibt ein „-“ -Symbol für Verkehrsflüsse zurück, die nicht mit einem regionalen NAT-Gateway verknüpft sind. Weitere Informationen zu regionalen NAT-Gateways finden Sie unter Regionale NAT-Gateways für automatische Multi-AZ-Erweiterung. Parquet-Datentyp: STRING	9

Feld	Beschreibung	Version
Verschlüsselungsstatus	Verschlüsselungsstatus des Datenflusses. Weitere Informationen zu VPC Encryption Controls finden Sie unter VPC-Verschlüsselung bei der Übertragung erzwingen. Die möglichen Werte sind: • 0 — nicht verschlüsselt. • 1 — Nitro-verschlüsselt. Es wird von der Nitro-Systemhardware verschlüsselt. • 2 — anwendungsverschlüsselt. Nur die folgenden Dateien gelten als anwendungsverschlüsselt: • fließt über den TCP-Port 443 für die Schnittstelle vom Endpunkt zum Service* AWS • fließt auf dem TCP-Port 443 für den Gateway-Endpunkt* • fließt über VPC-Endpunkt** zum verschlüsselten Redshift-Cluster • 3 — Nitro-verschlüsselt und anwendungsverschlüsselt. Der Wert ist '-', wenn VPC Encryption Controls nicht aktiviert ist oder wenn der Status FlowLog nicht abgerufen werden kann.  Note * Bei Schnittstellen- und Gateway-Endpunkten werden bei der Bestimmung des Verschlüsselungsstatus AWS nicht die Paketdaten berücksichtigt, sondern wir verlassen uns stattdessen auf den Port, der zur Annahme des Verschlüsselungsstatus verwendet wird. ** AWS Ermittelt den Verschlüsselungsstatus für bestimmte AWS verwaltete Endpunkte auf der Grundlage der TLS-Anforderung in der Dienstkonfiguration. Parquet-Datentyp: INT_32	10

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](#)
- [Keine Daten und übersprungene Datensätze](#)
- [Sicherheitsgruppen- und Netzwerk-ACL-Regeln](#)
- [IPv6 Verkehr](#)
- [TCP-Flag-Sequenz](#)
- [Verkehr über ein zonales NAT-Gateway](#)
- [Verkehr über ein regionales NAT-Gateway](#)
- [Datenverkehr durch ein Transit-Gateway](#)
- [Servicename, Verkehrspfad und Flow-Richtung](#)

Zulässiger und abgelehnter Datenverkehr

Im Folgenden finden Sie Beispiele für Standard-Flow-Protokolldatensätze.

In diesem Beispiel wurde der SSH-Datenverkehr (Zielport 22, TCP-Protokoll) von der IP-Adresse 172.31.16.139 zur Netzwerkschnittstelle mit der privaten IP-Adresse 172.31.16.21 und der ID eni-1235b8ca123456789 im Konto 123456789010 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
```

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-11111111aaaaaaaa - - - - - 1431280876 1431280934 - SKIPDATA
```

Note

Während des Aggregationsintervalls werden einige Flow-Protokolldatensätze möglicherweise übersprungen (siehe log-status in [Verfügbare Felder](#)). Dies kann durch eine interne AWS Kapazitätsbeschränkung oder einen internen Fehler verursacht werden. Wenn Sie VPC-Flow-Log-Gebühren anzeigen und einige Flow-Logs während des Flow-Log-Aggregationsintervalls übersprungen AWS Cost Explorer werden, ist die Anzahl der gemeldeten Flow-Logs höher als die Anzahl der von Amazon VPC veröffentlichten Flow-Logs. AWS Cost Explorer

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. Umgekehrt ACLs sind Netzwerke zustandslos, weshalb Antworten auf erlaubten Datenverkehr den Netzwerk-ACL-Regeln unterliegen.

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 Netzwerke zustandslos ACLs sind, wird der Antwort-Ping gelöscht und erreicht Ihren Heimcomputer nicht. 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 Verkehr

Der folgende Code ist ein Beispiel für einen Standard-Flow-Protokolldatensatz. Im Beispiel war SSH-Verkehr (Port 22) von der IPv6 Adresse 2001:db8:1234:a100:8d6e:3477:df66:f105 zur Netzwerkschnittstelle eni-1235b8ca123456789 im 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 second-to-last in diesem Abschnitt wird durch den Wert im 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 Server hat ein FIN-Flag (1) für die Verbindung auf Port 43418 an den Client gesendet. Der Client hat mit einem FIN an den Server auf Port 43418 geantwortet.

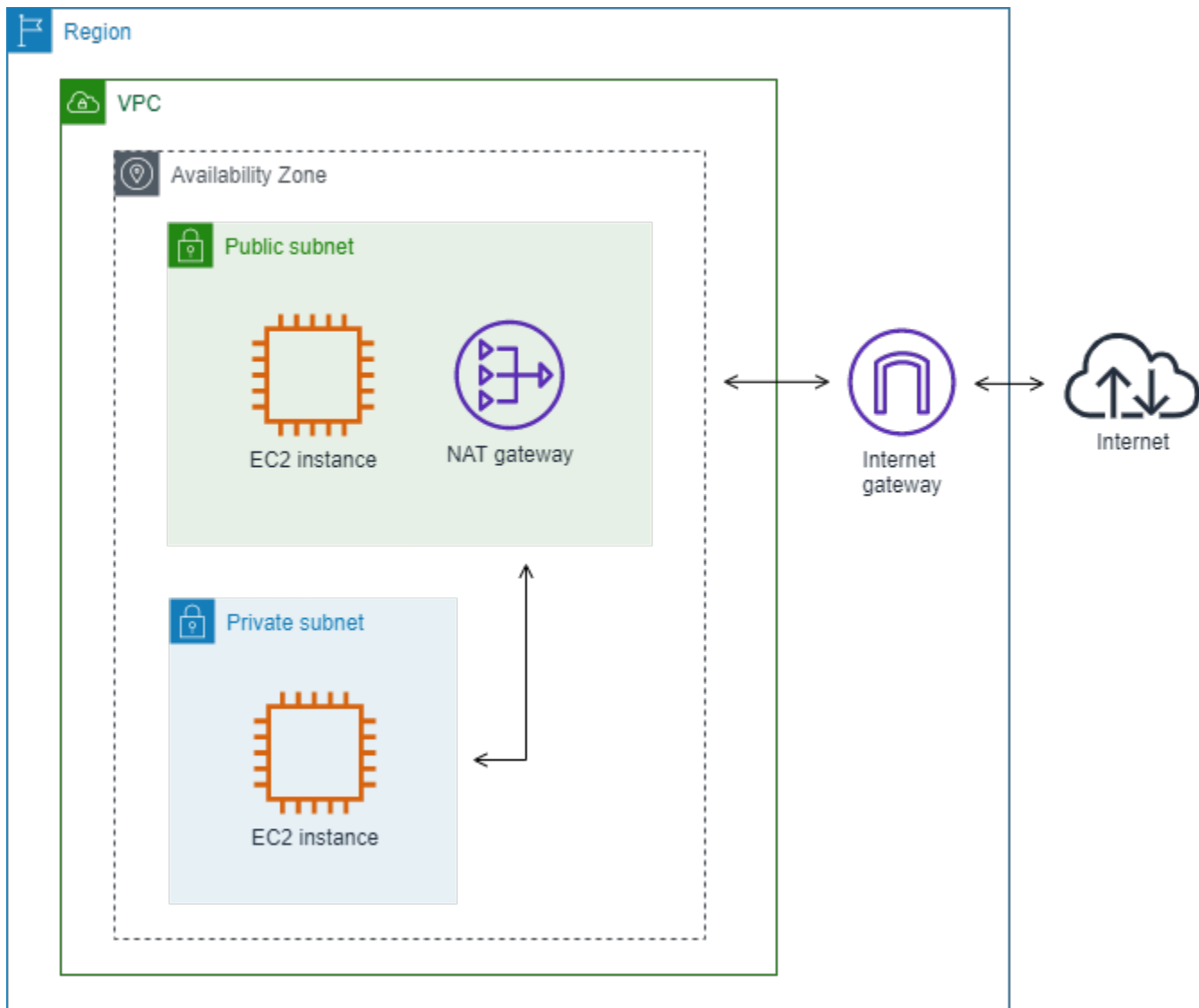
```
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
  eni-1235b8ca123456789 123456789010 IPv4 10.0.0.62 52.213.180.42 5001 43418 10.0.0.62
  52.213.180.42 6 63388 1219 1566848933 1566849113 ACCEPT 1 OK
3 vpc-abcdefab012345678 subnet-aaaaaaaa012345678 i-01234567890123456
  eni-1235b8ca123456789 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
```

Verkehr über ein zonales NAT-Gateway

In diesem Beispiel greift eine Instance in einem privaten Subnetz über ein zonales NAT-Gateway, das sich in einem öffentlichen Subnetz befindet, auf das Internet zu.



Das folgende benutzerdefinierte Flussprotokoll für die zonale NAT-Gateway-Netzwerkschnittstelle erfasst die folgenden Felder in der folgenden Reihenfolge.

```
instance-id interface-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Das Flussprotokoll zeigt den Datenfluss von der Instanz-IP-Adresse (10.0.1.5) über die zonale NAT-Gateway-Netzwerkschnittstelle zu einem Host im Internet (203.0.113.5). Bei der Netzwerkschnittstelle des zonalen NAT-Gateways handelt es sich um eine vom Anforderer verwaltete Netzwerkschnittstelle. Daher wird im Flow-Log-Datensatz ein „-“ -Symbol für das Feld angezeigt.

instance-id Die folgende Zeile zeigt den Verkehr von der Quell-Instanz zur Netzwerkschnittstelle des zonalen NAT-Gateways. Die Werte für die Felder dstaddr und pkt-dstaddr unterscheiden sich. In dem

dstaddr Feld wird die private IP-Adresse der zonalen NAT-Gateway-Netzwerkschnittstelle angezeigt, und in dem pkt-dstaddr Feld wird die endgültige Ziel-IP-Adresse des Hosts im Internet angezeigt.

```
- eni-1235b8ca123456789 10.0.1.5 10.0.0.220 10.0.1.5 203.0.113.5
```

Die nächsten beiden Zeilen zeigen den Verkehr von der zonalen NAT-Gateway-Netzwerkschnittstelle zum Zielhost im Internet und den Antwortverkehr vom Host zur NAT-Gateway-Netzwerkschnittstelle.

```
- 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 Antwortverkehr von der Netzwerkschnittstelle des zonalen NAT-Gateways zur Quell-Instance. Die Werte für die Felder srcaddr und pkt-srcaddr unterscheiden sich. Das srcaddr Feld zeigt die private IP-Adresse der zonalen NAT-Gateway-Netzwerkschnittstelle an, und das pkt-srcaddr Feld zeigt die IP-Adresse des Hosts im Internet an.

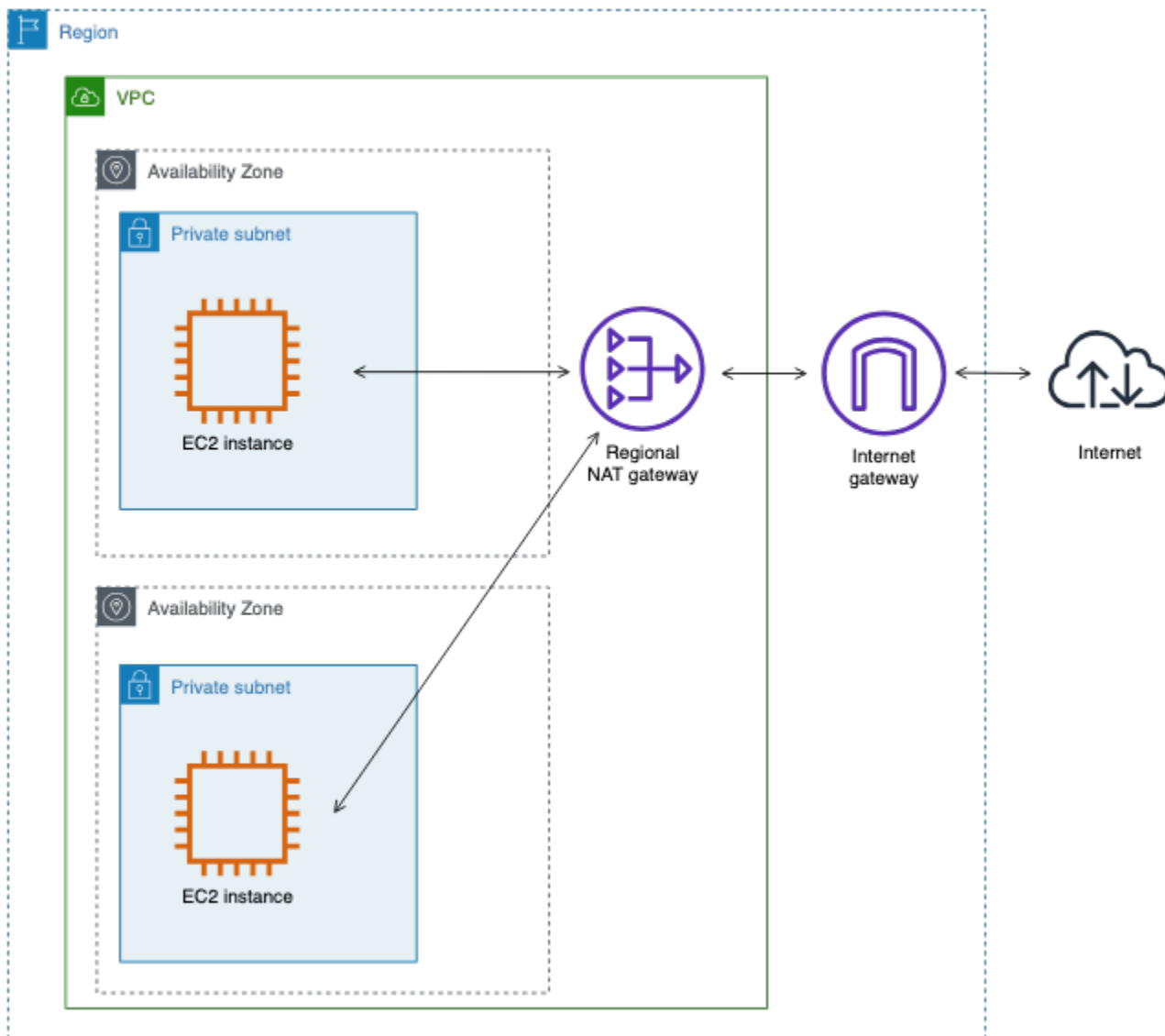
```
- eni-1235b8ca123456789 10.0.0.220 10.0.1.5 203.0.113.5 10.0.1.5
```

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. Im Gegensatz zur Netzwerkschnittstelle für das zonale NAT-Gateway ist diese Netzwerkschnittstelle keine zwischengeschaltete Netzwerkschnittstelle für den 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
```

Verkehr über ein regionales NAT-Gateway

Ein regionales NAT-Gateway kann eine Verbindung zu mehreren Subnetzen in verschiedenen Availability Zones herstellen. In diesem Beispiel greifen zwei Instances in privaten Subnetzen aus zwei verschiedenen Availability Zones über dasselbe regionale NAT-Gateway auf das Internet zu. Die folgenden Flussprotokolle zeigen den Datenverkehr von einer der Instances zum Internet über das regionale NAT-Gateway.



Das folgende benutzerdefinierte Flussprotokoll für das regionale NAT-Gateway erfasst die folgenden Felder in der folgenden Reihenfolge.

```
resource-id instance-id interface-id subnet-id srcaddr dstaddr pkt-srcaddr pkt-dstaddr
```

Das Flussprotokoll zeigt den Verkehrsfluss von der Instanz-IP-Adresse (10.0.1.5) über das regionale NAT-Gateway zu einem Host im Internet (203.0.113.5). instance-id, interface-id, und subnet-id gelten nicht für das regionale NAT-Gateway. Daher wird im Flow-Protokoll Datensatz für diese Felder ein „-“ -Symbol angezeigt. Stattdessen zeigt das resource-id Feld die ID des regionalen NAT-Gateways an. In den pkt-dstaddr Feldern dstaddr und wird die endgültige Ziel-IP-Adresse des Hosts im Internet angezeigt.

```
nat-1234567890abcdef - - - 10.0.1.5 203.0.113.5 10.0.1.5 203.0.113.5
```

Die nächsten beiden Zeilen zeigen den Verkehr vom regionalen NAT-Gateway (öffentliche IP-Adresse 107.22.182.139) zum Zielhost im Internet und den Antwortverkehr vom Host zum regionalen NAT-Gateway.

```
nat-1234567890abcdef - - - 107.22.182.139 203.0.113.5 107.22.182.139 203.0.113.5
nat-1234567890abcdef - - - 203.0.113.5 107.22.182.139 203.0.113.5 107.22.182.139
```

Die folgende Zeile zeigt den Antwortverkehr vom regionalen NAT-Gateway zur Quell-Instance. In den pkt-srcaddr Feldern srcaddr und wird die IP-Adresse des Hosts im Internet angezeigt.

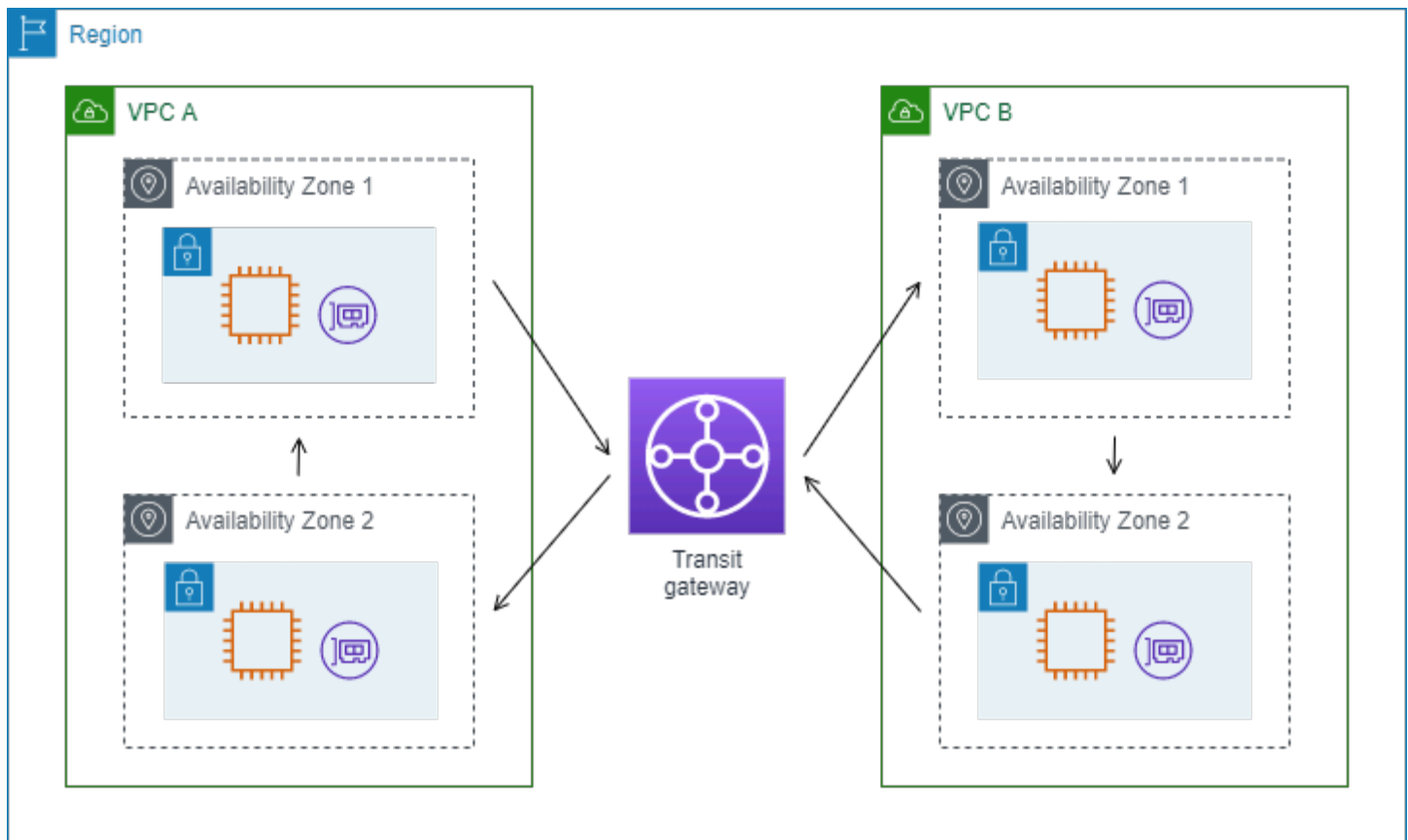
```
nat-1234567890abcdef - - - 203.0.113.5 10.0.1.5 203.0.113.5 10.0.1.5
```

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 instance-id Feld die ID der Instanz zurück, die der Netzwerkschnittstelle zugeordnet resource-id ist, und zwar '-'. Es gibt keinen Unterschied zwischen den pkt-dstaddr Feldern dstaddr und srcaddr und pkt-srcaddr.

```
- i-01234567890123456 eni-1111aaaa2222bbbb3 subnet-aaaaaaaa012345678 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 subnet-aaaaaaaa012345678 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-1111111111111111) und verlässt VPC B über eine andere (z. B. eni-2222222222222222).



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-3333333333333333 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-3333333333333333 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-1111111111111111, einer vom Anforderer verwalteten Netzwerkschnittstelle für das Transit-Gateway in Subnetz

subnet-11111111aaaaaaaa. 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-1111111111111111 123456789010 vpc-abcdefab012345678 subnet-11111111aaaaaaaa -
  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-2222222222222222, einer vom Anforderer verwalteten Netzwerkschnittstelle für das Transit-Gateway in Subnetz subnet-22222222bbbbbbbbbb 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-2222222222222222 123456789010 vpc-abcdefab012345678 subnet-22222222bbbbbbbbbb -
  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 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:

- Nachdem Sie ein Flow-Protokoll erstellt haben, werden die Flow-Protokolldaten erst dann angezeigt, wenn für die ausgewählte Netzwerkschnittstelle, das Subnetz oder die VPC aktiver Datenverkehr stattfindet.
- Sie können nur dann Flow-Logs aktivieren VPCs, wenn sich die Peer-VPC in Ihrem Konto befindet.
- 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.
- Wenn Ihre Netzwerkschnittstelle mehrere IPv4 Adressen hat und der Datenverkehr an eine sekundäre private IPv4 Adresse gesendet wird, zeigt das Flow-Protokoll die primäre private IPv4 Adresse in dem Feld `dstaddr` an. Erstellen Sie ein Flow-Protokoll mit dem Feld `pkt-dstaddr`, um die ursprüngliche Ziel-IP-Adresse zu erfassen.
- Wenn der Datenverkehr an eine Netzwerkschnittstelle gesendet wird und das Ziel keine der IP-Adressen der Netzwerkschnittstelle ist, zeigt das Flussprotokoll die primäre private IPv4 Adresse in dem `dstaddr` Feld an. Erstellen Sie ein Flow-Protokoll mit dem Feld `pkt-dstaddr`, um die ursprüngliche Ziel-IP-Adresse zu erfassen.
- Wenn der Datenverkehr von einer Netzwerkschnittstelle gesendet wird und es sich bei der Quelle nicht um eine der IP-Adressen der Netzwerkschnittstelle handelt, zeigt das Flow-Protokoll die primäre private IPv4 Adresse im `srcaddr` Feld an, wenn sich der Protokolleintrag auf einen Ausgangsfluss bezieht. Erstellen Sie ein Flow-Protokoll mit dem Feld `pkt-srcaddr`, um die ursprüngliche Quell-IP-Adresse zu erfassen. Wenn sich der Protokolleintrag auf einen eingehenden Datenfluss in die Netzwerkschnittstelle bezieht, wird die primäre private IP der Netzwerkschnittstelle nicht im Feld `srcaddr` angezeigt.
- Wenn Ihre Netzwerkschnittstelle einer [Nitro-basierten Instance](#) zugewiesen ist, beträgt das Aggregationsintervall immer 1 Minute oder weniger, unabhängig vom angegebenen maximalen Aggregationsintervall.

- Bei den Feldern `pkt-srcaddr` und `pkt-dstaddr` wird für dieses Feld möglicherweise die erhaltene Client-IP-Adresse anstelle der IP-Adresse der Zwischenebene angezeigt, wenn auf der Zwischenebene die Erhaltung der Client-IP-Adresse aktiviert ist.
- Für das Feld `traffic-path` ist der Wert für Flows durch Ressourcen in derselben VPC und Flows, die über ein lokales Outpost-Gateway laufen, derselbe.
- Während des Aggregationsintervalls werden einige Flow-Protokolldatensätze möglicherweise übersprungen (siehe `log-status` in [Verfügbare Felder](#)). Dies kann durch eine interne AWS Kapazitätsbeschränkung oder einen internen Fehler verursacht werden. Wenn Sie VPC-Flow-Log-Gebühren anzeigen und einige Flow-Logs während des Flow-Log-Aggregationsintervalls übersprungen AWS Cost Explorer werden, ist die Anzahl der gemeldeten Flow-Logs höher als die Anzahl der von Amazon VPC veröffentlichten Flow-Logs. AWS Cost Explorer
- Wenn Sie [VPC Block Public Access \(BPA\)](#) verwenden:
 - Flow-Protokolle für VPC BPA enthalten keine [übersprungenen Datensätze](#).
 - `bytes` sind nicht in Flow-Protokollen für VPC BPA enthalten, auch wenn Sie das Feld `bytes` in Ihr Flow-Protokoll aufnehmen.

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
- Der [Datenverkehr spiegelt](#) den Quellverkehr wider. Sie sehen nur den gespiegelten Zieldatenverkehr.
- Datenverkehr zur reservierten IP-Adresse des Standard-VPC-Routers.
- Datenverkehr zwischen einer Endpunkt-Netzwerkschnittstelle und einer Network Load Balancer-Netzwerkschnittstelle.
- ARP-Datenverkehr (Address Resolution Protocol).
- Datenverkehr auf einem kurzlebigen regionalen NAT-Gateway, der einige Minuten nach der Erstellung gelöscht wird.

Spezifische Einschränkungen für ECS-Felder, die in Version 7 verfügbar sind:

- ECS-Felder werden nicht berechnet, wenn die zugrunde liegenden ECS-Aufgaben nicht dem Eigentümer des Flow-Protokollabonnements gehören. Wenn Sie beispielsweise ein Subnetz (SubnetA) für ein anderes Konto (AccountB) freigeben und dann ein Flow-Protokollabonnement für SubnetA erstellen, wenn AccountB im freigegebenen Subnetz ECS-Aufgaben startet, erhält Ihr Abonnement Datenverkehrsprotokolle von ECS-Aufgaben, die von AccountB gestartet wurden. Die ECS-Felder für diese Protokolle werden aus Sicherheitsgründen jedoch nicht berechnet.
- Wenn Sie Flow-Log-Abonnements mit ECS-Feldern auf VPC/Subnet 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-Datenverkehr. Sie haben beispielsweise ein Subnetz (subnet-000000) und erstellen für dieses Subnetz ein Flow-Protokollabonnement mit ECS-Feldern (f1-00000000). subnet-000000In starten Sie eine EC2 Instance (i-00000000), die mit dem Internet verbunden ist und aktiv IP-Verkehr generiert. Sie starten auch eine ausgeführte ECS-Aufgabe (ECS-Task-1) im selben Subnetz. Da sowohl i-00000000 als auch ECS-Task-1 IP-Datenverkehr generieren, liefert Ihr Flow-Protokollabonnement f1-00000000 Datenverkehrsprotokolle für beide Entitäten. Allerdings enthält nur ECS-Task-1 die tatsächlichen ECS-Metadaten für die ECS-Felder, die Sie in Ihr logFormat aufgenommen haben. Für Datenverkehr in Bezug auf i-00000000 haben diese Felder den Wert „-“.
- ecs-container-id und ecs-second-container-id sind in der Reihenfolge angeordnet, in der der VPC-Flow-Protokollservice sie aus dem ECS-Ereignis-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 ANGEHALTEN übergeht, während die Aufgabe noch ausgeführt wird, 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 von den Upstream-Abhängigkeiten erhalten haben. Nachdem Sie eine neue Aufgabe gestartet haben, beginnen wir mit der Berechnung Ihrer ECS-Felder, 1) wenn wir den IP-Datenverkehr für die zugrunde liegende Netzwerkschnittstelle erhalten und 2) wenn wir das ECS-Ereignis erhalten, das die Metadaten für Ihre ECS-Aufgabe enthält, um anzuzeigen, dass die Aufgabe jetzt ausgeführt wird. Nachdem Sie eine Aufgabe beendet haben, beenden wir die Berechnung Ihrer ECS-Felder, 1) wenn wir keinen IP-Datenverkehr mehr für die zugrunde liegende Netzwerkschnittstelle oder IP-Datenverkehr mit einer Verzögerung von mehr als einem Tag

erhalten 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 [Netzwerkmodus](#) aws-vpc gestartet wurden.

encryption-status Feldspezifische Einschränkungen:

- Der Verschlüsselungsstatus kann in einigen Datenströmen '-' (nicht verfügbar) sein, da einige Netzwerk-Appliances den Verschlüsselungsstatus nur begrenzt melden können. Benutzer können diese Datenflüsse bei der Analyse ignorieren.
- Wenn der Datenfluss im Überwachungsmodus als verschlüsselt angezeigt wird, bedeutet das nicht, dass der Datenfluss im Erzwingungsmodus zulässig ist. Umgekehrt.
 - Wenn ein Datenfluss im Überwachungsmodus verschlüsselt wird, ist er im Erzwingungsmodus möglicherweise nicht konform:
 - Wenn der Flow eine ENI beinhaltet, die von einem AWS Dienst erstellt wurde, muss der Service Encryption Controls unterstützen.
 - Wenn der Datenfluss VPC-Peering durchläuft, erzwingt die gepeerte VPC möglicherweise keine Verschlüsselungskontrollen.
 - Wenn ein Flow im Überwachungsmodus nicht verschlüsselt ist, ist er im Erzwingungsmodus möglicherweise trotzdem konform, vorausgesetzt, der Dienst, der sich auf den Flow bezieht, wird als Ausnahme hinzugefügt.

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
- [Markieren Ihrer Bereitstellungsstreams](#) im Entwicklerhandbuch für Amazon Data Firehose

Arbeiten mit Flow-Protokollen

Sie können mit Flow-Logs mithilfe von Konsolen für Amazon EC2 und Amazon VPC arbeiten.

Aufgaben

- [1. Kontrollieren der Nutzung von Flow-Protokollen mit IAM](#)
- [2. Erstellen eines Flow-Protokolls](#)
- [3. Markieren eines Flow-Protokolls](#)
- [4. Löschen eines Flow-Protokolls](#)
- [Befehlszeilenübersicht](#)

1. Kontrollieren der Nutzung von Flow-Protokollen mit IAM

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.

JSON

```
{
  "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”](#).

2. Erstellen eines Flow-Protokolls

Sie können Flow-Logs 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 eines Flow-Protokolls, das in Amazon Data Firehose veröffentlicht”](#)

3. 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 EC2 Amazon-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 Ihr aus VPCs. Aktivieren Sie das Kontrollkästchen für die VPC.
- Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>. Wählen Sie im Navigationsbereich 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).

4. 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 EC2 Amazon-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 Ihr aus VPCs. Aktivieren Sie das Kontrollkästchen für die VPC.
 - Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>. Wählen Sie im Navigationsbereich 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.

Befehlszeilenübersicht

Sie können die auf dieser Seite beschriebenen Aufgaben über die Befehlszeile ausführen.

Erstellen eines Flow-Protokolls

- [create-flow-logs](#) (AWS CLI)

- [New-EC2FlowLog](#) (AWS Tools for Windows PowerShell)

Beschreiben eines Flow-Protokolls

- [describe-flow-logs](#) (AWS CLI)
- [Get-EC2FlowLog](#) (AWS Tools for Windows PowerShell)

Markieren eines Flow-Protokolls

- [create-tags](#) und [delete-tags](#) (AWS CLI)
- [New-EC2Tag](#) und [Remove-EC2Tag](#) (AWS Tools for Windows PowerShell)

Löschen eines Flow-Protokolls

- [delete-flow-logs](#) (AWS CLI)
- [Remove-EC2FlowLog](#) (AWS Tools for Windows PowerShell)

Veröffentlichen Sie Flow-Logs in CloudWatch Logs

Flow Logs können Flow-Protokolldaten direkt auf Amazon veröffentlichen CloudWatch. Amazon CloudWatch ist ein umfassender Überwachungs- und Beobachtbarkeitsservice. Es sammelt und verfolgt Metriken, Protokolle und Ereignisdaten aus verschiedenen AWS Ressourcen sowie aus Ihren eigenen Anwendungen und Diensten. CloudWatch bietet Einblicke in die Ressourcennutzung, die Anwendungsleistung und den Betriebszustand, sodass Sie systemweite Leistungsänderungen und potenzielle Probleme erkennen und darauf reagieren können. Mit CloudWatch können Sie Alarme einrichten, Protokolle und Metriken visualisieren und automatisch reagieren, um Ihre Cloud-Ressourcen zu sammeln und zu optimieren. Es ist ein unverzichtbares Tool, um die Zuverlässigkeit, Verfügbarkeit und Leistung Ihrer cloudbasierten Infrastruktur und Anwendungen sicherzustellen.

Bei der Veröffentlichung in CloudWatch Logs werden die 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](#)
- [Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch](#)
- [Zeigen Sie Flow-Protokolldatensätze mit CloudWatch Logs an](#)
- [Suche nach Flow-Protokoll-Datensätzen](#)
- [Protokolldatensätze für den Prozessablauf in CloudWatch Logs](#)

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:

JSON

```
{  
  "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.

JSON

```
{
  "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 unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Richtlinien.
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 und eine optionale Beschreibung sowie Tags für Ihre Richtlinie ein und wählen Sie dann Richtlinie erstellen aus.
5. Wählen Sie im Navigationsbereich Rollen aus.
6. Wählen Sie Create role (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.

Erstellen Sie ein Flow-Protokoll, das in Logs veröffentlicht wird CloudWatch

Sie können Flow-Logs 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.

Voraussetzung

Vergewissern Sie sich, dass der IAM-Prinzipal, den Sie für die Anfrage verwenden, über die Berechtigungen zum Aufrufen der Aktion `iam:PassRole` verfügt.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::111122223333:role/flow-log-role-name"
    }
  ]
}
```

So erstellen Sie ein Flow-Protokoll mithilfe der Konsole

1. Führen Sie eine der folgenden Aktionen aus:
 - Öffnen Sie die EC2 Amazon-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 Ihr aus VPCs. Aktivieren Sie das Kontrollkästchen für die VPC.
 - Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>. Wählen Sie im Navigationsbereich 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. Wenn Sie einen Namen eingeben, erstellen wir die Protokollgruppe, wenn Datenverkehr protokolliert werden muss.
 7. Wählen Sie für den Dienstzugriff eine bestehende [IAM-Servicerolle](#) aus, die berechtigt ist, Logs in CloudWatch Logs zu veröffentlichen, oder erstellen Sie eine neue Servicerolle.
 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-EC2FlowLog](#) (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
```

Zeigen Sie Flow-Protokolldatensätze mit CloudWatch Logs an

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)
- [CWLLogEreignis abrufen](#) (AWS Tools for Windows PowerShell)

Suche nach Flow-Protokoll-Datensätzen

Sie können Ihre Flow-Log-Datensätze, die in CloudWatch Logs veröffentlicht wurden, mithilfe der 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]
```

Protokolldatensätze für den Prozessablauf in CloudWatch Logs

Sie können Flow-Protokolldatensätze wie alle anderen von CloudWatch Logs erfassten Protokollereignisse verarbeiten. Weitere Informationen zur Überwachung von Protokolldaten und Metrikfiltern finden Sie unter [Metriken aus Protokollereignissen mithilfe von Filtern erstellen](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

Beispiel: Erstellen Sie einen CloudWatch Metrikfilter 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 (Alarmer) und All alarms (Alle Alarmer) 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.
- Denn 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 aus.

Veröffentlichen von Flow-Protokollen auf Amazon S3

Flow-Protokolle können Flow-Protokolldaten direkt in Amazon S3 veröffentlichen. Amazon S3 (Simple Storage Service) ist ein hochgradig skalierbarer und dauerhafter Objektspeicherservice. Er wurde entwickelt, um beliebige Datenmengen zu speichern und abzurufen, und zwar von jedem beliebigen Ort im Internet aus. S3 bietet branchenführende Haltbarkeit und Verfügbarkeit mit integrierten Features für die Versionsverwaltung von Daten, Verschlüsselung und Zugriffskontrolle.

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 S3.

Weitere Informationen zur Optimierung der Erfassung von VPC-Flow-Logs, der Flow-Log-Verarbeitung und der Flow-Log-Visualisierung finden Sie unter [Centralized Logging with OpenSearch](#) in der Lösungsbibliothek. AWS

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

- [Flow-Protokolldateien](#)
- [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 mit Amazon S3](#)

Flow-Protokolldateien

VPC-Flow-Protokolle sammeln Daten über den IP-Datenverkehr zu und von Ihrer VPC in Protokolldatensätzen, fassen diese Datensätze in Protokolldateien zusammen und veröffentlichen die Protokolldateien dann in 5-Minuten-Intervallen im Amazon-S3-Bucket. Es können mehrere Dateien veröffentlicht werden und jede Protokolldatei kann einige oder alle Flow-Protokolldatensätze für den in den letzten fünf Minuten aufgezeichneten IP-Datenverkehr enthalten.

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_f1-1234abcd_20180620T1620Z_fe123456.log.gz
```

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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012",
          "s3:x-amz-acl": "bucket-owner-full-control"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:logs:us-east-1:123456789012:*"
        }
      }
    }
  ]
}
```

```
]
}
```

Der ARN, für den Sie angeben, *my-s3-arn* 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 einer Einzelperson, sondern dem Prinzipal des Protokollzustellungsdienstes zu erteilen. AWS-Konto ARNs 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.

Beachten Sie, dass der Service zur Protokollbereitstellung die `HeadBucket`-Amazon-S3-API-Aktion aufruft, um die Existenz und den Speicherort des S3-Buckets zu überprüfen. Sie müssen dem Service zur Protokollbereitstellung nicht die Erlaubnis erteilen, diese Aktion aufzurufen. Der Service stellt trotzdem VPC-Flow-Protokolle bereit, auch wenn er nicht bestätigen kann, dass der S3-Bucket existiert und wo er sich befindet. In Ihren CloudTrail Protokollen wird jedoch ein `AccessDenied` Fehler `HeadBucket` beim Aufruf von auftreten.

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 von einem Flow-Protokoll erstellten 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 [Zugriffssteuerungslisten \(ACL\) – Übersicht](#) im Amazon-S3-Benutzerhandbuch.

Erstellen eines Flow-Protokolls, das in Amazon S3 veröffentlicht

Nachdem Sie Ihren Amazon S3 S3-Bucket erstellt und konfiguriert haben, können Sie Flow-Logs für Ihre Netzwerkschnittstellen, Subnetze und VPCs erstellen.

Voraussetzung

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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery"
      ]
    }
  ]
}
```

```
    ],  
    "Resource": "*"    
  }  
]  
}
```

So erstellen Sie ein Flow-Protokoll mithilfe der Konsole

1. Führen Sie eine der folgenden Aktionen aus:

- Öffnen Sie die EC2 Amazon-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 Ihr aus VPCs. Aktivieren Sie das Kontrollkästchen für die VPC.
- Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>. Wählen Sie im Navigationsbereich 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 akzeptierten Datenverkehr protokollieren.
- Ablehnen – Nur abgelehnten Datenverkehr protokollieren.
- 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 der Befehlszeile in Amazon S3 veröffentlicht

Verwenden Sie einen der folgenden Befehle:

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLog](#) (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 mit Amazon S3

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.

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.

So zeigen Sie in Amazon S3 veröffentlichte Flow-Protokolldatensätze an

1. Öffnen Sie die Amazon S3 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. Zum Beispiel `prefix//AWSLogsaccount_idregion/vpcflowlogs///. year month day`
4. Aktivieren Sie das Kontrollkästchen neben dem Dateinamen und wählen Sie dann Download (Herunterladen).

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 von Flow-Protokollen in Amazon Data Firehose

Flow-Protokolle können Flow-Protokolldaten direkt in Amazon Data Firehose veröffentlichen. Amazon Data Firehose ist ein vollständig verwalteter Service, der Datenströme in Echtzeit sammelt, transformiert und in verschiedene AWS Datenspeicher und Analysedienste überträgt. Er übernimmt die Datenerfassung in Ihrem Namen.

Wenn es um VPC-Flow-Protokolle geht, kann Firehose nützlich sein. VPC-Flow-Protokolle erfassen Informationen zum IP-Datenverkehr zu und von Netzwerkschnittstellen in Ihrer VPC. Diese Daten können für die Sicherheitsüberwachung, die Leistungsanalyse und die Einhaltung von Vorschriften entscheidend sein. Allerdings kann die Verwaltung der Speicherung und Verarbeitung dieses kontinuierlichen Stroms von Protokolldaten eine komplexe und ressourcenintensive Aufgabe sein.

Durch die Integration von Firehose in Ihre VPC-Flow-Protokolle können Sie diese Daten für Ihr bevorzugtes Ziel wie Amazon S3 oder Amazon Redshift bereitstellen. Firehose wird so skaliert, dass es die Erfassung, Transformation und Bereitstellung Ihrer VPC-Flow-Protokolle übernimmt und Sie von der operativen Last befreit. So können Sie sich auf die Analyse der Protokolle und die Ableitung von Erkenntnissen konzentrieren, anstatt sich Gedanken über die zugrunde liegende Infrastruktur machen zu müssen.

Darüber hinaus bietet Firehose Features wie Datentransformation, Komprimierung und Verschlüsselung, die die Effizienz und Sicherheit Ihrer Verarbeitungspipeline für VPC-Flow-Protokolle verbessern können. Die Verwendung von Firehose für VPC-Flow-Protokolle kann Ihre Datenverwaltung vereinfachen und ermöglicht es Ihnen, Erkenntnisse aus Ihren Netzwerkverkehrsdaten zu gewinnen.

Wenn Sie in Amazon Data Firehose veröffentlichen, werden Flow-Protokolldaten in einem Bereitstellungsstream von Amazon Data Firehose im reinen Textformat 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 eines Flow-Protokolls, das in Amazon Data Firehose veröffentlicht](#)

IAM-Rollen für die kontoübergreifende Bereitstellung

Wenn Sie in Amazon Data Firehose veröffentlichen, können Sie einen Bereitstellungsstream auswählen, der sich in demselben Konto wie die zu überwachende Ressource (das Quellkonto) oder in einem anderen Konto (dem Zielkonto) befindet. Um die kontenübergreifende 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. Wenn Sie Ihre Richtlinie erstellen, geben Sie die VPCs Netzwerkschnittstellen oder Subnetze, die Sie überwachen, mit dem Bedingungsschlüssel an. `iam:AssociatedResourceARN`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::123456789012:role/mySourceRole",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "delivery.logs.amazonaws.com"
        },
        "StringLike": {
          "iam:AssociatedResourceARN": [
            "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-0011223344556677"
          ]
        }
      }
    }
  ]
}
```

```

        ]
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery",
        "logs:ListLogDeliveries",
        "logs:GetLogDelivery"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::111122223333:role/
AWSLogDeliveryFirehoseCrossAccountRole"
    }
  ]
}

```

Stellen Sie sicher, dass Ihre Rolle die folgende Vertrauensrichtlinie hat, die es dem Protokollservice erlaubt, die Rolle zu übernehmen.

JSON

```

{
  "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 unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.
2. Wählen Sie im Navigationsbereich Richtlinien.
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 und eine optionale Beschreibung sowie Tags für Ihre Richtlinie ein und wählen Sie dann Richtlinie erstellen aus.
5. Wählen Sie im Navigationsbereich Rollen aus.
6. Wählen Sie Create role (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 AWSLogDeliveryFirehoseCrossAccountRole beginnt. Die Rolle muss die folgenden Berechtigungen enthalten.

JSON

```
{
  "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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333: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 unter <https://console.aws.amazon.com/iam/> die IAM-Konsole.

2. Wählen Sie im Navigationsbereich Richtlinien.
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 Create role (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 eines Flow-Protokolls, das in Amazon Data Firehose veröffentlicht

Sie können Flow-Logs für Ihre VPCs Subnetze oder Netzwerkschnittstellen erstellen.

Voraussetzungen

- Erstellen Sie einen Ziel-Bereitstellungsstream für Amazon Data Firehose. Verwenden Sie Direct Put als Quelle. Weitere Informationen finden Sie unter [Creating an Amazon Data Firehose delivery stream](#).

- Das Konto, das das Flow-Protokoll erstellt, muss eine IAM-Rolle verwenden, die die folgenden Berechtigungen zum Veröffentlichen von Flow-Protokollen in Amazon Data Firehose gewährt.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogDelivery",
        "logs>DeleteLogDelivery",
        "iam:CreateServiceLinkedRole",
        "firehose:TagDeliveryStream"
      ],
      "Resource": "*"
    }
  ]
}
```

- 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.

So erstellen Sie ein Flow-Protokolls, das in Amazon Data Firehose veröffentlicht

1. Führen Sie eine der folgenden Aktionen aus:
 - Öffnen Sie die EC2 Amazon-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 Ihr aus VPCs. Aktivieren Sie das Kontrollkästchen für die VPC.
 - Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>. Wählen Sie im Navigationsbereich 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:
 - An Amazon Data Firehose im selben Konto senden – Der Bereitstellungsstream und die zu überwachende Ressource befinden sich im selben Konto.
 - An Amazon Data Firehose in einem anderen Konto senden – Der Bereitstellungsstream und die zu überwachende Ressource befinden sich in unterschiedlichen Konten.
 6. Wählen Sie für den Stream-Namen von Amazon Data Firehose den Bereitstellungsstream aus, den Sie erstellt haben.
 7. [Nur kontoübergreifende Bereitstellung] Wählen Sie für den Servicezugriff eine bestehende [IAM-Servicerolle für die kontoübergreifende Bereitstellung](#) aus, die über die Berechtigungen zum Veröffentlichen von Protokollen verfügt, oder wählen Sie Berechtigungen einrichten aus, um die IAM-Konsole zu öffnen und eine Servicerolle zu erstellen.
 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 aus, um Tags auf das Flow-Protokoll anzuwenden.
 11. Wählen Sie Create flow log (Flussprotokoll erstellen) aus.

So erstellen Sie ein Flow-Protokoll, das in Amazon Data Firehose veröffentlicht wird, mithilfe der Befehlszeile

Verwenden Sie einen der folgenden Befehle:

- [create-flow-logs](#) (AWS CLI)
- [New-EC2FlowLog](#) (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
```

Nach der Erstellung des Flow-Protokolls können Sie 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 virtuellen privaten Clouds (VPCs) am häufigsten sprechen, oder Sie können die IP-Adressen mit den am häufigsten abgelehnten TCP-Verbindungen ermitteln.

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](#)
- [CloudFormation Generieren Sie die 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 Ihre VPCs und dann Ihre VPC aus.
 - Öffnen Sie die Amazon VPC-Konsole. Wählen Sie im Navigationsbereich die Option Subnets (Subnetze) und dann Ihr Subnetz aus.
 - Öffnen Sie die EC2 Amazon-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 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 `flow-logs-subscription-idvpcflowlogsathenadatabase< >`.

- Eine Athena-Arbeitsgruppe. Der Name der Arbeitsgruppe lautet < > < Startdatum > < Enddatum > Arbeitsgruppe flow-log-subscription-idpartition-load-frequency
- Eine partitionierte Athena-Tabelle, die Ihren Flow-Protokolldatensätzen entspricht. Der Tabellename lautet < > < Startdatum > < Enddatum >. flow-log-subscription-idpartition-load-frequency
- 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.

CloudFormation Generieren Sie die 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 CloudFormation Vorlage zu generieren.

```
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 Befehl [create-stack](#), um einen Stack mit der generierten Vorlage 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.

- VpcFlowLogsAcceptedTraffic— Die TCP-Verbindungen, die aufgrund Ihrer Sicherheitsgruppen und Ihres Netzwerks zugelassen wurden. ACLs
- VpcFlowLogsAdminPortTraffic— Die 10 IP-Adressen mit dem meisten Datenverkehr, aufgezeichnet von Anwendungen, die Anfragen an Administrator-Ports bearbeiten.
- VpcFlowLogsIPv4Verkehr — Die Gesamtzahl der aufgezeichneten IPv4 Datenverkehrs-Bytes.

- `VpcFlowLogsIPv6Verkehr` — Die Gesamtzahl der Byte des aufgezeichneten IPv6 Datenverkehrs.
- `VpcFlowLogsRejectedTCPTraffic`— Die TCP-Verbindungen, die aufgrund Ihrer Sicherheitsgruppen oder Ihres Netzwerks abgelehnt wurden ACLs.
- `VpcFlowLogsRejectedTraffic`— Der Datenverkehr, der aufgrund Ihrer Sicherheitsgruppen oder Ihres Netzwerks abgelehnt wurde ACLs.
- `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`— Das 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 `LogDestinationNotFoundException` " oder `'Zugriff verweigert für LogDestination '`](#)
- [Überschreiten des Amazon S3-Bucket-Richtlinienlimits](#)

- [LogDestination nicht zustellbar](#)
- [Die Datengröße der Flow-Protokolle stimmt nicht mit den Abrechnungsdaten überein](#)

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, oder [es sind SkipData Einträge vorhanden](#).

Lösung

Überprüfen Sie die Registerkarte Flow-Protokolle für die VPC, das Subnetz oder die Netzwerkschnittstelle. Beachten Sie, dass Sie keine Flow-Protokolle für eine VPC oder ein Subnetz beschreiben können, das mit Ihnen geteilt wurde, aber Sie können Flow-Protokolle für eine Netzwerkschnittstelle beschreiben, die Sie in einer VPC oder einem Subnetz erstellen, das mit Ihnen geteilt wurde. Sofern Fehler auftreten, werden sie in der Spalte Status angezeigt. Verwenden Sie alternativ den [describe-flow-logs](#) Befehl und überprüfen Sie den Wert, der in dem `DeliverLogsErrorMessage` Feld zurückgegeben wird.

Die folgenden Werte sind mögliche Fehlerwerte für den Status:

- `Rate limited`: Dieser Fehler kann auftreten, wenn die CloudWatch Protokolldrosselung angewendet wurde — wenn die Anzahl der Flow-Log-Datensätze 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 [CloudWatchServicekontingenten](#) 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 die Amazon VPC- oder EC2 Amazon-Konsole zeigt das Flow-Protokoll als `Active` an. 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 `LogDestinationNotFoundException` " 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 angezeigt: `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 angezeigt:
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.

Die Datengröße der Flow-Protokolle stimmt nicht mit den Abrechnungsdaten überein

Problem

Die Gesamtdatengröße Ihrer Flow-Protokolle entspricht nicht der in den Abrechnungsdaten angegebenen Größe.

Mögliche Ursachen

In Ihren Flow-Protokollen befinden sich ggf. SKIPDATA-Einträge. Eine Erläuterung der SKIPDATA-Einträge finden Sie unter [Keine Daten und übersprungene Datensätze](#).

Lösung

Vergewissern Sie sich, ob SKIPDATA-Einträge in Ihren Protokolleinträgen vorhanden sind, indem Sie Ihre Protokolle nach verschiedenen Einträgen im Protokollstatusfeld abfragen.

Beispielabfragen zur Prüfung nach SKIPDATA:

CW Insights:

```
fields @timestamp, @message, @logStream, @log
| filter interfaceId = 'eni-123'
| stats count(*) by interfaceId, logStatus
| sort by interfaceId, logStatus
```

Athena:

```
SELECT log_status, interface_id, count(1)
FROM vpc_flow_logs
WHERE interface_id IN ('eni-1', 'eni-2', 'eni-3')
GROUP BY log_status, interface_id
```

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](#)
- [Aktivieren oder Deaktivieren der NAU-Überwachung](#)
- [Alarm-Beispiel für NAU CloudWatch](#)

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. Dimensionen • 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. Dimensionen • 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. Dimensionen • 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. Dimensionen • Name: Service, Wert: EC2 • Name: Type, Wert: Resource • Name: Resource, Wert: Die VPC-ID. • Name: Class, Wert: NetworkAddressUsagePeered
ResourceCount	Eine kombinierte Ansicht der NAU-Nutzung über VPCs hinweg. Kriterien für die Berichterstattung • Alle 24 Stunden.

Metrik	Beschreibung
	Dimensionen • 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. Dimensionen • 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 aktivieren 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"  
}
```

Verstehen der Codes für Amazon VPC in Fakturierungs- und Nutzungsberichten

Wenn Sie Amazon VPC verwenden, nehmen wir entsprechende Codes in Ihre AWS-Fakturierungs- und Nutzungsberichte auf. Die Überprüfung dieser Codes hilft Ihnen, Ihre Kosten und Nutzungsmuster für Amazon VPC zu verstehen. Die Nachverfolgung und Verwaltung Ihrer Ausgaben ist für die Optimierung Ihrer Kosten unerlässlich.

Die folgenden Tabellen beschreiben die Codes für Amazon VPC, die in Ihren Fakturierungs- und Nutzungsberichten vorkommen. Eine Liste der Regionscodes in den Fakturierungs- und Nutzungsberichten finden Sie unter [AWS-Regions-Fakturierungscodes](#).

Fakturierungscodes für:

- [IP-Adressverwaltung](#)
- [VPC-Endpunkte](#)
- [Transit Gateways](#)
- [Netzwerkanalyse](#)
- [Datenverkehrsspiegelung](#)
- [VPC Lattice](#)
- [Konto- und regionsübergreifende Ressourcen](#)

Zugehörige Ressourcen

- [Amazon VPC – Preise](#)
- [AWS PrivateLink Preise](#)
- [AWS Transit Gateway Preise](#)
- [Preisgestaltung Amazon VPC Lattice](#)

IP-Adressverwaltung

Code	Beschreibung	Einheiten	Granularity
<i>region-</i> PublicIP v4:InUseAddress	Der Zeitpunkt, in dem öffentliche IPv4-Adressen von einer Ressource verwendet werden.	Stunden	Pro Sekunde
<i>region-</i> PublicIP v4:IdleAddress	Der Zeitpunkt, in dem öffentliche IPv4-Adressen nicht von einer Ressource verwendet werden.	Stunden	Pro Sekunde
<i>region-</i> PublicIP v4:ContiguousBlock	Der Einsatz von öffentlichen IPv4-Adressen in einem von Amazon bereitgestellten zusammenhängenden IPv4-Block.	Stunden	Stündlich
<i>region-</i> IPAddressesManager-IP-Hours	Der Zeitpunkt, in dem IP-Adressen von IPAM Advanced Tier verwaltet werden.	Stunden	Stündlich

VPC-Endpunkte

Code	Beschreibung	Einheiten	Granularity
<i>region-</i> VpcEndpoint-Hours	Der Zeitpunkt, in dem die VPC-Endpunkte der Schnittstelle bereitgestellt werden.	Stunden	Stündlich
<i>region-</i> VpcEndpoint-Bytes	Die von den VPC-Endpunkten der Schnittstelle verarbeiteten Daten.	GB	Stundensatz

Code	Beschreibung	Einheiten	Granularity
<i>region</i> -VpcEndpoint-GWLBE-Hours	Der Zeitpunkt, zu dem Gateway-Load-Balancer-Endpunkte bereitgestellt werden.	Stunden	Stündlich
<i>region</i> -VpcEndpoint-GWLBE-Bytes	Die von Gateway-Load-Balancer-Endpunkten verarbeiteten Daten.	GB	Stundensatz

Transit Gateways

Code	Beschreibung	Einheiten	Granularity
<i>region</i> -TransitGateway-Hours	Die Nutzung der Transit-Gateway-Anhänge.	Stunden	Stündlich
<i>region</i> -TransitGateway-Bytes	Die Daten, die von Transit-Gateways verarbeitet wurden.	GB	Stundensatz
<i>region</i> -TGW-Multicast-Consumer-Bytes	Die Daten, die von Multicast-Receiver-Instances verarbeitet wurden.	GB	Stundensatz

Netzwerkanalyse

Code	Beschreibung	Einheiten	Granularity
<i>region</i> -Analysis-Runs	Die Anzahl der Netzwerkpfade, die von Reachability Analyzer analysiert wurden.	Anzahl	Pro Analyse
<i>region</i> -NetworkInterface-Assessment	Die maximale Anzahl von Netzwerkschnittstellen, die von Network Access Analyzer analysiert wurden.	Anzahl	Pro Bewertung

Datenverkehrsspiegelung

Code	Beschreibung	Einheiten	Granularity
<i>region</i> -ENI-Mirror	Der Zeitpunkt, an dem eine Netzwerkschnittstelle für die Datenverkehrsspiegelung konfiguriert ist.	Stunden	Stündlich

VPC Lattice

Code	Beschreibung	Einheiten	Granularity
<i>region</i> -VPC Lattice-Service-Hourly	Die Laufzeit für VPC-Lattice-Services.	Stunden	Stündlich
<i>region</i> -VPC Lattice	Die Daten, die von VPC-Lattice-Services verarbeitet wurden.	GB	Stundensatz

Code	Beschreibung	Einheiten	Granularity
ce-DataProcessing-Bytes			
<i>region-</i> VpcLattice-RequestCount-Free	Die kostenlosen HTTP-Anfragen und TCP-Verbindungen.	Anzahl	Stündlich
<i>region-</i> VpcLattice-Service-Network-Resource-Hours	Die Laufzeit für VPC-Lattice-Service-Netzwerke.	Stunden	Stündlich

Konto- und regionsübergreifende Ressourcen

Code	Beschreibung	Einheiten	Granularity
<i>region-</i> VpcResource-Provider-Bytes	Die Daten, die von Anbieterr essourcen übergreifend über Konten oder Regionen hinweg übertragen wurden.	GB	Stundensatz
<i>region-</i> VpcResource-Consumer-Bytes	Die Daten, die von Verbrauch erressourcen übergreifend über Konten oder Regionen hinweg übertragen wurden.	GB	Stundensatz

Beschreiben Ihrer VPC-Netzwerkarchitektur

Amazon VPC ermöglicht es Ihnen, ein logisch isoliertes virtuelles Netzwerk in der AWS Cloud zu definieren, das als Virtual Private Cloud (VPC) bezeichnet wird. Erstellen Sie eine separate VPCs , um die Infrastruktur nach Arbeitslast oder organisatorischer Einheit zu isolieren. Sie können Ihre konfigurieren, VPCs indem Sie IP-Adressbereiche auswählen, Routing konfigurieren und Netzwerk-Gateways hinzufügen, um Sie VPCs miteinander, mit dem Internet oder mit Ihrem eigenen Unternehmensnetzwerk zu verbinden. Sie starten AWS Ressourcen wie EC2 Instances oder RDS-Instances in Ihrem VPCs.

In der folgenden Tabelle werden die wichtigsten Merkmale eines VPC-Netzwerks beschrieben. Ein Netzwerkadministrator kann diese Anleitung nutzen, um die Architektur und Konfiguration des VPC-Netzwerks zu beschreiben. Mit diesen Informationen lässt sich ein funktionell gleichwertiges Netzwerk vor Ort oder über einen anderen Cloud-Anbieter konfigurieren.

Merkmal	Description
Geografischer Standort	Amazon VPC wird in allen AWS Regionen weltweit gehostet. Sie können die Regionen für Ihr VPC-Netzwerk auswählen, in denen Ihre AWS Ressourcen Ihren Kunden am nächsten sind.
Subnets	Die Subnetze, die Sie für Sie definieren, VPCs definieren Netzwerkgrenzen und bestimmen die IP-Adressen für Ihre AWS Ressourcen. Sie können Subnetze in mehreren Availability Zones hinzufügen, um die Verfügbarkeit der Ressourcen zu erhöhen.
Netzwerkverbindbarkeit	Die Gateways, die Sie an Ihre VPCs Subnetze anhängen, um Konnektivität zwischen Ihrem VPC-Netzwerk und anderen Netzwerken, z. B. anderen Netzwerken VPCs oder Subnetzen, dem Internet oder Ihren lokalen Netzwerken, bereitzustellen.

Merkmal	Description
Sicherheitskontrollen	Die Sicherheitsgruppen, die Sie für Ihren Datenverkehr erstellen, VPCs steuern den Verkehr zu und von den zugehörigen Ressourcen, wie Rechenressourcen, Datenbankressourcen und Load Balancern. Jedes Subnetz hat eine Netzwerk-ACL, die den ein- und ausgehenden Datenverkehr steuert.
Verwaltung des Datenverkehrs	Routingregeln steuern den Verkehrsfluss zwischen Subnetzen und externen Standorten. VPCs Die von ELB bereitgestellten Load Balancer verteilen den eingehenden Datenverkehr auf mehrere Ziele wie EC2 Instances, Container und Lambda-Funktionen.

Geografischer Standort

Amazon VPC ist in jeder AWS Region weltweit verfügbar. Jede -Region ist ein separater geografischer Bereich. Sie können die Netzwerklatenz verringern, wenn Sie VPCs für Ihre Ressourcen in Regionen erstellen, die sich in der Nähe der Mehrheit Ihrer Benutzer befinden.

Sie können Amazon EC2 Global View verwenden, um Ihre VPCs in allen Regionen über eine grafische Benutzeroberfläche aufzulisten (es gibt keine gleichwertige programmatische Oberfläche). Mit der Amazon VPC-Konsole, der AWS API und den AWS Befehlszeilenschnittstellen müssen Sie die VPC-Ressourcen VPCs und die VPC-Ressourcen für jede Region einzeln auflisten.

Warum das wichtig ist

Nachdem Sie ermittelt haben, wo Sie sich VPCs befinden, können Sie entscheiden, ob Sie je nach Ihren Anforderungen ein funktionell gleichwertiges Netzwerk an denselben Standorten oder an verschiedenen Standorten konfigurieren möchten.

Um eine Zusammenfassung Ihrer Daten VPCs in allen Regionen zu erhalten

1. Öffnen Sie die Amazon EC2 Global View-Konsole zu <https://console.aws.amazon.com/ec2globalview/Hause>.
2. Überprüfen Sie auf der Registerkarte Region Explorer unter Zusammenfassung die Anzahl der Ressourcen für VPCs, die die Anzahl VPCs und die Anzahl der Regionen umfasst. Dies gilt sowohl für StandardprodukteVPCs , die in Ihrem Namen AWS erstellt werden, als auch für nicht standardmäßige Einstellungen VPCs , die Sie erstellen. Wählen Sie den unterstrichenen Text, um zu sehen, wie sich die VPC-Anzahl auf die Regionen verteilt. Wenn eine Region nur über eine VPC verfügt, ist dies höchstwahrscheinlich die Standard-VPC für die Region.
3. Wählen Sie auf der Registerkarte Globale Suche den Client-Filter Ressourcentyp = Vpc aus. Sie können die Ergebnisse weiter filtern, indem Sie eine Region oder ein Tag angeben.

Um das VPCs in eine Region zu bekommen, verwenden Sie AWS CLI

Verwenden Sie den Befehl [describe-vpcs](#). Sie müssen diesen Befehl in jeder Region ausführen, in der Sie ihn haben VPCs. Der `--query` Parameter beinhaltet nur die VPC IDs in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-vpcs \
  --region us-east-2 \
  --query "Vpcs[*].VpcId"
```

Jede Region hat eine Standard-VPC. Wenn Sie nicht die Standardeinstellung verwenden VPCs, können Sie sie aus den Ergebnissen ausschließen, indem Sie den folgenden Filter hinzufügen.

```
--filters Name=is-default,Values=false
```

Subnets

Ein Subnetz stellt eine logische Netzwerkgrenze in einer VPC dar. Weisen Sie beim Erstellen eines Subnetzes einen IP-Adressblock zu. Ressourcen, die Sie in einem Subnetz starten, werden IP-Adressen aus dem IP-Adressblock für das Subnetz zugewiesen. IP-Adressen ermöglichen es Ressourcen, über ein lokales Netzwerk oder das Internet miteinander zu kommunizieren.

Die Ressourcenübersicht in der Amazon-VPC-Konsole stellt die Subnetze für Ihre VPC visuell dar.

Warum das wichtig ist

Mithilfe von Subnetzen können Netzwerkadministratoren Sicherheitsgrenzen einrichten und den Datenverkehr zwischen den Anwendungsebenen kontrollieren. Indem Sie sich die IP-Adressen Ihrer Subnetze notieren, können Sie dafür sorgen, dass Ressourcen in einem funktionell gleichwertigen Netzwerk mit denselben Clients oder Anwendungen kommunizieren können wie in Ihrem VPC-Netzwerk.

So sehen Sie sich die Subnetze für eine VPC mithilfe der Ressourcenübersicht an

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich VPCs aus.
3. Aktivieren Sie das Kontrollkästchen für die VPC.
4. Wählen Sie die Registerkarte Ressourcenübersicht aus.
5. Wählen Sie im VPC-Detailbereich Details anzeigen aus. Im Bereich Subnetze werden alle Subnetze in der VPC mit den dazugehörigen IP-Adressbereichen aufgeführt. Fahren Sie mit dem Mauszeiger über ein Subnetz, um die zugehörige Routing-Tabelle und die Netzwerkverbindungen hervorzuheben. Für weitere Informationen klicken Sie auf den Link, um die Subnetz-Detailseite zu öffnen.

Um die Subnetze für eine VPC mit dem zu beschreiben AWS CLI

Verwenden Sie den Befehl [describe-subnets](#). Der Parameter `--filters` beschränkt die Suche auf die Beschreibung der Subnetze für die angegebene VPC. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-subnets \
  --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
  --query Subnets[*].
[SubnetId,AvailabilityZoneId,CidrBlock,Ipv6CidrBlockAssociationSet[0].Ipv6CidrBlock] \
  --output table
```

Es folgt eine Beispielausgabe. Die Spalten sind Subnetz-ID, AZ-ID, IPv4 Adressbereich und der erste IPv6 Adressbereich (falls vorhanden).

DescribeSubnets			
subnet-0d2d1b81e0bc9c6d4	usw2-az1	10.0.144.0/20	2600:1f14:1e6e:a003::/64
subnet-0e01d500780bb7468	usw2-az1	10.0.16.0/20	2600:1f14:1e6e:a001::/64

	subnet-0eb17d85f5dfd33b1		usw2-az2		10.0.128.0/20		2600:1f14:1e6e:a002::/64	
	subnet-0e990c67809773b19		usw2-az2		10.0.0.0/20		2600:1f14:1e6e:a000::/64	
+-----+-----+-----+-----+-----+-----+-----+-----+-----+								

Netzwerkonnektivität

Mit den von Amazon VPC bereitgestellten Konnektivitätsoptionen können Sie ein Netzwerk einrichten, das sich über mehrere Konten und Regionen sowie Remote-Netzwerke erstreckt VPCs .

Mithilfe der Ressourcenübersicht in der Amazon VPC-Konsole können Sie herausfinden, ob Sie Internet-Gateways, Internet-Gateways nur für ausgehenden Datenverkehr, NAT-Gateways oder Gateway-VPC-Endpunkte VPCs verwenden. Die Ressourcenübersicht zeigt keine Transit-Gateways, Peering-Verbindungen, Virtual Private Gateways oder andere Arten von eingesetzten VPC-Endpunkten. Sie können die vollständige Liste der Gateways und Peering-Verbindungen für eine VPC abrufen, indem Sie diese einzeln über die Konsole, die API oder eine Befehlszeilenschnittstelle beschreiben.

Warum das wichtig ist

Nachdem Sie die Konnektivität verstanden haben, die Ihr VPC-Netzwerk bietet, können Sie dafür sorgen, dass Ressourcen in einem funktionell gleichwertigen Netzwerk mit denselben lokalen und Remote-Ressourcen kommunizieren können.

So sehen Sie sich die Netzwerkverbindungen für eine VPC mithilfe der Ressourcenübersicht an

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich VPCs aus.
3. Aktivieren Sie das Kontrollkästchen für die VPC.
4. Wählen Sie die Registerkarte Ressourcenübersicht aus.
5. Wählen Sie im VPC-Detailbereich Details anzeigen aus. Im Bereich Netzwerkverbindungen werden alle Internet-Gateways, Internet-Gateways für ausgehenden Verkehr, NAT-Gateways und VPC-Gateway-Endpunkte aufgeführt. Wenn der Ressourcentyp nicht klar ist, fahren Sie mit dem Mauszeiger über das Linksymbol für die Netzwerkverbindung und überprüfen Sie die resultierende URL. Diese URL ist ein Link zu der Ressource in der Konsole und enthält den Ressourcentyp und die Ressourcen-ID (z. B. internetGatewayId=igw-0123456780abcdef).

Um die Netzwerkverbindungen für Ihre Nutzung der zu erhalten VPCs AWS CLI

1. Verwenden Sie den folgenden [describe-internet-gateways](#) Befehl, um die Internet-Gateways für die angegebene Region abzurufen. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-internet-gateways \
  --region us-east-2 \
  --query InternetGateways[*].[Attachments[0].VpcId,InternetGatewayId] \
  --output table
```

Es folgt eine Beispielausgabe. Die Spalten zeigen die VPC IDs und das Internet-GatewayIDs.

```
-----
|               DescribeInternetGateways               |
+-----+-----+
| None                | igw-04c61dba10EXAMPLE |
| vpc-0bf4c2739bEXAMPLE | igw-09737a4029EXAMPLE |
| vpc-060415a18fEXAMPLE | igw-0c562bd22aEXAMPLE |
| vpc-0ea9d41094EXAMPLE | igw-0e06f7033dEXAMPLE |
| vpc-03b86de356EXAMPLE | igw-0a9ff72d05EXAMPLE |
+-----+-----+
```

2. Verwenden Sie den folgenden Befehl [describe-egress-only-internet-gateways](#), um die Internet-Gateways für ausgehenden Datenverkehr für die angegebene Region abzurufen. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-egress-only-internet-gateways \
  --region us-east-2 \
  --query EgressOnlyInternetGateways[*].
[Attachments[0].VpcId,EgressOnlyInternetGatewayId] \
  --output table
```

Es folgt eine Beispielausgabe. In den Spalten werden die VPC IDs und das Internet-Gateway nur für ausgehenden Datenverkehr angezeigt. IDs

```
-----
|               DescribeEgressOnlyInternetGateways       |
+-----+-----+
```

```
| vpc-060415a18fEXAMPLE | eigw-0b8ca558acEXAMPLE |
+-----+-----+
```

3. Verwenden Sie den folgenden [describe-nat-gateways](#) Befehl, um die NAT-Gateways für die angegebene Region abzurufen. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-nat-gateways \
  --region us-east-2 \
  --query NatGateways[*].[VpcId,NatGatewayId,SubnetId] \
  --output table
```

Es folgt eine Beispielausgabe. Die Spalten zeigen die VPC IDs, das NAT-Gateway und IDs des Subnetzes.

```
-----
|                               DescribeNatGateways                               |
+-----+-----+-----+
| vpc-060415a18fEXAMPLE | nat-026316334aEXAMPLE | subnet-0eb17d85f5EXAMPLE |
| vpc-060415a18fEXAMPLE | nat-0f08bc5f52EXAMPLE | subnet-0d2d1b81e0EXAMPLE |
+-----+-----+-----+
```

4. Verwenden Sie den folgenden Befehl [describe-transit-gateway-vpc-attachments](#), um die Transit-Gateway-VPC-Anlagen für die angegebene Region abzurufen. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-transit-gateway-vpc-attachments \
  --region us-east-2 \
  --query TransitGatewayVpcAttachments[*].
[VpcId,TransitGatewayId,length(SubnetIds[])] \
  --output table
```

Es folgt eine Beispielausgabe. Die Spalten zeigen die VPC IDs, das Transit-Gateway IDs und die Anzahl der Subnetze.

```
-----
| DescribeTransitGatewayVpcAttachments |
+-----+-----+-----+
| vpc-0bf4c2739bEXAMPLE | tgw-055dc4e47bEXAMPLE | 4 |
| vpc-0ea9d41094EXAMPLE | tgw-055dc4e47bEXAMPLE | 2 |
+-----+-----+-----+
```

```
+-----+-----+-----+
```

5. Verwenden Sie den folgenden [describe-vpc-peering-connections](#) Befehl, um die Peering-Verbindungen für die VPCs in der angegebenen Region abzurufen. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-vpc-peering-connections \
  --region us-east-2 \
  --query VpcPeeringConnections[*].[AcceptorVpcInfo.VpcId,RequesterVpcInfo.VpcId] \
  --output table
```

Es folgt eine Beispielausgabe. Die Spalten zeigen die akzeptierende VPC IDs, die akzeptierenden VPC-Besitzer, die anfordernde VPC und die anfordernden IDs VPC-Besitzer.

```
-----
|                               DescribeVpcPeeringConnections                               |
|                                                                                           |
+-----+-----+-----+-----+
+
| vpc-0ea9d41094EXAMPLE | 123456789012 | vpc-03b86de356EXAMPLE | 123456789012 |
|                                                                                           |
+-----+-----+-----+-----+
+
```

6. Verwenden Sie den folgenden [describe-vpn-gateways](#) Befehl, um die virtuellen privaten Gateways für die angegebene Region abzurufen. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-vpn-gateways \
  --region us-east-2 \
  --query VpnGateways[*].[VpcAttachments[0].VpcId,VpnGatewayId] \
  --output table
```

Es folgt eine Beispielausgabe. Die Spalten zeigen die VPC IDs und das Virtual Private Gateway IDs.

```
-----
|                               DescribeVpnGateways                               |
|                                                                                           |
```

```
+-----+-----+
| vpc-0bf4c2739bEXAMPLE | vgw-0cb3226c4aEXAMPLE |
+-----+-----+
```

- Verwenden Sie den folgenden `describe-vpc-endpoints` Befehl, um die VPC-Endpunkte für die angegebene Region abzurufen. Der `--query`-Parameter umfasst nur die angegebenen Felder in der Ausgabe. Sie können nach Bedarf weitere Felder hinzufügen.

```
aws ec2 describe-vpc-endpoints \
  --region us-east-2 \
  --query 'VpcEndpoints[*].[VpcId,VpcEndpointType,ServiceName|ServiceNetworkArn|ResourceConfigurationArn]' \
  --output table
```

Es folgt eine Beispielausgabe. Die erste Spalte stellt die VPC-ID und die zweite Spalte den VPC-Endpunkttyp dar. Die dritte Spalte hängt vom Endpunkttyp ab und zeigt entweder den Servicenamen, den ARN für die Ressourcenkonfiguration oder den ARN des Servicenetzwerks.

```

|
| DescribeVpcEndpoints
|
+-----+-----+
+-----+-----+
+
| vpc-060415a18fcc9afde | Interface | com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387 |           |
| vpc-060415a18fcc9afde | Interface | com.amazonaws.vpce.us-west-2.vpce-
svc-007832a03d60fc387 |           |
| vpc-0bf4c2739bc05a694 | Gateway   | com.amazonaws.us-west-2.s3
|                           |           |
| vpc-0ea9d410947d27b7d | Interface | com.amazonaws.us-west-2.logs
|                           |           |
| vpc-0bf4c2739bc05a694 | Resource  | arn:aws:vpc-lattice:us-
east-2:123456789012:resourceconfiguration/rcfg-07129f3acded87625 |
| vpc-0bf4c2739bc05a694 | ServiceNetwork | arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e |
| vpc-0bf4c2739bc05a694 | ServiceNetwork | arn:aws:vpc-lattice:us-
east-2:123456789012:servicenetwork/sn-0808d1748faee0c1e |
+-----+-----+
+-----+-----+
+

```

Sicherheitskontrollen

Die von Amazon VPC bereitgestellten Sicherheitskontrollen bestimmen den Netzwerkzugriff auf Ihre VPCs und die in Ihrem VPCs bereitgestellten Ressourcen.

Warum das wichtig ist

Nachdem Sie den eingehenden Datenverkehr festgelegt haben, der Ihre Subnetze und Ressourcen erreichen darf, und den Ausgabedatenverkehr, der Ihre Subnetze und Ressourcen verlassen darf, können Sie die Firewall-Regeln planen, die für ein funktionsgleiches Netzwerk erforderlich sind.

Sicherheitskontrollen

- [Sicherheitsgruppen](#)
- [Netzwerk ACLs](#)

Sicherheitsgruppen

Eine Sicherheitsgruppe lässt bestimmten ein- und ausgehenden Datenverkehr auf Ressourcenebene zu. Sicherheitsgruppen sind der wichtigste Mechanismus zur Kontrolle des Zugriffs auf Ressourcen in Ihrem VPCs.

Um die Sicherheitsgruppen für Ihre zu erhalten VPCs

Verwenden Sie den folgenden [describe-security-groups](#) Befehl, um die Sicherheitsgruppen für die angegebene VPC anzuzeigen.

```
aws ec2 describe-security-groups \
  --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
  --query SecurityGroups[*].GroupId
```

So rufen Sie die Regeln einer Sicherheitsgruppe für den eingehenden Datenverkehr ab

Verwenden Sie den folgenden [describe-security-group-rules](#) Befehl, um die Regeln für die angegebene Sicherheitsgruppe anzuzeigen, wo sie sich IsEgress befindet `false`.

```
aws ec2 describe-security-group-rules \
  --filters Name=group-id,Values=sg-0abcdef1234567890 \
  --query 'SecurityGroupRules[?IsEgress==`false`]'
```

So rufen Sie die Regeln einer Sicherheitsgruppe für den ausgehenden Datenverkehr ab

Verwenden Sie den folgenden [describe-security-group-rules](#) Befehl, um die Regeln für die angegebene Sicherheitsgruppe anzuzeigen, wo sie sich IsEgress befindet `true`.

```
aws ec2 describe-security-group-rules \
  --filters Name=group-id,Values=sg-0abcdef1234567890 \
  --query 'SecurityGroupRules[?IsEgress==`true`]'
```

Netzwerk ACLs

Eine Netzwerk-Zugriffssteuerungsliste (ACL) erlaubt oder verweigert bestimmten eingehenden und ausgehenden Datenverkehr auf der Subnetzebene. Sie können das Netzwerk ACLs so verwenden, als defense-in-depth ob eine Ressource ohne die richtige Sicherheitsgruppe bereitgestellt wird.

Um das Netzwerk ACLs für Ihre Subnetze zu erhalten

Verwenden Sie den folgenden [describe-network-acls](#) Befehl, um das Netzwerk ACLs für die angegebene VPC und ihre Subnetzzuordnungen anzuzeigen.

```
aws ec2 describe-network-acls \
  --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
  --query "NetworkAcls[*].{ID:NetworkAclId,Subnets:Associations[].SubnetId}"
```

So rufen Sie die Regeln für eingehende Zugriffe für eine Netzwerk-ACL ab

Verwenden Sie den folgenden [describe-network-acls](#) Befehl, um die Regeln für die angegebene Netzwerk-ACL anzuzeigen, wo sie sich befindet `Egress: false`

```
aws ec2 describe-network-acls \
  --network-acl-ids acl-0abcdef1234567890 \
  --query 'NetworkAcls[*].Entries[?Egress==`false`]'
```

So rufen Sie die Regeln für ausgehende Zugriffe für eine Netzwerk-ACL ab

Verwenden Sie den folgenden [describe-network-acls](#) Befehl, um die Regeln für die angegebene Netzwerk-ACL anzuzeigen, wo sie sich Egress befindet `true`.

```
aws ec2 describe-network-acls \
```

```
--network-acl-ids acl-0abcdef1234567890 \  
--query 'NetworkAcls[*].Entries[?Egress=='true']'
```

Verwaltung des Datenverkehrs

Ein effektives Datenverkehrsmanagement kombiniert die Routing-Entscheidungen auf Netzwerkebene, die durch Routing-Tabellen bereitgestellt werden, mit den Verteilungsstrategien auf Anwendungsebene, die durch Load Balancing bereitgestellt werden.

Warum das wichtig ist

Netzwerkadministratoren müssen Subnetze, Routing, DNS-Auflösung und Load Balancing so gestalten, dass der Datenfluss optimiert und gleichzeitig die Sicherheitsgrenzen und Leistungsanforderungen eingehalten werden. Indem Sie sich die Konfiguration dieser Komponenten in Ihrem VPC-Netzwerk notieren, können Sie dafür sorgen, dass Ressourcen in einem funktionell gleichwertigen Netzwerk mit denselben Clients oder Geräten kommunizieren können wie in Ihrem VPC-Netzwerk.

Verwaltung des Datenverkehrs

- [Routing-Tabellen](#)
- [DHCP-Optionsliste](#)
- [Load Balancers](#)

Routing-Tabellen

Routentabellen bestimmen, wie der Netzwerkverkehr über Netzwerkgrenzen wie Subnetze VPCs, lokale Netzwerke und das Internet fließt.

Die Ressourcenübersicht in der Amazon-VPC-Konsole bietet eine visuelle Darstellung der Routing-Tabellen für Ihre VPC.

So sehen Sie sich die Routing-Tabellen für eine VPC mithilfe der Ressourcenübersicht an

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich VPCs aus.
3. Aktivieren Sie das Kontrollkästchen für die VPC.
4. Wählen Sie die Registerkarte Ressourcenübersicht aus.

5. Im Bereich Routing-Tabellen sind alle Routing-Tabellen für die VPC aufgeführt. Fahren Sie mit dem Mauszeiger über eine Routing-Tabelle, um die zugehörigen Subnetze und die Netzwerkverbindungen hervorzuheben. Für weitere Informationen klicken Sie auf den Link, um die Routing-Tabellen-Detailseite zu öffnen.

So beschreiben Sie Ihre Routing-Tabellen

Verwenden Sie den [describe-route-tables](#)Befehl, um die Routentabellen für die angegebene VPC und ihre Subnetzzuordnungen zu beschreiben.

```
aws ec2 describe-route-tables \
  --filters Name=vpc-id,Values=vpc-1234567890abcdef0 \
  --query "RouteTables[*].{ID:RouteTableId,Subnets:Associations[].SubnetId}"
```

So rufen Sie Routen für eine Routing-Tabelle ab

Verwenden Sie den [describe-route-tables](#)Befehl, um die Routen für die angegebene Routentabelle zu beschreiben.

```
aws ec2 describe-route-tables \
  --route-table-ids rtb-02ec01715bEXAMPLE \
  --query RouteTables[*].Routes
```

DHCP-Optionsliste

Ihre VPC verfügt über eine DHCP-Optionsliste, mit der Sie verschiedene Netzwerkeinstellungen konfigurieren können. Sie können beispielsweise benutzerdefinierte DNS-Server so konfigurieren, dass Ihre EC2 Instances interne Hostnamen mithilfe Ihrer vorhandenen DNS-Infrastruktur auflösen können. Weitere Informationen finden Sie unter [the section called “DHCP-Optionssatzkonzepte”](#).

So beschreiben Sie die DHCP-Optionen für Ihre VPC

Verwenden Sie den [describe-dhcp-options](#)Befehl, um die angegebenen DHCP-Optionen zu beschreiben. In diesem Beispiel wird auch die ID der DHCP-Optionen für die angegebene VPC mithilfe des Befehls [describe-vpcs](#) abgerufen.

```
aws ec2 describe-dhcp-options \
  --dhcp-options-id "$(aws ec2 describe-vpcs \
    --vpc-id vpc-1234567890abcdef0 \
```

```
--query Vpcs[].DhcpOptionsId --output text)"
```

Im Folgenden finden Sie eine Beispielausgabe für eine VPC, welche die DHCP-Standardoptionen verwendet.

```
{
  "DhcpOptions": [
    {
      "OwnerId": "415546850671",
      "Tags": [],
      "DhcpOptionsId": "dopt-1234567890abcdef0",
      "DhcpConfigurations": [
        {
          "Key": "domain-name",
          "Values": [
            {
              "Value": "us-west-2.compute.internal"
            }
          ]
        },
        {
          "Key": "domain-name-servers",
          "Values": [
            {
              "Value": "AmazonProvidedDNS"
            }
          ]
        }
      ]
    }
  ]
}
```

Load Balancers

Load Balancing verteilt eingehenden Datenverkehr von Clients auf mehrere Ziele. Load Balancer überwachen den Zustand von Zielen und entfernen fehlerhafte Ziele automatisch aus der Verteilung des Datenverkehrs, sodass nur fehlerfreie Ziele verwendet werden. Das verbessert die Verfügbarkeit und Leistung Ihrer Anwendung und optimiert die Ressourcennutzung. Weitere Informationen finden Sie im [Elastic Load Balancing-Benutzerhandbuch](#).

So beschreiben Sie Ihre Load Balancers

Verwenden Sie den [describe-load-balancers](#) Befehl, um die Load Balancer für die angegebene VPC anzuzeigen.

```
aws elbv2 describe-load-balancers \
  --query 'LoadBalancers[?VpcId==`vpc-1234567890abcdef0`].LoadBalancerArn'
```

Zugehörige Ressourcen

Die folgenden optionalen Services oder Features, die Sie möglicherweise in Ihrem VPC-Netzwerk verwenden:

- [Direct Connect](#)
- [AWS Network Firewall](#)
- [IPAM](#)
- [Datenverkehrsspiegelung](#)
- [VPC Flow Logs](#)

Verwaltung der Sicherheitsaufgaben für Amazon Virtual Private Cloud

Cloud-Sicherheit hat AWS 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 Ihnen helfen, Ihre Amazon VPC-Ressourcen zu überwachen und zu sichern.

Inhalt

- [Sicherstellen des Datenschutzes in Amazon Virtual Private Cloud](#)
- [VPC-Verschlüsselung bei der Übertragung erzwingen](#)
- [Identity and Access Management für Amazon VPC](#)
- [Infrastruktursicherheit in Amazon VPC](#)
- [Steuern Sie den Datenverkehr zu Ihren AWS Ressourcen mithilfe von Sicherheitsgruppen](#)
- [Steuerung des Datenverkehrs in Subnetzen mithilfe von Zugriffskontrolllisten für Netzwerke](#)
- [Ausfallsicherheit in Amazon Virtual Private Cloud](#)

- [Compliance-Validierung für Amazon Virtual Private Cloud](#)
- [Sperren Sie den öffentlichen Zugriff VPCs auf Subnetze](#)
- [Security best practices for your VPC](#)

Sicherstellen des Datenschutzes 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).
- Wird verwendet SSL/TLS , um mit AWS Ressourcen zu kommunizieren. Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein AWS CloudTrail. Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter [Arbeiten mit CloudTrail Pfaden](#) im AWS CloudTrail Benutzerhandbuch.
- 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 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-3](#).

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 AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. 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.

Sicherstellen der 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 ermöglichen bestimmten eingehenden und ausgehenden Datenverkehr auf Ressourcenebene (z. B. einer Instanz). EC2 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](#).
- **Netzwerkzugriffskontrolllisten (ACL):** Das Netzwerk ACLs erlaubt oder verweigert bestimmten eingehenden und ausgehenden Datenverkehr auf Subnetzebene. Weitere Informationen finden Sie unter [Steuerung des Datenverkehrs in Subnetzen mithilfe von Zugriffskontrolllisten für Netzwerke](#).
- **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, restriktive oder zu freigütige Sicherheitsgruppen- und Netzwerk-ACL-Regeln zu diagnostizieren. Weitere Informationen finden Sie unter [Protokollieren von IP-Datenverkehr mit VPC Flow Logs](#).
- **Datenverkehrsspiegelung:** Sie können Netzwerkdatenverkehr von einer elastic network interface einer EC2 Amazon-Instance kopieren. Anschließend können Sie den Datenverkehr an out-of-band Sicherheits- und Überwachungsgeräte senden. Weitere Informationen finden Sie im [Leitfaden zur Datenspiegelung](#).

VPC-Verschlüsselung bei der Übertragung erzwingen

VPC Encryption Controls ist eine Sicherheits- und Compliance-Funktion, die Ihnen eine zentrale, autoritative Kontrolle zur Überwachung des Verschlüsselungsstatus Ihrer Datenströme bietet, Ihnen hilft, Ressourcen zu identifizieren, die Klartext-Kommunikation ermöglichen, und Ihnen schließlich Mechanismen an die Hand gibt, um die Verschlüsselung während der Übertragung innerhalb und zwischen Ihrer VPCs Region durchzusetzen.

VPC Encryption Controls verwendet sowohl Verschlüsselung auf Anwendungsebene als auch integrierte Verschlüsselungsfunktionen der AWS Nitro-Systemhardware bei der Übertragung, um die Durchsetzung der Verschlüsselung sicherzustellen. Diese Funktion erweitert auch die native Verschlüsselung auf Hardwareebene über die modernen Nitro-Instanzen hinaus auf andere AWS Dienste wie Fargate, Application Load Balancer, Transit Gateways und viele andere.

Die Funktion wurde für alle entwickelt, die Transparenz und Kontrolle über den Verschlüsselungsstatus ihres gesamten Datenverkehrs sicherstellen möchten. Es ist besonders nützlich in Branchen, in denen Datenverschlüsselung für die Einhaltung von Compliance-Standards wie HIPAA FedRamp und PCI DSS von größter Bedeutung ist. Sicherheitsadministratoren und Cloud-Architekten können damit zentral Verschlüsselungsrichtlinien für die Übertragung in ihrer gesamten Umgebung anwenden AWS

Diese Funktion kann in zwei Modi verwendet werden: im Überwachungsmodus und im Erzwingungsmodus.

Die Verschlüsselung steuert die Modi

Überwachungsmodus

Im Überwachungsmodus bietet Encryption Controls Einblick in den Verschlüsselungsstatus des Datenverkehrs zwischen Ihren AWS Ressourcen innerhalb und zwischen Ihren Ressourcen VPCs. Es hilft Ihnen auch dabei, VPC-Ressourcen zu identifizieren, die bei der Übertragung keine Verschlüsselung erzwingen. Sie können Ihre VPC-Flow-Logs so konfigurieren, dass sie das erweiterte Feld ausgeben, `encryption-status` das Ihnen mitteilt, ob Ihr Datenverkehr verschlüsselt ist. Sie können auch die Konsole oder den `GetVpcResourcesBlockingEncryptionEnforcement` Befehl verwenden, um die Ressourcen zu identifizieren, die bei der Übertragung keine Verschlüsselung erzwingen.

 Note

Existierende VPCs können nur zuerst im Überwachungsmodus aktiviert werden. Auf diese Weise erhalten Sie Einblick in die Ressourcen, die Klartext-Verkehr zulassen oder zulassen könnten. Sie können den Erzwingungsmodus auf Ihrer VPC erst aktivieren, wenn diese Ressourcen mit der Durchsetzung der Verschlüsselung beginnen (oder Sie Ausnahmen für sie erstellen).

Modus erzwingen

Im Erzwingungsmodus verhindert VPC Encryption Controls, dass Sie Funktionen oder Dienste verwenden, die unverschlüsselten Datenverkehr innerhalb der VPC-Grenze zulassen. Sie können Encryption Controls im Erzwingungsmodus nicht direkt auf Ihrem vorhandenen System aktivieren. VPCs Sie müssen Encryption Controls zunächst im Überwachungsmodus aktivieren, nicht konforme Ressourcen identifizieren und ändern, um die Verschlüsselung bei der Übertragung zu erzwingen, und dann den Erzwingungsmodus aktivieren. Sie können Encryption Controls jedoch im Erzwingungsmodus für neue Geräte VPCs während der Erstellung aktivieren.

Wenn er aktiviert ist, verhindert der Erzwingungsmodus, dass Sie unverschlüsselte VPC-Ressourcen wie alte EC2 Instances, die keine native integrierte Verschlüsselung unterstützen, oder Internet-Gateways usw. erstellen oder anhängen. Wenn Sie eine nicht konforme Ressource in einer VPC mit verschlüsselungserzwungener Verschlüsselung ausführen möchten, müssen Sie eine Ausnahme für diese Ressource erstellen.

Überwachung des Verschlüsselungsstatus von Verkehrsströmen

Sie können den Verschlüsselungsstatus der Verkehrsflüsse innerhalb der VPC mithilfe des `encryption-status` Felds in Ihren VPC-Flussprotokollen überprüfen. Folgende Werte sind möglich:

- 0= nicht verschlüsselt
- 1= Nitroverschlüsselt (verwaltet von VPC Encryption Controls)
- 2= anwendungsverschlüsselt
 - fließt auf TCP-Port 443 für die Schnittstelle vom Endpunkt zum Dienst * AWS
 - fließt auf dem TCP-Port 443 für den Gateway-Endpunkt *
 - fließt über den VPC-Endpunkt zum verschlüsselten Redshift-Cluster **

- 3= sowohl Nitro- ALS auch anwendungsverschlüsselt
- (-)= Verschlüsselungsstatus Unbekannt oder VPC-Verschlüsselungssteuerung ist ausgeschaltet

Hinweis:

* Bei Schnittstellen- und Gateway-Endpunkten werden bei der Bestimmung des Verschlüsselungsstatus AWS nicht die Paketdaten berücksichtigt, sondern der verwendete Port verwendet, um den Verschlüsselungsstatus anzunehmen.

** AWS Ermittelt den Verschlüsselungsstatus für bestimmte AWS verwaltete Endpunkte auf der Grundlage der TLS-Anforderung in der Dienstkonfiguration.

Einschränkungen von VPC Flow Log

- Um Flow-Logs für VPC Encryption Controls zu aktivieren, müssen Sie manuell neue Flow-Logs mit dem Feld encryption-status erstellen. Das Feld für den Verschlüsselungsstatus wird nicht automatisch zu vorhandenen Flow-Protokollen hinzugefügt.
- Es wird empfohlen, die Felder \$ {traffic-path} und \$ {flow-direction} zu den Flow-Logs hinzuzufügen, um detailliertere Informationen in den Flow-Logs zu erhalten.

Beispiel:

```
aws ec2 create-flow-logs \  
--resource-type VPC \  
--resource-ids vpc-12345678901234567 \  
--traffic-type ALL \  
--log-group-name my-flow-logs \  
--deliver-logs-permission-arn arn:aws:iam::123456789101:role/publishFlowLogs \  
--log-format '${encryption-status} ${srcaddr} ${dstaddr} ${srcport} ${dstport} \  
${protocol} ${traffic-path} ${flow-direction} ${reject-reason}'
```

Ausnahmen von VPC-Verschlüsselungskontrollen

Der Erzwingungsmodus für VPC-Verschlüsselungskontrollen erfordert, dass alle Ihre Ressourcen in der VPC die Verschlüsselung erzwingen. Dadurch wird die Verschlüsselung innerhalb einer AWS Region gewährleistet. Möglicherweise verfügen Sie jedoch über Ressourcen wie Internet-Gateway, NAT-Gateway oder Virtual Private Gateway, die Konnektivität außerhalb AWS von Netzwerken ermöglichen, in denen Sie für die Konfiguration und Aufrechterhaltung der end-to-

end Verschlüsselung verantwortlich sind. Um diese Ressourcen mit erzwungener Verschlüsselung auszuführen VPCs, können Sie Ressourcenausschlüsse erstellen. Ein Ausschluss führt zu einer überprüfbaren Ausnahme für Ressourcen, bei denen der Kunde für die Aufrechterhaltung der Verschlüsselung verantwortlich ist (in der Regel auf Anwendungsebene).

Es gibt nur 8 unterstützte Ausnahmen für VPC Encryption Controls. Wenn Sie über diese Ressourcen in Ihrer VPC verfügen und in den Erzwingungsmodus wechseln möchten, müssen Sie diese Ausschlüsse hinzufügen, wenn Sie vom Überwachungs- in den Erzwingungsmodus wechseln. Andere Ressourcen können nicht ausgeschlossen werden. Sie können Ihre VPC in den Erzwingungsmodus migrieren, indem Sie Ausnahmen für diese Ressourcen erstellen. Sie sind für die Verschlüsselung des Datenverkehrs zu und von diesen Ressourcen verantwortlich

- Internet Gateway
- NAT-Gateway
- Internet Gateway nur für ausgehenden Datenverkehr
- VPC-Peering-Verbindungen zur Verschlüsselung sind nicht erzwungen VPCs (detaillierte Szenarien finden Sie im Abschnitt VPC-Peering-Unterstützung)
- Virtual Private Gateway
- Lambda-Funktionen in Ihrer VPC
- VPC-Gitter
- Elastisches Dateisystem

Arbeitsablauf bei der Implementierung

1. Überwachung aktivieren — VPC-Verschlüsselungssteuerung im Überwachungsmodus erstellen
2. Traffic analysieren — Überprüfen Sie die Flow-Logs, um den Verschlüsselungsstatus des Datenverkehrs zu überwachen
3. Ressourcen analysieren — Identifizieren Sie mithilfe der Konsole oder eines `GetVpcResourcesBlockingEncryptionEnforcement` Befehls die Ressourcen, die bei der Übertragung keine Verschlüsselung erzwingen.
4. Vorbereiten [Optional] — Planen Sie Ressourcenmigrationen und erforderliche Ausnahmen, wenn Sie den Erzwingungsmodus aktivieren möchten
5. Erzwingen [Optional] — Wechseln Sie in den Erzwingungsmodus, wobei die erforderlichen Ausnahmen konfiguriert sind

6. Audit — Kontinuierliche Überwachung der Einhaltung der Vorschriften mithilfe von Flow Logs

Eine ausführliche Anleitung zur Einrichtung finden Sie im Blog [Einführung in VPC-Verschlüsselungskontrollen: Verschlüsselung bei der Übertragung innerhalb und zwischen Regionen VPCs erzwingen](#).

Status der VPC-Verschlüsselung steuert

VPC-Verschlüsselungskontrollen können einen der folgenden Status haben:

creating

VPC-Verschlüsselungskontrollen werden auf der VPC erstellt.

modify-in-progress

Die VPC-Verschlüsselungssteuerung wird auf der VPC geändert

deleting

VPC-Verschlüsselungskontrollen werden auf der VPC gelöscht

available

VPC-Verschlüsselungskontrollen konnten den Überwachungsmodus oder den Erzwingungsmodus auf der VPC erfolgreich implementieren

AWS Serviceunterstützung und Kompatibilität

Um die Einhaltung der Verschlüsselungsvorschriften zu gewährleisten, muss eine Ressource stets die Verschlüsselung während der Übertragung erzwingen, entweder auf der Hardware- oder auf der Anwendungsebene. Bei den meisten Ressourcen sind keine Maßnahmen von Ihnen erforderlich.

Dienste mit automatischer Konformität

Die meisten AWS Dienste, die von unterstützt PrivateLinks werden PrivateLink, einschließlich Cross-Region, akzeptieren Datenverkehr, der auf Anwendungsebene verschlüsselt wurde. Sie müssen keine Änderungen an diesen Ressourcen vornehmen. AWS unterbricht automatisch jeglichen Datenverkehr, der dies nicht tut application-layer-encrypted. Zu einigen Ausnahmen gehören Redshift-Cluster (sowohl bereitgestellt als auch serverlos, bei denen Sie die zugrunde liegenden Ressourcen manuell migrieren müssen)

Ressourcen, die automatisch migriert werden

Network Load Balancers, Application Load Balancers, Fargate-Cluster und EKS Control Plane werden automatisch auf Hardware migriert, die Verschlüsselung nativ unterstützt, sobald Sie den Monitormodus aktivieren. Sie müssen diese Ressourcen nicht ändern. AWS wickelt die Migration automatisch ab.

Ressourcen, die eine manuelle Migration erfordern

Bestimmte VPC-Ressourcen und -Dienste erfordern, dass Sie die zugrunde liegenden Instance-Typen auswählen. Alle modernen EC2 Instances unterstützen die Verschlüsselung bei der Übertragung. Sie müssen keine Änderungen vornehmen, wenn Ihre Dienste bereits moderne EC2 Instanzen verwenden. Sie können die Konsole oder den `GetVpcResourcesBlockingEncryptionEnforcement` Befehl verwenden, um festzustellen, ob einer dieser Dienste ältere Instanzen verwendet. Wenn Sie solche Ressourcen identifizieren, müssen Sie sie auf eine der modernen EC2 Instanzen aktualisieren, die die native Verschlüsselung der Nitro-Systemhardware unterstützt. Zu diesen Services gehören EC2 Instances, Auto Scaling Groups, RDS (All Databases and Document-DB), ElastiCache Provisioned, Amazon Redshift Provisioned Clusters, EKS, ECS-, Provisioned und EMR. EC2 OpenSearch

Kompatible Ressourcen:

Die folgenden Ressourcen sind mit VPC Encryption Controls kompatibel:

- [Nitro-basierte Instanzen EC2](#)
- Network Load Balancer (mit Einschränkungen)
- Application Load Balancer
- AWS Fargate-Cluster
- Amazon Elastic Kubernetes Service (EKS)
- Amazon EC2 Auto Scaling Scaling-Gruppen
- Amazon Relational Database Service (RDS — Alle Datenbanken)
- ElastiCache Knotenbasierte Amazon-Cluster
- Von Amazon Redshift bereitgestellte und serverlose Cluster
- Amazon Elastic Container Service (ECS) — EC2 Container-Instances
- OpenSearch Amazon-Dienst
- Amazon Elastic MapReduce (EMR)

- Amazon Managed Streaming for Apache Kafka (Amazon MSK)
- VPC-Verschlüsselungskontrollen erzwingen die Verschlüsselung auf der Anwendungsebene für alle AWS Dienste, auf die über PrivateLink zugegriffen wird. Jeglicher Datenverkehr, der auf Anwendungsebene nicht verschlüsselt ist, wird von PrivateLink Endpunkten, die in der VPC gehostet werden, mit Verschlüsselungskontrollen im Erzwingungsmodus gelöscht.

Dienstspezifische Einschränkungen

Einschränkungen des Network Load Balancer

TLS-Konfiguration: Sie können einen TLS-Listener nicht verwenden, um die Arbeit der Verschlüsselung und Entschlüsselung auf Ihren Load Balancer auszulagern, wenn Sie Encryption Controls auf der enthaltenden VPC durchsetzen. Sie können Ihre Ziele jedoch so konfigurieren, dass sie die TLS-Verschlüsselung und -Entschlüsselung durchführen

Redshift bereitgestellt und serverlos

Kunden können auf einer VPC, die über einen vorhandenen Cluster/Endpunkt verfügt, nicht in den Enforce-Modus wechseln. Um VPC Encryption Controls mit Redshift zu verwenden, müssen Sie Ihren Cluster oder Namespace aus einem Snapshot wiederherstellen. Erstellen Sie für bereitgestellte Cluster einen Snapshot Ihres vorhandenen Redshift-Clusters und stellen Sie ihn dann mithilfe des Snapshot-Vorgangs „Wiederherstellung aus dem Cluster“ wieder her. Erstellen Sie für Serverless einen Snapshot Ihres vorhandenen Namespace und stellen Sie ihn dann mithilfe des Vorgangs „Wiederherstellung aus dem Snapshot“ in Ihrer serverlosen Arbeitsgruppe wieder her. Beachten Sie, dass VPC Encryption Controls nicht auf vorhandenen Clustern oder Namespaces aktiviert werden kann, ohne den Snapshot- und Wiederherstellungsprozess durchzuführen. Informationen zur Erstellung von Snapshots finden Sie in der [Amazon Redshift Redshift-Dokumentation](#).

Amazon MSK (Verwaltetes Streaming für Apache Kafka)

Diese Funktionalität wird in neuen Clustern für 4.1 in ihrer eigenen VPC unterstützt. Die folgenden Schritte helfen Ihnen bei der Verwendung von VPC-Verschlüsselung mit MSK.

- Kunde aktiviert VPC-Verschlüsselung auf einer VPC ohne andere MSK-Cluster
- Der Kunde erstellt einen Cluster mit Kafka Version 4.1 und dem Instanztyp M7g

Regional- und Zonenbeschränkungen

- Subnetze der lokalen Zone: Im Erzwingungsmodus nicht unterstützt — müssen aus der VPC gelöscht werden

VPC-Peering-Unterstützung

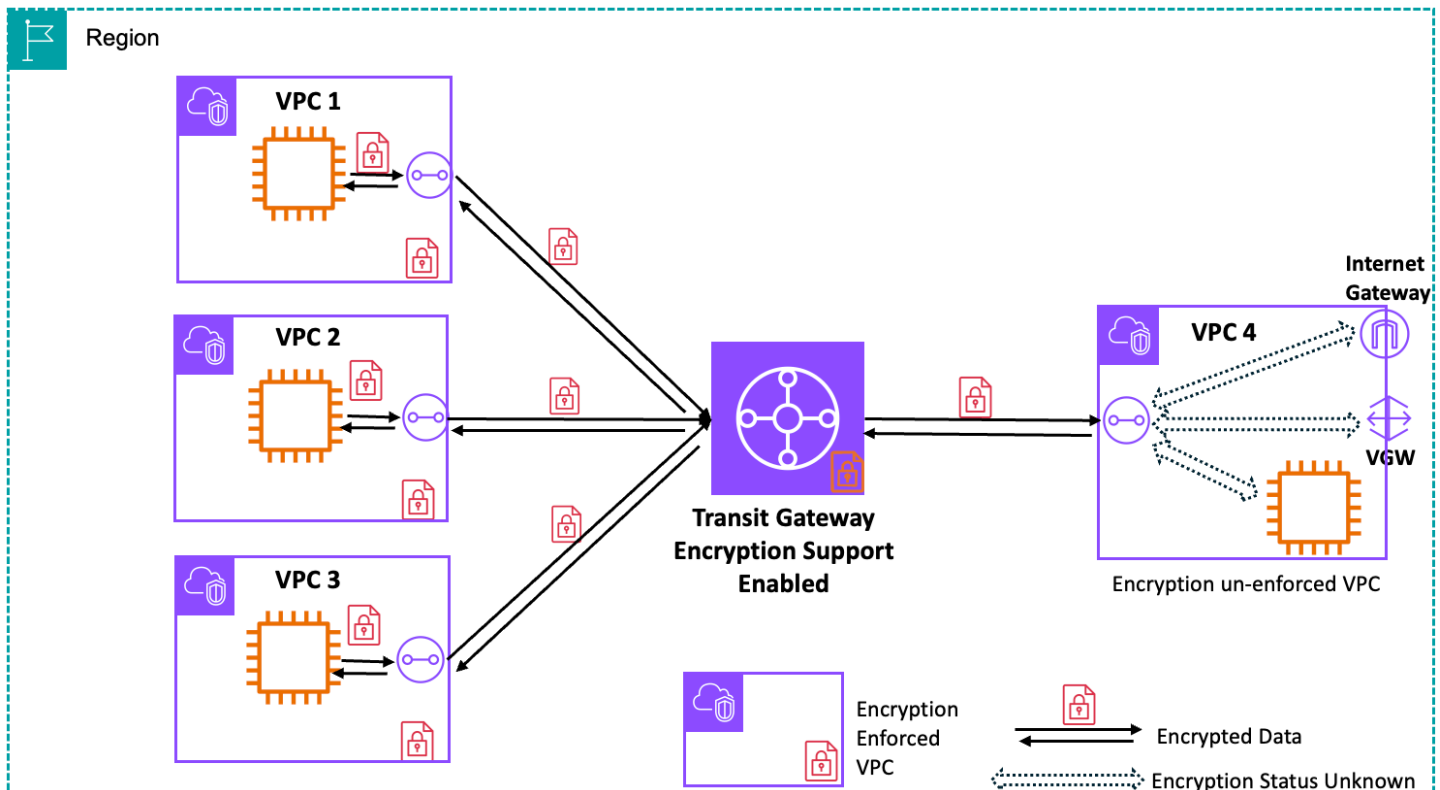
Um die Verschlüsselung während der Übertragung mit VPC-Peering zwischen zwei zu gewährleisteten VPCs, VPCs müssen sich die beiden in derselben Region befinden und die Verschlüsselungskontrollen müssen im Erzwingungsmodus ohne Ausnahmen aktiviert sein. Sie müssen einen Peering-Ausschluss erstellen, wenn Sie eine VPC mit erzwungener Verschlüsselung per Peer mit einer anderen VPC verbinden möchten, die sich entweder in einer anderen Region befindet oder für die im Erzwingungsmodus keine Verschlüsselungskontrollen aktiviert sind (ohne Ausschlüsse).

Wenn VPCs sich zwei im Erzwingungsmodus befinden und miteinander Peering betreiben, können Sie den Modus nicht von „Erzwingen“ in „Überwachen“ ändern. Sie müssten zuerst einen Peering-Ausschluss erstellen, bevor Sie den VPC Encryption Controls-Modus zur Überwachung ändern können.

Unterstützung für Transit Gateway Gateway-Verschlüsselung

Sie müssen die Verschlüsselungsunterstützung auf einem Transit Gateway explizit aktivieren, um den Verkehr zwischen Ihnen zu verschlüsseln, auf VPCs denen die Verschlüsselungssteuerung aktiviert ist. Durch die Aktivierung der Verschlüsselung auf dem vorhandenen Transit Gateway werden die bestehenden Verkehrsflüsse nicht unterbrochen, und die Migration von VPC-Anhängen zu verschlüsselten Lanes erfolgt nahtlos und automatisch. Der Verkehr zwischen zwei Personen VPCs im Erzwingungsmodus (ohne Ausschlüsse) über das Transit Gateway durchquert zu 100% verschlüsselte Spuren. Durch die Verschlüsselung auf dem Transit Gateway können Sie auch zwei Geräte miteinander verbinden VPCs , die sich ebenfalls in unterschiedlichen Encryption Controls-Modi befinden. Sie sollten es verwenden, wenn Sie Verschlüsselungskontrollen in einer VPC erzwingen möchten, die mit einer non-encryption-enforced VPC verbunden ist. In einem solchen Szenario wird Ihr gesamter Datenverkehr innerhalb Ihrer durch Verschlüsselung erzwungenen VPC, einschließlich des Datenverkehrs zwischen den VPCs, verschlüsselt. Der Datenverkehr zwischen den VPCs wird zwischen den Ressourcen in der durch Verschlüsselung erzwungenen VPC und dem Transit Gateway verschlüsselt. Darüber hinaus hängt die Verschlüsselung von den Ressourcen ab, zu denen der Datenverkehr in der nicht erzwungenen VPC geleitet wird, und es kann nicht garantiert

werden, dass sie verschlüsselt ist (da sich die VPC nicht im Erzwingungsmodus befindet). Alle VPCs müssen sich in derselben Region befinden. (Einzelheiten finden Sie [hier](#)).



- In diesem Diagramm VPC3 haben VPC 1, VPC 2 und VPC Verschlüsselungssteuerungen im Erzwingungsmodus und sie sind mit VPC 4 verbunden, auf der Encryption Controls im Überwachungsmodus ausgeführt werden.
- Der gesamte Datenverkehr zwischen VPC1 VPC2 und VPC3 wird verschlüsselt.
- Zur Erläuterung: Jeder Datenverkehr zwischen einer Ressource in VPC 1 und einer Ressource in VPC 4 wird bis zum Transit Gateway mit der von der Nitro-Systemhardware angebotenen Verschlüsselung verschlüsselt. Darüber hinaus hängt der Verschlüsselungsstatus von der Ressource in VPC 4 ab und es kann nicht garantiert werden, dass sie verschlüsselt ist.

Weitere Informationen zur Unterstützung der Transit Gateway Gateway-Verschlüsselung finden Sie in [der Transit-Gateway-Dokumentation](#).

Preisgestaltung

Preisinformationen finden Sie unter [Amazon VPC-Preise](#).

AWS CLI Befehlsreferenz

Einrichtung und Konfiguration

- [aws ec2 create-vpc-encryption-control](#)
- [war ec2 modify-vpc-encryption-control](#)
- [als ec2 tgw modify-transit-gateway](#)

Überwachung und Fehlerbehebung

- [aws ec2 describe-vpc-encryption-controls](#)
- [aws get-vpc-resources-blocking ec2 — Durchsetzung der Verschlüsselung](#)
- [aws ec2 create-flow-logs](#)
- [war ec2 describe-flow-logs](#)
- [AWS-Protokollabfrage](#)

Bereinigen

- [aws ec2 delete-vpc-encryption-control](#)

Weitere Ressourcen

Eine ausführliche Anleitung zur Einrichtung finden Sie im Blog [Einführung in VPC-Verschlüsselungskontrollen: Verschlüsselung bei der Übertragung innerhalb und zwischen Regionen VPCs erzwingen](#).

Ausführlichere API-Informationen finden Sie im [EC2 API-Referenzhandbuch](#).

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](#)
- [Authentifizieren mit Identitäten](#)
- [Verwalten des Zugriffs mithilfe von Richtlinien.](#)
- [Funktionsweise von der Amazon VPC mit IAM](#)
- [Beispiele für Amazon VPC-Richtlinien](#)
- [Fehlerbehebung für Amazon VPC-Identität und -Zugriff](#)
- [AWS verwaltete Richtlinien für Amazon Virtual Private Cloud](#)
- [Verwenden von serviceverknüpften Rollen für VPC](#)

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 sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter [So melden Sie sich bei Ihrem AWS-Konto an](#) im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter [AWS Signature Version 4 for API requests](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Tasks that require root user credentials](#) im IAM-Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Verwenden Sie möglichst temporäre Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter [Erfordern, dass menschliche Benutzer für den Zugriff AWS mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter](#) verwenden müssen.

Eine [IAM-Gruppe](#) spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter [Anwendungsfälle für IAM-Benutzer](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie [von einer Benutzer-](#)

[zu einer IAM-Rolle \(Konsole\) wechseln](#) AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter [Methoden, um eine Rolle zu übernehmen](#) im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für Verbundbenutzerzugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, dienstübergreifenden Zugriff und Anwendungen, die auf Amazon ausgeführt werden. EC2 Weitere Informationen finden Sie unter [Kontoübergreifender Ressourcenzugriff in IAM](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mithilfe von Richtlinien.

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an Identitäten oder Ressourcen anhängen. AWS Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcen und unter welchen Bedingungen durchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind) sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter [Choose between managed policies and inline policies](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen 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. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#).

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

Zugriffskontrolllisten () ACLs

Zugriffskontrolllisten (ACLs) steuern, welche Principals (Kontomitglieder, Benutzer oder Rollen) über Zugriffsberechtigungen für eine Ressource verfügen. ACLs ähneln ressourcenbasierten Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Dienste, die Unterstützung ACLs bieten. AWS WAF Weitere Informationen finden Sie unter [Übersicht über ACLs die Zugriffskontrollliste \(ACL\)](#) im Amazon Simple Storage Service Developer Guide.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im -IAM-Benutzerhandbuch.
- **Richtlinien zur Dienstkontrolle (SCPs)** — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter [Service-Kontrollrichtlinien](#) im AWS Organizations -Benutzerhandbuch.
- **Richtlinien zur Ressourcenkontrolle (RCPs)** — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter [Richtlinien zur Ressourcenkontrolle \(RCPs\)](#).
- **Sitzungsrichtlinien** – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die daraus resultierenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter [Bewertungslogik für Richtlinien](#) im IAM-Benutzerhandbuch.

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

- [Aktionen](#)
- [Ressourcen](#)
- [Bedingungsschlüssel](#)
- [Ressourcenbasierte Amazon VPC-Richtlinien](#)
- [Autorisierung auf der Basis von Markierungen](#)
- [IAM-Rollen](#)

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 Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs 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 der Amazon VPC-Aktionen finden Sie unter [Von Amazon definierte Aktionen EC2](#) in der Service Authorization Reference.

Ressourcen

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

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, 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 EC2 Amazon-API-Aktionen beinhalten mehrere Ressourcen. Um mehrere Ressourcen in einer einzigen Anweisung anzugeben, trennen Sie sie ARNs durch Kommas.

```
"Resource": [  
    "resource1",  
    "resource2"  
]
```

Eine Liste der Amazon VPC-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter [Von Amazon definierte Ressourcentypen EC2](#) in der Service Authorization Reference.

Bedingungsschlüssel

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

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. 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. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Alle EC2 Amazon-Aktionen unterstützen die Tasten `aws:RequestedRegion` und `ec2:Region` Condition. 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 der Amazon VPC-Bedingungsschlüssel finden Sie unter [Bedingungsschlüssel für Amazon EC2](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter [Von Amazon definierte Aktionen EC2](#).

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 Prinzipaleinheit 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 [Kontoübergreifender Ressourcenzugriff in IAM](#) 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 [Bedingungelement](#) einer Richtlinie mithilfe von Bedingungsschlüsseln Tag-Informationen an. Weitere Informationen finden Sie im EC2 Amazon-Benutzerhandbuch unter Erteilen der [Erlaubnis, Ressourcen während der Erstellung zu kennzeichnen](#).

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 [AssumeRole](#) oder [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-Managementkonsole 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

- [Best Practices für Richtlinien](#)
- [Verwenden der Amazon VPC-Konsole.](#)
- [Erstellen einer VPC mit einem öffentlichen Subnetz](#)
- [Ändern und Löschen von VPC-Ressourcen](#)
- [Verwalten von Sicherheitsgruppen](#)
- [Sicherheitsgruppenregeln verwalten](#)
- [Starten von Instances in einem bestimmten Subnetz](#)
- [Starten von Instances in einer bestimmten VPC](#)
- [Sperrt den öffentlichen Zugriff VPCs auf Subnetze](#)
- [Weitere Beispiele für Amazon VPC-Richtlinien](#)

Best Practices 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. Beachten Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Richtlinien 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 [Von AWS verwaltete Richtlinien](#) oder [Von AWS verwaltete Richtlinien für Auftragsfunktionen](#) 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. 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 [Richtlinienvvalidierung mit 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 [Sicherer API-Zugriff mit MFA](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Best Practices 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 Minimalsatz 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.

JSON

```
{
  "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 Subnetze VPCs, 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.

JSON

```

{
  "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.

JSON

```

{
  "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.

JSON

```
{
  "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"
        },
        "ForAnyValue: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.

JSON

```
{
  "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:us-east-1:123456789012:security-group/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Vpc": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSecurityGroupRules",
        "ec2:DescribeTags"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifySecurityGroupRules"
      ],
      "Resource": "arn:aws:ec2:us-east-1:123456789012: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.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:us-east-1::image/ami-*",
        "arn:aws:ec2:us-east-1:123456789012:instance/*",
        "arn:aws:ec2:us-east-1:123456789012:subnet/subnet-1234567890abcdef0",
        "arn:aws:ec2:us-east-1:123456789012:network-interface/*",
        "arn:aws:ec2:us-east-1:123456789012:volume/*",
        "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
        "arn:aws:ec2:us-east-1:123456789012:security-group/sg-0abcdef1234567890"
      ]
    }
  ]
}
```

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.

Die Richtlinie gewährt Rollen außerdem die Erlaubnis, nur Instances zu starten AMIs, die das Tag "department=dev" verwenden.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:us-east-1:123456789012:subnet/*",
      "Condition": {
        "ArnEquals": {
          "ec2:Vpc": "arn:aws:ec2:us-east-1:123456789012:vpc/vpc-1234567890abcdef0"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:us-east-1::image/ami-*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/department": "dev"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": "ec2:RunInstances",
      "Resource": [
        "arn:aws:ec2:us-east-1:123456789012:instance/*",
        "arn:aws:ec2:us-east-1:123456789012:volume/*",
        "arn:aws:ec2:us-east-1:123456789012:network-interface/*",

```

```

        "arn:aws:ec2:us-east-1:123456789012:key-pair/*",
        "arn:aws:ec2:us-east-1:123456789012:security-group/*"
    ]
}

```

Sperrt den öffentlichen Zugriff VPCs auf Subnetze

Die folgenden Richtlinienbeispiele gewähren Rollen die Erlaubnis, mit der [VPC-Funktion Block Public Access \(BPA\)](#) zu arbeiten, um den öffentlichen Zugriff auf Ressourcen in VPCs und Subnetzen zu blockieren.

Beispiel 1: Erlauben Sie den schreibgeschützten Zugriff auf Kontoeinstellungen für VPC BPA und VPC-BPA-Ausschlüsse.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VPCBPAREadOnlyAccess",
      "Action": [
        "ec2:DescribeVpcBlockPublicAccessOptions",
        "ec2:DescribeVpcBlockPublicAccessExclusions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}

```

Beispiel 2: Erlauben Sie den vollständigen Lese- und Schreibzugriff auf die Kontoeinstellungen für VPC BPA und die VPC-BPA-Ausschlüsse.

JSON

```

{

```

```
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "VPCBPAPFullAccess",
    "Action": [
      "ec2:DescribeVpcBlockPublicAccessOptions",
      "ec2:DescribeVpcBlockPublicAccessExclusions",
      "ec2:ModifyVpcBlockPublicAccessOptions",
      "ec2:CreateVpcBlockPublicAccessExclusion",
      "ec2:ModifyVpcBlockPublicAccessExclusion",
      "ec2>DeleteVpcBlockPublicAccessExclusion"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
```

Beispiel 3 — Erlauben Sie den Zugriff auf alle, EC2 APIs mit Ausnahme der Änderung der VPC BPA-Einstellungen und der Erstellung von Ausnahmen.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EC2FullAccess",
      "Action": [
        "ec2:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "VPCBPAPartialAccess",
      "Action": [
        "ec2:ModifyVpcBlockPublicAccessOptions",
        "ec2:CreateVpcBlockPublicAccessExclusion"
      ],
      "Effect": "Deny",
      "Resource": "*"
    }
  ]
}
```

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

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-Endpunkt-Services \(AWS PrivateLink\)](#)
- [VPC-Peering](#)

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-Managementkonsole 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, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu 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 in AWS-Konten Ihrem Besitz gewähren können, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen AWS-Konto , dem Sie](#) gehören.
- 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 [Kontoübergreifender Ressourcenzugriff in IAM](#) 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 sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

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

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (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: Amazon VPCFull Access

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 [Amazon VPCFull Access](#) in der Referenz für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: Amazon VPCRead OnlyAccess

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 [Amazon VPCRead OnlyAccess](#) in der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: Amazon VPCCross AccountNetworkInterfaceOperations

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 [Amazon VPCCross AccountNetworkInterfaceOperations](#) in der Referenz zu AWS verwalteten Richtlinien.

AWS verwaltete Richtlinie: AWSService RoleFor NATGateway

Sie können die AWSServiceRoleForNATGateway-Richtlinie an Ihre IAM-Identitäten anfügen. Diese Richtlinie gewährt Berechtigungen, die es der Identität ermöglichen, in Ihrem Namen zu arbeiten, um regionale NAT-Gateways automatisch zu skalieren.

Informationen zu den Berechtigungen für diese Richtlinie finden Sie unter [AWSServiceRoleForNATGateway](#) in der Referenz zu von AWS verwalteten 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.

Änderungen	Beschreibung	Datum
the section called “VPCFullZ ugriff auf Amazon” – Aktualisierung auf eine bestehende Richtlinie	Der AWSIPAMService RolePolicy verwalteten Richtlinie (ec2:ModifyManagedPrefixList, undec2:Ge	31. Oktober 2025

Änderungen	Beschreibung	Datum
	tManagedPrefixListEntries) wurden Aktionen hinzugefügt: DescribeManagedPrefixLists, um IPAM das Ändern und Lesen verwalteter Präfixlisten zu ermöglichen.	
the section called “AWSServiceRoleForNATGateway” – Neue Richtlinie	Eine neue AWSServiceRoleForNATGateway Richtlinie ermöglicht es der Identität, regionale NAT-Gateways automatisch zu skalieren.	19. November 2025
the section called “VPCFullIzugriff auf Amazon” – Aktualisierung auf eine bestehende Richtlinie	Die DisassociateSecurityGroupVpc Aktionen AssociateSecurityGroupVpcDescribeSecurityGroupVpcAssociations, und wurden hinzugefügt, mit VPCs denen Sie Zuordnungen zu Sicherheitsgruppen zuordnen, trennen und anzeigen können.	9. Dezember 2024
the section called “AmazonVPCRead OnlyAccess” – Aktualisierung auf eine bestehende Richtlinie	Die DescribeSecurityGroupVpcAssociations Aktion wurde hinzugefügt, mit der Sie Sicherheitsgruppenzuordnungen zu anzeigen können VPCs.	9. Dezember 2024
the section called “VPCFullIzugriff auf Amazon” – Aktualisierung auf eine bestehende Richtlinie	Die Aktion GetSecurityGroupsForVpc wurde hinzugefügt, mit der Sie Sicherheitsgruppen abrufen können, die in Ihrer VPC verwendet werden können.	8. Februar 2024

Änderungen	Beschreibung	Datum
the section called “Amazon VPCRead OnlyAccess” – Aktualisierung auf eine bestehende Richtlinie	Die Aktion GetSecurityGroupsForVpc wurde hinzugefügt, mit der Sie Sicherheitsgruppen abrufen können, die in Ihrer VPC verwendet werden können.	8. Februar 2024
the section called “Amazon VPCCross AccountNetworkInterfaceOperations” – Aktualisierung auf eine bestehende Richtlinie	Die UnassignIpv6Addresses Aktionen AssignIpv6Addresses und, mit denen Sie die IPv6 Adressen verwalten können, die Netzwerkschnittstellen zugeordnet sind, wurden hinzugefügt.	25. September 2023
the section called “Amazon VPCRead OnlyAccess” – Aktualisierung auf eine bestehende Richtlinie	Die DescribeSecurityGroupRules-Aktion wurde hinzugefügt, mit der Sie Sicherheitsgruppen regeln anzeigen können.	2. August 2021
the section called “VPCFullZugriff auf Amazon” – Aktualisierung auf eine bestehende Richtlinie	Die DescribeSecurityGroupRules- und ModifySecurityGroupRules-Aktionen wurden hinzugefügt, mit denen Sie Sicherheitsgruppen regeln anzeigen und ändern können.	2. August 2021
the section called “VPCFullZugriff auf Amazon” – Aktualisierung auf eine bestehende Richtlinie	Es wurden Aktionen für Carrier-Gateways, IPv6 Pools, lokale Gateways und lokale Gateway-Routentabellen hinzugefügt.	23. Juni 2021

Änderungen	Beschreibung	Datum
the section called “Amazon VPCRead OnlyAccess” – Aktualisierung auf eine bestehende Richtlinie	Es wurden Aktionen für Carrier-Gateways, IPv6 Pools, lokale Gateways und lokale Gateway-Routentabellen hinzugefügt.	23. Juni 2021

Verwenden von serviceverknüpften Rollen für VPC

Amazon VPC verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist ein einzigartiger Typ von IAM-Rolle, die direkt mit VPC verknüpft ist. Dienstverknüpfte Rollen sind von VPC vordefiniert und enthalten alle Berechtigungen, die der Dienst benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von VPC, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. VPC definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur VPC ihre Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre VPC-Ressourcen, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entfernen können.

Informationen zu anderen Diensten, die dienstverknüpfte Rollen unterstützen, finden Sie unter [AWS Dienste, die mit IAM funktionieren](#). Suchen Sie in der Spalte Dienstverknüpfte Rollen nach den Diensten, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Dienstbezogene Rollenberechtigungen für VPC

VPC verwendet die serviceverknüpfte Rolle mit dem Namen `AWSServiceRoleForNATGateway`—Diese serviceverknüpfte Rolle ermöglicht es Amazon VPC, in Ihrem Namen Elastic IP-Adressen zuzuweisen, um regionale NAT-Gateways automatisch zu skalieren, Ihre vorhandenen Elastic auf Anfrage regionalen NAT-Gateways zuzuordnen und IPs zu trennen und Netzwerkschnittstellen zu beschreiben, um Ihre bestehende Infrastruktur zu identifizieren und automatisch in neue Availability Zones zu expandieren.

Die AWSService RoleFor NATGateway serviceverknüpfte Rolle vertraut darauf, dass die folgenden Services die Rolle übernehmen:

- `ec2-nat-gateway.amazonaws.com`

Die genannte Rollenberechtigungsrichtlinie AWSNATGateway ServiceRolePolicy ermöglicht es VPC, die folgenden Aktionen für die angegebenen Ressourcen durchzuführen:

- Aktion: `AllocateAddress` auf Service Managed EIPs , um die Zuteilung in EIPs Ihrem Namen vorzunehmen. Service Managed EIPs verarbeitet das nachfolgende Tagging mit vom Service verwalteten Tags automatisch. `ReleaseAddress`
- Aktion: `AssociateAddress` auf Ihre bereits vorhandenen Elastic IP-Adressen, um sie auf Anfrage manuell Ihrem regionalen NAT-Gateway zuzuordnen.
- Aktion: `DisassociateAddress` auf Ihre bereits vorhandenen Elastic IP-Adressen, um sie auf Anfrage aus dem regionalen NAT-Gateway zu entfernen.
- Aktion: `DescribeAddresses` Um öffentliche IP-Adressinformationen von einem Kunden zu erhalten, die Ihnen ein Mitarbeiter EIPs zur Verfügung gestellt hat.
- Aktion: `DescribeNetworkInterface` Auf Ihren vorhandenen Netzwerkschnittstellen zur automatischen Identifizierung der Availability Zones, in denen sich Ihre Infrastruktur befindet, und zur automatischen Skalierung auf neue Zonen.

Sie müssen Berechtigungen konfigurieren, damit eine Benutzer, Gruppen oder Rollen eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen können. Weitere Informationen finden Sie unter [serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für VPC erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein NAT-Gateway mit einem „regionalen“ Verfügbarkeitsmodus in der AWS-Managementkonsole, der oder der AWS API erstellen AWS CLI, erstellt VPC die serviceverknüpfte Rolle für Sie.

Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Wenn Sie den VPC-Dienst vor dem 1. Januar 2017 verwendet haben, als er begann, serviceverknüpfte Rollen zu unterstützen, hat VPC die AWSService RoleFor

NATGateway Rolle außerdem in Ihrem Konto erstellt. Weitere Informationen finden Sie unter [Eine neue Rolle ist in meinem erschienen](#). AWS-Konto

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie ein NAT-Gateway mit einem „regionalen“ Verfügbarkeitsmodus erstellen, erstellt VPC die serviceverknüpfte Rolle erneut für Sie.

Sie können auch die IAM-Konsole verwenden, um eine serviceverknüpfte Rolle mit dem Anwendungsfall zu erstellen. `AWSServiceRoleForNATGateway` Erstellen Sie in der AWS CLI oder der AWS API eine dienstverknüpfte Rolle mit dem `ec2-nat-gateway.amazonaws.com` Dienstnamen. Weitere Informationen finden Sie unter [Erstellen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch. Wenn Sie diese serviceverknüpfte Rolle löschen, können Sie mit demselben Verfahren die Rolle erneut erstellen.

Bearbeiten einer serviceverknüpften Rolle für VPC

In VPC können Sie die `AWSServiceRoleForNATGateway` serviceverknüpfte Rolle nicht bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für VPC

Wenn Sie ein Feature oder einen Service, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte Entität, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch die Ressourcen für Ihre serviceverknüpfte Rolle zunächst bereinigen, bevor Sie sie manuell löschen können.

Note

Wenn der VPC-Dienst die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

Um VPC-Ressourcen zu löschen, die verwendet werden von AWSService RoleFor NATGateway

- Löschen Sie alle regionalen NAT-Gateways in allen Regionen, in denen sie bereitgestellt wurden.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die oder die AWS API AWS CLI, um die AWSService RoleFor NATGateway serviceverknüpfte Rolle zu löschen. Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Unterstützte Regionen für dienstverknüpfte VPC-Rollen

VPC unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [AWS -Regionen und Endpunkte](#).

VPC unterstützt nicht die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Sie können die AWSService RoleFor NATGateway Rolle in den folgenden Regionen verwenden.

Name der Region	Regions-ID	Support in VPC
USA Ost (Nord-Virginia)	us-east-1	Ja
USA Ost (Ohio)	us-east-2	Ja
USA West (Nordkalifornien)	us-west-1	Ja
USA West (Oregon)	us-west-2	Ja
Afrika (Kapstadt)	af-south-1	Ja
Asien-Pazifik (Hongkong)	ap-east-1	Ja
Asien-Pazifik (Taipeh)	ap-east-2	Ja
Asien-Pazifik (Jakarta)	ap-southeast-3	Ja
Asien-Pazifik (Mumbai)	ap-south-1	Ja
Asien-Pazifik (Hyderabad)	ap-south-2	Ja

Name der Region	Regions-ID	Support in VPC
Asien-Pazifik (Osaka)	ap-northeast-3	Ja
Asien-Pazifik (Seoul)	ap-northeast-2	Ja
Asien-Pazifik (Singapore)	ap-southeast-1	Ja
Asien-Pazifik (Sydney)	ap-southeast-2	Ja
Asien-Pazifik (Tokyo)	ap-northeast-1	Ja
Asien-Pazifik (Melbourne)	ap-southeast-4	Ja
Asien-Pazifik (Malaysia)	ap-southeast-5	Ja
Asien-Pazifik (Neuseeland)	ap-southeast-6	Ja
Asien-Pazifik (Thailand)	ap-southeast-7	Ja
Kanada (Zentral)	ca-central-1	Ja
Kanada West (Calgary)	ca-west-1	Ja
Europa (Frankfurt)	eu-central-1	Ja
Europa (Zürich)	eu-central-2	Ja
Europa (Irland)	eu-west-1	Ja
Europa (London)	eu-west-2	Ja
Europa (Milan)	eu-south-1	Ja
Europa (Spain)	eu-south-2	Ja
Europa (Paris)	eu-west-3	Ja
Europa (Stockholm)	eu-north-1	Ja
Israel (Tel Aviv)	il-central-1	Ja

Name der Region	Regions-ID	Support in VPC
Naher Osten (Bahrain)	me-south-1	Ja
Naher Osten (VAE)	me-central-1	Ja
Naher Osten (Saudi-Arabien)	me-west-1	Ja
Mexiko (Zentral)	mx-central-1	Ja
Südamerika (São Paulo)	sa-east-1	Ja
AWS GovCloud (US-Ost)	us-gov-east-1	Nein
AWS GovCloud (US-West)	us-gov-west-1	Nein

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.

Netzwerkisolierung

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk in Ihrem eigenen logisch isolierten Bereich in der AWS Cloud. Verwenden Sie VPCs es separat, um die Infrastruktur nach Arbeitslast oder organisatorischer Einheit 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 PrivateLink](#) damit 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

Ziehen Sie die folgenden Optionen zur Steuerung des Netzwerkverkehrs zu den Ressourcen in Ihrer VPC, wie z. B. EC2 Instances, in Betracht:

- Verwenden Sie [Sicherheitsgruppen](#) als primären Mechanismus zur Steuerung des Netzwerkzugriffs auf Ihre VPCs. Verwenden Sie bei Bedarf das [Netzwerk](#), ACLs um eine zustandslose, grobe Netzwerksteuerung zu ermöglichen. Sicherheitsgruppen sind vielseitiger als Netzwerke ACLs, da sie statusbehaftete Pakete filtern und Regeln erstellen können, die auf andere Sicherheitsgruppen verweisen. Das Netzwerk ACLs kann als sekundäre Kontrolle (z. B. zur Abwehr einer bestimmten Teilmenge des Datenverkehrs) oder als Schutzwall für Subnetze auf hoher Ebene eingesetzt werden. Da Netzwerke ACLs für ein ganzes Subnetz gelten, können sie auch so verwendet werden, als ob defense-in-depth eine Instance jemals ohne die richtige Sicherheitsgruppe gestartet wird.
- 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 Netzwerkrouuten, um Ihre Konnektivitätsanforderungen zu erfüllen.
- Erwägen Sie die Verwendung zusätzlicher Sicherheitsgruppen oder Netzwerkschnittstellen, um den Datenverkehr der EC2 Amazon-Instance-Verwaltung getrennt vom regulären Anwendungsdatenverkehr zu kontrollieren 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 Direct Connect , um private Verbindungen von Ihren Remote-Netzwerken zu Ihren herzustellen VPCs. Weitere Informationen finden Sie unter [Network-to-Amazon VPC-Konnektivitätsoptionen](#).
- Verwenden Sie [VPC Flow-Protokolle](#), um den Datenverkehr zu überwachen, der Ihre Instances erreicht.
- Verwenden Sie [AWS Security Hub CSPM](#), 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.

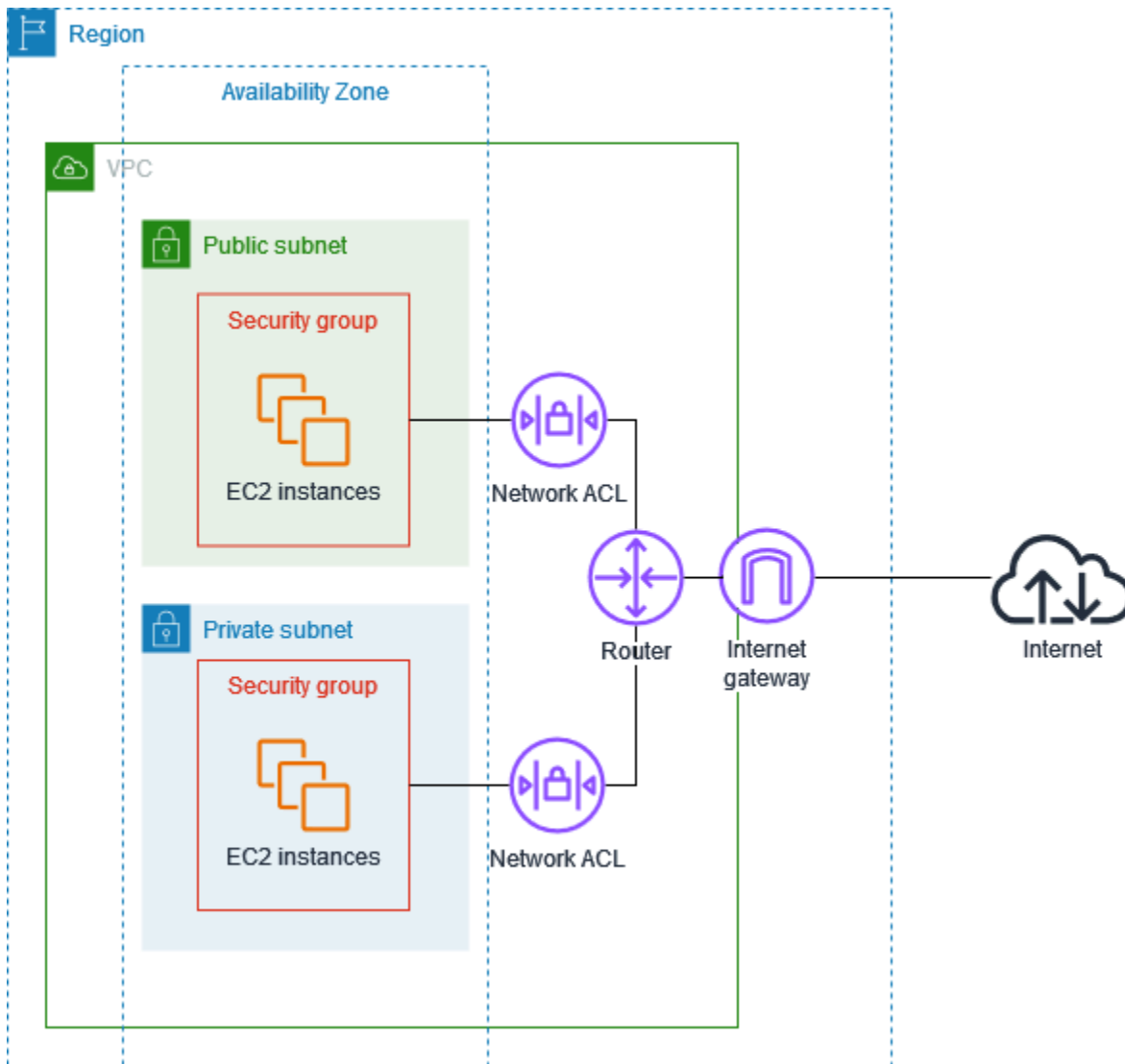
Vergleichen Sie Sicherheitsgruppen und Netzwerk ACLs

In der folgenden Tabelle sind die grundlegenden Unterschiede zwischen Sicherheitsgruppen und Netzwerken ACLs zusammengefasst.

Merkmal	Sicherheitsgruppe	Netzwerk-ACL
Betriebsniveau	Instance-Ebene	Subnetzniveau
Scope	Gilt für alle Instances, die mit der Sicherheitsgruppe verbunden sind.	Gilt für alle Instances in den verbundenen Subnetzen
Art der Regel	Nur Regeln zulassen	Zulassen- und Verweigern-Regeln
Regelauswertung	Alle Regeln werden vor dem Erlauben von Datenverkehr ausgewertet.	Bewertet Regeln in aufsteigender Reihenfolge, bis eine Übereinstimmung für den Datenverkehr gefunden wird
Datenverkehr zurücksenden	Automatisch zugelassen (zustands behaftet)	Muss ausdrücklich erlaubt sein (zustandslos)

Das folgende Diagramm zeigt die Sicherheitsebenen, die von Sicherheitsgruppen und Netzwerken bereitgestellt ACLs 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.



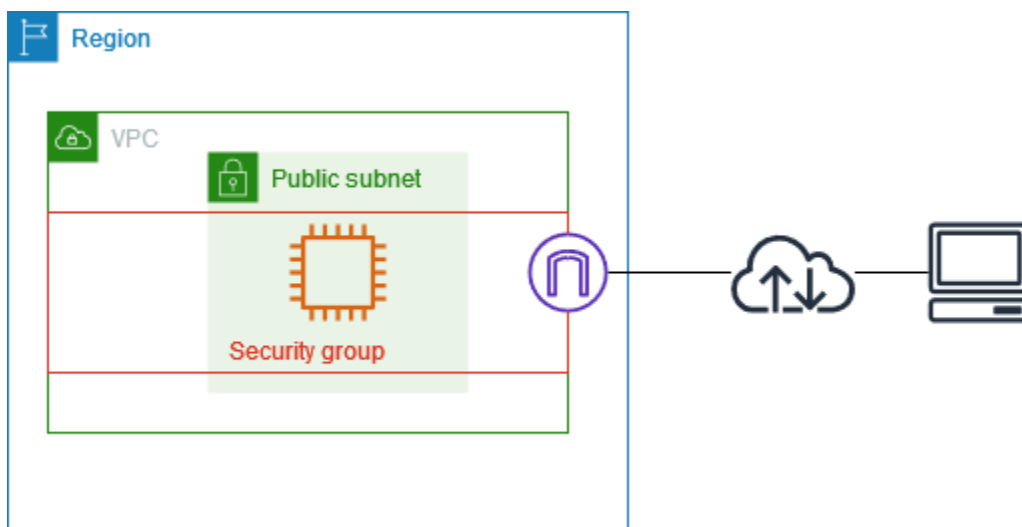
Sie können Ihre Instances nur mit Sicherheitsgruppen sichern. Sie können jedoch ein Netzwerk ACLs als zusätzliche Verteidigungsebene hinzufügen. Weitere Informationen finden Sie unter [Beispiel: Steuern des Zugriffs auf Instances in einem Subnetz](#).

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. Wenn Sie beispielsweise einer EC2 Instance eine Sicherheitsgruppe zugeordnet haben, steuert diese den eingehenden 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 Instanz. EC2 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

- [Sicherheitsgruppengrundlagen](#)
- [Beispiel für eine Sicherheitsgruppe](#)

- [Sicherheitsgruppenregeln](#)
- [Standard-Sicherheitsgruppen für Ihre VPCs](#)
- [Erstellen einer Sicherheitsgruppe für Ihre VPC](#)
- [Konfigurieren von Sicherheitsgruppenregeln](#)
- [Löschen einer Sicherheitsgruppe](#)
- [Ordnen Sie Sicherheitsgruppen mehreren zu VPCs](#)
- [Sicherheitsgruppen mit AWS Organizations teilen](#)

Preisgestaltung

Für die Nutzung von Sicherheitsgruppen fallen keine zusätzlichen Gebühren an.

Sicherheitsgruppengrundlagen

- Sie können eine Sicherheitsgruppe Ressourcen zuweisen, die in derselben VPC wie die Sicherheitsgruppe erstellt wurden, oder Ressourcen in einer anderen, VPCs wenn Sie die [Sicherheitsgruppe mithilfe der Funktion Security Group VPC Association](#) anderen VPCs in derselben Region zuordnen. Sie können auch 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.
 - Bei Namen von Sicherheitsgruppen wird nicht zwischen Groß- und Kleinschreibung unterschieden.
 - 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)
 - EC2 Amazon-Instanz-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](#).

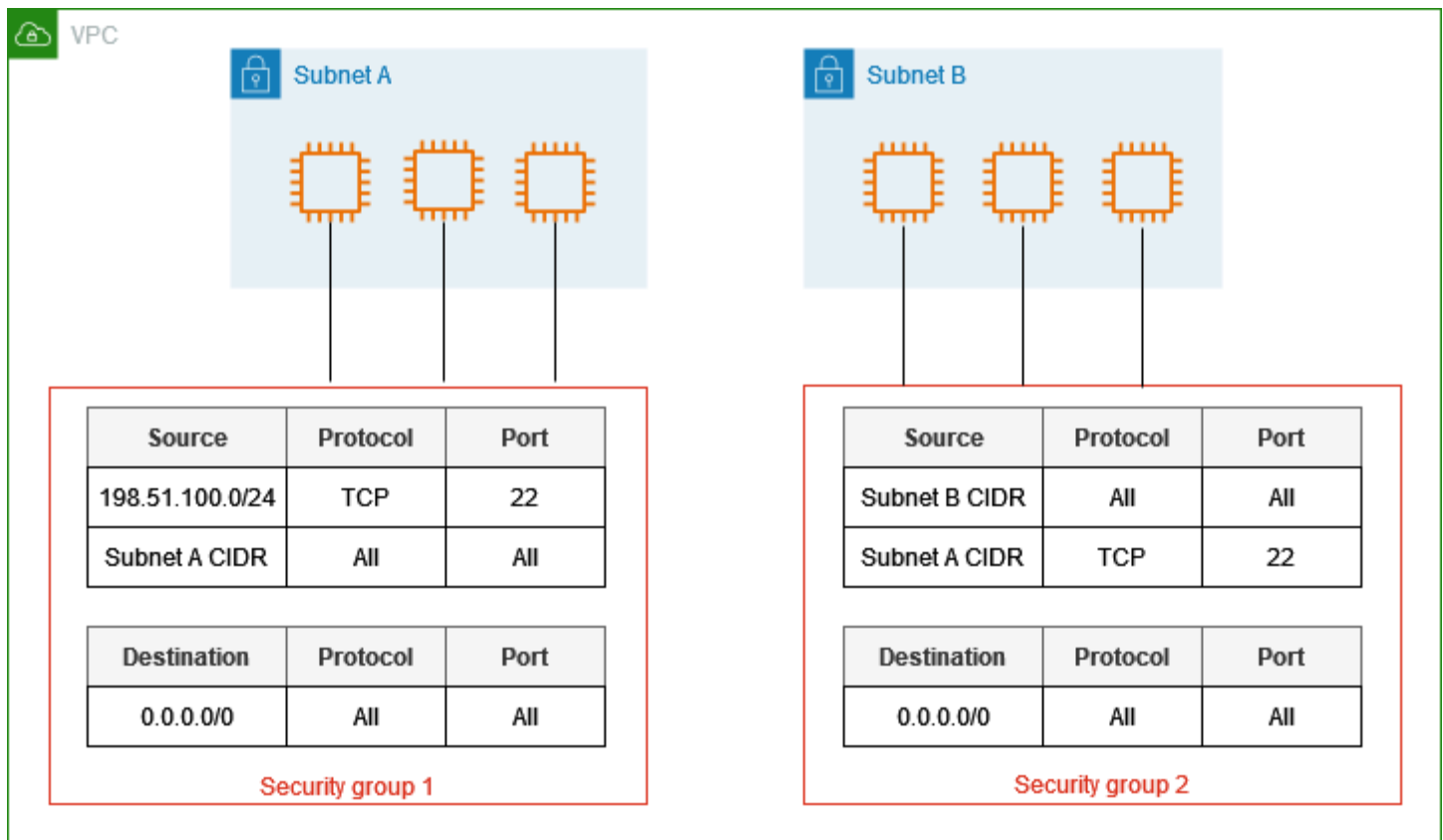
Best Practices

- 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 Regeln für eingehenden Datenverkehr für die Ports 22 (SSH) oder 3389 (RDP) hinzufügen, damit Sie auf Ihre EC2 Instances zugreifen können, autorisieren Sie nur bestimmte IP-Adressbereiche. Wenn Sie 0.0.0.0/0 (IPv4) und: :/ (IPv6) angeben, kann jeder mit dem angegebenen Protokoll von jeder IP-Adresse aus 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.
- Erwägen Sie die Einrichtung eines Netzwerks ACLs mit Regeln, die Ihren Sicherheitsgruppen ähneln, um Ihrer VPC eine zusätzliche Sicherheitsebene hinzuzufügen. Weitere Informationen zu den Unterschieden zwischen Sicherheitsgruppen und Netzwerken finden Sie ACLs unter [Vergleichen Sie 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](#)
- [Komponenten einer Sicherheitsgruppenregel](#)
- [Referenzierung von Sicherheitsgruppen](#)
- [Größe der Sicherheitsgruppe](#)
- [Veraltete Sicherheitsgruppenregeln](#)

Sicherheitsgruppen – Grundlagen für Regeln

Es folgen die grundlegenden Merkmale von Sicherheitsgruppenregeln:

- 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. Detaillierte Anweisungen finden Sie unter [Konfigurieren von Sicherheitsgruppenregeln](#).
- Die Auswirkung einiger Regeländerungen kann davon abhängen, wie der Datenverkehr nachverfolgt wird. Weitere Informationen finden Sie unter [Verbindungsverfolgung](#) im EC2 Amazon-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“ \(siehe Amazon Route 53 Resolver im Amazon Route 53 Developer Guide\) oder als DNS bezeichnet wird. AmazonProvided](#) Um DNS-Anfragen durch den Route 53 Resolver zu filtern, verwenden Sie die [DNS-Firewall des Route 53 Resolver](#).

Komponenten einer Sicherheitsgruppenregel

Nachfolgend sind die Komponenten der Regeln für eingehende und ausgehende Sicherheitsgruppen aufgeführt:

- **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-Echoanforderung oder Typ 128 für Echoanforderung. ICMPv6 Weitere Informationen finden Sie unter [Regeln für Ping/ICMP](#) im EC2 Amazon-Benutzerhandbuch.
- **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 einzige Adresse. IPv4 Sie müssen die /32-Präfixlänge verwenden. Beispiel, 203.0.113.1/32.
 - Eine einzige IPv6 Adresse. Sie müssen die /128-Präfixlänge verwenden. Beispiel, 2001:db8:1234:1a00::123/128.
 - Ein IPv4 Adressbereich in CIDR-Blocknotation. Beispiel, 203.0.113.0/24.
 - Ein IPv6 Adressbereich in CIDR-Blocknotation. Beispiel, 2001:db8:1234:1a00::/64.
 - Die ID einer Präfixliste. Beispiel, p1-1234abc1234abc123. Weitere Informationen finden Sie unter [Verwaltete Präfixlisten](#).
 - Die ID einer Sicherheitsgruppe. Beispiel, 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 ._-:/()#,@[]+=;{}!\$*.

Beispiele finden Sie unter [Sicherheitsgruppenregeln für verschiedene Anwendungsfälle](#) im EC2 Amazon-Benutzerhandbuch.

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
<code>sg-0abcdef1234567890</code>	TCP	22

Berücksichtigen Sie Folgendes, wenn Sie in einer Sicherheitsgruppenregel auf eine Sicherheitsgruppe verweisen:

- Sie können eine Sicherheitsgruppe in der eingehenden Regel einer anderen Sicherheitsgruppe referenzieren, wenn eine der folgenden Bedingungen erfüllt ist:
 - Die Sicherheitsgruppen sind mit der gleichen VPC verknüpft.
 - Es besteht eine Peering-Verbindung zwischen den VPCs , denen die Sicherheitsgruppen zugeordnet sind.
 - Zwischen den, VPCs denen die Sicherheitsgruppen zugeordnet sind, befindet sich ein Transit-Gateway.
- Sie können eine Sicherheitsgruppe in der ausgehenden Regel referenzieren, wenn eine der folgenden Bedingungen erfüllt ist:
 - Die Sicherheitsgruppen sind mit der gleichen VPC verknüpft.
 - Es besteht eine Peering-Verbindung zwischen den VPCs , denen die Sicherheitsgruppen zugeordnet sind.
- Es werden keine Regeln aus der referenzierten Sicherheitsgruppe der Sicherheitsgruppe hinzugefügt, die darauf verweist.
- Bei Regeln für eingehenden Datenverkehr können die mit einer Sicherheitsgruppe verknüpften EC2 Instances eingehenden Datenverkehr von den privaten IP-Adressen von den Netzwerkschnittstellen der EC2 Instances empfangen, die der referenzierten Sicherheitsgruppe zugeordnet sind.
- Bei Regeln für ausgehenden Datenverkehr können die mit einer Sicherheitsgruppe verknüpften EC2 Instances ausgehenden Datenverkehr von den Netzwerkschnittstellen der EC2 Instances, die der referenzierten Sicherheitsgruppe zugeordnet sind, an die privaten IP-Adressen senden.
- Bei den folgenden Aktionen gewähren wir keine Autorisierung gegen Sicherheitsgruppen, auf die verwiesen wird: `AuthorizeSecurityGroupIngress`, `AuthorizeSecurityGroupEgress`,

`RevokeSecurityGroupIngress` und `RevokeSecurityGroupEgress`. Wir prüfen nur, ob die Sicherheitsgruppe vorhanden ist. Daraus resultiert Folgendes:

- Das Festlegen der Sicherheitsgruppe, auf die in den IAM-Richtlinien für diese Aktionen verwiesen wird, hat keine Auswirkung.
- Wenn eine Sicherheitsgruppe, auf die verwiesen wird, einem anderen Konto gehört, empfängt das Besitzerkonto keine CloudTrail Ereignisse für diese Aktionen.

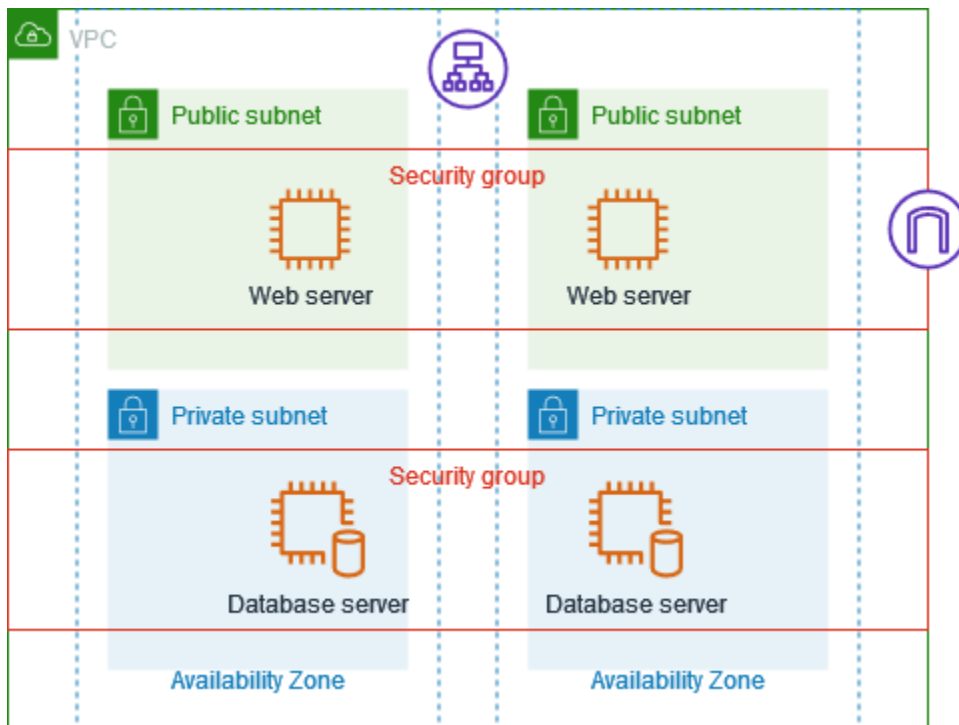
Einschränkung

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 verwaltete AWS 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. Weitere Informationen finden Sie unter [Aktualisieren Ihrer Sicherheitsgruppen, um auf Peer-Sicherheitsgruppen zu verweisen](#) im Handbuch für Amazon-VPC-Peering.

Wenn Sie eine Sicherheitsgruppenregel haben, die auf eine Sicherheitsgruppe in einer Peer-VPC oder einer freigegebenen VPC verweist, und die Sicherheitsgruppe in der freigegebenen VPC gelöscht oder die VPC-Peering-Verbindung gelöscht wird, wird die Sicherheitsgruppenregel als veraltet markiert. Sie können veraltete Sicherheitsgruppenregeln genau wie alle anderen Sicherheitsgruppenregeln löschen.

Standard-Sicherheitsgruppen für Ihre VPCs

Ihre Standardsicherheitsgruppe 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 angeben, verknüpfen wir die Instance mit der Standardsicherheitsgruppe für ihre VPC.

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 folgende Tabelle beschreibt die Standard-Eingangsregeln für eine Standardsicherheitsgruppe.

Quelle	Protocol (Protokoll)	Port-Bereich	Description
<i>sg-1234567890abcdef0</i>	Alle	Alle	Lässt eingehenden Datenverkehr von allen Ressourcen zu,

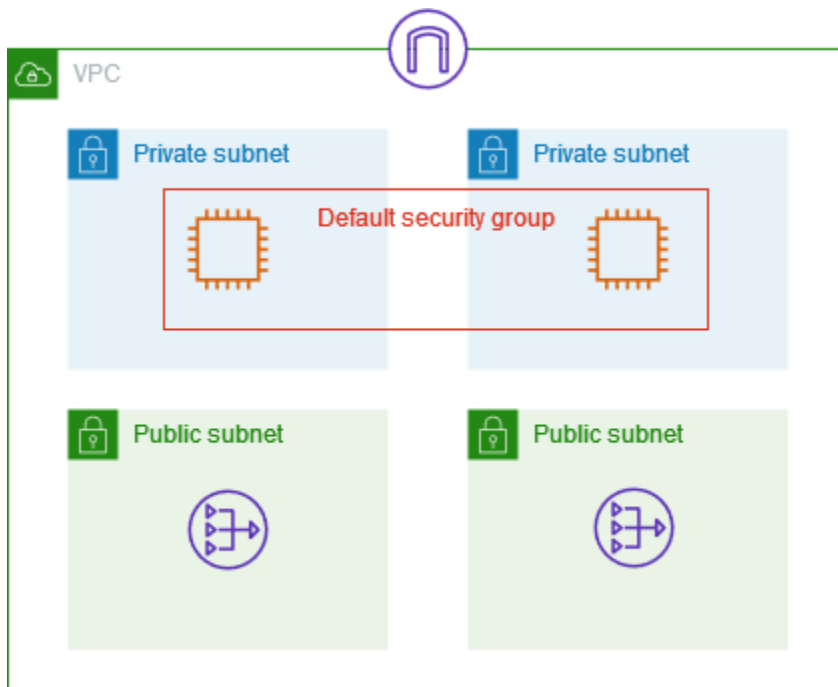
Quelle	Protocol (Protokoll)	Port-Bereich	Description
			die dieser Sicherheitsgruppe zugewiesen sind. Die Quelle ist die ID dieser Sicherheitsgruppe.

Die folgende Tabelle beschreibt die Standard-Ausgangsregeln für eine Standardsicherheitsgruppe.

Ziel	Protocol (Protokoll)	Port-Bereich	Beschreibung
0.0.0.0/0	Alle	Alle	Lässt den gesamten ausgehenden Datenverkehr IPv4 zu.
::/0	Alle	Alle	Lässt den gesamten ausgehenden Verkehr IPv6 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 die Standardregeln und ist mit zwei EC2 Instances verknüpft, 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.



Erstellen einer Sicherheitsgruppe für Ihre VPC

Ihre Virtual Private Cloud (VPC) verfügt über eine Standardsicherheitsgruppe. Sie können zusätzliche Sicherheitsgruppen erstellen. Sicherheitsgruppen können nur mit Ressourcen in der VPC verwendet werden, für die sie erstellt wurden.

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. Sie können Regeln hinzufügen, wenn Sie eine Sicherheitsgruppe erstellen oder zu einem späteren Zeitpunkt. Weitere Informationen finden Sie unter [Sicherheitsgruppenregeln](#).

Erforderliche -Berechtigungen

Stellen Sie zuerst sicher, dass Sie über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie hier:

- [Verwalten von Sicherheitsgruppen](#)
- [Sicherheitsgruppenregeln verwalten](#)

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 Sicherheitsgruppe nach der Erstellung nicht mehr ändern.
5. Wählen Sie für VPC die VPC aus, in der Sie die Ressourcen erstellen werden, denen Sie die Sicherheitsgruppe zuordnen.
6. (Optional) Wählen Sie Regeln für eingehenden Datenverkehr aus, um Regeln für den eingehenden Datenverkehr hinzuzufügen. Wählen Sie für jede Regel Regel hinzufügen aus und geben Sie das Protokoll, den Port und die Quelle an. Weitere Informationen finden Sie unter [Konfigurieren von Sicherheitsgruppenregeln](#).
7. (Optional) Wählen Sie Regeln für ausgehenden Datenverkehr aus, um ausgehende Regeln hinzuzufügen. Wählen Sie für jede Regel Regel hinzufügen aus und geben Sie das Protokoll, den Port und das Ziel an.
8. (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.
9. Wählen Sie Sicherheitsgruppe erstellen aus.

Um eine Sicherheitsgruppe zu erstellen, verwenden Sie AWS CLI

Verwenden Sie den Befehl [create-security-group](#).

Alternativ können Sie eine neue Sicherheitsgruppe erstellen, indem Sie eine bestehende Gruppe kopieren. Wenn Sie eine Sicherheitsgruppe kopieren, fügen wir automatisch die gleichen Regeln für ein- und ausgehenden Datenverkehr wie die ursprüngliche Sicherheitsgruppe hinzu und verwenden die gleiche VPC wie die ursprüngliche Sicherheitsgruppe. Sie können einen Namen und eine Beschreibung für die neue Sicherheitsgruppe eingeben. Sie können optional eine andere VPC auswählen und die Regeln für ein- und ausgehenden Datenverkehr nach Bedarf ändern. Jedoch können Sie eine Sicherheitsgruppe nicht von einer Region in eine andere Region kopieren.

So erstellen Sie eine Sicherheitsgruppe auf der Grundlage einer bestehenden Gruppe

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie eine Sicherheitsgruppe.
4. Wählen Sie Aktionen, In neue Sicherheitsgruppe kopieren aus.

5. Geben Sie einen Namen und eine Beschreibung für die Sicherheitsgruppe ein.
6. (Optional) Wählen Sie bei Bedarf eine andere VPC aus.
7. (Optional) Fügen Sie die Sicherheitsgruppenregeln nach Bedarf hinzu, entfernen oder bearbeiten Sie sie.
8. Wählen Sie Sicherheitsgruppe erstellen aus.

Konfigurieren von Sicherheitsgruppenregeln

Nachdem Sie eine Sicherheitsgruppe erstellt haben, können Sie ihre Sicherheitsgruppenregeln hinzufügen, aktualisieren und löschen. Wenn Sie eine Regel hinzufügen, aktualisieren oder löschen, wird die Änderung automatisch auf die Ressourcen angewendet, die mit der Sicherheitsgruppe verknüpft sind.

Erforderliche Berechtigungen

Stellen Sie zuerst sicher, dass Sie über die erforderlichen Berechtigungen verfügen. Weitere Informationen finden Sie unter [Sicherheitsgruppenregeln verwalten](#).

Protokolle und Ports

- Wenn Sie in der Konsole einen vordefinierten Typ auswählen, werden Protokoll und Portbereich für Sie angegeben. Um einen Portbereich einzugeben, müssen Sie einen der folgenden benutzerdefinierten Typen auswählen: Benutzerdefiniertes TCP oder Benutzerdefiniertes UDP.
- Mit dem AWS CLI können Sie mithilfe der `--port` Optionen `--protocol` und eine einzelne Regel mit einem einzigen Port hinzufügen. Um mehrere Regeln oder eine Regel mit einem Portbereich hinzuzufügen, verwenden Sie stattdessen die Option `--ip-permissions`.

Quellen und Ziele

- Mit der Konsole können Sie Folgendes als Quellen für Regeln für eingehenden Datenverkehr oder als Ziele für Regeln für ausgehenden Datenverkehr angeben.
 - Benutzerdefiniert — Ein IPv4 CIDR-Block, ein IPv6 CIDR-Block, eine Sicherheitsgruppe oder eine Präfixliste.
 - Anywhere- IPv4 — Der IPv4 0.0.0.0/0 CIDR-Block.
 - Anywhere- IPv6 — Der :::/0 CIDR-Block. IPv6
 - Meine IP — Die öffentliche IPv4 Adresse Ihres lokalen Computers.

- Mit der AWS CLI können Sie mithilfe der Option einen IPv4 CIDR-Block oder mithilfe der `--cidr` Option eine Sicherheitsgruppe angeben. `--source-group` Verwenden Sie die Option, um eine Präfixliste oder einen IPv6 CIDR-Block anzugeben. `--ip-permissions`

 Warning

Wenn Sie Anywhere- wählenIPv4, lassen Sie Verkehr von allen IPv4 Adressen zu. Wenn Sie Anywhere- wählenIPv6, lassen Sie Verkehr von allen IPv6 Adressen zu. Es empfiehlt sich, nur die spezifischen IP-Adressbereiche zu autorisieren, die Zugriff auf Ihre Ressourcen benötigen.

So konfigurieren Sie Sicherheitsgruppenregeln 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 unter Aktionen oder auf der Registerkarte Regeln für eingehenden Datenverkehr die Option Bearbeiten von Regeln für eingehenden Datenverkehr aus, um die Regeln für den eingehenden Datenverkehr zu bearbeiten.
 - a. Um eine Regel hinzuzufügen, wählen Sie Regel hinzufügen aus und geben Sie den Typ, das Protokoll, den Port und die Quelle für die Regel ein.

Wenn es sich beim Typ um TCP oder UDP handelt, 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 für Sie konfiguriert.

- b. Ändern Sie das Protokoll, die Beschreibung und die Quelle nach Bedarf, um eine Regel zu aktualisieren. Sie können jedoch den Quellentyp nicht ändern. Wenn es sich bei der Quelle beispielsweise um einen IPv4 CIDR-Block handelt, können Sie keinen IPv6 CIDR-Block, keine Präfixliste oder keine Sicherheitsgruppe angeben.
- c. Klicken Sie auf die Schaltfläche Löschen, um eine Regel zu löschen.

5. Um die Regeln für den ausgehenden Datenverkehr zu bearbeiten, wählen Sie Regeln für ausgehenden Datenverkehr bearbeiten unter Aktionen oder auf der Registerkarte Regeln für ausgehenden Datenverkehr aus.
 - a. Um eine Regel hinzuzufügen, wählen Sie Regel hinzufügen aus und geben Sie den Typ, das Protokoll, den Port und das Ziel für die Regel ein. Sie können auch eine optionale Beschreibung eingeben.

Wenn es sich beim Typ um TCP oder UDP handelt, 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 für Sie konfiguriert.
 - b. Ändern Sie das Protokoll, die Beschreibung und die Quelle nach Bedarf, um eine Regel zu aktualisieren. Sie können jedoch den Quellentyp nicht ändern. Wenn es sich bei der Quelle beispielsweise um einen IPv4 CIDR-Block handelt, können Sie keinen IPv6 CIDR-Block, keine Präfixliste oder keine Sicherheitsgruppe angeben.
 - c. Klicken Sie auf die Schaltfläche Löschen, um eine Regel zu löschen.
6. Wählen Sie Regeln speichern aus.

Um Sicherheitsgruppenregeln mit dem zu konfigurieren AWS CLI

- Hinzufügen — Verwenden Sie die [authorize-security-group-egress](#)Befehle [authorize-security-group-ingress](#)und.
- Entfernen — Verwenden Sie die [revoke-security-group-egress](#)Befehle [revoke-security-group-ingress](#)und.
- Ändern — Verwenden Sie die Befehle [modify-security-group-rules](#), [update-security-group-rule-descriptions-ingress](#) und [-descriptions-egress](#). [update-security-group-rule](#)

Löschen einer Sicherheitsgruppe

Wenn Sie eine von Ihnen erstellte Sicherheitsgruppe nicht mehr benötigen, können Sie diese löschen.

Voraussetzungen

- Die Sicherheitsgruppe kann mit keinen Ressourcen verknüpft werden.

- Die Sicherheitsgruppe kann nicht von einer Regel in einer anderen Sicherheitsgruppe referenziert werden.
- Die Sicherheitsgruppe kann nicht die Standardsicherheitsgruppe für eine VPC sein.

Löschen einer Sicherheitsgruppe mithilfe der Konsole

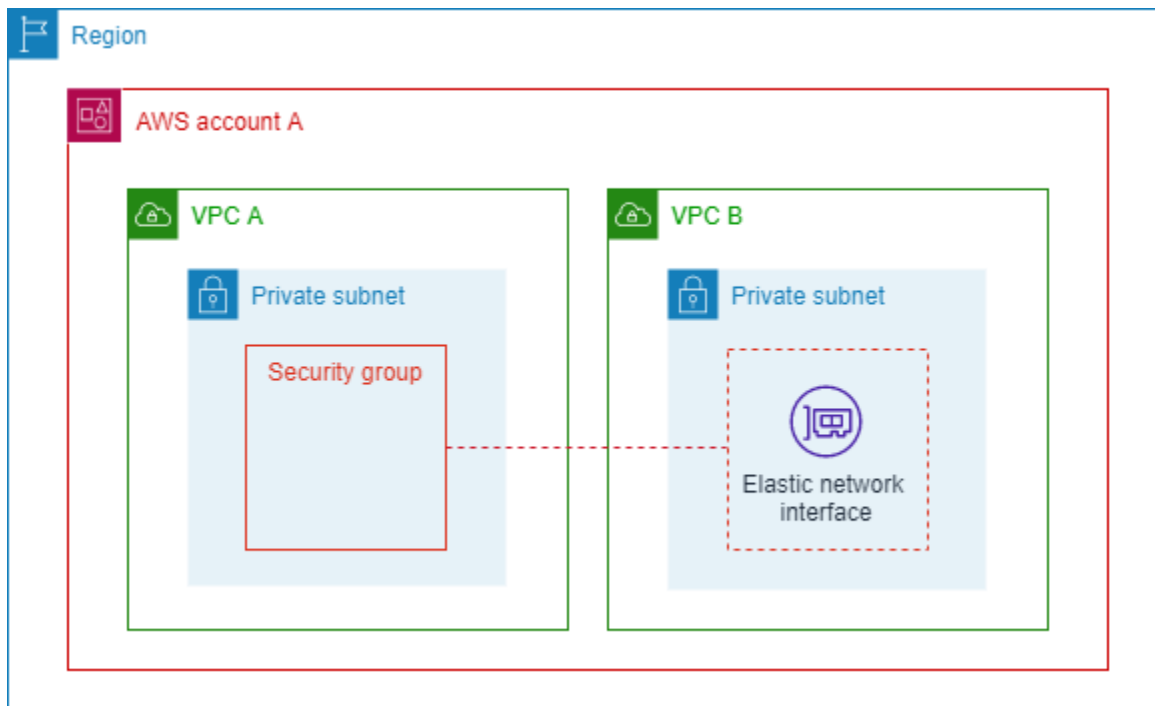
1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich die Option Sicherheitsgruppen aus.
3. Wählen Sie die Sicherheitsgruppe und dann Aktionen, Sicherheitsgruppe löschen aus.
4. Wenn Sie mehr als eine Sicherheitsgruppe ausgewählt haben, werden Sie zur Bestätigung aufgefordert. Wenn einige der Sicherheitsgruppen nicht gelöscht werden können, wird der Status der einzelnen Sicherheitsgruppen angezeigt, der angibt, ob sie gelöscht werden. Geben Sie Löschen ein, um den Löschvorgang zu bestätigen.
5. Wählen Sie Löschen aus.

Um eine Sicherheitsgruppe mit dem zu löschen AWS CLI

Verwenden Sie den Befehl [delete-security-group](#).

Ordnen Sie Sicherheitsgruppen mehreren zu VPCs

Wenn Sie mehrere Workloads haben VPCs , die dieselben Netzwerksicherheitsanforderungen haben, können Sie die Funktion Sicherheitsgruppen-VPC-Zuordnungen verwenden, um eine Sicherheitsgruppe mehreren VPCs in derselben Region zuzuordnen. Auf diese Weise können Sie Sicherheitsgruppen für mehrere VPCs in Ihrem Konto an einem Ort verwalten und verwalten.



Das obige Diagramm zeigt AWS Konto A mit zwei VPCs darin. Jeder von ihnen VPCs hat Workloads, die in einem privaten Subnetz ausgeführt werden. In diesem Fall haben die Workloads in den Subnetzen von VPC A und B dieselben Anforderungen an den Netzwerkdatenverkehr, sodass Konto A das Feature für Sicherheitsgruppen-VPC-Zuordnungen verwenden kann, um die Sicherheitsgruppe in VPC A mit VPC B zu verknüpfen. Alle an der verknüpften Sicherheitsgruppe vorgenommenen Aktualisierungen werden automatisch auf den Datenverkehr der Workloads im Subnetz von VPC B angewendet.

Anforderungen des Features für Sicherheitsgruppen-VPC-Zuordnungen

- Sie müssen Eigentümer der VPC sein oder eines der VPC-Subnetze für Sie freigegeben haben, um eine Sicherheitsgruppe mit der VPC zu verknüpfen.
- Die VPC und die Sicherheitsgruppe müssen sich in derselben AWS Region befinden.
- Sie können eine Standardsicherheitsgruppe nicht mit einer anderen VPC oder eine Sicherheitsgruppe mit einer Standard-VPC verknüpfen.
- Sowohl der Eigentümer der Sicherheitsgruppe als auch der Eigentümer der VPC können die VPC-Zuordnungen der Sicherheitsgruppe einsehen.

Services, die dieses Feature unterstützen

- Amazon API Gateway (APIs nur REST)

- AWS Auto Scaling
- CloudFormation
- Amazon EC2
- Amazon EFS
- Amazon EKS
- Amazon FSx
- AWS PrivateLink
- Amazon Route 53
- ELB
 - Application Load Balancer
 - Network Load Balancer

Verknüpfen einer Sicherheitsgruppe mit einer anderen VPC

In diesem Abschnitt wird erklärt, wie Sie AWS-Managementkonsole und die verwenden AWS CLI , um eine Sicherheitsgruppe zuzuordnen VPCs.

AWS Management Console

So verknüpfen Sie eine Sicherheitsgruppe mit einer anderen VPC

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Klicken Sie im linken Navigationsbereich auf Sicherheitsgruppen.
3. Wählen Sie eine Sicherheitsgruppe aus, um die Details anzuzeigen.
4. Wählen Sie die Registerkarte VPC-Zuordnungen aus.
5. Wählen Sie Associate VPC (VPC zuordnen) aus.
6. Wählen Sie unter VPC-ID eine VPC aus, die der Sicherheitsgruppe zugeordnet werden soll.
7. Wählen Sie Associate VPC (VPC zuordnen) aus.

Command line

So verknüpfen Sie eine Sicherheitsgruppe mit einer anderen VPC

1. Erstellen Sie eine VPC-Zuordnung mit [associate-security-group-vpc](#).

2. Überprüfen Sie den Status einer VPC-Assoziation mit [describe-security-group-vpc-associations](#) und warten Sie, bis der Status angezeigt wird. `associated`

Die VPC ist nun mit der Sicherheitsgruppe verknüpft.

Sobald Sie die VPC mit der Sicherheitsgruppe verknüpft haben, können Sie z. B. [eine Instance in der VPC starten und diese neue Sicherheitsgruppe auswählen](#) oder [diese Sicherheitsgruppe in einer bestehenden Sicherheitsgruppenregel referenzieren](#).

Aufheben der Verknüpfung einer Sicherheitsgruppe mit einer anderen VPC

In diesem Abschnitt wird erklärt, wie Sie mit AWS-Managementkonsole und die die Zuordnung AWS CLI zu einer Sicherheitsgruppe aufheben können. VPCs Sie sollten dies tun, wenn Sie die Sicherheitsgruppe löschen möchten. Sicherheitsgruppen können nicht gelöscht werden, wenn sie zugeordnet sind. Sie können die Zuordnung zu einer Sicherheitsgruppe nur dann aufheben, wenn es in der zugehörigen VPC keine Netzwerkschnittstellen gibt, die diese Sicherheitsgruppe verwenden.

AWS Management Console

So heben Sie die Zuordnung einer Sicherheitsgruppe zu einer VPC auf

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Klicken Sie im linken Navigationsbereich auf Sicherheitsgruppen.
3. Wählen Sie eine Sicherheitsgruppe aus, um die Details anzuzeigen.
4. Wählen Sie die Registerkarte VPC-Zuordnungen aus.
5. Wählen Sie VPC-Zuordnung aufheben aus.
6. Wählen Sie unter VPC-ID eine VPC aus, deren Zuordnung zur Sicherheitsgruppe aufgehoben werden soll.
7. Wählen Sie VPC-Zuordnung aufheben aus.
8. Zeigen Sie den Status der Aufhebung der Zuordnung auf der Registerkarte „VPC-Zuordnungen“ an und warten Sie, bis der Status `disassociated` lautet.

Command line

So heben Sie die Verknüpfung einer Sicherheitsgruppe mit einer VPC auf

1. Trennen Sie eine VPC-Zuordnung zu. [disassociate-security-group-vpc](#)

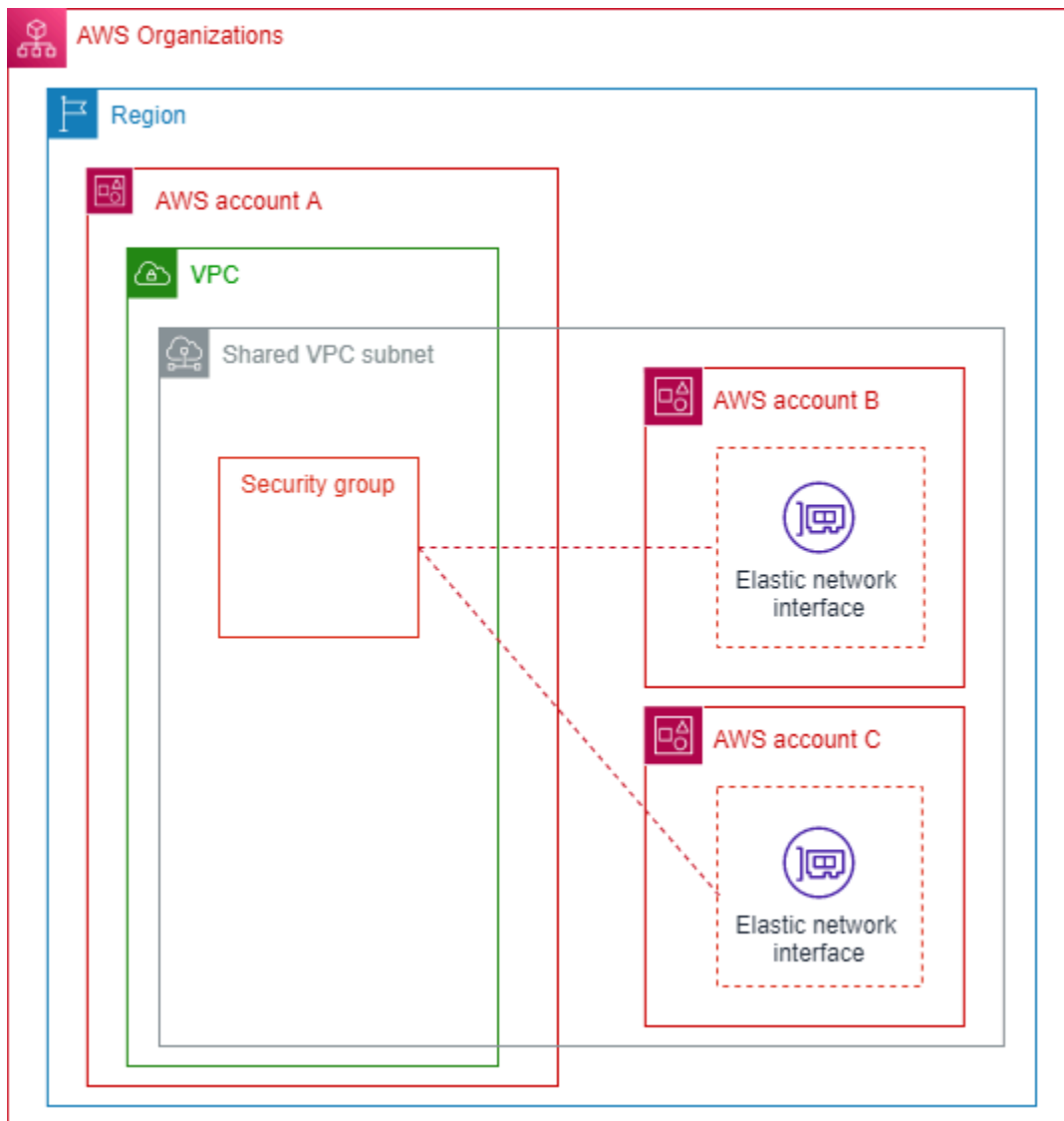
2. Überprüfen Sie den Status einer VPC-Dissoziation mit [describe-security-group-vpc-associations](#) und warten Sie, bis der Status angezeigt wird. `disassociated`

Die Zuordnung der VPC zur Sicherheitsgruppe ist nun aufgehoben.

Sicherheitsgruppen mit AWS Organizations teilen

Mit der Funktion „Gemeinsame Sicherheitsgruppe“ können Sie eine Sicherheitsgruppe mit Konten anderer AWS Organizations in derselben AWS Region teilen und die Sicherheitsgruppe für die Verwendung durch diese Konten verfügbar machen.

Das folgende Diagramm zeigt, wie Sie die Funktion „Gemeinsame Sicherheitsgruppe“ verwenden können, um die Verwaltung von Sicherheitsgruppen für alle Konten in Ihren AWS Organizations zu vereinfachen:



Dieses Diagramm zeigt drei Konten, die Teil derselben Organisation sind. Konto A teilt sich ein VPC-Subnetz mit den Konten B und C. Konto A teilt die Sicherheitsgruppe mit den Konten B und C mithilfe des Features für freigegebene Sicherheitsgruppen. Die Konten B und C verwenden dann diese Sicherheitsgruppe, wenn sie Instances im freigegebenen Subnetz starten. Dadurch kann Konto A die Sicherheitsgruppe verwalten. Alle Aktualisierungen der Sicherheitsgruppe gelten für die Ressourcen, die von den Konten B und C im freigegebenen VPC-Subnetz ausgeführt werden.

Anforderungen des Features für freigegebene Sicherheitsgruppen

- Dieses Feature ist nur für Konten in derselben Organisation in AWS Organizations verfügbar. Die [gemeinsame Nutzung von Ressourcen](#) muss in AWS Organizations aktiviert sein.
- Das Konto, das die Sicherheitsgruppe freigibt, muss sowohl die VPC als auch die Sicherheitsgruppe besitzen.

- Sie können keine Standardsicherheitsgruppen freigeben.
- Sie können keine Sicherheitsgruppen freigeben, die sich in einer Standard-VPC befinden.
- Teilnehmerkonten können Sicherheitsgruppen in einer freigegebenen VPC erstellen, aber sie können diese Sicherheitsgruppen nicht freigeben.
- Damit ein IAM-Prinzipal eine Sicherheitsgruppe gemeinsam nutzen kann, ist ein Mindestsatz an Berechtigungen erforderlich. AWS RAM Verwenden Sie die von `AmazonEC2FullAccess` und `AWSResourceAccessManagerFullAccess` verwalteten IAM-Richtlinien, um sicherzustellen, dass Ihre IAM-Prinzipale über die erforderlichen Berechtigungen verfügen, um freigegebene Sicherheitsgruppen freizugeben und zu nutzen. Wenn Sie eine benutzerdefinierte IAM-Richtlinie verwenden, sind die Aktionen `c2:PutResourcePolicy` und `ec2:DeleteResourcePolicy` erforderlich. Dies sind IAM-Aktionen, die nur für Berechtigungen gelten. Wenn einem IAM-Prinzipal diese Berechtigungen nicht erteilt wurden, tritt beim Versuch, die Sicherheitsgruppe mit AWS RAM freizugeben, ein Fehler auf.

Services, die dieses Feature unterstützen

- Amazon API Gateway
- Amazon EC2
- Amazon ECS
- Amazon EFS
- Amazon EKS
- Amazon EMR
- Amazon FSx
- Amazon ElastiCache
- AWS Elastic Beanstalk
- AWS Glue
- Amazon MQ
- Amazon SageMaker KI
- ELB
 - Application Load Balancer
 - Network Load Balancer

So wirkt sich dieses Feature auf bestehende Kontingente aus

Es gelten [Kontingente für Sicherheitsgruppen](#). Für das Kontingent „Sicherheitsgruppen pro Netzwerkschnittstelle“ gilt jedoch das Minimum des Kontingents von Eigentümer und Teilnehmer, wenn ein Teilnehmer sowohl eigene als auch freigegebene Gruppen auf einer Elastic-Network-Schnittstelle (ENI) verwendet.

Beispiel zur Veranschaulichung, wie sich dieses Feature auf das Kontingent auswirkt:

- Kontingent für Eigentümerkonten: 4 Sicherheitsgruppen pro Schnittstelle
- Kontingent für Teilnehmerkonten: 5 Sicherheitsgruppen pro Schnittstelle.
- Der Eigentümer gibt die Gruppen SG-O1, SG-O2, SG-O3, SG-O4, SG-O5 für den Teilnehmer frei. Der Teilnehmer hat bereits eigene Gruppen in der VPC: SG-P1, SG-P2, SG-P3, SG-P4, SG-P5.
- Wenn der Teilnehmer eine ENI erstellt und nur seine eigenen Gruppen verwendet, kann er alle 5 Sicherheitsgruppen (SG-P1, SG-P2, SG-P3, SG-P4, SG-P5) zuordnen, da dies sein Kontingent ist.
- Wenn der Teilnehmer eine ENI erstellt und alle freigegebenen Gruppen darauf verwendet, kann er nur bis zu 4 Gruppen zuordnen. In diesem Fall ist das Kontingent für eine solche ENI das Minimum der Kontingente von Eigentümer und Teilnehmer. Mögliche gültige Konfigurationen sehen wie folgt aus:
 - SG-O1, SG-P1, SG-P2, SG-P3
 - SG-O1, SG-O2, SG-O3, SG-O4

Freigeben einer Sicherheitsgruppe

In diesem Abschnitt wird erklärt, wie Sie AWS-Managementkonsole und die verwenden AWS CLI , um eine Sicherheitsgruppe mit anderen Konten in Ihrer Organisation zu teilen.

AWS Management Console

So geben Sie eine Sicherheitsgruppe frei

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Klicken Sie im linken Navigationsbereich auf Sicherheitsgruppen.
3. Wählen Sie eine Sicherheitsgruppe aus, um die Details anzuzeigen.
4. Wählen Sie die Registerkarte Sharing (Freigabe).
5. Klicken Sie auf Sicherheitsgruppe freigeben.

6. Wählen Sie **Create resource share (Ressourcenfreigabe erstellen)** aus. Daraufhin wird die AWS RAM Konsole geöffnet, in der Sie die Ressourcenfreigabe für die Sicherheitsgruppe erstellen.
7. Geben Sie einen Namen für die Ressourcenfreigabe ein.
8. Wählen Sie unter **Ressourcen** – optional die Option **Sicherheitsgruppen** aus.
9. Wählen Sie eine Sicherheitsgruppe aus. Die Sicherheitsgruppe kann keine Standardsicherheitsgruppe sein und kann nicht mit der Standard-VPC verknüpft werden.
10. Wählen Sie **Weiter** aus.
11. Überprüfen Sie die Aktionen, die Prinzipale ausführen dürfen, und wählen Sie **Weiter** aus.
12. Wählen Sie unter **Prinzipale** – optional die Option **Zulassen der Freigabe nur innerhalb der eigenen Organisation** aus.
13. Wählen Sie unter **Prinzipale** einen der folgenden Prinzipaltypen aus und geben Sie die entsprechenden Nummern ein:
 - **AWS Konto:** Die Kontonummer eines Kontos in Ihrer Organisation.
 - **Organisation:** Die AWS Organisations-ID.
 - **Organisationseinheit (OU):** Die ID einer OU in der Organisation.
 - **IAM-Rolle:** Der ARN einer IAM-Rolle. Das Konto, das die Rolle erstellt hat, muss Mitglied derselben Organisation sein wie das Konto, das diese Ressourcenfreigabe erstellt.
 - **IAM-Benutzer:** Der ARN eines IAM-Benutzers. Das Konto, das den Benutzer erstellt hat, muss Mitglied derselben Organisation sein wie das Konto, das diese Ressourcenfreigabe erstellt.
 - **Service-Prinzipal:** Sie können eine Sicherheitsgruppe nicht für einen Service-Prinzipal freigeben.
14. Wählen Sie **Hinzufügen** aus.
15. Wählen Sie **Weiter** aus.
16. Wählen Sie **Create resource share (Ressourcenfreigabe erstellen)** aus.
17. Warten Sie unter **Freigegebene Ressourcen**, bis der Status von **Associated** angezeigt wird. Wenn die Zuordnung einer Sicherheitsgruppe fehlschlägt, kann dies auf eine der oben genannten Einschränkungen zurückzuführen sein. Sehen Sie sich die Details der Sicherheitsgruppe und die Registerkarte **Freigabe** auf der Detailseite an, um alle Meldungen zu sehen, die sich darauf beziehen, warum eine Sicherheitsgruppe möglicherweise nicht freigegeben werden kann.

18. Kehren Sie zur Liste der Sicherheitsgruppen der VPC-Konsole zurück.
19. Wählen Sie die Sicherheitsgruppe, die Sie freigegeben haben.
20. Wählen Sie die Registerkarte Sharing (Freigabe). Ihre AWS RAM Ressource sollte dort sichtbar sein. Ist dies nicht der Fall, ist die Erstellung der Ressourcenfreigabe möglicherweise fehlgeschlagen und Sie müssen sie möglicherweise neu erstellen.

Command line

So geben Sie eine Sicherheitsgruppe frei

1. Sie müssen zunächst eine Ressourcenfreigabe für die Sicherheitsgruppe erstellen, mit der Sie die Ressource teilen möchten AWS RAM. Anweisungen zum Erstellen einer Ressourcenfreigabe AWS RAM mithilfe von finden Sie unter [Erstellen einer Ressourcenfreigabe AWS RAM im AWS RAM](#) Benutzerhandbuch AWS CLI
2. Um erstellte Ressourcenfreigabebezuordnungen anzuzeigen, verwenden Sie [get-resource-share-associations](#).

Die Sicherheitsgruppe ist nun freigegeben. Sie können die Sicherheitsgruppe auswählen, wenn Sie [eine EC2 Instance in einem gemeinsam genutzten Subnetz innerhalb derselben VPC starten](#).

Beenden der Freigabe einer Sicherheitsgruppe

In diesem Abschnitt wird erklärt, wie Sie die AWS-Managementkonsole und die verwenden AWS CLI , um die gemeinsame Nutzung einer Sicherheitsgruppe mit anderen Konten in Ihrer Organisation zu beenden.

AWS Management Console

So beenden Sie die Freigabe einer Sicherheitsgruppe

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Klicken Sie im linken Navigationsbereich auf Sicherheitsgruppen.
3. Wählen Sie eine Sicherheitsgruppe aus, um die Details anzuzeigen.
4. Wählen Sie die Registerkarte Sharing (Freigabe).
5. Wählen Sie eine Ressourcenfreigabe für eine Sicherheitsgruppe aus und klicken Sie auf Freigabe beenden.
6. Wählen Sie Ja, die Freigabe beenden aus.

Command line

So beenden Sie die Freigabe einer Sicherheitsgruppe

Löschen Sie die Ressource, die gemeinsam genutzt wird mit [delete-resource-share](#).

Die Sicherheitsgruppe wird nicht mehr freigegeben. Nachdem der Eigentümer die Freigabe einer Sicherheitsgruppe beendet hat, gelten die folgenden Regeln:

- Elastic Network Interfaces (ENIs) für bestehende Teilnehmer erhalten weiterhin alle Aktualisierungen der Sicherheitsgruppenregeln, die an Sicherheitsgruppen vorgenommen werden, die nicht gemeinsam genutzt werden. Das Beenden der Freigabe hindert den Teilnehmer nur daran, neue Verknüpfungen mit der nicht freigegebenen Gruppe herzustellen.
- Teilnehmer können die nicht gemeinsam genutzte Sicherheitsgruppe nicht mehr mit einer Gruppe verknüpfen, die ENIs ihnen gehört.
- Die Teilnehmer können diejenigen beschreiben und löschen ENIs , die noch nicht gemeinsam genutzten Sicherheitsgruppen zugeordnet sind.
- Wenn die Teilnehmer immer noch der nicht gemeinsam genutzten Sicherheitsgruppe ENIs zugeordnet sind, kann der Besitzer die nicht gemeinsam genutzte Sicherheitsgruppe nicht löschen. Der Besitzer kann die Sicherheitsgruppe erst löschen, nachdem die Teilnehmer die Zuordnung der Sicherheitsgruppe zu all ihren Gruppen getrennt (entfernt) haben. ENIs
- Teilnehmer können keine neuen EC2 Instances mit einer ENI starten, die einer nicht gemeinsam genutzten Sicherheitsgruppe zugeordnet ist.

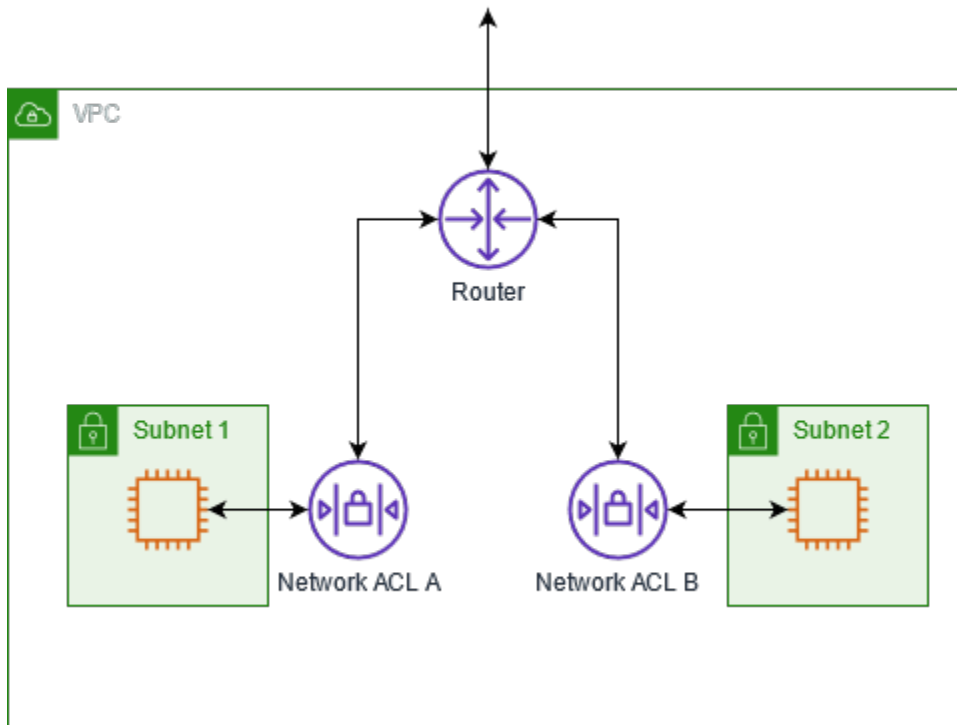
Steuerung des Datenverkehrs in Subnetzen mithilfe von Zugriffskontrolllisten für Netzwerke

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 des Netzwerks fallen keine zusätzlichen Gebühren an ACLs.

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.



Informationen zu den Unterschieden zwischen Sicherheitsgruppen und Netzwerken ACLs finden Sie unter [Vergleichen Sie Sicherheitsgruppen und Netzwerk ACLs](#).

Inhalt

- [Grundlagen von Netzwerk-ACLs](#)
- [Regeln für Netzwerk-ACLs](#)
- [Standard-Netzwerk-ACL für eine VPC](#)
- [Benutzerdefiniertes Netzwerk ACLs für Ihre VPC](#)
- [Pfad MTU Discovery und Netzwerk ACLs](#)
- [Erstellen einer Netzwerk-ACL für Ihre VPC](#)
- [Verwalten von Netzwerk-ACL-Zuordnungen für Ihre VPC](#)
- [Löschen einer Netzwerk-ACL für Ihre VPC](#)
- [Beispiel: Steuern des Zugriffs auf Instances in einem Subnetz](#)

Grundlagen von Netzwerk-ACLs

Im Folgenden finden Sie die grundlegenden Dinge, die Sie über Netzwerke wissen sollten, ACLs bevor Sie beginnen.

Netzwerk-ACL-Zuordnungen

- 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 [benutzerdefinierte Netzwerk-ACL](#) erstellen und einem Subnetz zuordnen. So können Sie bestimmten eingehenden oder ausgehenden Datenverkehr auf der Subnetzebene verweigern.
- 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.

Regeln für Netzwerk-ACLs

- Eine Netzwerk-ACL hat Regeln für eingehenden und ausgehenden Datenverkehr. Es gibt [Kontingente \(oder Beschränkungen\) für die Anzahl der Regeln, die Sie pro Netzwerk-ACL einsetzen können](#). 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, was bedeutet, dass Informationen über zuvor gesendeten oder empfangenen Datenverkehr nicht gespeichert werden. 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 eine Sicherheitsgruppe beispielsweise eingehenden Datenverkehr zu einer EC2 Instance

zulässt, werden Antworten unabhängig von den Regeln für ausgehende Sicherheitsgruppen automatisch zugelassen.

Einschränkungen

- Es gibt Kontingente (auch als Limits bezeichnet) für das Netzwerk. ACLs Weitere Informationen finden Sie unter [Netzwerk ACLs](#).
- Das Netzwerk ACLs kann DNS-Anfragen an oder vom Route 53 Resolver (auch bekannt als VPC+2-IP-Adresse oder AmazonProvided DNS) nicht blockieren. Um DNS-Anfragen durch den Route 53 Resolver zu filtern, können Sie [DNS-Firewall des Route 53 Resolver](#) aktivieren.
- Das Netzwerk ACLs kann den Datenverkehr zum Instanz-Metadatendienst (IMDS) nicht blockieren. Informationen zur Verwaltung des Zugriffs auf IMDS finden [Sie unter Konfiguration der Instance-Metadatenoptionen](#) im EC2 Amazon-Benutzerhandbuch.
- Das Netzwerk filtert ACLs keinen Datenverkehr, der zu und von folgenden Zielen bestimmt ist:
 - Amazon Domain Name Services (DNS)
 - Amazon Dynamic Host Configuration Protocol (DHCP)
 - EC2 Amazon-Instanz-Metadaten
 - Amazon-ECS-Endpunkte für Aufgabenmetadaten
 - Lizenzaktivierung für Windows-Instances
 - Amazon Time Sync Service
 - Reservierte IP-Adressen, die vom Standard-VPC-Router verwendet werden

Regeln für Netzwerk-ACLs

Sie können Regeln zur Standard-Netzwerk-ACL hinzufügen oder daraus entfernen oder ein zusätzliches 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.

Beispiele für Regeln finden Sie unter [the section called “Beispiel: Steuern des Zugriffs auf Instances in einem Subnetz”](#).

Überlegungen

- Es gibt Kontingente (auch als Limits bezeichnet) für die Anzahl der Regeln pro Netzwerk ACLs. Weitere Informationen finden Sie unter [Amazon VPC-Kontingente](#).
- Wenn Sie eine Regel zu einer ACL hinzufügen oder daraus löschen, sind alle Subnetze, die der ACL zugeordnet sind, von dieser Änderung betroffen. Die Änderungen werden nach kurzer Zeit wirksam.
- Wenn Sie eine Regel mithilfe eines Befehlszeilentools oder der EC2 Amazon-API hinzufügen, wird der CIDR-Bereich automatisch in seine 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.
- Es kann sinnvoll sein, eine deny-(verweigern-)Regel zu erstellen, wenn Sie einen großen Portbereich freigeben müssen, einzelne Ports innerhalb dieses Bereichs jedoch gesperrt werden sollen. Geben Sie der deny-Regel eine niedrigere Zahl als der Regel, die den gesamten Portbereich freigibt.
- Gehen Sie vorsichtig vor, wenn Sie Regeln gleichzeitig zu einer Netzwerk-ACL hinzufügen und daraus löschen. Wenn Sie eingehende oder ausgehende Regeln löschen und dann mehr neue Einträge hinzufügen, als erlaubt sind, (siehe [Amazon VPC-Kontingente](#), werden die zum Löschen ausgewählten Einträge entfernt und neue Einträge werden nicht hinzugefügt. Dies kann zu unerwarteten Verbindungsproblemen führen und den Zugriff auf und von Ihrer VPC verhindern.

Standard-Netzwerk-ACL für eine VPC

Ihre Virtual Private Cloud (VPC) verfügt automatisch über eine Standard-Netzwerk-ACL. Eine 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 Regeln, bei denen die Regelnummer ein Sternchen (*) ist. Diese Regeln sorgen dafür, dass Pakete, die mit keiner anderen Regel übereinstimmen, abgelehnt werden.

Sie können eine Standard-Netzwerk-ACL ändern, indem Sie Regeln ergänzen oder die nummerierten Standardregeln entfernen. Sie können keine Regeln löschen, deren Nummer ein Sternchen enthält.

Standardregeln für eingehenden Datenverkehr

Die folgende Tabelle zeigt die Standardregeln für eingehenden Datenverkehr für eine Standard-Netzwerk-ACL. Die Regeln für IPv6 werden nur hinzugefügt, wenn Sie die VPC mit einem zugehörigen IPv6 CIDR-Block erstellen oder der VPC einen IPv6 CIDR-Block zuordnen. Wenn Sie jedoch die Regeln für eingehenden Datenverkehr einer Standard-Netzwerk-ACL geändert haben, fügen wir die Regel, die den gesamten eingehenden IPv6 Verkehr zulässt, nicht hinzu, wenn Sie der VPC einen IPv6 Block zuordnen.

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/ Verweigern
100	Der gesamte Verkehr IPv4	Alle	Alle	0.0.0.0/0	ERLAUBEN
101	Der gesamte IPv6 Verkehr	Alle	Alle	::/0	ERLAUBEN
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY
*	Der gesamte IPv6 Verkehr	Alle	Alle	::/0	DENY

Standardregeln für ausgehenden Datenverkehr

Die folgende Tabelle zeigt die Standardregeln für ausgehenden Datenverkehr für eine Standard-Netzwerk-ACL. Die Regeln für IPv6 werden nur hinzugefügt, wenn Sie die VPC mit einem

zugehörigen IPv6 CIDR-Block erstellen oder der VPC einen IPv6 CIDR-Block zuordnen. Wenn Sie jedoch die Regeln für ausgehenden Datenverkehr einer Standard-Netzwerk-ACL geändert haben, fügen wir die Regel, die den gesamten ausgehenden IPv6 Verkehr zulässt, nicht hinzu, wenn Sie der VPC einen IPv6 Block zuordnen.

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Zielbereich	Erlauben/Verweigern
100	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	ERLAUBEN
101	Der gesamte Verkehr IPv6	Alle	Alle	::/0	ERLAUBEN
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY
*	Der gesamte IPv6 Verkehr	Alle	Alle	::/0	DENY

Benutzerdefiniertes Netzwerk ACLs für Ihre VPC

Sie können eine benutzerdefinierte Netzwerk-ACL erstellen und einem Subnetz zuordnen. So können Sie bestimmten eingehenden oder ausgehenden Datenverkehr auf der Subnetzebene verweigern. Weitere Informationen finden Sie unter [the section called “Erstellen einer Netzwerk-ACL”](#).

Jede Netzwerk-ACL enthält eine Standardregel für eingehenden Datenverkehr und eine Standardregel für ausgehenden Datenverkehr, deren Regelnummer ein Sternchen (*) ist. Über diese Regel wird sichergestellt, dass Pakete, die mit keiner anderen Regel übereinstimmen, abgelehnt werden.

Sie können eine Netzwerk-ACL ändern, indem Sie Regeln ergänzen oder entfernen. Sie können keine Regeln löschen, deren Nummer ein Sternchen enthält.

Für jede hinzugefügte Regel muss eine entsprechende Regel für ausgehenden oder eingehenden Datenverkehr existieren, die Antworten ermöglicht. Weitere Informationen zur Auswahl des passenden Bereichs für flüchtige Ports finden Sie unter [Flüchtige Ports](#).

Beispiel: Regeln für eingehenden Datenverkehr

Die folgende Tabelle zeigt die Beispielregeln für eingehenden Datenverkehr für eine Netzwerk-ACL. Die Regeln für IPv6 werden nur hinzugefügt, wenn der VPC ein IPv6 CIDR-Block zugeordnet ist. IPv4 und der IPv6 Verkehr werden separat bewertet. Daher gilt keine der IPv4 Verkehrsregeln für den IPv6 Verkehr. Sie können IPv6 Regeln neben den entsprechenden IPv4 Regeln oder die IPv6 Regeln nach der letzten IPv4 Regel hinzufügen.

Wenn ein Paket im Subnetz eingeht, werden die Regeln für eingehenden Datenverkehr der Netzwerk-ACL, die mit dem Subnetz verknüpft ist, nacheinander ausgewertet, beginnend mit der Regel mit der niedrigsten Nummer. Nehmen wir zum Beispiel an, es gibt IPv4 Datenverkehr, der für den HTTPS-Port (443) bestimmt ist. Das Paket stimmt nicht mit Regel 100 oder 105 überein. Es entspricht Regel 110, die den Datenverkehr in das Subnetz zulässt. Wenn das Paket für Port 139 (NetBIOS) bestimmt gewesen wäre, würde es keiner der nummerierten Regeln entsprechen, sodass die *-Regel für den IPv4 Verkehr das Paket letztendlich ablehnt.

Regel Nr.	Typ	Protocol (Protokol l)	Port-Bereich	Source	Erlauben/Verweiger n	Kommentare
100	HTTP	TCP	80	0.0.0.0/0	ERLAUBEN	Lässt eingehenden HTTP-Verkehr von einer beliebigen Adresse aus zu. IPv4
105	HTTP	TCP	80	::/0	ERLAUBEN	Erlaubt eingehenden HTTP-Verkehr von einer beliebigen Adresse aus. IPv6
110	HTTPS	TCP	443	0.0.0.0/0	ERLAUBEN	Erlaubt eingehenden HTTPS-Verkehr von einer beliebigen Adresse aus. IPv4
115	HTTPS	TCP	443	::/0	ERLAUBEN	Erlaubt eingehenden HTTPS-Verkehr von einer beliebigen Adresse aus. IPv6

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigerun	Kommentare
120	SSH	TCP	22	192.0.2.0/24	ERLAUBEN	Ermöglicht eingehenden SSH-Verkehr aus dem öffentlichen IPv4 Adressbereich Ihres Heimnetzwerks (über das Internet-Gateway).
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ERLAUBEN	Ermöglicht eingehenden IPv4 Rückverkehr aus dem Internet (für Anfragen, die aus dem Subnetz stammen).
145	Custom TCP	TCP	32768-65535	:::0	ERLAUBEN	Erlaubt eingehenden IPv6 Rückverkehr aus dem Internet (für Anfragen, die ihren Ursprung im Subnetz haben).
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY	Verweigert den gesamten eingehenden IPv4 Datenverkehr, der noch nicht durch eine vorherige Regel behandelt wurde (nicht änderbar).

Regel Nr.	Typ	Protocol (Protokol l)	Port-Bere ich	Source	Erlauben/ Verweiger n	Kommentare
*	Gesamter Datenverk ehr	Alle	Alle	::/0	DENY	Verweigert den gesamten eingehend en IPv6 Verkehr, der noch nicht durch eine vorherige Regel behandelt wurde (nicht änderbar).

Regeln für ausgehenden Datenverkehr

Die folgende Tabelle zeigt die Beispielregeln für ausgehenden Datenverkehr für eine benutzerdefinierte Netzwerk-ACL. Die Regeln für IPv6 werden nur hinzugefügt, wenn der VPC ein IPv6 CIDR-Block zugeordnet ist. IPv4 und der IPv6 Verkehr werden separat bewertet. Daher gilt keine der IPv4 Verkehrsregeln für den IPv6 Verkehr. Sie können IPv6 Regeln neben den entsprechenden IPv4 Regeln oder die IPv6 Regeln nach der letzten IPv4 Regel hinzufügen.

Regel Nr.	Typ	Protocol (Protokol l)	Port-Bere ich	Zielberei ch	Erlauben/ Verweiger n	Kommentare
100	HTTP	TCP	80	0.0.0.0/0	ERLAUBEN	Ermöglicht ausgehend en IPv4 HTTP-Verk ehr vom Subnetz zum Internet.
105	HTTP	TCP	80	::/0	ERLAUBEN	Lässt ausgehenden IPv6 HTTP-Verkehr vom Subnetz zum Internet zu.
110	HTTPS	TCP	443	0.0.0.0/0	ERLAUBEN	Lässt ausgehenden IPv4 HTTPS-Verkehr

Regel Nr.	Typ	Protocol (Protokol l)	Port-Bere ich	Zielberei ch	Erlauben/ Verweiger n	Kommentare
						vom Subnetz zum Internet zu.
115	HTTPS	TCP	443	::/0	ERLAUBEN	Ermöglicht ausgehenden IPv6 HTTPS-Verkehr vom Subnetz zum Internet.
120	Custom TCP	TCP	1024-65535	192.0.2.0/24	ERLAUBEN	Lässt ausgehende Antworten für den SSH-Datenverkehr von Ihrem Heimnetzwerk zu.
140	Custom TCP	TCP	32768-65535	0.0.0.0/0	ERLAUBEN	Ermöglicht ausgehende IPv4 Antworten an Clients im Internet (z. B. das Bereitstellen von Webseiten).
145	Custom TCP	TCP	32768-65535	::/0	ERLAUBEN	Ermöglicht ausgehende IPv6 Antworten an Clients im Internet (z. B. das Bereitstellen von Webseiten).
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY	Verweigert den gesamten ausgehenden IPv4 Datenverkehr, der noch nicht durch eine vorherige Regel behandelt wurde.

Regel Nr.	Typ	Protocol (Protokol l)	Port-Bere ich	Zielberei ch	Erlauben/ Verweiger n	Kommentare
*	Gesamter Datenverk ehr	Alle	Alle	::/0	DENY	Verweigert den gesamten ausgehend en IPv6 Datenverkehr, der noch nicht durch eine vorherige Regel behandelt wurde.

Flüchtige Ports

Die Beispiel-Netzwerk-ACL im vorhergehenden Abschnitt verwendet den flüchtigen Portbereich 32768 bis 65535. Möglicherweise möchten Sie jedoch ACLs je nach Clienttyp, den Sie verwenden oder mit dem Sie kommunizieren, einen anderen Bereich für Ihr Netzwerk 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.
- Anfragen, die von ELB ausgehen, verwenden die 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 Anfrage von einer Instance in Ihrer VPC ausgeht, muss Ihre Netzwerk-ACL über eine Regel für eingehenden Datenverkehr verfügen, um Datenverkehr zu den spezifischen Ports des Betriebssystems zuzulassen.

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.

Benutzerdefiniertes Netzwerk und andere Dienste ACLs 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 das Subnetz für Ihre Back-End-Instances über eine Netzwerk-ACL verfügt, in der Sie eine Ablehnungsregel für den gesamten Datenverkehr mit einer CIDR-Quelle `0.0.0.0/0` oder der CIDR-Quelle des Subnetzes hinzugefügt haben, kann Ihr Load Balancer keine Integritätsprüfungen an den Instances durchführen. Weitere Informationen zu den empfohlenen Netzwerk-ACL-Regeln für Load Balancer und Backend-Instances finden Sie unter:

- [Netzwerk ACLs für Ihren Application Load Balancer](#)
- [Netzwerk ACLs für Ihren Network Load Balancer](#)
- [Netzwerk ACLs für Ihren Classic Load Balancer](#)

Beheben von Problemen mit der Erreichbarkeit

Reachability Analyzer ist ein Tool zur statischen Konfigurationsanalyse. Mit Reachability Analyzer können Sie die Netzwerkerreichbarkeit zwischen zwei Ressourcen in Ihrer VPC analysieren und debuggen. Reachability Analyzer erzeugt hop-by-hop Details zum virtuellen Pfad zwischen diesen Ressourcen, wenn sie erreichbar sind, und identifiziert andernfalls die blockierende Komponente. Zum Beispiel kann er fehlende oder falsch konfigurierte Netzwerk-ACL-Regeln identifizieren.

Weitere Informationen finden Sie im [Leitfaden Reachability Analyzer](#).

Pfad MTU Discovery und Netzwerk ACLs

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.

Denn wenn ein Host ein Paket sendet IPv4, das größer als die MTU des empfangenden Hosts oder die MTU eines Geräts auf dem Pfad ist, verwirft der empfangende Host oder das empfangende Gerät 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 (Maximum Transmission Unit, 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 EC2 Amazon-Benutzerhandbuch.

Erstellen einer Netzwerk-ACL für Ihre VPC

Die folgenden Aufgaben zeigen Ihnen, wie Sie eine Netzwerk-ACL erstellen, Regeln zur Netzwerk-ACL hinzufügen und die Netzwerk-ACL dann einem Subnetz zuweisen.

Aufgaben

- [Schritt 1: Erstellen einer Netzwerk-ACL](#)
- [Schritt 2: Regeln hinzufügen](#)
- [Schritt 3: Zuweisen eines Subnetzes zu einer Netzwerk-ACL](#)
- [\(Optional\) Netzwerk ACLs mit Firewall Manager verwalten](#)

Schritt 1: Erstellen einer Netzwerk-ACL

Sie können für Ihre VPC benutzerdefinierte Netzwerk-ACLs erstellen. Die ersten Regeln für eine benutzerdefinierte Netzwerk-ACL blockieren den gesamten ein- und ausgehenden Datenverkehr. Die neue benutzerdefinierte Netzwerk-ACL ist standardmäßig keinem Subnetz zugewiesen und muss explizit Subnetzen zugewiesen werden.

Erstellen eines Netzwerk-Monitors mithilfe der Konsole

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 Netzwerk-ACL erstellen.
4. (Optional) Geben Sie unter Name einen Namen für Ihre Netzwerk-ACL ein.
5. Wählen Sie für VPC die VPC aus.
6. (Optional) Für Tags wählen Sie Tag hinzufügen aus und geben den Tag-Schlüssel und -Wert ein.
7. Klicken Sie auf Netzwerk-ACL erstellen.

Erstellen einer Netzwerk-ACL mithilfe der Befehlszeile

- [create-network-acl](#) (AWS CLI)
- [New-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

Schritt 2: Regeln hinzufügen

Sie können Regeln ergänzen, die ein- oder ausgehenden Datenverkehr zulassen oder verweigern.

Regeln werden ausgehend von der Regel mit der niedrigsten Nummer 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.

Wenn Sie die EC2 Amazon-API oder ein Befehlszeilentool verwenden, können Sie Regeln nicht 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.

Hinzufügen von Regeln zu einer Netzwerk-ACL mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich Netzwerk aus ACLs.
3. Wählen Sie die Netzwerk-ACL aus.
4. Gehen Sie zum Hinzufügen einer eingehenden Regel wie folgt vor:
 - a. Wählen Sie die Registerkarte Inbound rules (Regeln für eingehenden Datenverkehr) aus.
 - b. Wählen Sie auf der Seite Regeln für eingehenden Datenverkehr bearbeiten die Option Neue Regel hinzufügen aus.
 - c. Geben Sie eine noch ungenutzte Regelnummer ein, einen Typ, ein Protokoll, einen Portbereich, eine Quelle und ob der Datenverkehr zugelassen oder verweigert werden soll. Bei einigen Typen werden das Protokoll und der Port automatisch ausgefüllt. Wenn Sie nach einem Portbereich gefragt werden, geben Sie eine Portnummer oder einen Portbereich (z. B. 49152-65535) ein.

Wenn Sie ein Protokoll nutzen möchten, das nicht in der Liste enthalten ist, wählen Sie Benutzerdefiniertes Protokoll als Typ und anschließend das Protokoll aus. Weitere Informationen finden Sie unter [IANA-Protokollnummern](#).

- d. Wählen Sie Änderungen speichern aus.
5. Gehen Sie zum Hinzufügen einer ausgehenden Regel wie folgt vor:
 - a. Wählen Sie die Registerkarte Outbound rules (Ausgehende Regeln).
 - b. Wählen Sie Ausgehende Regeln bearbeiten, Neue Regel hinzufügen aus.
 - c. Geben Sie eine noch ungenutzte Regelnummer ein, einen Typ, ein Protokoll, einen Portbereich, eine Quelle und ob der Datenverkehr zugelassen oder verweigert werden soll. Bei einigen Typen werden das Protokoll und der Port automatisch ausgefüllt. Wenn Sie nach einem Portbereich gefragt werden, geben Sie eine Portnummer oder einen Portbereich (z. B. 49152-65535) ein.

Wenn Sie ein Protokoll nutzen möchten, das nicht in der Liste enthalten ist, wählen Sie Benutzerdefiniertes Protokoll als Typ und anschließend das Protokoll aus. Weitere Informationen finden Sie unter [IANA-Protokollnummern](#).

- d. Wählen Sie Änderungen speichern aus.

Hinzufügen einer Regel zu einer Netzwerk-ACL mithilfe der Befehlszeile

- [create-network-acl-entry](#) (AWS CLI)
- [New-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

Ersetzen einer Regel in einer Netzwerk-ACL mithilfe der Befehlszeile

- [replace-network-acl-entry](#) (AWS CLI)
- [Set-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

Löschen einer Regel aus einer Netzwerk-ACL mithilfe der Befehlszeile

- [delete-network-acl-entry](#) (AWS CLI)
- [Remove-EC2NetworkAclEntry](#) (AWS Tools for Windows PowerShell)

Schritt 3: 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. Wählen Sie im Navigationsbereich Netzwerk und ACLs 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.

(Optional) Netzwerk ACLs mit Firewall Manager verwalten

AWS Firewall Manager vereinfacht Ihre Netzwerk-ACL-Administrations- und Wartungsaufgaben für mehrere Konten und Subnetze. Mit Firewall Manager können Sie Konten und Subnetze in Ihrer Organisation überwachen und die von Ihnen definierten Netzwerk-ACL-Konfigurationen automatisch

anwenden. Firewall Manager ist besonders nützlich, wenn Sie Ihre gesamte Organisation schützen möchten oder wenn Sie häufig neue Subnetze hinzufügen, die Sie automatisch vor einem zentralen Administratorkonto 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 dem Netzwerk definiert haben möchten ACLs, das Sie in Ihrem gesamten Unternehmen verwenden. Sie legen fest, welche Konten und Subnetze in Ihrer Organisation in den Geltungsbereich der Richtlinie von Firewall Manager fallen. Firewall Manager meldet den Konformitätsstatus des Netzwerks ACLs für Subnetze im Geltungsbereich, und Sie können Firewall Manager so konfigurieren, dass die Wiederherstellung nicht konformer Netzwerke automatisiert wird. ACLs

Weitere Informationen finden Sie in den folgenden Ressourcen im AWS Firewall Manager - Entwicklerhandbuch:

- [AWS Firewall Manager Voraussetzungen](#)
- [AWS Firewall Manager Netzwerk-ACL-Richtlinien einrichten](#)
- [Verwenden von Netzwerk-ACL-Richtlinien mit Firewall Manager](#)

Verwalten von Netzwerk-ACL-Zuordnungen für Ihre VPC

Jedes Subnetz ist einer Netzwerk-ACL zugeordnet. Wenn Sie ein Subnetz erstellen, wird dieses zunächst der Standardnetzwerk-ACL für die VPC zugeordnet. Sie können eine benutzerdefinierte Netzwerk-ACL erstellen und diese mit einem oder mehreren Subnetzen verknüpfen, wodurch die vorherige Netzwerk-ACL-Verknüpfung ersetzt wird.

Aufgaben

- [Beschreiben Ihrer Netzwerk-ACL-Zuweisungen](#)
- [Ändern der Subnetze, die einer Netzwerk-ACL zugeordnet sind](#)
- [Ändern der Netzwerk-ACL, die einem Subnetz zugeordnet ist](#)

Beschreiben Ihrer Netzwerk-ACL-Zuweisungen

Sie können die Netzwerk-ACL beschreiben, die einem Subnetz zugewiesen ist, und Sie können auch beschreiben, welche Subnetze einer Netzwerk-ACL zugewiesen sind.

So beschreiben Sie die Netzwerk-ACL, die einem Subnetz zugewiesen ist, mithilfe der Konsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich Subnetze aus.
3. Wählen Sie das Subnetz aus.
4. Wählen Sie die Registerkarte Netzwerk-ACL aus.

Zur Beschreibung der Netzwerk-ACL, die einem Subnetz zugeordnet ist, verwenden Sie den AWS CLI

Verwenden Sie den folgenden [describe-network-acls](#) Befehl, um die Netzwerk-ACL aufzulisten, die dem angegebenen Subnetz zugeordnet sind.

```
aws ec2 describe-network-acls --filters Name=association.subnet-id,Values=subnet-0d2d1b81e0bc9c6d4 --query NetworkAcls[*].NetworkACLId
```

Es folgt eine Beispielausgabe.

```
[  
  "acl-03701d1f82d8c3fd6"  
]
```

Beschreiben der Subnetze, die einer Netzwerk-ACL zugewiesen ist, mithilfe der Konsole

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.
4. Wählen Sie die Registerkarte Subnetzzuordnungen aus.

Um die Subnetze zu beschreiben, die einer Netzwerk-ACL zugeordnet sind, verwenden Sie AWS CLI

Verwenden Sie den folgenden [describe-network-acls](#) Befehl, um die Subnetze aufzulisten, die der angegebenen Netzwerk-ACL zugeordnet sind.

```
aws ec2 describe-network-acls --network-acl-ids acl-060415a18fcc9afde --query NetworkAcls[*].Associations[].SubnetId
```

Es folgt eine Beispielausgabe.

```
[  
  "subnet-0d2d1b81e0bc9c6d4",  
  "subnet-0e990c67809773b19",  
  "subnet-0eb17d85f5dfd33b1",  
  "subnet-0e01d500780bb7468"  
]
```

Ändern der Subnetze, die einer Netzwerk-ACL zugeordnet sind

Sie können die Zuordnung einer benutzerdefinierten Netzwerk-ACL zu einem Subnetz aufheben. Nachdem Sie die Verknüpfung eines Subnetz mit einer benutzerdefinierten Netzwerk-ACL entfernt haben, ordnen wir es automatisch der Standard-Netzwerk-ACL für die VPC zu. Die Änderungen werden nach kurzer Zeit wirksam.

Ändern der Subnetze, die einer Netzwerk-ACL zugeordnet sind

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich die Option Netzwerk ACLs aus.
3. Wählen Sie die Netzwerk-ACL aus.
4. Wählen Sie Aktionen, Subnetzzuordnungen bearbeiten aus.
5. Entfernen Sie das Subnetz aus Ausgewählte Subnetze.
6. Wählen Sie Änderungen speichern aus.

Ändern der Netzwerk-ACL, die einem Subnetz zugeordnet ist

Sie können die einem Subnetz zugeordnete Netzwerk-ACL ändern. Wenn Sie beispielsweise ein Subnetz erstellen, wird dieses zunächst der Standardnetzwerk-ACL für die VPC zugeordnet. Wenn Sie eine benutzerdefinierte Netzwerk-ACL erstellen, wenden Sie die Netzwerk-ACL-Regeln an, indem Sie die Netzwerk-ACL einem oder mehreren Subnetzen zuweisen.

Nachdem Sie die Netzwerk-ACL für ein Subnetz geändert haben, werden die Änderungen nach einer kurzen Zeit wirksam.

Ändern der Netzwerk-ACL, die einem Subnetz zugeordnet ist

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.

2. Wählen Sie im Navigationsbereich Subnetze aus.
3. Wählen Sie das Subnetz aus.
4. Wählen Sie Aktionen, Netzwerk-ACL-Zuordnung bearbeiten aus.
5. Wählen Sie unter Netzwerk-ACL-ID die Netzwerk-ACL aus, die dem Subnetz zugeordnet werden soll, und überprüfen Sie die Regeln für ein- und ausgehende Zugriffe für die ausgewählte Netzwerk-ACL.
6. Wählen Sie Speichern.

So ersetzen Sie Netzwerk-ACL-Zuordnungen mithilfe der Befehlszeile

- [replace-network-acl-association](#) (AWS CLI)
- [Set-EC2NetworkAclAssociation](#) (AWS Tools for Windows PowerShell)

Löschen einer Netzwerk-ACL für Ihre VPC

Wenn Sie eine Netzwerk-ACL nicht mehr benötigen, können Sie sie löschen. Sie können eine Netzwerk-ACL nicht löschen, wenn ihr Subnetze zugeordnet sind. Die Standardnetzwerk-ACL kann nicht gelöscht werden.

So entfernen Sie Subnetzzuordnungen mithilfe der Konsole aus einer Netzwerk-ACL

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich Netzwerk aus ACLs. Der Spalte Verknüpft mit können Sie entnehmen, wie viele Subnetze jeder Netzwerk-ACL zugeordnet sind. Diese Spalte ist –, wenn keine zugehörigen Subnetze vorhanden sind.
3. Wählen Sie die Netzwerk-ACL aus.
4. Wählen Sie Aktionen, Subnetzzuordnungen bearbeiten aus.
5. Entfernen von Subnetzzuordnungen.
6. Wählen Sie Änderungen speichern aus.

Um Ihr Netzwerk ACLs, einschließlich Verknüpfungen, mithilfe der Befehlszeile zu beschreiben

- [describe-network-acls](#) (AWS CLI)
- [Get-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

So ersetzen Sie Netzwerk-ACL-Zuordnungen mithilfe der Befehlszeile

- [replace-network-acl-association](#) (AWS CLI)
- [Set-EC2NetworkAclAssociation](#) (AWS Tools for Windows PowerShell)

So löschen Sie eine Netzwerk-ACL mit der Konsole

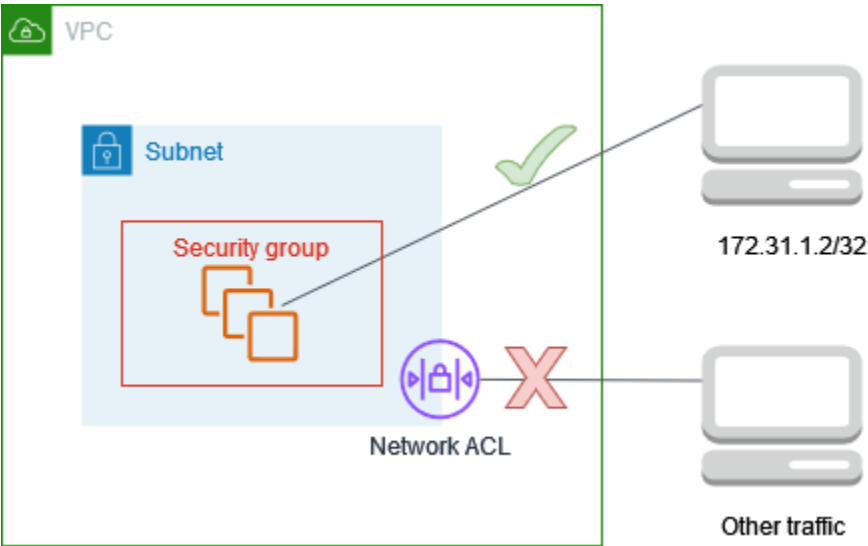
1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im Navigationsbereich Netzwerk aus ACLs.
3. Wählen Sie die Netzwerk-ACL aus.
4. Wählen Sie Aktionen, Netzwerk löschen ACLs.
5. Wenn Sie zur Bestätigung aufgefordert werden, geben Sie **delete** ein und wählen Sie dann Löschen aus.

So löschen Sie eine Netzwerk-ACL mit der Befehlszeile

- [delete-network-acl](#) (AWS CLI)
- [Remove-EC2NetworkAcl](#) (AWS Tools for Windows PowerShell)

Beispiel: Steuern des Zugriffs auf Instances in einem Subnetz

In diesem Beispiel können die Instances im Subnetz miteinander kommunizieren und sind für administrative Aufgaben von vertrauenswürdigen Remote-Computern aus zugreifbar. Der Remotecomputer kann ein Computer in Ihrem lokalen Netzwerk, wie in der Abbildung dargestellt, oder eine Instance in einem anderen Subnetz oder VPC sein. Die Netzwerk-ACL-Regeln für das Subnetz und die Sicherheitsgruppenregeln für die Instances erlauben den Zugriff von der IP-Adresse Ihres Remote-Computers aus. Der gesamte Datenverkehr aus dem Internet oder anderen Netzwerken wird verweigert.



Das Verwenden einer Netzwerk-ACL bietet die Flexibilität, Sicherheitsgruppen oder Sicherheitsgruppenregeln für Instances zu ändern und die Netzwerk-ACL als zusätzliche Schutzebene zu nutzen. Wenn Sie beispielsweise versehentlich die Sicherheitsgruppe aktualisieren, um eingehenden SSH-Zugriff von überall aus zu ermöglichen, die Netzwerk-ACL den Zugriff jedoch nur über den IP-Adressbereich des Remote-Computers zulässt, dann verweigert die Netzwerk-ACL eingehenden SSH-Verkehr von allen anderen IP-Adressen.

Regeln für Netzwerk-ACLs

Im Folgenden finden Sie Beispiele für eingehende Regeln für die mit dem Subnetz verbundene Netzwerk-ACL. Diese Regeln gelten für alle Instances im Subnetz.

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 aus zu.

Regel Nr.	Typ	Protocol (Protokoll)	Port-Bereich	Source	Erlauben/Verweigern	Kommentare
*	Gesamter Datenverkehr	Alle	Alle	0.0.0.0/0	DENY	Verweigert jeglichen anderen eingehenden Datenverkehr.

Im Folgenden finden Sie Beispiele für ausgehende Regeln für die mit dem Subnetz verbundene Netzwerk-ACL. Netzwerk-ACLs sind zustandslos. Daher benötigen Sie eine Regel, die Antworten auf den eingehenden Datenverkehr zulässt.

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.

Sicherheitsgruppenregeln

Im Folgenden finden Sie Beispiele für eingehende Regeln für die mit den Instances verbundene Sicherheitsgruppe. Diese Regeln gelten für alle Instances, die mit der Sicherheitsgruppe verbunden sind. Ein Benutzer mit dem privaten Schlüssel für das mit den Instances verknüpfte Schlüsselpaar kann sich über SSH vom Remote-Computer aus mit den Instances verbinden.

Protokolltyp	Protocol (Protokoll)	Port-Bereich	Source	Kommentare
Gesamter Datenverkehr	Alle	Alle	<i>sg-123456 7890abcde f0</i>	Erlauben Sie die Kommunikation zwischen allen Instances, die dieser Sicherheitsgruppe zugeordnet sind.
SSH	TCP	22	<i>172.31.1.2/32</i>	Lässt eingehenden SSH-Zugriff von dem Remote-Computer zu.

Im Folgenden finden Sie Beispiele für ausgehende Regeln für die mit den Instances verbundene Sicherheitsgruppe. Sicherheitsgruppen sind zustandsbehaftet. Daher benötigen Sie keine Regel, die Antworten auf eingehenden Datenverkehr zulässt.

Protokolltyp	Protocol (Protokoll)	Port-Bereich	Zielbereich	Kommentare
Gesamter Datenverkehr	Alle	Alle	<i>sg-123456 7890abcde f0</i>	Erlauben Sie die Kommunikation zwischen allen Instances, die dieser Sicherheitsgruppe zugeordnet sind.

Protokolltyp	Protocol (Protokoll)	Port-Bereich	Zielbereich	Kommentare
				tsgruppe zugeordnet sind.

Unterschiede zwischen Netzwerk ACLs - und Sicherheitsgruppen

In der folgenden Tabelle sind die grundlegenden Unterschiede zwischen Netzwerk ACLs - und Sicherheitsgruppen zusammengefasst.

Merkmal	Netzwerk-ACL	Sicherheitsgruppe
Betriebsniveau	Subnetzniveau	Instance-Ebene
Scope	Gilt für alle Instances in den verbundenen Subnetzen	Gilt für alle Instances, die mit der Sicherheitsgruppe verbunden sind.
Art der Regel	Zulassen- und Verweigern-Regeln	Nur Regeln zulassen
Regelauswertung	Bewertet Regeln in aufsteigender Reihenfolge, bis eine Übereinstimmung für den Datenverkehr gefunden wird	Alle Regeln werden vor dem Erlauben von Datenverkehr ausgewertet.
Datenverkehr zurücksenden	Muss ausdrücklich erlaubt sein (zustandslos)	Automatisch zugelassen (zustands behaftet)

Ausfallsicherheit in Amazon Virtual Private Cloud

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

AWS-Regionen sind die wichtigsten Bausteine, die jeweils einen eigenen geografischen Standort mit mehreren physisch getrennten und isolierten Availability Zones repräsentieren. Diese Availability Zones sind durch eine Netzwerkstruktur mit niedriger Latenz, hohem Durchsatz und hoher Redundanz verbunden, die eine nahtlose Kommunikation und Datenübertragung zwischen ihnen ermöglicht.

Die Architektur der Availability Zones ist ein wesentliches Unterscheidungsmerkmal, da sie weitaus robuster und fehlertoleranter als herkömmliche Konfigurationen mit einem oder mehreren Rechenzentren konzipiert sind. Durch die Verteilung von Ressourcen auf mehrere Availability Zones innerhalb einer Region können Anwendungen und Datenbanken so konzipiert werden, dass ein automatischer Failover zwischen den Zonen ohne Unterbrechung des Service erfolgt. Dieses Maß an Redundanz und Hochverfügbarkeit ist eine wichtige Voraussetzung für geschäftskritische Workloads und ermöglicht es Unternehmen, ausfallsichere cloudnative Lösungen zu entwickeln.

Darüber hinaus ermöglichen der Umfang und die globale Reichweite der AWS Infrastruktur den Kunden, ihre Anwendungen näher am Endbenutzer bereitzustellen, wodurch die Latenz reduziert und das Benutzererlebnis insgesamt verbessert wird. Die Verfügbarkeit mehrerer Regionen auf der ganzen Welt ermöglicht auch eine effektive Datensouveränität und Compliance, da Kunden Daten innerhalb der geografischen Grenzen speichern und verarbeiten können, die für ihre spezifischen regulatorischen und geschäftlichen Anforderungen erforderlich sind.

Durch die Nutzung der AWS globalen Infrastruktur können Unternehmen ihre Cloud-Umgebungen so gestalten, dass sie hochverfügbar, fehlertolerant und skalierbar sind und sich flexibel an sich ändernde Anforderungen und sich entwickelnde Geschäftsanforderungen anpassen können. Diese robuste Grundlage ist eine wichtige Voraussetzung für die erfolgreiche Implementierung moderner, cloudbasierter Anwendungen und Services.

[Weitere Informationen zu Availability Zones AWS-Regionen und Availability Zones finden Sie unter Globale Infrastruktur AWS .](#)

Sie können Ihre so konfigurieren VPCs , dass sie die Ausfallsicherheitsanforderungen für Ihre Workloads erfüllt. 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. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der [AWS Sicherheitsdokumentation](#).

Sperren Sie den öffentlichen Zugriff VPCs auf Subnetze

VPC Block Public Access (BPA) ist ein zentralisiertes Sicherheitsfeature, das es Ihnen ermöglicht, den öffentlichen Internetzugang zu VPC-Ressourcen für ein gesamtes AWS -Konto zu unterbinden und so die Einhaltung von Sicherheitsanforderungen zu gewährleisten und gleichzeitig Flexibilität für spezifische Ausnahmen und Auditfunktionen zu bieten.

Das VPC-BPA-Feature hat die folgenden Modi:

- Bidirektional: Der gesamte Verkehr zu und von Internet-Gateways und Internet-Gateways für ausgehenden Datenverkehr in dieser Region (mit Ausnahme von ausgeschlossenen Netzwerken und Subnetzen) wird blockiert. VPCs
- Nur eingehender Datenverkehr: Der gesamte Internetverkehr zu den VPCs in dieser Region (mit Ausnahme von Subnetzen, die ausgeschlossen sind) wird blockiert. VPCs Nur der Datenverkehr von und zu NAT-Gateways und Internet-Gateways nur für ausgehenden Verkehr wird zugelassen, da diese Gateways nur den Aufbau von ausgehenden Verbindungen erlauben.

Sie können für dieses Feature auch „Ausschlüsse“ für Datenverkehr erstellen, den Sie nicht blockieren möchten. Ein Ausschluss ist ein Modus, der auf eine einzelne VPC oder ein Subnetz angewendet werden kann, der es vom VPC-BPA-Modus des Kontos ausnimmt und bidirektionalen oder nur ausgehenden Zugriff erlaubt.

Ausschlüsse können einen der folgenden Modi haben:

- **Bidirektional:** Der gesamte Internetverkehr zu und von den ausgeschlossenen VPCs Subnetzen und Subnetzen ist zulässig.
- **Nur ausgehender Internetverkehr:** Ausgehender Internetverkehr aus den ausgeschlossenen Subnetzen und Subnetzen ist zulässig. VPCs Eingehender Internetverkehr zu den ausgeschlossenen und den ausgeschlossenen Subnetzen wird blockiert. VPCs Dies gilt nur, wenn VPC-BPA auf „Bidirektional“ eingestellt ist.

Inhalt

- [VPC-BPA-Grundlagen](#)
- [Bewerten der Auswirkungen von VPC-BPA und Überwachen von VPC-BPA](#)
- [Erweitertes Beispiel](#)

VPC-BPA-Grundlagen

Dieser Abschnitt behandelt wichtige Details zu VPC BPA, einschließlich der Services, die es unterstützen und wie Sie damit arbeiten können.

Inhalt

- [Regionale Verfügbarkeit](#)
- [AWS Auswirkungen auf den Service und Support](#)
- [VPC-BPA-Einschränkungen](#)
- [Steuerung des Zugriffs auf VPC BPA mit einer IAM-Richtlinie](#)
- [Aktivieren des bidirektionalen VPC-BPA-Modus für Ihr Konto](#)
- [Ändern des VPC-BPA-Modus auf nur eingehenden Datenverkehr](#)
- [Erstellen und Löschen von Ausschlüssen](#)
- [Aktivieren von VPC BPA auf Organisationsebene](#)

Regionale Verfügbarkeit

VPC BPA ist in allen [AWS Handelsregionen einschließlich GovCloud der Regionen](#) China erhältlich.

In diesem Leitfaden finden Sie auch Informationen zur Verwendung von Network Access Analyzer und Reachability Analyzer mit VPC BPA. Beachten Sie, dass Network Access Analyzer und

Reachability Analyzer nicht in allen kommerziellen Regionen verfügbar sind. Informationen zur regionalen Verfügbarkeit von Network Access Analyzer und Reachability Analyzer finden Sie unter [Einschränkungen](#) im Handbuch für Network Access Analyzer sowie unter [Überlegungen](#) im Leitfaden Reachability Analyzer.

AWS Auswirkungen auf den Service und Support

Die folgenden Ressourcen und Services unterstützen VPC BPA und der Datenverkehr zu diesen Services und Ressourcen wird durch VPC BPA beeinträchtigt:

- Internet-Gateway: Der gesamte eingehende und ausgehende Datenverkehr wird blockiert.
- Internet-Gateway nur für ausgehenden Verkehr: Der gesamte ausgehende Datenverkehr wird blockiert. Internet-Gateways nur für ausgehenden Verkehr lassen keinen eingehenden Datenverkehr zu.
- Gateway Load Balancer (GWLB): Der gesamte ein- und ausgehende Datenverkehr wird blockiert, auch wenn das Subnetz mit GWLB-Endpunkten ausgeschlossen ist.
- NAT-Gateway: Der gesamte eingehende und ausgehende Datenverkehr wird blockiert. NAT-Gateways benötigen ein Internet-Gateway für die Internetverbindung.
- Mit dem Internet verbundener Network Load Balancer: Der gesamte ein- und ausgehende Datenverkehr wird blockiert. Mit dem Internet verbundene Network Load Balancer benötigen ein Internet-Gateway für die Internetverbindung.
- Mit dem Internet verbundener Application Load Balancer: Der gesamte ein- und ausgehende Datenverkehr wird blockiert. Mit dem Internet verbundene Application Load Balancer benötigen ein Internet-Gateway für die Internetverbindung.
- Amazon CloudFront VPC Origins: Der gesamte eingehende und ausgehende Verkehr ist blockiert.
- Direct Connect: Der gesamte eingehende und ausgehende Verkehr, der öffentliche virtuelle Schnittstellen (öffentliche IPv4 oder globale IPv6 Unicast-Adressen) verwendet, ist blockiert. Dieser Datenverkehr nutzt das Internet-Gateway (oder das Internet-Gateway nur für ausgehenden Datenverkehr) für die Konnektivität.
- AWS Global Accelerator: Eingehender Datenverkehr zu VPCs wird blockiert, unabhängig davon, ob das Ziel anderweitig über das Internet zugänglich ist oder nicht.
- AWS Network Firewall: Der gesamte ein- und ausgehende Datenverkehr wird blockiert, auch wenn das Subnetz mit Firewall-Endpunkten ausgeschlossen ist.
- AWS Wavelength Carrier-Gateway: Der gesamte eingehende und ausgehende Verkehr ist blockiert.

Datenverkehr im Zusammenhang mit privater Konnektivität, wie z. B. Datenverkehr für die folgenden Services und Ressourcen, wird von VPC BPA nicht blockiert oder beeinträchtigt:

- AWS Client VPN
- AWS CloudWAN
- AWS Outposts lokales Gateway
- AWS Site-to-Site VPN
- Transit Gateway
- AWS Verified Access

Important

- Wenn Sie eingehenden und ausgehenden Datenverkehr über eine Appliance weiterleiten (z. B. ein Sicherheits- oder Überwachungstool eines Drittanbieters), die auf einer EC2 Instance in einem Subnetz ausgeführt wird, muss bei Verwendung von VPC BPA dieses Subnetz ausgeschlossen werden, damit der Datenverkehr ein- und ausfließen kann. Andere Subnetze, die Datenverkehr an das Appliance-Subnetz und nicht an das Internet-Gateway senden, müssen nicht als Ausnahmen ergänzt werden.
- Privater Datenverkehr, der von Ressourcen in Ihrer VPC an andere in Ihrer VPC ausgeführte Services, wie z. B. den Route-53-Resolver, gesendet wird, ist auch dann zulässig, wenn VPC BPA aktiviert ist, da er nicht über ein Internet-Gateway in Ihrer VPC läuft. Es ist möglich, dass diese Services in Ihrem Namen Anfragen an Ressourcen außerhalb der VPC stellen, z. B. um eine DNS-Abfrage aufzulösen, und Informationen über die Aktivität von Ressourcen innerhalb Ihrer VPC preisgeben, wenn sie nicht durch andere Sicherheitskontrollen abgeschwächt werden.

VPC-BPA-Einschränkungen

Der VPC BPA-Modus für eingehenden Datenverkehr wird in Local Zones (LZs) nicht unterstützt, in denen NAT-Gateways und Internet-Gateways nur für ausgehenden Datenverkehr nicht zulässig sind.

Steuerung des Zugriffs auf VPC BPA mit einer IAM-Richtlinie

Beispiele für IAM-Richtlinien, die allow/deny auf die VPC BPA-Funktion zugreifen, finden Sie unter [Sperrt den öffentlichen Zugriff VPCs auf Subnetze](#)

Aktivieren des bidirektionalen VPC-BPA-Modus für Ihr Konto

Der bidirektionale VPC BPA-Modus blockiert den gesamten Verkehr zu und von Internet-Gateways und Internet-Gateways nur für ausgehenden Datenverkehr in dieser Region (mit Ausnahme von ausgeschlossenen Netzwerken und Subnetzen). VPCs Weitere Informationen über Ausschlüsse finden Sie unter [Erstellen und Löschen von Ausschlüssen](#).

Important

Wir empfehlen Ihnen dringend, die Workloads, die Internetzugang benötigen, gründlich zu überprüfen, bevor Sie VPC BPA in Ihren Produktionskonten aktivieren.

Note

- Um VPC BPA in den Subnetzen VPCs und in Ihrem Konto zu aktivieren, müssen Sie Eigentümer der VPCs Subnetze und sein.
- Wenn Sie derzeit VPC-Subnetze für andere Konten freigeben, gilt der vom Eigentümer des Subnetzes erzwungene VPC-BPA-Modus auch für den Datenverkehr der Teilnehmer, aber die Teilnehmer können die VPC-BPA-Einstellungen, die sich auf das freigegebene Subnetz auswirken, nicht kontrollieren.

AWS-Managementkonsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie Einstellungen für den öffentlichen Zugriff bearbeiten aus.
4. Wählen Sie Blockieren des öffentlichen Zugriffs aktivieren und Bidirektional und anschließend Änderungen speichern aus.
5. Warten Sie, bis sich der Status zu Ein ändert. Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

Der bidirektionale Modus von VPC BPA ist nun aktiviert.

AWS CLI

1. Aktivieren Sie VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

2. Zeigen Sie den Status von VPC BPA an:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Ändern des VPC-BPA-Modus auf nur eingehenden Datenverkehr

Der VPC BPA-Modus blockiert den gesamten Internetverkehr zu den VPCs in dieser Region (mit Ausnahme von Subnetzen, die VPCs ausgeschlossen sind). Nur der Datenverkehr von und zu NAT-Gateways und Internet-Gateways nur für ausgehenden Verkehr wird zugelassen, da diese Gateways nur den Aufbau von ausgehenden Verbindungen erlauben.

AWS-Managementkonsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie Einstellungen für den öffentlichen Zugriff bearbeiten aus.
4. Ändern Sie die Richtung auf Nur eingehenden Zugriff.
5. Speichern Sie die Änderungen und warten Sie, bis der Status aktualisiert wird. Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

AWS CLI

1. Ändern Sie die Blockierrichtung von VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-ingress
```

Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

2. Zeigen Sie den Status von VPC BPA an:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

Erstellen und Löschen von Ausschlüssen

Ein VPC-BPA-Ausschluss ist ein Modus, der auf eine einzelne VPC oder ein Subnetz angewendet werden kann, der es vom VPC-BPA-Modus des Kontos ausnimmt und bidirektionalen oder nur ausgehenden Zugriff erlaubt. Sie können VPC-BPA-Ausschlüsse für VPCs und Subnetze erstellen, auch wenn VPC BPA für das Konto nicht aktiviert ist, um sicherzustellen, dass der Datenverkehr der Ausschlüsse nicht unterbrochen wird, wenn VPC BPA aktiviert ist. Ein Ausschluss für eine VPC gilt automatisch für alle Subnetze in der VPC.

Sie können maximal 50 Ausschlüsse erstellen. Informationen zum Anfordern einer Grenzwerverhöhung finden Sie unter VPC BPA exclusions per account in [Amazon VPC-Kontingente](#).

AWS-Managementkonsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Führen Sie auf der Registerkarte Öffentlichen Zugriff blockieren unter Ausnahmen eine der folgenden Aktionen aus:
 - Um eine Ausnahme zu löschen, wählen Sie die Ausnahme und dann Aktionen > Ausnahmen löschen aus.
 - Um eine Ausnahme zu erstellen, wählen Sie Ausnahmen erstellen und fahren Sie mit den weiteren Schritten fort.
4. Wählen Sie eine Blockierrichtung aus:
 - Bidirektional: Lässt den gesamten Internetverkehr zu und von den ausgeschlossenen Netzen und Subnetzen zu. VPCs

- Nur ausgehender Internetverkehr: Erlaubt ausgehenden Internetverkehr aus den ausgeschlossenen Netzen und Subnetzen. VPCs Blockiert eingehenden Internetverkehr in die ausgeschlossenen Netze und Subnetze. VPCs Diese Einstellung gilt, wenn VPC-BPA auf Bidirektional eingestellt ist.
5. Wählen Sie eine VPC oder ein Subnetz aus.
 6. Wählen Sie Ausschlüsse erstellen aus.
 7. Warten Sie, bis sich der Status Ausschluss auf Aktiv ändert. Möglicherweise müssen Sie die Ausschlusstabelle aktualisieren, damit die Änderung angezeigt wird.

Der Ausschluss wurde erstellt.

AWS CLI

1. Ändern Sie die Richtung der Ausschlusserlaubnis:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. Es kann einige Zeit dauern, bis der Ausschlussstatus aktualisiert wird. So zeigen Sie den Status des Ausschlusses an:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --exclusion-ids exclusion-id
```

Aktivieren von VPC BPA auf Organisationsebene

Wenn Sie AWS Organizations verwenden, um Konten in Ihrer Organisation zu verwalten, können Sie eine [AWS deklarative Organisationsrichtlinie](#) verwenden, um VPC BPA für die Konten in der Organisation durchzusetzen. Weitere Informationen über die deklarative Richtlinie für VPC BPA finden Sie unter [Supported declarative policies](#) im AWS -Organizations-Benutzerhandbuch.

Note

- Sie können die deklarative Richtlinie für VPC BPA verwenden, um zu konfigurieren, ob Ausschlüsse zulässig sind. Sie können mit der Richtlinie jedoch keine Ausschlüsse erstellen. Um Ausnahmen zu erstellen, müssen Sie sie weiterhin in dem Konto erstellen,

das Eigentümer der VPC ist. Weitere Informationen zum Erstellen von VPC-BPA-Ausschlüssen finden Sie unter [Erstellen und Löschen von Ausschlüssen](#).

- Wenn die deklarative Richtlinie für VPC BPA aktiviert ist, wird in den Einstellungen für Öffentlichen Zugriff blockieren die Option Von der deklarativen Richtlinie verwaltet angezeigt, und Sie können die Einstellungen für VPC BPA auf Kontoebene nicht ändern.

Bewerten der Auswirkungen von VPC-BPA und Überwachen von VPC-BPA

Dieser Abschnitt enthält Informationen darüber, wie Sie die Auswirkungen von VPC BPA bewerten können, bevor Sie es aktivieren, und wie Sie überwachen, ob der Datenverkehr nach dem Aktivieren blockiert wird.

Inhalt

- [Bewerten der Auswirkungen von VPC BPA mithilfe von Network Access Analyzer](#)
- [Überwachen der VPC-BPA-Auswirkungen mit Flow-Protokollen](#)
- [Verfolgen Sie das Löschen von Ausschlüssen mit CloudTrail](#)
- [Überprüfen mit Reachability Analyzer, ob die Konnektivität blockiert ist](#)

Bewerten der Auswirkungen von VPC BPA mithilfe von Network Access Analyzer

In diesem Abschnitt verwenden Sie Network Access Analyzer, um die Ressourcen in Ihrem Konto anzuzeigen, die ein Internet-Gateway verwenden, bevor Sie VPC BPA aktivieren und den Zugriff blockieren. Verwenden Sie diese Analyse, um die Auswirkungen des Aktivierens von VPC BPA in Ihrem Konto und des Blockierens von Datenverkehr zu verstehen.

Note

- Network Access Analyzer unterstützt IPv6 dies nicht. Sie können ihn also nicht verwenden, um die möglichen Auswirkungen von VPC BPA auf ausgehenden Internet-Gateway-Datenverkehr zu überprüfen. IPv6
- Die Analysen, die Sie mit Network Access Analyzer durchführen, sind kostenpflichtig. Weitere Informationen finden Sie unter [Preisgestaltung](#) im Handbuch für Network Access Analyzer.

- Informationen über die regionale Verfügbarkeit von Network Access Analyzer finden Sie unter [Einschränkungen](#) im Handbuch für Network Access Analyzer.

AWS-Managementkonsole

1. Öffnen Sie die Network Insights-Konsole unter. AWS <https://console.aws.amazon.com/networkinsights/>
2. Wählen Sie Network Access Analyzer aus.
3. Klicken Sie auf Netzwerkzugriffsbereich erstellen.
4. Wählen Sie Auswirkungen von VPC Block Public Access bewerten und dann Weiter aus.
5. Die Vorlage ist bereits so konfiguriert, dass sie den Datenverkehr zu und von den Internet-Gateways in Ihrem Konto analysiert. Sie können dies unter Quelle und Ziel einsehen.
6. Wählen Sie Weiter aus.
7. Klicken Sie auf Netzwerkzugriffsbereich erstellen.
8. Wählen Sie den gerade erstellten Bereich aus und klicken Sie auf Analysieren.
9. Warten Sie, bis die Analyse abgeschlossen ist.
10. Zeigen Sie die Ergebnisse der Analyse an. Jede Zeile unter Erkenntnisse zeigt einen Netzwerkpfad, den ein Paket in einem Netzwerk zu oder von einem Internet-Gateway in Ihrem Konto nehmen kann. Wenn Sie in diesem Fall VPC BPA aktivieren und keines der in diesen Ergebnissen aufgeführten VPCs und oder Subnetze als VPC-BPA-Ausschlüsse konfiguriert ist, wird der Datenverkehr zu diesen VPCs und Subnetzen eingeschränkt.
11. Analysieren Sie jedes Ergebnis, um die Auswirkungen von VPC BPA auf Ihre Ressourcen zu verstehen. VPCs

Die Analyse der Auswirkungen ist abgeschlossen.

AWS CLI

1. Erstellen Sie einen Netzwerkzugriffsbereich:

```
aws ec2 create-network-insights-access-scope --region us-east-2 --match-paths  
"Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"  
"Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
```

2. Starten Sie die Analyse des Bereichs:

```
aws ec2 start-network-insights-access-scope-analysis --region us-east-2 --  
network-insights-access-scope-id nis-id
```

3. Rufen Sie die Ergebnisse der Analyse ab:

```
aws ec2 get-network-insights-access-scope-analysis-findings --region us-east-2  
--network-insights-access-scope-analysis-id nisa-0aa383a1938f94cd1 --max-items  
1
```

Die Ergebnisse zeigen den Verkehr zu und von den Internet-Gateways in allen Bereichen Ihres Kontos VPCs . Die Ergebnisse sind als „Ergebnisse“ zusammengefasst. "FindingId,:" AnalysisFinding -1" gibt an, dass dies das erste Ergebnis der Analyse ist. Beachten Sie, dass es mehrere Erkenntnisse gibt, die jeweils auf einen Datenverkehrsfluss hinweisen, der durch die Aktivierung von VPC BPA beeinträchtigt wird. Das erste Ergebnis zeigt, dass der Datenverkehr an einem Internet-Gateway (" SequenceNumber „: 1) begann, an eine NACL (" SequenceNumber „: 2) an eine Sicherheitsgruppe (" SequenceNumber „: 3) weitergeleitet wurde und an einer Instanz (" SequenceNumber „: 4) endete.

4. Analysieren Sie die Ergebnisse, um die Auswirkungen von VPC BPA auf Ihre Ressourcen zu verstehen. VPCs

Die Analyse der Auswirkungen ist abgeschlossen.

Überwachen der VPC-BPA-Auswirkungen mit Flow-Protokollen

VPC-Flow-Protokolle ist ein Feature, mit dem Sie Informationen über den IP-Datenverkehr zu und von Elastic-Network-Schnittstellen in Ihrer VPC erfassen können. Sie können dieses Feature verwenden, um den Datenverkehr zu überwachen, der durch VPC BPA daran gehindert wird, Ihre Instance-Netzwerkschnittstellen zu erreichen.

Erstellen Sie ein Flow-Protokoll für Ihre VPC anhand der Schritte unter [Arbeiten mit Flow-Protokollen](#).

Stellen Sie beim Erstellen des Flow-Protokolls sicher, dass Sie ein benutzerdefiniertes Format verwenden, das das Feld `reject-reason` enthält.

Wenn Sie die Flow-Protokolle anzeigen und der Datenverkehr zu einer ENI aufgrund von VPC-BPA abgelehnt wird, wird im Flow-Protokolleintrag ein `reject-reason` von BPA angezeigt.

Zusätzlich zu den standardmäßigen [Einschränkungen](#) für VPC-Flow-Protokolle sind die folgenden, für VPC BPA spezifischen Einschränkungen zu beachten:

- Flow-Protokolle für VPC BPA enthalten keine [übersprungenen Datensätze](#).
- [bytes](#) sind nicht in Flow-Protokollen für VPC BPA enthalten, auch wenn Sie das Feld bytes in Ihr Flow-Protokoll aufnehmen.

Verfolgen Sie das Löschen von Ausschlüssen mit CloudTrail

In diesem Abschnitt wird erklärt, wie Sie AWS CloudTrail das Löschen von VPC-BPA-Ausschlüssen überwachen und verfolgen können.

AWS-Managementkonsole

Sie können alle gelöschten Ausnahmen im CloudTrail Ereignisverlauf einsehen, indem Sie in der Konsole unter Ressourcentyp > AWS::EC2::VPCLockPublicAccessExclusion suchen.

AWS CloudTrail <https://console.aws.amazon.com/cloudtrailv2/>

AWS CLI

Mit dem Befehl `lookup-events` können Sie die Ereignisse im Zusammenhang mit dem Löschen von Ausschlüssen anzeigen:

```
aws cloudtrail lookup-events --lookup-attributes  
AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCLockPublicAccessExclusion
```

Überprüfen mit Reachability Analyzer, ob die Konnektivität blockiert ist

[VPC Reachability Analyzer](#) kann verwendet werden, um zu bewerten, ob bestimmte Netzwerkpfade angesichts Ihrer Netzwerkkonfiguration, einschließlich der Einstellungen für VPC BPA, erreicht werden können oder nicht.

Informationen zur regionalen Verfügbarkeit von Reachability Analyzer finden Sie unter [Überlegungen](#) im Leitfaden Reachability Analyzer.

AWS-Managementkonsole

1. Öffnen Sie die AWS Network Insights-Konsole unter <https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer>.

2. Klicken Sie auf Pfad erstellen und analysieren.
3. Wählen Sie als Quelltyp die Option Internet-Gateways aus und wählen Sie dann aus der Dropdown-Liste Quelle das Internet-Gateway aus, für das Sie den Datenverkehr blockieren möchten.
4. Wählen Sie unter Zieltyp die Option Instances aus und wählen Sie dann aus dem Dropdown-Menü Ziel die Instance aus, zu der Sie den Datenverkehr blockieren möchten.
5. Klicken Sie auf Pfad erstellen und analysieren.
6. Warten Sie, bis die Analyse abgeschlossen ist. Dies kann einige Minuten dauern.
7. Sobald dies abgeschlossen ist, sollten Sie sehen, dass der Erreichbarkeitsstatus Nicht erreichbar lautet und dass die Pfaddetails zeigen, dass `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` die Ursache für dieses Erreichbarkeitsproblem ist.

AWS CLI

1. Erstellen Sie einen Netzwerkpfad mit der ID des Internet-Gateways, von dem aus Sie den Datenverkehr blockieren möchten (Quelle), und der ID der Instance, zu der Sie den Datenverkehr blockieren möchten (Ziel):

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --  
destination instance-id --protocol TCP
```

2. Starten Sie eine Analyse des Netzwerkpfads:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-  
path-id nip-id
```

3. Rufen Sie die Ergebnisse der Analyse ab:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-  
insights-analysis-ids nia-id
```

4. Prüfen Sie, ob `VPC_BLOCK_PUBLIC_ACCESS_ENABLED` das `ExplanationCode` für die fehlende Erreichbarkeit ist.

Erweitertes Beispiel

Dieser Abschnitt enthält ein erweitertes Beispiel, das Ihnen hilft zu verstehen, wie das Feature VPC Block Public Access in verschiedenen Szenarien funktioniert. Jedes Szenario baut auf dem vorherigen Szenario auf, daher ist es wichtig, dass Sie die Schritte in der richtigen Reihenfolge ausführen.

Important

Gehen Sie dieses Beispiel nicht in einem Produktionskonto durch. Wir empfehlen Ihnen dringend, die Workloads, die Internetzugang benötigen, gründlich zu überprüfen, bevor Sie VPC BPA in Ihren Produktionskonten aktivieren.

Note

Sie benötigen bestimmte Ressourcen in Ihrem Konto, um das VPC-BPA-Feature vollständig zu verstehen. In diesem Abschnitt stellen wir eine CloudFormation Vorlage zur Verfügung, mit der Sie die Ressourcen bereitstellen können, die Sie benötigen, um die Funktionsweise dieser Funktion vollständig zu verstehen. Mit den Ressourcen, die Sie mit der CloudFormation Vorlage bereitstellen, und den Analysen, die Sie mit Network Access Analyzer und Reachability Analyzer durchführen, fallen Kosten an. Wenn Sie die Vorlage in diesem Abschnitt verwenden, stellen Sie sicher, dass Sie die Bereinigungsschritte abschließen, wenn Sie mit diesem Beispiel fertig sind.

Inhalt

- [CloudFormation Vorlage bereitstellen \(optional\)](#)
- [Anzeigen der Auswirkungen von VPC BPA mit Network Access Analyzer](#)
- [Szenario 1: Herstellen einer Verbindung zu Instances ohne aktiviertes VPC BPA](#)
- [Szenario 2: Aktivieren von VPC BPA im bidirektionalen Modus](#)
- [Szenario 3: Ändern des VPC BPA auf nur eingehenden Datenverkehrsmodus](#)
- [Szenario 4: Erstellen eines Ausschlusses](#)
- [Szenario 5: Ändern des Ausschlussmodus](#)
- [Szenario 6: Ändern des VPC-BPA-Modus](#)
- [Bereinigen](#)

CloudFormation Vorlage bereitstellen (optional)

Sie benötigen eine VPC, Subnetze, Instances und andere Ressourcen, um zu demonstrieren, wie dieses Feature funktioniert. Um die Durchführung dieser Demonstration zu erleichtern, haben wir unten eine CloudFormation -Vorlage bereitgestellt, mit der Sie schnell die für die Szenarien in dieser Demo erforderlichen Ressourcen einrichten können. Dieser Schritt ist optional und möglicherweise möchten Sie sich nur die Diagramme in den Szenarien in diesem Abschnitt ansehen.

Note

- Mit den Ressourcen, die Sie in diesem Abschnitt mit der CloudFormation Vorlage erstellen, sind Kosten verbunden, z. B. die Kosten für das NAT-Gateway und öffentliche IPv4 Adressen. Um übermäßige Kosten zu vermeiden, stellen Sie sicher, dass Sie die Bereinigungsschritte durchführen, um alle für dieses Beispiel erstellten Ressourcen zu entfernen.
- Diese CloudFormation Vorlage erstellt die zugrunde liegenden Ressourcen, die für VPC BPA benötigt werden, aktiviert jedoch nicht die VPC BPA-Funktion selbst. Die hier bereitgestellten Ressourcen sollen Ihnen dabei helfen, die VPC-BPA-Funktion zu verstehen und zu testen, sobald Sie diese separat aktivieren möchten.

Die Vorlage erstellt die folgenden Ressourcen in Ihrem Konto:

- Internet-Gateway nur für ausgehenden Verkehr
- Internet-Gateway
- NAT-Gateway
- Zwei öffentliche Subnetze
- Ein privates Subnetz
- Zwei EC2 Instanzen mit öffentlichen und privaten Adressen IPv4
- Eine EC2 Instanz mit einer IPv6 Adresse und einer privaten IPv4 Adresse
- Eine EC2 Instanz nur mit einer privaten IPv4 Adresse
- Sicherheitsgruppe, die eingehenden SSH- und ICMP-Datenverkehr zulässt und den gesamten ausgehenden Datenverkehr erlaubt
- VPC-Flow-Protokoll
- Ein EC2 Instance Connect-Endpunkt in Subnetz B

Kopieren Sie die nachstehende Vorlage und speichern Sie sie in einer YAML-Datei.

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Creates a VPC with public and private subnets, NAT gateway, and EC2
instances for VPC BPA.

Parameters:
  InstanceAMI:
    Description: ID of the Amazon Machine Image (AMI) to use with the instances
    launched by this template
    Type: AWS::EC2::Image::Id
  InstanceType:
    Description: EC2 Instance type to use with the instances launched by this template
    Type: String
    Default: t2.micro

Resources:

  # VPC
  VPCBPA:
    Type: AWS::EC2::VPC
    Properties:
      CidrBlock: 10.0.0.0/16
      EnableDnsHostnames: true
      EnableDnsSupport: true
      InstanceTenancy: default
      Tags:
        - Key: Name
          Value: VPC BPA

  # VPC IPv6 CIDR
  VPCBPAIPv6CidrBlock:
    Type: AWS::EC2::VPCCidrBlock
    Properties:
      VpcId: !Ref VPCBPA
      AmazonProvidedIpv6CidrBlock: true

  # EC2 Key Pair
  VPCBPAKeyPair:
    Type: AWS::EC2::KeyPair
    Properties:
      KeyName: vpc-bpa-key

  # Internet Gateway
```

```
VPCBPAINternetGateway:
  Type: AWS::EC2::InternetGateway
  Properties:
    Tags:
      - Key: Name
        Value: VPC BPA Internet Gateway

VPCBPAINternetGatewayAttachment:
  Type: AWS::EC2::VPCEGatewayAttachment
  Properties:
    VpcId: !Ref VPCBPA
    InternetGatewayId: !Ref VPCBPAINternetGateway

# Egress-Only Internet Gateway
VPCBPAEgressOnlyInternetGateway:
  Type: AWS::EC2::EgressOnlyInternetGateway
  Properties:
    VpcId: !Ref VPCBPA

# Subnets
VPCBPAPublicSubnetA:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPCBPA
    CidrBlock: 10.0.1.0/24
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: VPC BPA Public Subnet A

VPCBPAPublicSubnetB:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPCBPA
    CidrBlock: 10.0.2.0/24
    MapPublicIpOnLaunch: true
    Tags:
      - Key: Name
        Value: VPC BPA Public Subnet B

VPCBPAPrivateSubnetC:
  Type: AWS::EC2::Subnet
  Properties:
    VpcId: !Ref VPCBPA
```

```
CidrBlock: 10.0.3.0/24
MapPublicIpOnLaunch: false
Ipv6CidrBlock: !Select [0, !GetAtt VPCBPA.Ipv6CidrBlocks]
AssignIpv6AddressOnCreation: true
Tags:
  - Key: Name
    Value: VPC BPA Private Subnet C
```

NAT Gateway

```
VPCBPANATGateway:
  Type: AWS::EC2::NatGateway
  Properties:
    AllocationId: !GetAtt VPCBPANATGatewayEIP.AllocationId
    SubnetId: !Ref VPCBPAPublicSubnetB
    Tags:
      - Key: Name
        Value: VPC BPA NAT Gateway
```

```
VPCBPANATGatewayEIP:
  Type: AWS::EC2::EIP
  Properties:
    Domain: vpc
    Tags:
      - Key: Name
        Value: VPC BPA NAT Gateway EIP
```

Route Tables

```
VPCBPAPublicRouteTable:
  Type: AWS::EC2::RouteTable
  Properties:
    VpcId: !Ref VPCBPA
    Tags:
      - Key: Name
        Value: VPC BPA Public Route Table
```

```
VPCBPAPublicRoute:
  Type: AWS::EC2::Route
  DependsOn: VPCBPAInternetGatewayAttachment
  Properties:
    RouteTableId: !Ref VPCBPAPublicRouteTable
    DestinationCidrBlock: 0.0.0.0/0
    GatewayId: !Ref VPCBPAInternetGateway
```

```
VPCBPAPublicSubnetARouteTableAssoc:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
  SubnetId: !Ref VPCBPAPublicSubnetA
```

```
  RouteTableId: !Ref VPCBPAPublicRouteTable
```

```
VPCBPAPublicSubnetBRouteTableAssoc:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
  SubnetId: !Ref VPCBPAPublicSubnetB
```

```
  RouteTableId: !Ref VPCBPAPublicRouteTable
```

```
VPCBPAPrivateRouteTable:
```

```
Type: AWS::EC2::RouteTable
```

```
Properties:
```

```
  VpcId: !Ref VPCBPA
```

```
  Tags:
```

```
    - Key: Name
```

```
      Value: VPC BPA Private Route Table
```

```
VPCBPAPrivateRoute:
```

```
Type: AWS::EC2::Route
```

```
Properties:
```

```
  RouteTableId: !Ref VPCBPAPrivateRouteTable
```

```
  DestinationCidrBlock: 0.0.0.0/0
```

```
  NatGatewayId: !Ref VPCBPANATGateway
```

```
VPCBPAPrivateSubnetCRoute:
```

```
Type: AWS::EC2::Route
```

```
Properties:
```

```
  RouteTableId: !Ref VPCBPAPrivateRouteTable
```

```
  DestinationIpv6CidrBlock: ::/0
```

```
  EgressOnlyInternetGatewayId: !Ref VPCBPAEgressOnlyInternetGateway
```

```
VPCBPAPrivateSubnetCRouteTableAssociation:
```

```
Type: AWS::EC2::SubnetRouteTableAssociation
```

```
Properties:
```

```
  SubnetId: !Ref VPCBPAPrivateSubnetC
```

```
  RouteTableId: !Ref VPCBPAPrivateRouteTable
```

```
# EC2 Instances Security Group
```

```
VPCBPAINstancesSecurityGroup:
```

```
Type: AWS::EC2::SecurityGroup
```

```
Properties:
```

```
  GroupName: VPC BPA Instances Security Group
```

```
GroupDescription: Allow SSH and ICMP access
```

```
SecurityGroupIngress:
```

- IpProtocol: tcp
FromPort: 22
ToPort: 22
CidrIp: 0.0.0.0/0
- IpProtocol: icmp
FromPort: -1
ToPort: -1
CidrIp: 0.0.0.0/0

```
VpcId: !Ref VPCBPA
```

```
Tags:
```

- Key: Name
Value: VPC BPA Instances Security Group

```
# EC2 Instances
```

```
VPCBPAInstanceA:
```

```
Type: AWS::EC2::Instance
```

```
Properties:
```

- ImageId: !Ref InstanceAMI
- InstanceType: t2.micro
- KeyName: !Ref VPCBPAKeyPair
- SubnetId: !Ref VPCBPAPublicSubnetA
- SecurityGroupIds:
 - !Ref VPCBPAInstancesSecurityGroup
- Tags:
 - Key: Name
Value: VPC BPA Instance A

```
VPCBPAInstanceB:
```

```
Type: AWS::EC2::Instance
```

```
Properties:
```

- ImageId: !Ref InstanceAMI
- InstanceType: !Ref InstanceType
- KeyName: !Ref VPCBPAKeyPair
- SubnetId: !Ref VPCBPAPublicSubnetB
- SecurityGroupIds:
 - !Ref VPCBPAInstancesSecurityGroup
- Tags:
 - Key: Name
Value: VPC BPA Instance B

```
VPCBPAInstanceC:
```

```
Type: AWS::EC2::Instance
```

Properties:

```
ImageId: !Ref InstanceAMI
InstanceType: !Ref InstanceType
KeyName: !Ref VPCBPAKeyPair
SubnetId: !Ref VPCBPAPrivateSubnetC
SecurityGroupIds:
  - !Ref VPCBPAInstancesSecurityGroup
Tags:
  - Key: Name
    Value: VPC BPA Instance C
```

VPCBPAInstanceD:

```
Type: AWS::EC2::Instance
Properties:
  ImageId: !Ref InstanceAMI
  InstanceType: !Ref InstanceType
  KeyName: !Ref VPCBPAKeyPair
  NetworkInterfaces:
    - DeviceIndex: '0'
      GroupSet:
        - !Ref VPCBPAInstancesSecurityGroup
      SubnetId: !Ref VPCBPAPrivateSubnetC
      Ipv6AddressCount: 1
  Tags:
    - Key: Name
      Value: VPC BPA Instance D
```

Flow Logs IAM Role**VPCBPAFlowLogRole:**

```
Type: AWS::IAM::Role
Properties:
  AssumeRolePolicyDocument:
    Version: '2012-10-17'
    Statement:
      - Effect: Allow
        Principal:
          Service: vpc-flow-logs.amazonaws.com
        Action: 'sts:AssumeRole'
  Tags:
    - Key: Name
      Value: VPC BPA Flow Logs Role
```

VPCBPAFlowLogPolicy:

```
Type: AWS::IAM::Policy
```


Properties:

PolicyName: VPC-BPA-FlowLogsPolicy

PolicyDocument:

Version: '2012-10-17'

Statement:

- Effect: Allow

Action:

- 'logs:CreateLogGroup'
- 'logs:CreateLogStream'
- 'logs:PutLogEvents'
- 'logs:DescribeLogGroups'
- 'logs:DescribeLogStreams'

Resource: '*'

Roles:

- !Ref VPCBPAFlowLogRole

Flow Logs**VPCBPAFlowLog:**

Type: AWS::EC2::FlowLog

Properties:

ResourceId: !Ref VPCBPA

ResourceType: VPC

TrafficType: ALL

LogDestinationType: cloud-watch-logs

LogGroupName: /aws/vpc-flow-logs/VPC-BPA

DeliverLogsPermissionArn: !GetAtt VPCBPAFlowLogRole.Arn

LogFormat: '\${version} \${account-id} \${interface-id} \${srcaddr} \${dstaddr} \${srcport} \${dstport} \${protocol} \${packets} \${bytes} \${start} \${end} \${action} \${log-status} \${vpc-id} \${subnet-id} \${instance-id} \${tcp-flags} \${type} \${pkt-srcaddr} \${pkt-dstaddr} \${region} \${az-id} \${sublocation-type} \${sublocation-id} \${pkt-src-aws-service} \${pkt-dst-aws-service} \${flow-direction} \${traffic-path} \${reject-reason}'

Tags:

- Key: Name

Value: VPC BPA Flow Logs

EC2 Instance Connect Endpoint**VPCBPAEC2InstanceConnectEndpoint:**

Type: AWS::EC2::InstanceConnectEndpoint

Properties:**SecurityGroupIds:**

- !Ref VPCBPAINstancesSecurityGroup

SubnetId: !Ref VPCBPAPublicSubnetB

Outputs:

VPCBPAVPCId:

Description: A reference to the created VPC

Value: !Ref VPCBPA

Export:

Name: vpc-id

VPCBPAPublicSubnetAId:

Description: The ID of the public subnet A

Value: !Ref VPCBPAPublicSubnetA

VPCBPAPublicSubnetAName:

Description: The name of the public subnet A

Value: VPC BPA Public Subnet A

VPCBPAPublicSubnetBId:

Description: The ID of the public subnet B

Value: !Ref VPCBPAPublicSubnetB

VPCBPAPublicSubnetBName:

Description: The name of the public subnet B

Value: VPC BPA Public Subnet B

VPCBPAPrivateSubnetCId:

Description: The ID of the private subnet C

Value: !Ref VPCBPAPrivateSubnetC

VPCBPAPrivateSubnetCName:

Description: The name of the private subnet C

Value: VPC BPA Private Subnet C

VPCBPAINstanceAId:

Description: The ID of instance A

Value: !Ref VPCBPAINstanceA

VPCBPAINstanceBId:

Description: The ID of instance B

Value: !Ref VPCBPAINstanceB

VPCBPAINstanceCId:

Description: The ID of instance C

Value: !Ref VPCBPAINstanceC

VPCBPAINstanceDId:

Description: The ID of instance D

```
Value: !Ref VPCBPAINstanceD
```

AWS-Managementkonsole

1. Öffnen Sie die CloudFormation Konsole unter. <https://console.aws.amazon.com/cloudformation/>
2. Wählen Sie Stack erstellen aus und laden Sie die YAML-Vorlagendatei hoch.
3. Führen Sie die Schritte durch, um die Vorlage zu starten. Sie müssen eine [Image-ID](#) und einen [Instance-Typ](#) (wie t2.micro) eingeben. Sie müssen außerdem die Möglichkeit haben, eine IAM-Rolle für Sie CloudFormation zu erstellen, damit Sie das Flow-Protokoll erstellen können und über welche Rechte Sie sich CloudWatch anmelden können.
4. Sobald Sie den Stack gestartet haben, zeigen Sie auf der Registerkarte Ereignisse den Fortschritt an und stellen Sie sicher, dass der Stack abgeschlossen ist, bevor Sie fortfahren.

AWS CLI

1. Führen Sie den folgenden Befehl aus, um den CloudFormation Stack zu erstellen:

```
aws cloudformation create-stack --stack-name VPC-BPA-stack --template-body  
file://sampltemplate.yaml --capabilities CAPABILITY_IAM --region us-east-2
```

Ausgabe:

```
{  
  "StackId": "arn:aws:cloudformation:us-east-2:470889052923:stack/VPC-BPA-  
stack/8a7a2cc0-8001-11ef-b196-06386a84b72f"  
}
```

2. Zeigen Sie den Fortschritt an und stellen Sie sicher, dass der Stack abgeschlossen ist, bevor Sie fortfahren:

```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

Anzeigen der Auswirkungen von VPC BPA mit Network Access Analyzer

In diesem Abschnitt verwenden Sie Network Access Analyzer, um die Ressourcen in Ihrem Konto anzuzeigen, die das Internet-Gateway nutzen. Verwenden Sie diese Analyse, um die Auswirkungen des Aktivierens von VPC BPA in Ihrem Konto und des Blockierens von Datenverkehr zu verstehen.

Informationen über die regionale Verfügbarkeit von Network Access Analyzer finden Sie unter [Einschränkungen](#) im Handbuch für Network Access Analyzer.

AWS-Managementkonsole

1. Öffnen Sie die AWS Network Insights-Konsole unter <https://console.aws.amazon.com/networkinsights/>.
2. Wählen Sie Network Access Analyzer aus.
3. Klicken Sie auf Netzwerkzugriffsbereich erstellen.
4. Wählen Sie Auswirkungen von VPC Block Public Access bewerten und dann Weiter aus.
5. Die Vorlage ist bereits so konfiguriert, dass sie den Datenverkehr zu und von den Internet-Gateways in Ihrem Konto analysiert. Sie können dies unter Quelle und Ziel einsehen.
6. Wählen Sie Weiter aus.
7. Klicken Sie auf Netzwerkzugriffsbereich erstellen.
8. Wählen Sie den gerade erstellten Bereich aus und klicken Sie auf Analysieren.
9. Warten Sie, bis die Analyse abgeschlossen ist.
10. Zeigen Sie die Ergebnisse der Analyse an. Jede Zeile unter Erkenntnisse zeigt einen Netzwerkpfad, den ein Paket in einem Netzwerk zu oder von einem Internet-Gateway in Ihrem Konto nehmen kann. Wenn Sie in diesem Fall VPC BPA aktivieren und keines der in diesen Ergebnissen aufgeführten VPCs und oder Subnetze als VPC-BPA-Ausschlüsse konfiguriert ist, wird der Datenverkehr zu diesen VPCs und Subnetzen eingeschränkt.
11. Analysieren Sie jedes Ergebnis, um die Auswirkungen von VPC BPA auf Ihre Ressourcen zu verstehen. VPCs

Die Analyse der Auswirkungen ist abgeschlossen.

AWS CLI

1. Erstellen Sie einen Netzwerkzugriffsbereich:

```
aws ec2 create-network-insights-access-scope --match-paths
"Source={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
"Destination={ResourceStatement={ResourceTypes=["AWS::EC2::InternetGateway"]}}"
--region us-east-2
```

Ausgabe:

```
{
  "NetworkInsightsAccessScope": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "NetworkInsightsAccessScopeArn": "arn:aws:ec2:us-
east-2:470889052923:network-insights-access-scope/nis-04cad3c4b3a1d5e3e",
    "CreatedDate": "2024-09-30T15:55:53.171000+00:00",
    "UpdatedDate": "2024-09-30T15:55:53.171000+00:00"
  },
  "NetworkInsightsAccessScopeContent": {
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "MatchPaths": [
      {
        "Source": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        },
        "Destination": {
          "ResourceStatement": {
            "ResourceTypes": [
              "AWS::EC2::InternetGateway"
            ]
          }
        }
      ]
    ]
  }
}
```

2. Starten Sie die Analyse des Bereichs:

```
aws ec2 start-network-insights-access-scope-analysis --network-insights-access-scope-id nis-04cad3c4b3a1d5e3e --region us-east-2
```

Ausgabe:

```
{
  "NetworkInsightsAccessScopeAnalysis": {
    "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
    "NetworkInsightsAccessScopeAnalysisArn": "arn:aws:ec2:us-east-2:470889052923:network-insights-access-scope-analysis/nisa-0aa383a1938f94cd1",
    "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
    "Status": "running",
    "StartDate": "2024-09-30T15:56:59.109000+00:00",
    "AnalyzedEniCount": 0
  }
}
```

3. Rufen Sie die Ergebnisse der Analyse ab:

```
aws ec2 get-network-insights-access-scope-analysis-findings --network-insights-access-scope-analysis-id nisa-0aa383a1938f94cd1 --region us-east-2 --max-items 1
```

Ausgabe:

```
{
  "AnalysisFindings": [
    {
      "NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
      "NetworkInsightsAccessScopeId": "nis-04cad3c4b3a1d5e3e",
      "FindingId": "AnalysisFinding-1",
      "FindingComponents": [
        {
          "SequenceNumber": 1,
          "Component": {
            "Id": "igw-04a5344b4e30486f1",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:internet-gateway/igw-04a5344b4e30486f1",
            "Name": "VPC BPA Internet Gateway"
          },
          "OutboundHeader": {
```

```

        "DestinationAddresses": [
            "10.0.1.85/32"
        ],
    },
    "InboundHeader": {
        "DestinationAddresses": [
            "10.0.1.85/32"
        ],
        "DestinationPortRanges": [
            {
                "From": 22,
                "To": 22
            }
        ],
        "Protocol": "6",
        "SourceAddresses": [
            "0.0.0.0/5",
            "100.0.0.0/10",
            "96.0.0.0/6"
        ],
        "SourcePortRanges": [
            {
                "From": 0,
                "To": 65535
            }
        ]
    },
    "Vpc": {
        "Id": "vpc-0762547ec48b6888d",
        "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/vpc-0762547ec48b6888d",
        "Name": "VPC BPA"
    }
},
{
    "SequenceNumber": 2,
    "AclRule": {
        "Cidr": "0.0.0.0/0",
        "Egress": false,
        "Protocol": "all",
        "RuleAction": "allow",
        "RuleNumber": 100
    },
    "Component": {

```

```

        "Id": "acl-06194fc3a4a03040b",
        "Arn": "arn:aws:ec2:us-east-2:470889052923:network-acl/
acl-06194fc3a4a03040b"
    },
    {
        "SequenceNumber": 3,
        "Component": {
            "Id": "sg-093dde06415d03924",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:security-group/
sg-093dde06415d03924",
            "Name": "VPC BPA Instances Security Group"
        },
        "SecurityGroupRule": {
            "Cidr": "0.0.0.0/0",
            "Direction": "ingress",
            "PortRange": {
                "From": 22,
                "To": 22
            },
            "Protocol": "tcp"
        }
    },
    {
        "SequenceNumber": 4,
        "AttachedTo": {
            "Id": "i-058db34f9a0997895",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:instance/
i-058db34f9a0997895",
            "Name": "VPC BPA Instance A"
        },
        "Component": {
            "Id": "eni-0fa23f2766f03b286",
            "Arn": "arn:aws:ec2:us-east-2:470889052923:network-interface/
eni-0fa23f2766f03b286"
        },
        "InboundHeader": {
            "DestinationAddresses": [
                "10.0.1.85/32"
            ],
            "DestinationPortRanges": [
                {
                    "From": 22,
                    "To": 22
                }
            ]
        }
    }
]

```



```

    }
  ],
  "Protocol": "6",
  "SourceAddresses": [
    "0.0.0.0/5",
    "100.0.0.0/10",
    "96.0.0.0/6"
  ],
  "SourcePortRanges": [
    {
      "From": 0,
      "To": 65535
    }
  ]
},
"Subnet": {
  "Id": "subnet-035d235a762eed04",
  "Arn": "arn:aws:ec2:us-east-2:470889052923:subnet/subnet-035d235a762eed04",
  "Name": "VPC BPA Public Subnet A"
},
"Vpc": {
  "Id": "vpc-0762547ec48b6888d",
  "Arn": "arn:aws:ec2:us-east-2:470889052923:vpc/vpc-0762547ec48b6888d",
  "Name": "VPC BPA"
}
]
}
],
"AnalysisStatus": "succeeded",
"NetworkInsightsAccessScopeAnalysisId": "nisa-0aa383a1938f94cd1",
"NextToken":
"eyJ0ZXh0VG9rZW4iOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfgQ=="
}

```

Die Ergebnisse zeigen den Verkehr zu und von den Internet-Gateways in allen Bereichen Ihres Kontos VPCs . Die Ergebnisse sind als „Ergebnisse“ zusammengefasst. "FindingId,": "AnalysisFinding -1" gibt an, dass dies das erste Ergebnis der Analyse ist. Beachten Sie, dass es mehrere Erkenntnisse gibt, die jeweils auf einen Datenverkehrsfluss hinweisen, der durch die Aktivierung von VPC BPA beeinträchtigt wird. Das erste Ergebnis zeigt, dass der

Datenverkehr an einem Internet-Gateway (" SequenceNumber „: 1) begann, an eine NACL (" SequenceNumber „: 2) an eine Sicherheitsgruppe (" SequenceNumber „: 3) weitergeleitet wurde und an einer Instanz (" SequenceNumber „: 4) endete.

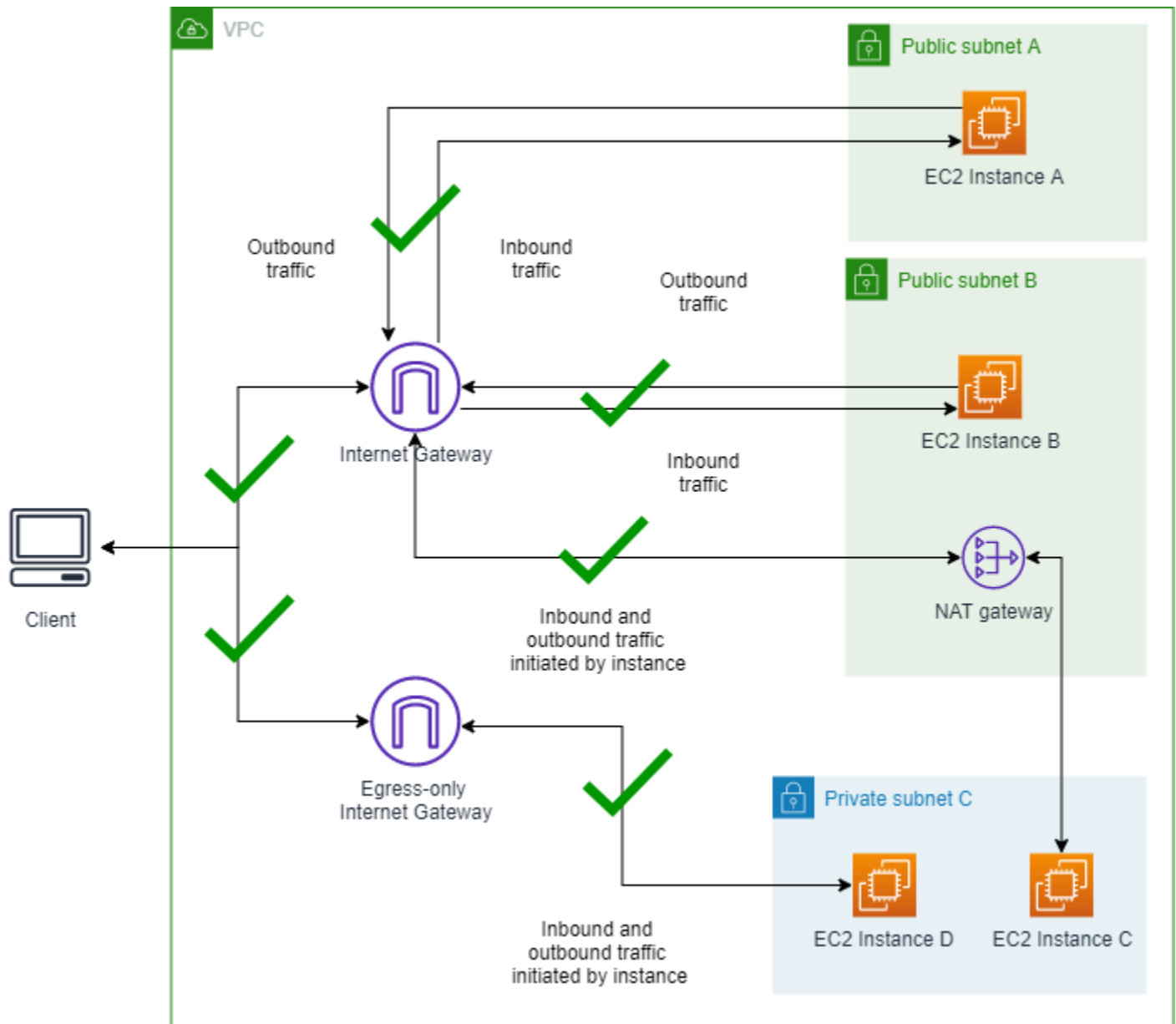
4. Analysieren Sie die Ergebnisse, um die Auswirkungen von VPC BPA auf Ihre Ressourcen zu verstehen. VPCs

Die Analyse der Auswirkungen ist abgeschlossen.

Szenario 1: Herstellen einer Verbindung zu Instances ohne aktiviertes VPC BPA

In diesem Abschnitt sind EC2 Instances in den öffentlichen Subnetzen A und B vom Internet aus über das Internet-Gateway erreichbar, das sowohl eingehenden als auch ausgehenden Datenverkehr ermöglicht. Die Instances C und D im privaten Subnetz können ausgehenden Datenverkehr über das NAT-Gateway oder das Internet-Gateway nur für ausgehenden Datenverkehr initiieren, sind jedoch nicht direkt vom Internet aus erreichbar. Diese Einrichtung bietet Internetzugriff auf einige Ressourcen und schützt gleichzeitig andere. Als Zweck dieses Abschnitts stellen Sie eine Verbindung zu allen Instances her und pingen eine öffentliche IP-Adresse an, um eine Baseline festzulegen und sicherzustellen, dass alle Instances erreicht werden können, bevor Sie VPC BPA aktivieren.

Diagramm einer VPC ohne aktiviertes VPC BPA:



1.1 Herstellen einer Verbindung zu Instances

Führen Sie diesen Abschnitt aus, um eine Verbindung zu Ihren Instances mit deaktiviertem VPC BPA herzustellen, um sicherzustellen, dass Sie problemlos eine Verbindung herstellen können. Alle mit dem CloudFormation für dieses Beispiel erstellten Instanzen haben Namen wie „VPC BPA Instance A“.

AWS-Managementkonsole

1. Öffnen Sie die EC2 Amazon-Konsole unter <https://console.aws.amazon.com/ec2/>.
2. Öffnen Sie die Details zu Instance A.

3. Stellen Sie mithilfe der Option `EC2 Instance Connect > Connect using Instance Connect Endpoint Connect` zu EC2 Instanz A her.
4. Wählen Sie `Connect` aus. Sobald Sie erfolgreich eine Verbindung mit der Instance hergestellt haben, pingen Sie `www.amazon.com` an, um zu überprüfen, ob Sie ausgehende Anfragen an das Internet senden können.
5. Verwenden Sie die gleiche Methode, die Sie für die Verbindung zu Instance A verwendet haben, um eine Verbindung zu den Instances B, C und D herzustellen. Pingen Sie von jeder Instance aus `www.amazon.com` an, um zu überprüfen, ob Sie ausgehende Anfragen an das Internet senden können.

AWS CLI

1. Pingen Sie Instanz A mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Verkehr zu überprüfen:

```
ping 18.225.8.244
```

Ausgabe:

```
Pinging 18.225.8.244 with 32 bytes of data:
Reply from 18.225.8.244: bytes=32 time=51ms TTL=110
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

2. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_   ~_   #####_           Amazon Linux 2023
~~   _#####\   ~~       ###|
```

```

~#/_ https://aws.amazon.com/linux/amazon-linux-2023
~V~' '->
~~~ /
~._. _/
/ /
/m/'
Last login: Fri Sep 27 18:27:57 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING www-amazon-com.customer.fastly.net (18.65.233.187) 56(84) bytes of data.
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=15 ttl=58 time=2.06 ms
64 bytes from 18.65.233.187 (18.65.233.187): icmp_seq=16 ttl=58 time=2.26 ms

```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

3. Pingen Sie Instanz B mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Verkehr zu überprüfen:

```
ping 3.18.106.198
```

Ausgabe:

```

Pinging 3.18.106.198 with 32 bytes of data:
Reply from 3.18.106.198: bytes=32 time=83ms TTL=110
Reply from 3.18.106.198: bytes=32 time=54ms TTL=110

```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

4. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-east-2 --connection-type eice
```

Ausgabe:

```

A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
, # ~_ #### Amazon Linux 2023
~_#####\ ~_ ###|
~#/_ https://aws.amazon.com/linux/amazon-linux-2023
~V~' '->

```

```

~~~      /
~~..    _/
/ /
/m/'
Last login: Fri Sep 27 18:12:27 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=1 ttl=249 time=1.55 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=2 ttl=249 time=1.67 ms

```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

5. Stellen Sie eine Verbindung zu Instance C her, da es keine öffentliche IP-Adresse zum Pingen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pingen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-east-2 --connection-type eice
```

Ausgabe:

```

A newer release of "Amazon Linux" is available.
Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #    ~_   #####          Amazon Linux 2023
~~  _#####\   ~~      ###|
~~      #/  __  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~      /
~~..    _/
/ /
/m/'
Last login: Thu Sep 19 20:31:26 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=1 ttl=248 time=1.75 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=2 ttl=248 time=1.97 ms

```

```
64 bytes from server-3-160-24-26.cmh68.r.cloudfront.net (18.65.233.187):
icmp_seq=3 ttl=248 time=1.08 ms
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

6. Stellen Sie eine Verbindung zu Instance D her, da es keine öffentliche IP-Adresse zum Pinggen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pingen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-east-2 --connection-type eice
```

Ausgabe:

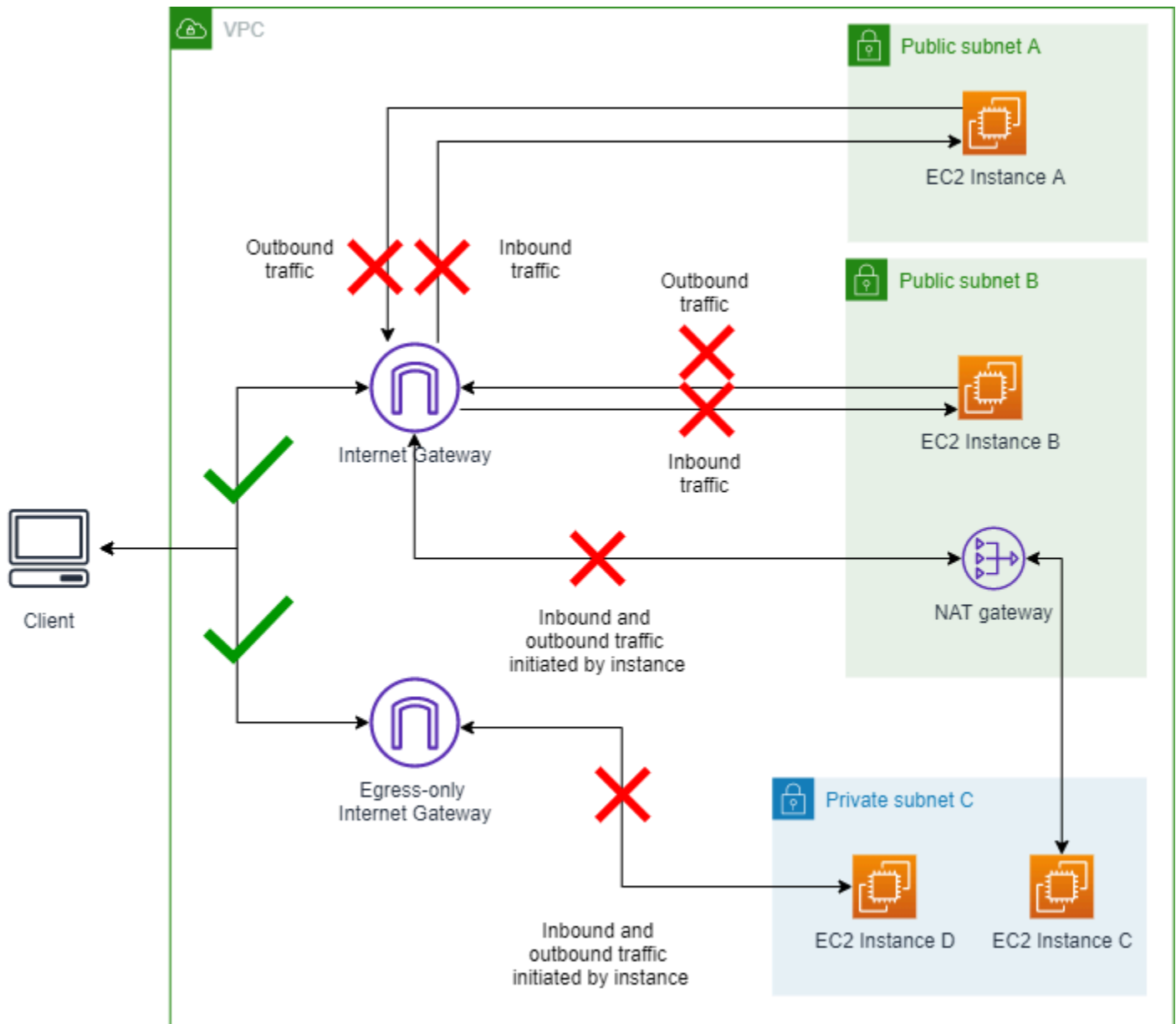
```
The authenticity of host '10.0.3.59' can't be established.
ECDSA key fingerprint is SHA256:c4naBCqbC61/cExDyccEproNU+1HHSpMSz12J6c0tIZA8g.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.3.59' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #    ~_  #####          Amazon Linux 2023
~~  _#####\  ~~      ###|
~~      #/  __  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~..  _/
_/  _/
_/m/'
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:ee00:7:49a5:5fd4:b121
(2600:9000:25f3:ee00:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
(2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.19 ms
64 bytes from 2600:9000:25f3:ee00:7:49a5:5fd4:b121
(2600:9000:25f3:ee00:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.38 ms
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

Szenario 2: Aktivieren von VPC BPA im bidirektionalen Modus

In diesem Abschnitt aktivieren Sie VPC BPA und blockieren den Datenverkehr zu und von den Internet-Gateways in Ihrem Konto.

Diagramm mit Darstellung des aktivierten bidirektionalen Modus von VPC BPA:



2.1 Aktivieren des bidirektionalen VPC-BPA-Modus

Führen Sie diesen Abschnitt aus, um VPC BPA zu aktivieren. Der bidirektionale VPC BPA-Modus blockiert den gesamten Verkehr zu und von Internet-Gateways und Internet-Gateways nur für

ausgehenden Datenverkehr in dieser Region (mit Ausnahme von ausgeschlossenen Netzwerken und Subnetzen). VPCs

AWS-Managementkonsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie Einstellungen für den öffentlichen Zugriff bearbeiten aus.
4. Wählen Sie Blockieren des öffentlichen Zugriffs aktivieren und Bidirektional und anschließend Änderungen speichern aus.
5. Warten Sie, bis sich der Status zu Ein ändert. Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

VPC BPA ist jetzt aktiviert.

AWS CLI

1. Verwenden Sie den Befehl `modify-vpc-block-public-access-options`, um VPC BPA zu aktivieren:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

2. Zeigen Sie den Status von VPC BPA an:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

2.2 Herstellen einer Verbindung zu Instances

Führen Sie diesen Abschnitt aus, um eine Verbindung mit Ihren Instances herzustellen.

AWS-Managementkonsole

1. Pingen Sie die öffentliche IPv4 Adresse von Instance A und Instance B wie in Szenario 1. Beachten Sie, dass der Datenverkehr blockiert ist.

2. Stellen Sie mithilfe der Option `Instance Connect > Connect using EC2 Instance Connect Endpoint` eine Verbindung zu EC2 Instanz A her, wie Sie es in Szenario 1 getan haben. Stellen Sie sicher, dass Sie die Endpunkt-Option verwenden.
3. Wählen Sie `Connect` aus. Sobald Sie erfolgreich eine Verbindung zur Instance hergestellt haben, pingen Sie `www.amazon.com` an. Beachten Sie, dass der gesamte ausgehende Datenverkehr blockiert ist.
4. Verwenden Sie die gleiche Methode, die Sie für die Verbindung zu Instance A verwendet haben, um eine Verbindung zu den Instances B, C und D herzustellen und ausgehende Anfragen an das Internet zu testen. Beachten Sie, dass der gesamte ausgehende Datenverkehr blockiert ist.

AWS CLI

1. Pingen Sie Instance A mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Verkehr zu überprüfen:

```
ping 18.225.8.244
```

Ausgabe:

```
Pinging 18.225.8.244 with 32 bytes of data:
```

```
Request timed out.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

2. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-east-2 --connection-type eice
```

Ausgabe:

```
The authenticity of host '10.0.1.85' can't be established.  
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWl0B/Ke04IM+hadjsoLJeRTWBk.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.
```

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~_  ####_      Amazon Linux 2023
~~  _#####\  ~~  ###|
~~      #/  ____  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~      /
~~._.  _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

3. Pingen Sie Instanz B mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Verkehr zu überprüfen:

```
ping 3.18.106.198
```

Ausgabe:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

4. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-east-2 --connection-type eice
```

Ausgabe:

```
The authenticity of host '10.0.2.98' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVLDthcCfI0IPIJMUiItA0LYKRNLGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
```

```
,      #  ~_  ####      Amazon Linux 2023
~~  _#####\  ~~      ###|
~~      #/  ___  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~      /
~~..  _/
/ /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

5. Stellen Sie eine Verbindung zu Instance C her, da es keine öffentliche IP-Adresse zum Pinggen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pingen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #  ~_  ####      Amazon Linux 2023
~~  _#####\  ~~      ###|
~~      #/  ___  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~      /
~~..  _/
/ /
/m/'
Last login: Tue Sep 24 15:17:56 2024 from 10.0.2.86
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

6. Stellen Sie eine Verbindung zu Instance D her, da es keine öffentliche IP-Adresse zum Pinggen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und

pingen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #   ~_   #####           Amazon Linux 2023
~~  _#####\   ~~      ###|
~~      #/  ____  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~..  _/
_/  _/
_/m/'
Last login: Fri Sep 27 16:42:01 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:8200:7:49a5:5fd4:b121
(2600:9000:25f3:8200:7:49a5:5fd4:b121)) 56 data bytes
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

2.3 Optional: Überprüfen mit Reachability Analyzer, ob die Konnektivität blockiert ist

[VPC Reachability Analyzer](#) kann verwendet werden, um zu verstehen, ob bestimmte Netzwerkpfade angesichts Ihrer Netzwerkkonfiguration, einschließlich der Einstellungen für VPC BPA, erreicht werden können oder nicht. In diesem Beispiel analysieren Sie denselben Netzwerkpfad, der zuvor versucht wurde, um zu bestätigen, dass VPC BPA der Grund für die fehlende Konnektivität ist.

AWS-Managementkonsole

1. Rufen Sie die Network-Insights-Konsole unter <https://console.aws.amazon.com/networkinsights/home#ReachabilityAnalyzer> auf.
2. Klicken Sie auf Pfad erstellen und analysieren.

3. Wählen Sie als Quelltyp die Option Internet-Gateways aus und wählen Sie dann aus dem Dropdown-Menü Quelle das Internet-Gateway mit der Bezeichnung VPC-BPA-Internet-Gateway aus.
4. Wählen Sie als Zieltyp die Option Instances aus und wählen Sie aus dem Dropdown-Menü Ziel die Instance mit der Bezeichnung VPC-BPA-Instance A aus.
5. Klicken Sie auf Pfad erstellen und analysieren.
6. Warten Sie, bis die Analyse abgeschlossen ist. Dies kann einige Minuten dauern.
7. Sobald dies abgeschlossen ist, sollten Sie sehen, dass der Erreichbarkeitsstatus Nicht erreichbar lautet und dass die Pfaddetails zeigen, dass VPC_BLOCK_PUBLIC_ACCESS_ENABLED die Ursache ist.

AWS CLI

1. Erstellen Sie einen Netzwerkpfad unter Verwendung der ID des Internet-Gateways mit der Bezeichnung VPC-BPA-Internet-Gateway und der ID der Instance mit der Bezeichnung VPC-BPA-Instance A:

```
aws ec2 --region us-east-2 create-network-insights-path --source igw-id --  
destination instance-id --protocol TCP
```

2. Starten Sie eine Analyse des Netzwerkpfads:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-  
path-id nip-id
```

3. Rufen Sie die Ergebnisse der Analyse ab:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-  
insights-analysis-ids nia-id
```

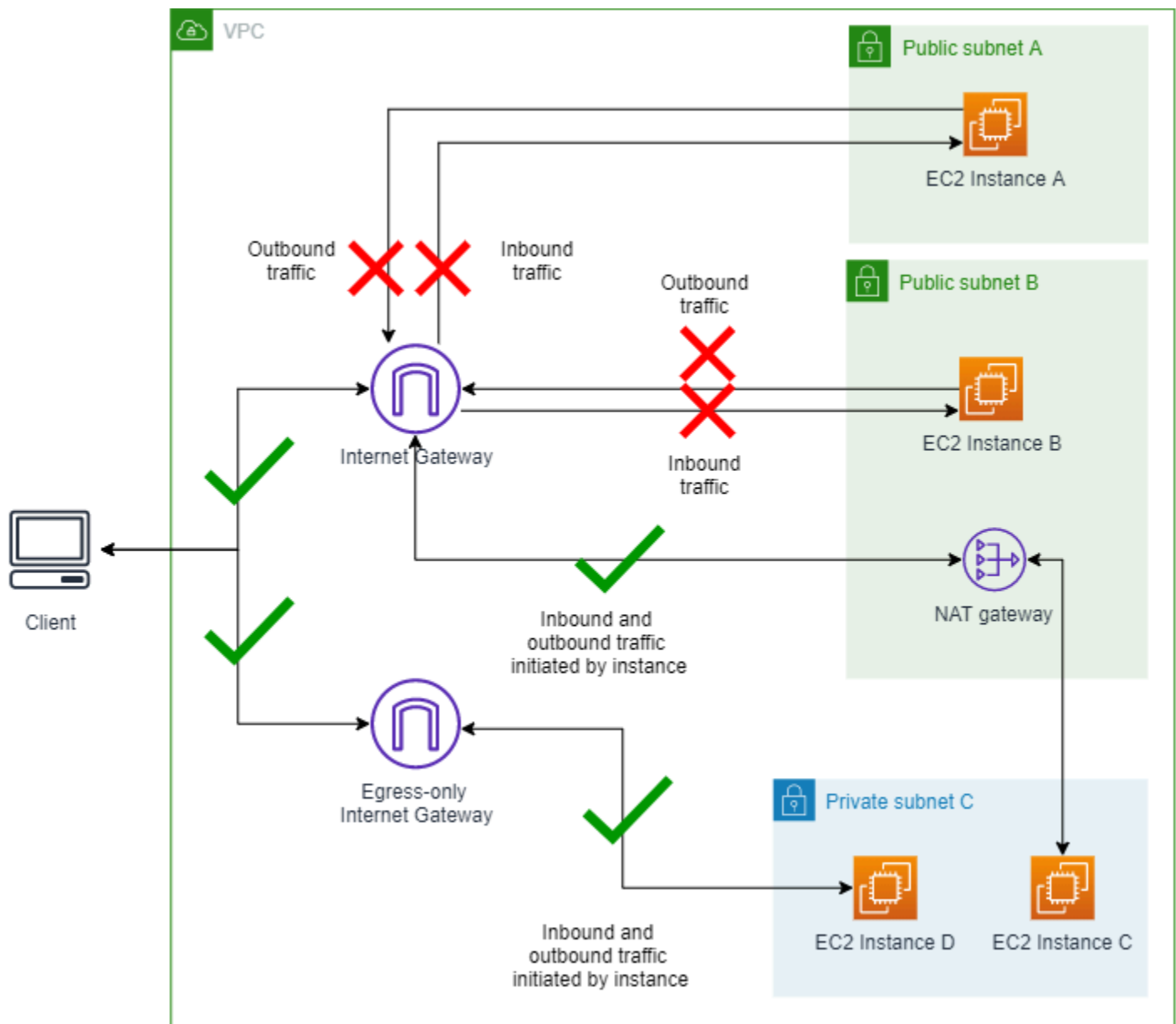
4. Prüfen Sie, ob VPC_BLOCK_PUBLIC_ACCESS_ENABLED das ExplanationCode für die fehlende Erreichbarkeit ist.

Beachten Sie, dass Sie auch das können: [Überwachen der VPC-BPA-Auswirkungen mit Flow-Protokollen](#)

Szenario 3: Ändern des VPC BPA auf nur eingehenden Datenverkehrsmodus

In diesem Abschnitt ändern Sie die VPC-BPA-Verkehrsrichtung und lassen nur Datenverkehr zu, der ein NAT-Gateway oder ein Internet-Gateway nur für ausgehenden Datenverkehr verwendet. EC2 Die Instanzen A und B in den öffentlichen Subnetzen sind vom Internet aus nicht erreichbar, da BPA den eingehenden Verkehr über das Internet Gateway blockiert. Die Instanzen C und D im privaten Subnetz können weiterhin ausgehenden Datenverkehr über das NAT-Gateway und das Internet-Gateway nur für ausgehenden Datenverkehr initiieren und erreichen daher weiterhin das Internet.

Diagramm des aktivierten Modus nur für eingehenden Datenverkehr von VPC BPA:



3.1 Ändern des Modus auf nur eingehenden Datenverkehr

Schließen Sie diesen Abschnitt ab, um den Modus zu ändern.

AWS-Managementkonsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie auf der Registerkarte Öffentlichen Zugriff blockieren die Option Einstellungen für öffentlichen Zugriff bearbeiten aus.
4. Ändern Sie die Einstellungen für den öffentlichen Zugriff in der VPC-Konsole und ändern Sie die Richtung auf Nur eingehender Datenverkehr.
5. Speichern Sie die Änderungen und warten Sie, bis der Status aktualisiert wird. Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

AWS CLI

1. Ändern Sie den VPC-BPA-Modus:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-ingress
```

Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

2. Zeigen Sie den Status von VPC BPA an:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

3.2 Herstellen einer Verbindung zu Instances

Führen Sie diesen Abschnitt aus, um eine Verbindung zu den Instances herzustellen.

AWS-Managementkonsole

1. Pingen Sie die öffentliche IPv4 Adresse von Instance A und Instance B an, wie Sie es in Szenario 1 getan haben. Beachten Sie, dass der Datenverkehr blockiert ist.

2. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance A und B her und pingen Sie von dort aus `www.amazon.com` an. Beachten Sie, dass Sie von Instance A oder B aus keine öffentliche Website im Internet anpingen können und der Datenverkehr blockiert ist.
3. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance C und D her und pingen Sie von dort aus `www.amazon.com` an. Beachten Sie, dass Sie von Instance C oder D aus eine öffentliche Website im Internet anpingen können und der Datenverkehr erlaubt ist.

AWS CLI

1. Pingen Sie Instance A mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Datenverkehr zu überprüfen:

```
ping 18.225.8.244
```

Ausgabe:

```
Pinging 18.225.8.244 with 32 bytes of data:  
  
Request timed out.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

2. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-east-2 --connection-type eice
```

Ausgabe:

```
The authenticity of host '10.0.1.85' can't be established.  
ECDSA key fingerprint is SHA256:3zo/gSss+HAZ+7eTyWl0B/Ke04IM+hadjsolJERTWBk.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.0.1.85' (ECDSA) to the list of known hosts.  
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:  
Run "/usr/bin/dnf check-release-update" for full release and version update info  
,      #_   ~_   ####_      Amazon Linux 2023
```

```

~~ _#####\  ~~      ###|
~~          #/  ____  https://aws.amazon.com/linux/amazon-linux-2023
~~          V~'  '->
~~~          /
~~._.  _/
/ /
/m/'
Last login: Fri Sep 27 14:16:53 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

3. Pingen Sie Instanz B mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Verkehr zu überprüfen:

```
ping 3.18.106.198
```

Ausgabe:

```

Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.

```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

4. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-east-2 --connection-type eice
```

Ausgabe:

```

The authenticity of host '10.0.2.98 ' can't be established.
ECDSA key fingerprint is SHA256:0IjXKKyVlDthcCfI0IPIJMUiItAOLYKRNlGTYURnFXo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.98' (ECDSA) to the list of known hosts.
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #   ~_  #####      Amazon Linux 2023
~~ _#####\  ~~      ###|
~~          #/  ____  https://aws.amazon.com/linux/amazon-linux-2023

```

```

~ ~      V~' ' ->
~ ~ ~      /
~ ~ . .   _/
_ / /
/m/'
Last login: Fri Sep 27 14:18:16 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

5. Stellen Sie eine Verbindung zu Instance C her, da es keine öffentliche IP-Adresse zum Pingen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pingen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-east-2 --connection-type eice
```

Ausgabe:

```

A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_ ~\ #####_      Amazon Linux 2023
~ ~ \#####\ ~ ~ \###|
~ ~ \#/ ____ https://aws.amazon.com/linux/amazon-linux-2023
~ ~      V~' ' ->
~ ~ ~      /
~ ~ . .   _/
_ / /
/m/'
Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=2 ttl=248 time=1.40 ms

```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

6. Stellen Sie eine Verbindung zu Instance D her, da es keine öffentliche IP-Adresse zum Pinggen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pinggen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_   ~\   #####_   Amazon Linux 2023
~~  \#####\   ~   \###|
~~      \#/   ____   https://aws.amazon.com/linux/amazon-linux-2023
~~          V~'   '->
~~~~
~~~~
~~._.   _/
   _/   _/
   _/m/'

Last login: Fri Sep 27 16:48:38 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:5800:7:49a5:5fd4:b121
(2600:9000:25f3:5800:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
(2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=14 ttl=58 time=1.47 ms
64 bytes from 2600:9000:25f3:5800:7:49a5:5fd4:b121
(2600:9000:25f3:5800:7:49a5:5fd4:b121): icmp_seq=16 ttl=58 time=1.59 ms
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

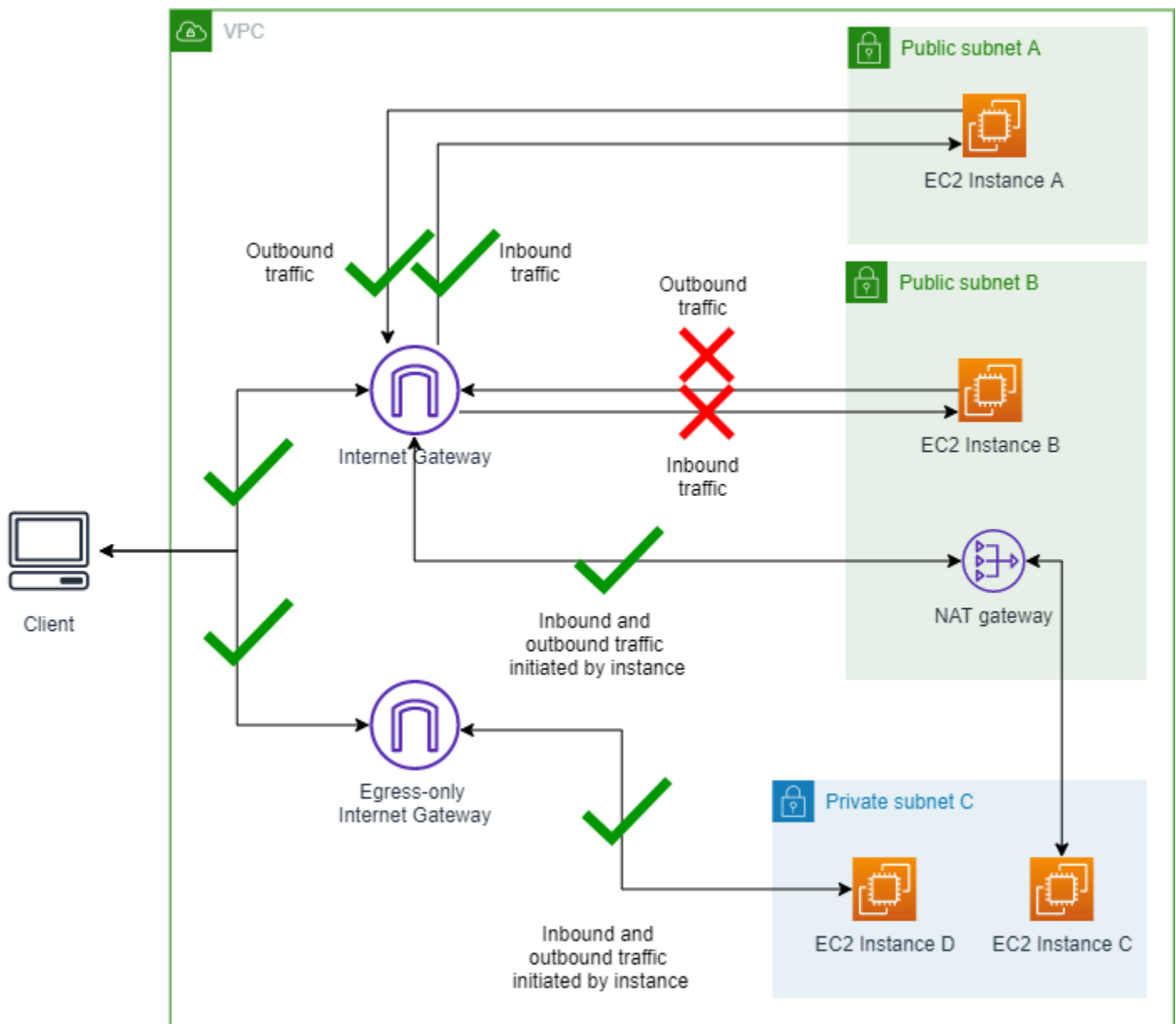
Szenario 4: Erstellen eines Ausschlusses

In diesem Abschnitt erstellen Sie einen Ausschluss. VPC BPA blockiert dann nur den Datenverkehr in den Subnetzen ohne Ausschluss. Ein VPC-BPA-Ausschluss ist ein Modus, der auf eine einzelne VPC oder ein Subnetz angewendet werden kann, der es vom VPC-BPA-Modus des Kontos ausnimmt und bidirektionalen oder nur ausgehenden Zugriff erlaubt. Sie können VPC-BPA-Ausschlüsse für VPCs

und Subnetze erstellen, auch wenn VPC BPA für das Konto nicht aktiviert ist, um sicherzustellen, dass der Datenverkehr der Ausschlüsse nicht unterbrochen wird, wenn VPC BPA aktiviert ist.

In diesem Beispiel erstellen wir einen Ausschluss für Subnetz A, um zu zeigen, wie sich VPC BPA auf den Datenverkehr zu Ausschlüssen auswirkt.

Diagramm des aktivierten Modus nur für eingehenden Datenverkehr von VPC BPA und des Ausschlusses von Subnetz A mit aktiviertem bidirektionalen Modus:



4.1 Erstellen eines Ausschlusses für Subnetz A

Führen Sie diesen Abschnitt aus, um eine Ausnahme zu erstellen. Ein VPC-BPA-Ausschluss ist ein Modus, der auf eine einzelne VPC oder ein Subnetz angewendet werden kann, der es vom VPC-BPA-Modus des Kontos ausnimmt und bidirektionalen oder nur ausgehenden Zugriff erlaubt. Sie können VPC-BPA-Ausschlüsse für VPCs und Subnetze erstellen, auch wenn VPC BPA für das Konto nicht aktiviert ist, um sicherzustellen, dass der Datenverkehr der Ausschlüsse nicht unterbrochen wird, wenn VPC BPA aktiviert ist.

AWS-Managementkonsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie auf der Registerkarte Öffentlichen Zugriff blockieren unter Ausschlüsse die Option Ausschlüsse erstellen aus.
4. Wählen Sie VPC BPA Public Subnet A aus, stellen Sie sicher, dass die Zulässigkeitsrichtung Bidirektional ausgewählt ist, und wählen Sie dann Ausschlüsse erstellen aus.
5. Warten Sie, bis sich der Status Ausschluss auf Aktiv ändert. Möglicherweise müssen Sie die Ausschlusstabelle aktualisieren, damit die Änderung angezeigt wird.

Der Ausschluss wurde erstellt.

AWS CLI

1. Ändern Sie die Richtung der Ausschlusserlaubnis:

```
aws ec2 --region us-east-2 create-vpc-block-public-access-exclusion --subnet-id subnet-id --internet-gateway-exclusion-mode allow-bidirectional
```

2. Es kann einige Zeit dauern, bis der Ausschlussstatus aktualisiert wird. So zeigen Sie den Status des Ausschlusses an:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusions --exclusion-ids exclusion-id
```

4.2 Herstellen einer Verbindung zu Instances

Führen Sie diesen Abschnitt aus, um eine Verbindung zu den Instances herzustellen.

AWS-Managementkonsole

1. Pingen Sie die öffentliche IPv4 Adresse von Instanz A. Beachten Sie, dass Datenverkehr zulässig ist.
2. Pingen Sie die öffentliche IPv4 Adresse von Instanz B. Beachten Sie, dass der Verkehr blockiert ist.
3. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance A her und pingen Sie `www.amazon.com` an. Beachten Sie, dass Sie von Instance A aus eine öffentliche Website im Internet anpingen können, da der Datenverkehr erlaubt ist.
4. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance B her und pingen Sie von dort aus `www.amazon.com` an. Beachten Sie, dass Sie von Instance B aus keine öffentliche Website im Internet anpingen können, da der Datenverkehr blockiert ist.
5. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance C und D her und pingen Sie von dort aus `www.amazon.com` an. Beachten Sie, dass Sie von Instance C oder D aus eine öffentliche Website im Internet anpingen können, da der Datenverkehr erlaubt ist.

AWS CLI

1. Pingen Sie Instance A mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Datenverkehr zu überprüfen:

```
ping 18.225.8.244
```

Ausgabe:

```
Pinging 18.225.8.244 with 32 bytes of data:  
  
Reply from 18.225.8.244: bytes=32 time=51ms TTL=110  
Reply from 18.225.8.244: bytes=32 time=61ms TTL=110
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

2. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_   ~_   #####_      Amazon Linux 2023
~~  _#####\   ~~      ###|
~~      #/   __   https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'   '->
~~~~
~~.  _  _/
/ /
/m/'
Last login: Fri Sep 27 17:58:12 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=1 ttl=249 time=1.03 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=2 ttl=249 time=1.72 ms
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

3. Pingen Sie Instanz B mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Verkehr zu überprüfen:

```
ping 3.18.106.198
```

Ausgabe:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

4. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:


```
aws ec2-instance-connect ssh --instance-id i-08552a0774b5c8f72 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #    ~_  #####          Amazon Linux 2023
~~  _#####\  ~~      ###|
~~      #/  ___  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~..  _/
_/ /
/m/'
Last login: Fri Sep 27 18:12:03 2024 from 3.16.146.5
[ec2-user@ip-10-0-2-98 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

5. Stellen Sie eine Verbindung zu Instance C her, da es keine öffentliche IP-Adresse zum Pinggen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pinggen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-east-2 --connection-type eice
```

Ausgabe

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #    ~_  #####          Amazon Linux 2023
~~  _#####\  ~~      ###|
~~      #/  ___  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~..  _/
_/ /
```

```

/m/'

Last login: Tue Sep 24 15:28:09 2024 from 10.0.2.86

[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com

PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.

64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=1 ttl=248 time=1.84 ms
64 bytes from server-3-160-24-126.cmh68.r.cloudfront.net (18.65.233.187):
  icmp_seq=2 ttl=248 time=1.40 ms

```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

6. Stellen Sie eine Verbindung zu Instance D her, da es keine öffentliche IP-Adresse zum Pingen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pingen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```

aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-east-2 --connection-type eice

```

Ausgabe

```

A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~\  ####_      Amazon Linux 2023
~~  \#####\  ~~  \###|
~~      \#/  __  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~  ._.  _/
  _/  _/
    _/m/'

Last login: Fri Sep 27 18:00:52 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING
www.amazon.com(g2600-141f-4000-059a-0000-0000-3bd4.deploy.static.akamaitechnologie
(2600:141f:4000:59a::3bd4)) 56 data bytes

```

```
64 bytes from
g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
(2600:141f:4000:59a::3bd4): icmp_seq=1 ttl=48 time=15.9 ms
64 bytes from
g2600-141f-4000-059a-0000-0000-0000-3bd4.deploy.static.akamaitechnologies.com
(2600:141f:4000:59a::3bd4): icmp_seq=2 ttl=48 time=15.8 ms
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

4.3 Optional: Überprüfen der Konnektivität mit Reachability Analyzer

Unter Verwendung desselben Netzwerkpfads, der in Reachability Analyzer in Szenario 2 erstellt wurde, können Sie nun eine neue Analyse durchführen und bestätigen, dass der Pfad erreichbar ist, nachdem ein Ausschluss für das öffentliche Subnetz A erstellt wurde.

Informationen zur regionalen Verfügbarkeit von Reachability Analyzer finden Sie unter [Überlegungen](#) im Leitfaden Reachability Analyzer.

AWS-Managementkonsole

1. Klicken Sie im Netzwerkpfad, den Sie zuvor in der Network-Insights-Konsole erstellt haben, auf Analyse erneut ausführen.
2. Warten Sie, bis die Analyse abgeschlossen ist. Dieser Vorgang kann einige Minuten dauern.
3. Bestätigen Sie, dass der Pfad nun erreichbar ist.

AWS CLI

1. Starten Sie eine neue Analyse unter Verwendung der zuvor erstellten Netzwerkpfad-ID:

```
aws ec2 --region us-east-2 start-network-insights-analysis --network-insights-path-id nip-id
```

2. Rufen Sie die Ergebnisse der Analyse ab:

```
aws ec2 --region us-east-2 describe-network-insights-analyses --network-insights-analysis-ids nia-id
```

3. Stellen Sie sicher, dass der Erklärungscode VPC_BLOCK_PUBLIC_ACCESS_ENABLED nicht mehr vorhanden ist.

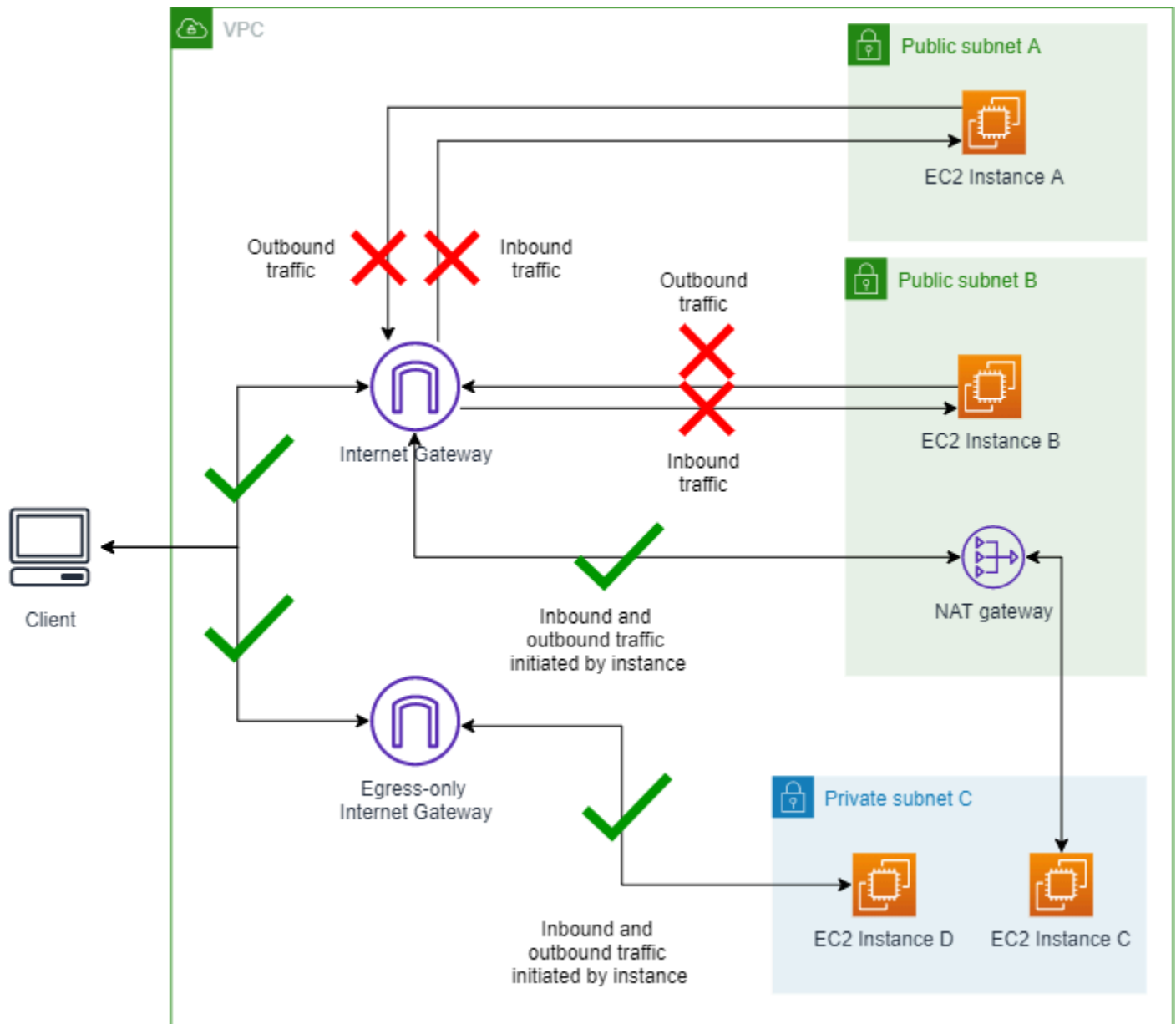
Szenario 5: Ändern des Ausschlussmodus

In diesem Abschnitt ändern Sie die Richtung des zulässigen Datenverkehrs für den Ausschluss, um zu sehen, wie sich dies auf VPC BPA auswirkt.

Note

In diesem Szenario ändern Sie den Ausschlussmodus auf „Nur ausgehend“. Beachten Sie, dass in diesem Fall die Ausnahmeregelung „Nur ausgehend“ in Subnetz A keinen ausgehenden Datenverkehr zulässt. Das ist widersprüchlich, da Sie erwarten würden, dass damit ausgehender Datenverkehr zugelassen wird. Da BPA auf Kontoebene jedoch nur für eingehenden Datenverkehr gilt, werden nur ausgehende Ausschlüsse ignoriert, und das Routing von Subnetz A zu einem Internet-Gateway wird durch VPC BPA eingeschränkt, was ausgehenden Datenverkehr blockiert. Um ausgehenden Datenverkehr in Subnetz A zu aktivieren, müssten Sie VPC BPA in den bidirektionalen Modus schalten.

Diagramm des aktivierten Modus nur für eingehenden Datenverkehr von VPC BPA und des Ausschlusses von Subnetz A mit aktiviertem Modus nur für ausgehenden Verkehr:



5.1 Änderung der Richtung der Ausschlussregeln in nur ausgehenden Datenverkehr

Schließen Sie diesen Abschnitt ab, um die Richtung der Ausschlussregeln zu ändern.

AWS-Managementkonsole

1. Bearbeiten Sie den Ausschluss, den Sie in Szenario 4 erstellt haben, und ändern Sie die Zulässigkeitsrichtung in Nur für ausgehenden Datenverkehr.
2. Wählen Sie Änderungen speichern aus.
3. Warten Sie, bis sich der Status Ausschluss auf Aktiv ändert. Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

Möglicherweise müssen Sie die Ausschlusstabelle aktualisieren, damit die Änderung angezeigt wird.

AWS CLI

1. Ändern Sie die Richtung der Ausschlusserlaubnis:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-exclusion --exclusion-id exclusion-id --internet-gateway-exclusion-mode allow-egress
```

Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

2. Es kann einige Zeit dauern, bis der Ausschlussstatus aktualisiert wird. So zeigen Sie den Status des Ausschlusses an:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-exclusion
```

5.2 Herstellen einer Verbindung zu Instances

Führen Sie diesen Abschnitt aus, um eine Verbindung zu den Instances herzustellen.

AWS-Managementkonsole

1. Pingen Sie die öffentliche IPv4 Adresse von Instance A und B. Beachten Sie, dass der Datenverkehr blockiert ist.
2. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance A und B her und pingen Sie www.amazon.com an. Beachten Sie, dass Sie von Instance A oder B aus keine öffentliche Website im Internet anpingen können, da der Datenverkehr blockiert ist.
3. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance C und D her und pingen Sie von dort aus www.amazon.com an. Beachten Sie, dass Sie von Instance C oder D aus eine öffentliche Website im Internet anpingen können, da der Datenverkehr erlaubt ist.

AWS CLI

1. Pingen Sie Instance A mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Datenverkehr zu überprüfen:

```
ping 18.225.8.244
```

Ausgabe:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

2. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~\  ####_      Amazon Linux 2023
~~  \#####\  ~~      \###|
~~      \#/  __  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~  ._.  _/
    _/  _/
    _/m/'

Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

3. Pingen Sie Instanz B mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Verkehr zu überprüfen:

```
ping 3.18.106.198
```

Ausgabe:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

4. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~\  #####_      Amazon Linux 2023
~~  \#####\  ~~  \###|
~~      \#/  __  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~  ._.  _/
  _/  _/
    _/m/'

Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

5. Stellen Sie eine Verbindung zu Instance C her, da es keine öffentliche IP-Adresse zum Pinggen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pinggen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:


```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~\  ####_      Amazon Linux 2023
~~  \#####\  ~~      \###|
~~      \#/  ____  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~~~
~~._.  _/
  _/  _/
    _/m/'

Last login: Fri Sep 27 18:00:31 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:a600:7:49a5:5fd4:b121
(2600:9000:25f3:a600:7:49a5:5fd4:b121)) 56 data bytes
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
(2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=1 ttl=58 time=1.51 ms
64 bytes from 2600:9000:25f3:a600:7:49a5:5fd4:b121
(2600:9000:25f3:a600:7:49a5:5fd4:b121): icmp_seq=2 ttl=58 time=1.49 ms
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

6. Stellen Sie eine Verbindung zu Instance D her, da es keine öffentliche IP-Adresse zum Pinggen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pingen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~\  ####_      Amazon Linux 2023
~~  \#####\  ~~      \###|
```

```

~ ~      \#/  ____  https://aws.amazon.com/linux/amazon-linux-2023
~ ~      V~'  '->
~ ~ ~
~ ~ . _ .  /
  /  /
  /m/'

Last login: Fri Sep 27 18:13:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com
PING www.amazon.com(2606:2cc0::374 (2606:2cc0::374)) 56 data bytes
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=1 ttl=58 time=1.21 ms
64 bytes from 2606:2cc0::374 (2606:2cc0::374): icmp_seq=2 ttl=58 time=1.51 ms

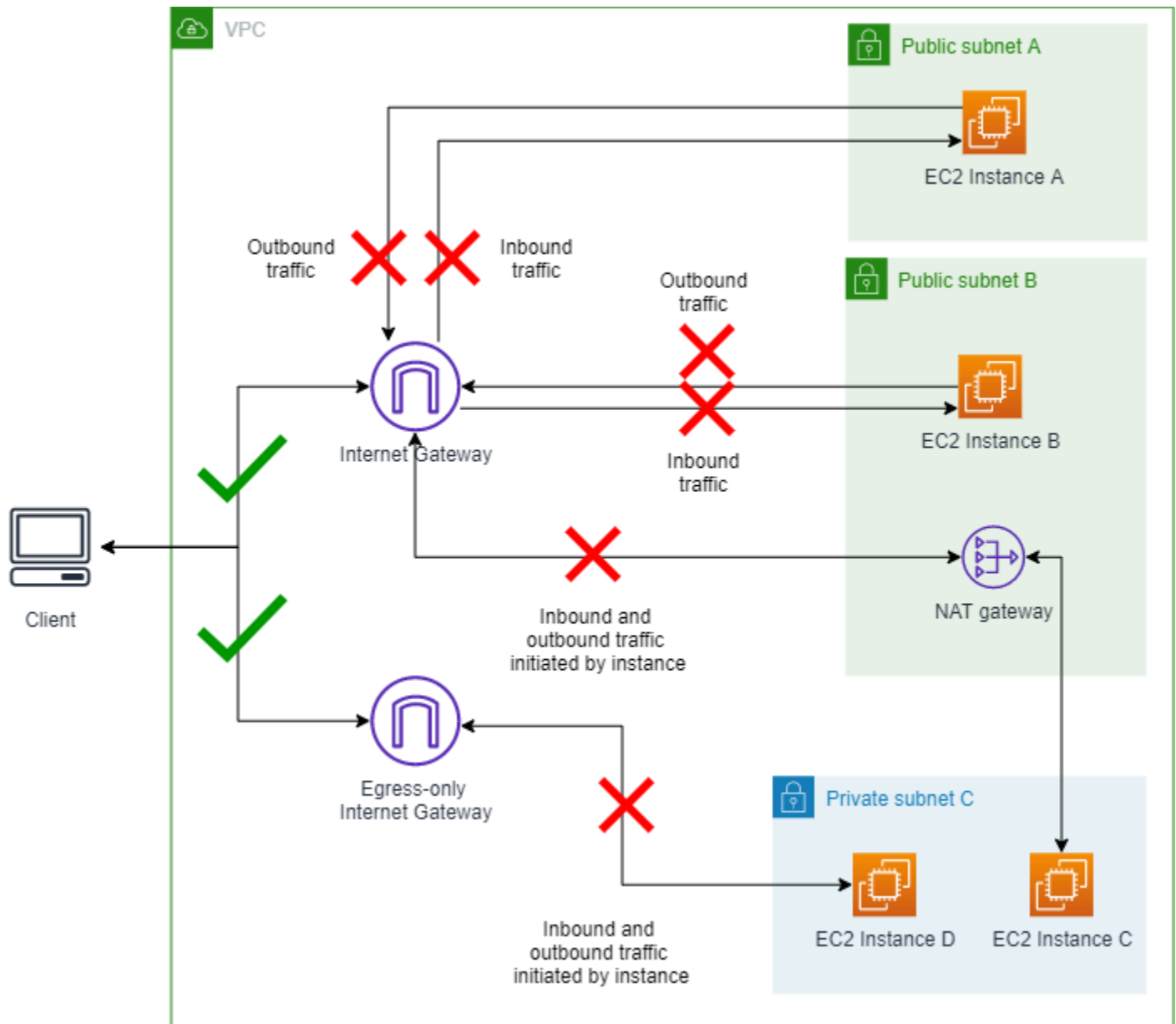
```

Beachten Sie, dass der Ping erfolgreich ist und der Datenverkehr nicht blockiert wird.

Szenario 6: Ändern des VPC-BPA-Modus

In diesem Abschnitt ändern Sie die Blockierrichtung von VPC BPA, um zu sehen, wie sich dies auf den Datenverkehr auswirkt. In diesem Szenario blockiert VPC BPA, das im bidirektionalen Modus aktiviert ist, den gesamten Datenverkehr wie in Szenario 1. Sofern ein Ausschluss keinen Zugang zu einem NAT-Gateway oder einem Internet-Gateway nur für ausgehenden Verkehr hat, wird der Verkehr blockiert.

Diagramm des aktivierten bidirektionalen Modus von VPC BPA und des Ausschlusses von Subnetz A mit aktiviertem Modus nur für ausgehenden Verkehr:



6.1 Ändern von VPC BPA in den bidirektionalen Modus

Schließen Sie diesen Abschnitt ab, um den VPC-BPA-Modus zu ändern.

AWS-Managementkonsole

1. Öffnen Sie die Amazon-VPC-Konsole unter <https://console.aws.amazon.com/vpc/>.
2. Wählen Sie im linken Navigationsbereich die Option Einstellungen aus.
3. Wählen Sie Einstellungen für den öffentlichen Zugriff bearbeiten aus.

4. Ändern Sie die Blockierrichtung auf Bidirektional und wählen Sie dann Änderungen speichern aus.
5. Warten Sie, bis sich der Status zu Ein ändert. Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

AWS CLI

1. Ändern Sie die Blockierrichtung von VPC BPA:

```
aws ec2 --region us-east-2 modify-vpc-block-public-access-options --internet-gateway-block-mode block-bidirectional
```

Es kann einige Minuten dauern, bis die VPC-BPA-Einstellungen wirksam werden und der Status aktualisiert wird.

2. Zeigen Sie den Status von VPC BPA an:

```
aws ec2 --region us-east-2 describe-vpc-block-public-access-options
```

6.2 Herstellen einer Verbindung zu Instances

Führen Sie diesen Abschnitt aus, um eine Verbindung zu den Instances herzustellen.

AWS-Managementkonsole

1. Pingen Sie die öffentliche IPv4 Adresse von Instance A und B. Beachten Sie, dass der Datenverkehr blockiert ist.
2. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance A und B her und pingen Sie www.amazon.com an. Beachten Sie, dass Sie von Instance A oder B aus keine öffentliche Website im Internet anpingen können, da der Datenverkehr blockiert ist.
3. Stellen Sie wie in Szenario 1 mithilfe von EC2 Instance Connect eine Verbindung zu Instance C und D her und pingen Sie von dort aus www.amazon.com an. Beachten Sie, dass Sie von Instance C oder D aus keine öffentliche Website im Internet anpingen können, da der Datenverkehr blockiert ist.

AWS CLI

1. Pingen Sie Instance A mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Datenverkehr zu überprüfen:

```
ping 18.225.8.244
```

Ausgabe:

```
Pinging 18.225.8.244 with 32 bytes of data:
Request timed out.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

2. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~\  ####_      Amazon Linux 2023
~~  \#####\  ~~      \###|
~~      \#/  __  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~  ._.  _/
  _/  _/
    _/m/'

Last login: Fri Sep 27 18:17:44 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

3. Pingen Sie Instanz A mithilfe der öffentlichen IPv4 Adresse an, um den eingehenden Verkehr zu überprüfen:

```
ping 3.18.106.198
```

Ausgabe:

```
Pinging 3.18.106.198 with 32 bytes of data:
Request timed out.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

4. Verwenden Sie die private IPv4 Adresse, um eine Verbindung herzustellen und den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-058db34f9a0997895 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_   ~\   #####_      Amazon Linux 2023
~~  \#####\  ~~      \###|
~~      \#/  __  https://aws.amazon.com/linux/amazon-linux-2023
~~      V~'  '->
~~~~
~~  ._.  _/
  _/  _/
    _/m/'

Last login: Fri Sep 27 18:09:55 2024 from 3.16.146.5
[ec2-user@ip-10-0-1-85 ~]$ ping www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (18.65.233.187) 56(84) bytes of data.
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

5. Stellen Sie eine Verbindung zu Instance C her, da es keine öffentliche IP-Adresse zum Pinggen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pinggen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-04eca55f2a482b2c4 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~\  ####_      Amazon Linux 2023
~~  \#####\  ~~      \###|
~~      \#/  ___      https://aws.amazon.com/linux/amazon-linux-2023
~~          V~'  '->
~~~~
~~~~
~~._.  _/
    _/  _/
    _/m/'

Last login: Fri Sep 27 18:19:45 2024 from 3.16.146.5
[ec2-user@ip-10-0-3-180 ~]$ ping www.amazon.com
PING www.amazon.com(2600:9000:25f3:6200:7:49a5:5fd4:b121
(2600:9000:25f3:6200:7:49a5:5fd4:b121)) 56 data bytes
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

6. Stellen Sie eine Verbindung zu Instance D her, da es keine öffentliche IP-Adresse zum Pingen gibt, verwenden Sie EC2 Instance Connect, um eine Verbindung herzustellen, und pingen Sie dann eine öffentliche IP von der Instance aus, um den ausgehenden Verkehr zu überprüfen:

```
aws ec2-instance-connect ssh --instance-id i-05f9e6a9cfac1dba0 --region us-east-2 --connection-type eice
```

Ausgabe:

```
A newer release of "Amazon Linux" is available. Version 2023.5.20240916:
Run "/usr/bin/dnf check-release-update" for full release and version update info
,      #_  ~\  ####_      Amazon Linux 2023
~~  \#####\  ~~      \###|
~~      \#/  ___      https://aws.amazon.com/linux/amazon-linux-2023
~~          V~'  '->
~~~~
~~~~
~~._.  _/
    _/  _/
    _/m/'
```

```
  _/  _/  
_/_/m/'
```

```
Last login: Fri Sep 27 18:20:58 2024 from 3.16.146.5  
[ec2-user@ip-10-0-3-59 ~]$ ping www.amazon.com  
PING www.amazon.com(2600:9000:25f3:b400:7:49a5:5fd4:b121  
(2600:9000:25f3:b400:7:49a5:5fd4:b121)) 56 data bytes
```

Beachten Sie, dass der Ping fehlschlägt und der Datenverkehr blockiert wird.

Bereinigen

In diesem Abschnitt löschen Sie alle Ressourcen, die Sie für dieses erweiterte Beispiel erstellt haben. Es ist wichtig, die Ressourcen zu bereinigen, um übermäßige zusätzliche Gebühren für in Ihrem Konto erstellte Ressourcen zu vermeiden.

Löschen Sie die Ressourcen CloudFormation

Füllen Sie diesen Abschnitt aus, um die Ressourcen zu löschen, die Sie mit der CloudFormation Vorlage erstellt haben.

AWS-Managementkonsole

1. Öffnen Sie die CloudFormation Konsole unter <https://console.aws.amazon.com/cloudformation/>.
2. Wählen Sie den VPC-BPA-Stack aus.
3. Wählen Sie Löschen aus.
4. Sobald Sie mit dem Löschen des Stacks begonnen haben, können Sie auf der Registerkarte Ereignisse den Fortschritt verfolgen und sicherstellen, dass der Stack gelöscht wird. Möglicherweise müssen Sie das [Löschen des Stacks erzwingen](#), damit er vollständig gelöscht wird.

AWS CLI

1. Löschen Sie den CloudFormation Stapel. Möglicherweise müssen Sie das [Löschen des Stacks erzwingen](#), damit er vollständig gelöscht wird.

```
aws cloudformation delete-stack --stack-name VPC-BPA-stack --region us-east-2
```

2. Zeigen Sie den Fortschritt an und stellen Sie sicher, dass der Stack gelöscht wurde.


```
aws cloudformation describe-stack-events --stack-name VPC-BPA-stack --region us-east-2
```

Verfolgen Sie das Löschen von Ausschlüssen mit CloudTrail

Füllen Sie diesen Abschnitt aus, um das Löschen von Ausschlüssen mithilfe von zu verfolgen AWS CloudTrail. CloudTrail Einträge werden angezeigt, wenn Sie eine Ausnahme löschen.

AWS-Managementkonsole

Sie können alle gelöschten Ausnahmen im CloudTrail Event-Verlauf einsehen, indem Sie in der AWS CloudTrail Konsole unter <https://console.aws.amazon.com/cloudtrailv2/Ressourcentyp> > AWSEC2::: VPCBlock PublicAccessExclusion suchen.

AWS CLI

Mit dem Befehl „lookup-events“ können Sie die Ereignisse im Zusammenhang mit dem Löschen von Ausschlüssen anzeigen:

```
aws cloudtrail lookup-events --lookup-attributes  
AttributeKey=ResourceType,AttributeValue=AWS::EC2::VPCBlockPublicAccessExclusion
```

Das erweiterte Beispiel ist abgeschlossen.

Security best practices for your 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 Region. AWS Die Verwendung mehrerer Availability Zones macht Ihre Produktionsanwendungen hochverfügbar, fehlertolerant und skalierbar.

- Verwenden Sie Sicherheitsgruppen, um den Datenverkehr zu EC2 Instances in Ihren Subnetzen zu kontrollieren. Weitere Informationen finden Sie unter [Sicherheitsgruppen](#).
- Verwenden Sie das Netzwerk ACLs , um den eingehenden und ausgehenden Verkehr auf Subnetzebene zu kontrollieren. Weitere Informationen finden Sie unter [Steuerung des Datenverkehrs in Subnetzen mithilfe von Zugriffskontrolllisten für Netzwerke](#).
- 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 unbeabsichtigte Netzwerkzugriffe auf Ressourcen in unserer 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-Logs, die Ihren EC2 Amazon-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 der [Amazon FAQs VPC](#).

Verwenden von Amazon VPC mit anderen AWS-Services

Amazon Virtual Private Cloud (VPC) ist ein grundlegender AWS-Service, der eine sichere, anpassbare Netzwerkumgebung für Ihre Cloud-Infrastruktur bereitstellt. Sie können nicht nur Ihre eigene VPC erstellen und verwalten, sondern auch die Integration zwischen VPC und anderen AWS-Services nutzen, um umfassende Lösungen zu entwickeln, die auf Ihre spezifischen Anforderungen zugeschnitten sind.

Sie können Ihre VPC mit verschiedenen AWS-Services über AWS PrivateLink verbinden. Dies ermöglicht eine private Konnektivität zwischen Ihrer VPC und unterstützten AWS-Services oder On-Premises-Anwendungen, wodurch der Netzwerkverkehr im AWS-Netzwerk gehalten wird und eine Gefährdung durch das öffentliche Internet vermieden wird. Dies ist besonders nützlich, um strenge Sicherheitsgrenzen und Compliance-Anforderungen einzuhalten.

Um die Sicherheit Ihrer VPC weiter zu erhöhen, können Sie AWS Network Firewall verwenden. Mit diesem verwalteten Firewall-Service können Sie Sicherheitsrichtlinien auf Netzwerkebene definieren und durchsetzen und dabei sowohl den Nord-Süd- als auch den Ost-West-Datenverkehr innerhalb Ihrer VPC filtern. Durch die Kopplung der Netzwerk-Firewall mit Ihrer VPC können Sie Ihre Verteidigungsstrategie verbessern und Ihre Cloud-Ressourcen vor unbefugtem Zugriff oder böswilligen Aktivitäten schützen.

Darüber hinaus können Sie den DNS-Datenverkehr innerhalb Ihrer VPC mithilfe der DNS-Firewall von Route 53 Resolver filtern. Mit dieser Funktion können Sie benutzerdefinierte DNS-Filterregeln erstellen, um zu kontrollieren, welche Domänen Ihre VPC-Ressourcen auflösen können, wodurch eine zusätzliche Ebene der Sicherheit und Compliance-Durchsetzung geschaffen wird.

Wenn Sie auf Erreichbarkeitsprobleme zwischen Ressourcen innerhalb Ihrer VPC oder mit Verbindung zu Ihrer VPC stoßen, können Sie Reachability Analyzer nutzen. Reachability Analyzer führt virtuelle Konnektivitätstests durch, um detaillierte Hop-By-Hop-Pfadinformationen bereitzustellen und alle blockierenden Komponenten zu identifizieren. Dieses Tool zur Fehlerbehebung kann Ihnen helfen, Probleme mit der Netzwerkkonnektivität schnell zu erkennen und zu lösen.

Durch die Integration dieser ergänzenden AWS-Services in Ihre VPC können Sie leistungsstarke, sichere und belastbare Cloud-Lösungen entwickeln, die Ihren individuellen Geschäfts- und Architekturanforderungen gerecht werden.

Inhalt

- [Verbinden Ihrer VPC mit anderen Services mithilfe von AWS PrivateLink](#)

- [Filtern von Netzwerkverkehr mit AWS Network Firewall](#)
- [Filtern von DNS-Datenverkehr mit Route 53 Resolver DNS Firewall](#)
- [Beheben von Erreichbarkeitsproblemen mit Reachability Analyzer](#)

Verbinden Ihrer VPC mit anderen Services mithilfe von AWS PrivateLink

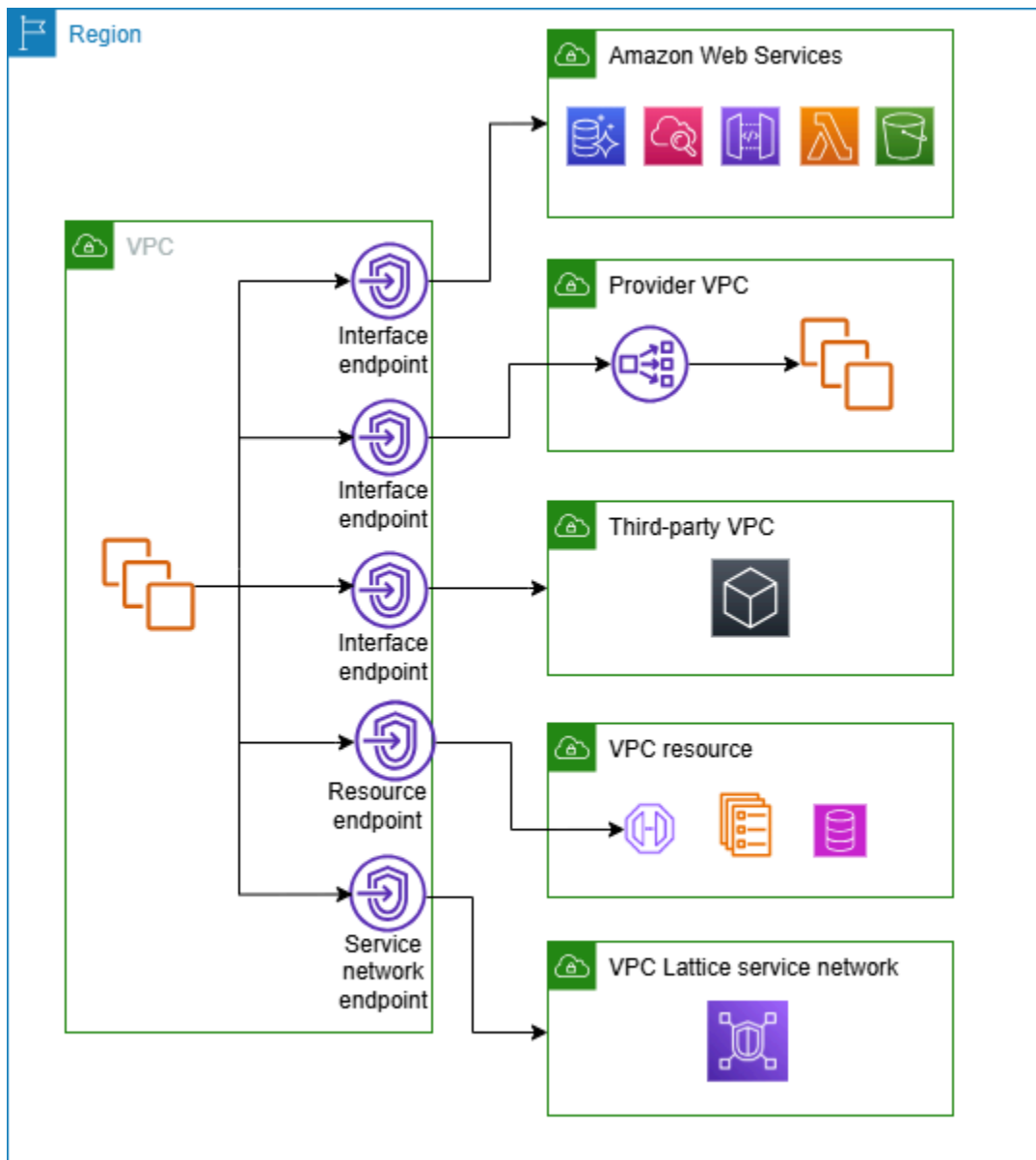
AWS PrivateLink stellt eine private Verbindung zwischen Virtual Private Clouds (VPCs) und unterstützten AWS-Services, von anderen AWS-Konten gehosteten Services, unterstützten AWS Marketplace-Services und unterstützten Ressourcen her. Sie benötigen kein Internet-Gateway, kein NAT-Gerät und auch keine Direct Connect- oder AWS Site-to-Site VPN-Verbindung, um mit dem Service oder der Ressource zu kommunizieren.

Erstellen Sie zur Verwendung von AWS PrivateLink einen VPC-Endpunkt in allen Subnetzen, von denen aus Sie auf den Service oder die Ressource zugreifen müssen. Dadurch werden Elastic-Netzwerk-Schnittstellen in den angegebenen Subnetzen erstellt, die als Eintrittspunkte für den Datenverkehr dienen, der für den Service oder die Ressource bestimmt ist.

Sie können auch Ihren eigenen von AWS PrivateLink gestützten VPC-Endpunkt-Service erstellen und anderen AWS-Kunden Zugriff auf Ihren Service erteilen. PrivateLink ermöglicht die Erstellung von privaten API-Endpunkten, sodass Unternehmen ihre eigenen Services anderen AWS-Kunden sicher zugänglich machen können. Dies ermöglicht es Unternehmen, ihre internen Fähigkeiten zu monetarisieren, Ökosysteme für die Zusammenarbeit zu fördern und die Kontrolle darüber zu behalten, wie auf ihre Services zugegriffen wird und wie diese genutzt werden.

Einer der Hauptvorteile der Nutzung von AWS PrivateLink ist die Möglichkeit, sichere, private Konnektivität herzustellen, ohne dass herkömmliche Netzwerkstrukturen wie Internet-Gateways, NAT-Geräte oder VPN-Verbindungen erforderlich sind. Dies trägt dazu bei, die Netzwerkarchitektur zu vereinfachen, die Angriffsfläche zu reduzieren und die allgemeine Sicherheit zu verbessern, indem der Datenverkehr auf das AWS-Netzwerk beschränkt bleibt.

Das folgende Diagramm veranschaulicht gängige Anwendungsfälle für AWS PrivateLink. Die VPC verfügt über mehrere EC2-Instances in einem privaten Subnetz, das über fünf VPC-Endpunkte auf Ressourcen zugreifen kann. Es gibt drei VPC-Schnittstellen-Endpunkte, einen Ressourcen-VPC-Endpunkt und einen VPC-Endpunkt für das Servicenetzwerk.



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 filtern AWS Network Firewall. 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 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-Standardereinstellungen. 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 Domainnamen 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-Ressource	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.

DNS-Firewall-Ressource	Beschreibung
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 Analyse der statischen Konfiguration. Mit Reachability Analyzer können Sie die Netzwerkerreichbarkeit zwischen zwei Ressourcen in Ihrer VPC analysieren und debuggen. Reachability Analyzer erstellt Hop-by-Hop-Details des virtuellen Pfads 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

Amazon Virtual Private Cloud (VPC) ist ein grundlegender Baustein im AWS-Ökosystem, mit dem Sie isolierte virtuelle Netzwerke bereitstellen können, die auf Ihre spezifischen Anforderungen zugeschnitten sind. Durch die Erstellung und Verwaltung Ihrer eigenen VPCs erhalten Sie die volle Kontrolle über die Netzwerkkumgebung, einschließlich der Möglichkeit, IP-Adressbereiche, Subnetze, Routing-Tabellen und Konnektivitätsoptionen zu definieren.

Dieser Abschnitt enthält drei Beispielkonfigurationen für Ihre Virtual Private Clouds (VPCs), die jeweils für eine andere Gruppe von Anforderungen konzipiert sind:

- VPC für eine Testumgebung: Diese Konfiguration zeigt, wie Sie eine VPC erstellen, die Sie als Entwicklungs- oder Testumgebung verwenden können.
- VPC für Web- und Datenbankserver: Diese Konfiguration zeigt, wie Sie eine VPC erstellen, die Sie für eine ausfallsichere Architektur in einer Produktionsumgebung verwenden können.
- VPC mit Servern in privaten Subnetzen und NAT: In dieser erweiterten Konfiguration werden alle EC2-Instances in privaten Subnetzen bereitgestellt, wobei ein NAT-Gateway einen sicheren ausgehenden Internetzugang ermöglicht. Dies ist ein Beispiel, bei dem Sie die direkte Internetverbindung auf Ihre Ressourcen beschränken und gleichzeitig die erforderliche ausgehende Kommunikation ermöglichen müssen.

Durch die Bereitstellung dieser VPC-Beispielkonfigurationen möchten wir die Flexibilität und die Anpassungsoptionen veranschaulichen, die bei der Gestaltung Ihrer Cloud-Netzwerkkumgebung verfügbar sind. Das spezifische VPC-Setup, das Sie wählen, sollte auf der Architektur, den Sicherheitsanforderungen und den allgemeinen Geschäftszielen Ihrer Anwendung basieren. Eine sorgfältige Planung Ihrer VPC-Infrastruktur kann Ihnen helfen, ein robustes, skalierbares und sicheres virtuelles Netzwerk aufzubauen, das das Wachstum und die Entwicklung Ihrer Cloud-basierten Workloads unterstützt.

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-Szenarios](#) im Benutzerhandbuch für AWS Site-to-Site VPN.
- Um Ihre VPCs miteinander und mit Ihrem eigenen Netzwerk zu verbinden, sehen Sie sich die [Beispiel-Szenarios für Transit-Gateways](#) unter 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.

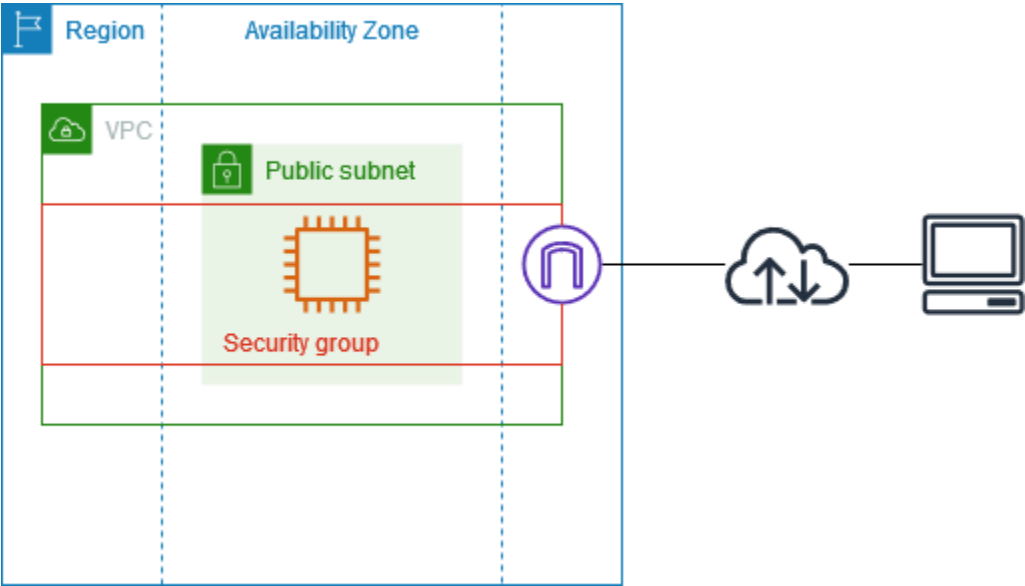
Inhalt

- [Übersicht](#)
- [1. Erstellen Sie die VPC](#)
- [2. Bereitstellen der Anwendung](#)
- [3. Testen Sie Ihre Konfiguration](#)
- [4. 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.

Bestimmungsort	Ziel
10.0.0.0/16	Local
2001:db8:1234:1a00::/56	Lokal
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.

Quelle	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
<i>Öffentlicher IPv4-Adressbereich Ihres Netzwerks</i>	TCP	22	(Optional) Lässt eingehenden SSH-Zugriff von IPv4-IP-Adressen in Ihrem Netzwerk zu
<i>IPv6-Adressbereich Ihres Netzwerks</i>	TCP	22	(Optional) Lässt eingehenden SSH-Zugriff von IPv6-IP-Adressen in Ihrem Netzwerk zu
<i>Öffentlicher IPv4-Adressbereich Ihres Netzwerks</i>	TCP	3389	(Optional) Lässt eingehenden RDP-Zugriff von IPv4-IP-Adressen in Ihrem Netzwerk zu
<i>IPv6-Adressbereich Ihres Netzwerks</i>	TCP	3389	(Optional) Lässt eingehenden RDP-Zugriff von IPv6-IP-Adressen in Ihrem Netzwerk zu

1. 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 Zu erstellende Ressourcen die Option 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 VPC erstellen aus.

2. Bereitstellen der Anwendung

Es gibt eine Vielzahl von Möglichkeiten für die Bereitstellung von EC2-Instances. Zum 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 AMI](#) im Benutzerhandbuch für Amazon EC2. Alternativ können Sie [EC2 Image Builder](#) verwenden, um Ihr Amazon Machine Image (AMI) zu erstellen und zu verwalten.

3. 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](#).

4. 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

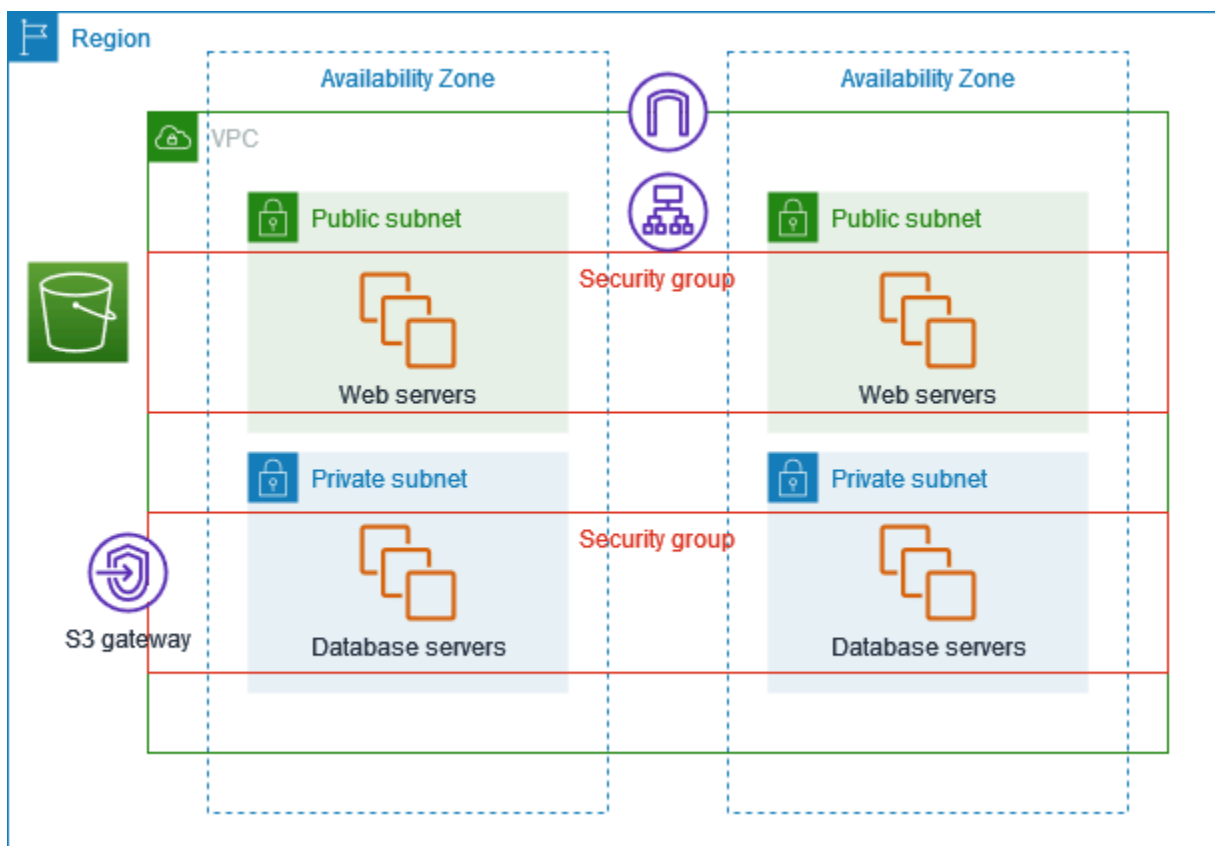
Dieses Beispiel zeigt, wie Sie eine VPC erstellen, die Sie für eine zweistufige Architektur in einer Produktionsumgebung verwenden können. Um die Ausfallsicherheit zu erhöhen, stellen Sie die Server in zwei Availability Zones bereit.

Inhalt

- [-Übersicht](#)
- [1. Erstellen Sie die VPC](#)
- [2. Bereitstellen der Anwendung](#)
- [3. Testen Sie Ihre Konfiguration](#)
- [4. 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. 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-Endpoint 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 Routentabelle für die öffentlichen Subnetze mit Routen für IPv4 sowohl IPv6 als auch. Wenn Sie Subnetze vom IPv4 Typ „Nur“ anstelle von Dual-Stack-Subnetzen erstellen, enthält Ihre Routing-Tabelle nur die Routen. IPv4

Bestimmungsort	Ziel
<i>10.0.0.0/16</i>	Local
<i>2001:db8:1234:1a00::/56</i>	Lokal
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

Im Folgenden finden Sie ein Beispiel für eine Routentabelle für die privaten Subnetze mit lokalen Routen für und. IPv4 IPv6 Wenn Sie IPv4 nur Subnetze erstellt haben, enthält Ihre Routing-Tabelle nur die Route. IPv4 Die letzte Route sendet Datenverkehr für Amazon S3 an den Gateway-VPC-Endpunkt.

Bestimmungsort	Ziel
<i>10.0.0.0/16</i>	Local
<i>2001:db8:1234:1a00::/56</i>	local
<i>s3-prefix-list-id</i>	<i>s3-gateway-id</i>

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.

Quelle	Protocol (Protokoll)	Port-Bereich	Description
<i>ID of the security group for the load balancer</i>	TCP	80	Lässt eingehenden HTTP-Zugriff vom Load Balancer zu
<i>ID of the security group for the load balancer</i>	TCP	443	Lässt eingehenden HTTP-Zugriff vom Load Balancer zu
<i>Public IPv4 address range of your network</i>	TCP	22	(Optional) Ermöglicht eingehenden SSH-Zugriff von IPv4 IP-Adressen in Ihrem Netzwerk
<i>IPv6 address range of your network</i>	TCP	22	(Optional) Ermöglicht eingehenden SSH-Zugriff von IPv6 IP-Adressen in Ihrem Netzwerk
<i>Public IPv4 address range of your network</i>	TCP	3389	(Optional) Ermöglicht eingehenden RDP-Zugriff von IPv4 IP-Adressen in Ihrem Netzwerk

Quelle	Protocol (Protokoll)	Port-Bereich	Description
<i>IPv6 address range of your network</i>	TCP	3389	(Optional) Ermöglicht eingehenden RDP-Zugriff von IPv6 IP-Adressen in Ihrem Netzwerk

Ziel	Protocol (Protokoll)	Port-Bereich	Description
<i>ID of the security group for instances running Microsoft SQL Server</i>	TCP	1433	Lässt ausgehenden Microsoft -SQL-Server-Zugriff auf die Datenbankserver zu
<i>ID of the security group for instances running MySQL</i>	TCP	3306	Lässt ausgehenden MySQL-Server-Zugriff auf die Datenbankserver zu

Datenbankserver

Die folgenden Sicherheitsgruppenregeln berechtigen die Datenbankserver, Lese- und Schreibenanforderungen von den Webservern zu empfangen.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentare
<i>ID of the web server security group</i>	TCP	1433	Lässt eingehenden Microsoft SQL Server-Zugriff von Webservern zu
<i>ID of the web server security group</i>	TCP	3306	Lässt eingehenden MySQL-Zugriff von den Webservern zu

Ziel	Protocol (Protokoll)	Port-Bereich	Kommentare
0.0.0.0/0	TCP	80	Ermöglicht ausgehenden HTTP-Zugriff auf das Internet über IPv4
0.0.0.0/0	TCP	443	Ermöglicht ausgehenden HTTPS-Zugriff auf das Internet über IPv4

Weitere Informationen zu Sicherheitsgruppen für Amazon RDS-DB-Instances finden Sie unter [Zugriffskontrolle mit Sicherheitsgruppen](#) im Amazon RDS-Benutzerhandbuch.

1. 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. Die VPC konfigurieren:
 - a. Lassen Sie die automatische Generierung von Namenstags aktiviert, um Namenstags für die VPC-Ressourcen zu erstellen, oder deaktivieren Sie sie, um Ihre eigenen Namenstags für die VPC-Ressourcen bereitzustellen.
 - b. Für den IPv4 CIDR-Block können Sie den Standardvorschlag beibehalten oder alternativ den CIDR-Block eingeben, der für Ihre Anwendung oder Ihr Netzwerk erforderlich ist. Weitere Informationen finden Sie unter [the section called “VPC-CIDR-Blöcke”](#).
 - c. (Optional) Wenn Ihre Anwendung über IPv6 Adressen kommuniziert, wählen Sie IPv6 CIDR-Block, von Amazon bereitgestellter CIDR-Block. IPv6
 - d. Wählen Sie eine Tenancy-Option aus. Diese Option definiert, ob EC2 Instances, die Sie in der VPC starten, auf Hardware ausgeführt werden, die mit anderen geteilt wird, AWS-Konten oder auf Hardware, die nur für Sie bestimmt ist. Wenn Sie die Tenancy der VPC als Tenancy wählen, verwenden EC2 InstancesDefault, 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 EC2 Amazon-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. Subnetze konfigurieren:

- 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 standardmäßigen CIDR-Blöcke für die Subnetze beibehalten oder alternativ die CIDR-Blöcke der 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.

2. 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, EC2 Instanzen bereitzustellen. Beispiel:

- [Assistent zum EC2 Starten von Amazon-Instanzen](#)
- [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 Ihre Anwendung erforderliche Mindest-Serverkapazität aufrechtzuerhalten.

Sie können [ELB](#) verwenden, um den Verkehr 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 AWS: So wählen Sie](#) aus.

3. 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](#).

4. 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.

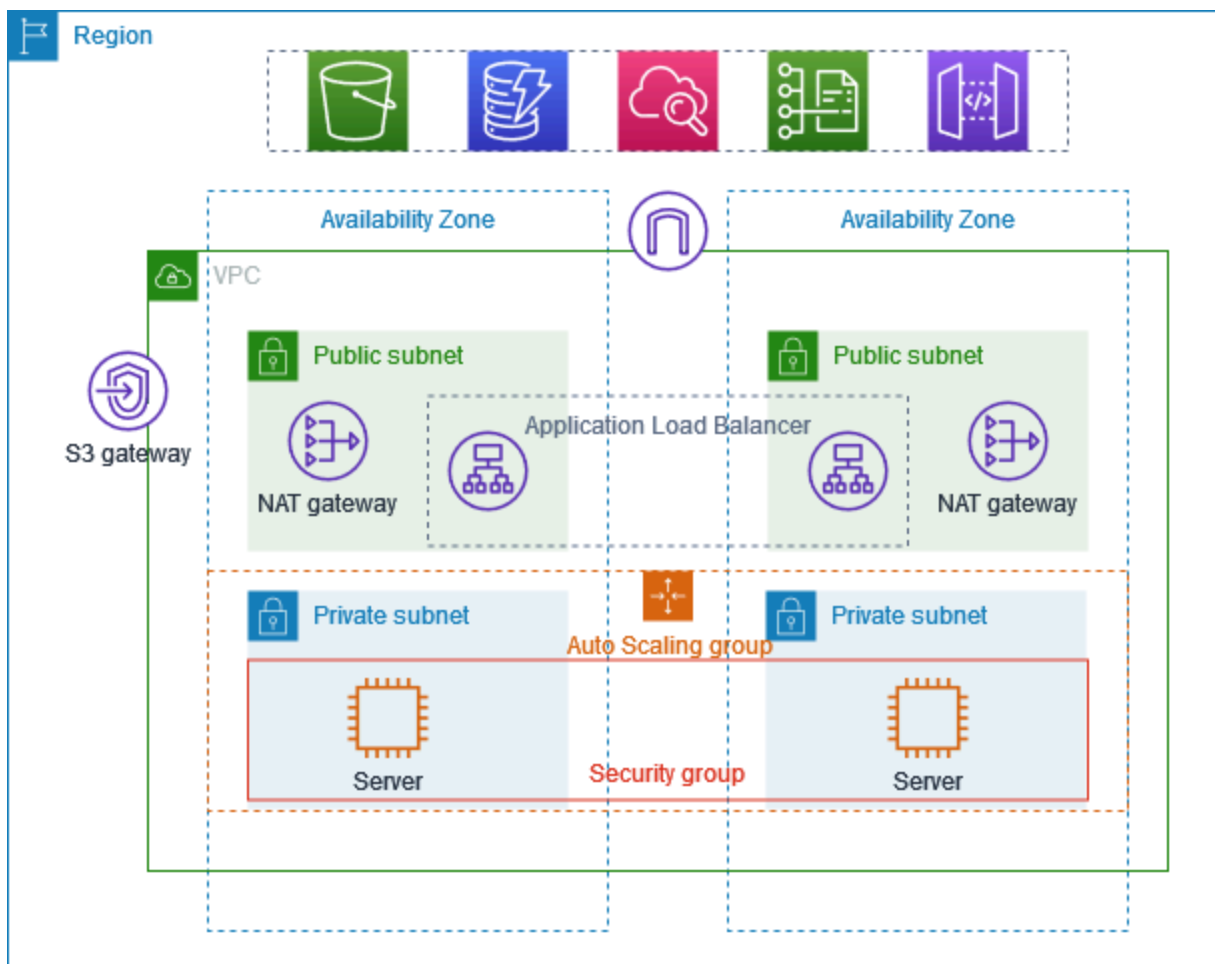
Inhalt

- [-Übersicht](#)

- [1. Erstellen Sie die VPC](#)
- [2. Bereitstellen der Anwendung](#)
- [3. Testen Sie Ihre Konfiguration](#)
- [4. 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.

Das Folgende ist ein Beispiel für die Routing-Tabelle für die öffentlichen Subnetze mit Routen für IPv4 sowohl IPv6 als auch. Wenn Sie Subnetze vom IPv4 Typ „Nur“ anstelle von Dual-Stack-Subnetzen erstellen, enthält Ihre Routing-Tabelle nur die Routen. IPv4

Bestimmungsort	Ziel
<i>10.0.0.0/16</i>	Local
<i>2001:db8:1234:1a00::/56</i>	Lokal
0.0.0.0/0	<i>igw-id</i>
::/0	<i>igw-id</i>

Im Folgenden finden Sie ein Beispiel für eine Routentabelle für eines der privaten Subnetze mit Routen für sowohl als auch. IPv4 IPv6 Wenn Sie Subnetze vom Typ „IPv4-only“ erstellt haben, enthält die Routentabelle nur die Routen. IPv4 Die letzte Route sendet Datenverkehr für Amazon S3 an den Gateway-VPC-Endpunkt.

Bestimmungsort	Ziel
<i>10.0.0.0/16</i>	Local
<i>2001:db8:1234:1a00::/56</i>	Lokal
0.0.0.0/0	<i>nat-gateway-id</i>
::/0	<i>eigw-id</i>
<i>s3-prefix-list-id</i>	<i>s3-gateway-id</i>

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.

Quelle	Protocol (Protokoll)	Port-Bereich	Kommentare
<i>ID of the load balancer security group</i>	<i>listener protocol</i>	<i>listener port</i>	Erlaubt eingehenden Datenverkehr vom Load Balancer auf dem Listener-Port
<i>ID of the load balancer security group</i>	<i>health check protocol</i>	<i>health check port</i>	Erlaubt Zustandsüberprüfungs-Datenverkehr vom Load Balancer

1. 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 Zu erstellende Ressourcen die Option 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. Für den IPv4 CIDR-Block können Sie den Standardvorschlag beibehalten oder alternativ den CIDR-Block eingeben, der für Ihre Anwendung oder Ihr Netzwerk erforderlich ist.
 - c. Wenn Ihre Anwendung über IPv6 Adressen kommuniziert, wählen Sie IPv6CIDR-Block, von Amazon bereitgestellter CIDR-Block. IPv6

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 Ihre Anwendung über IPv6 Adressen kommuniziert, wählen Sie für Internet-Gateway nur für ausgehenden Ausgang 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 VPC erstellen aus.

2. 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 für Ihre Anwendung erforderliche Mindest-Serverkapazität aufrechtzuerhalten.

So starten Sie Instances mithilfe einer Auto-Scaling-Gruppe

1. Erstellen Sie eine Startvorlage, um die Konfigurationsinformationen anzugeben, die zum Starten Ihrer EC2 Instances mithilfe von Amazon EC2 Auto Scaling erforderlich sind. step-by-stepEine Anleitung finden Sie unter [Erstellen einer Startvorlage für Ihre Auto Scaling Scaling-Gruppe](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

2. Erstellen Sie eine Auto Scaling Scaling-Gruppe, bei der es sich um eine Sammlung von EC2 Instances mit einer minimalen, maximalen und gewünschten Größe handelt. [step-by-step](#)Eine Anleitung finden Sie unter [Erstellen einer Auto Scaling Scaling-Gruppe mithilfe einer Startvorlage](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.
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 [Elastic Load Balancing User Guide und Use ELB](#) im Amazon EC2 Auto Scaling Scaling-Benutzerhandbuch.

3. 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](#).

4. 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”](#).

VPC-Tutorials

Amazon Virtual Private Cloud (VPC) ist die Grundlage Ihrer Netzwerkinfrastruktur in AWS. Die AWS-Managementkonsole bietet zwar eine benutzerfreundliche Oberfläche, aber die AWS-Befehlszeilenschnittstelle (CLI) bietet mehr Flexibilität und Automatisierungsfunktionen für die Erstellung und Verwaltung Ihrer VPC-Ressourcen.

In diesem Handbuch werden zwei wesentliche Szenarien der VPC-Bereitstellung beschrieben:

- Ein grundlegendes VPC-Setup mit einem öffentlichen Subnetz – ideal für einfache Webanwendungen
- Eine erweiterte VPC-Konfiguration mit privaten und öffentlichen Subnetzen sowie NAT-Gateways – geeignet für mehrstufige Anwendungen

In diesen Tutorials lernen Sie Folgendes:

- VPCs mit unterschiedlichen Subnetzkonfigurationen erstellen
- Internet- und NAT-Gateways einrichten
- Routing-Tabellen und Sicherheitsgruppen konfigurieren
- AWS CLI-Befehle verwenden, um die Netzwerkinfrastruktur zu verwalten
- Bewährte AWS-Netzwerkmethoden implementieren

Wir beginnen mit der Einrichtung Ihrer AWS-Netzwerkinfrastruktur über die Befehlszeile.

Tutorials

- [Erste Schritte mit Amazon VPC mithilfe der CLI AWS](#)
- [Erstellen einer VPC mit privaten Subnetzen und NAT-Gateways mit der AWS CLI](#)

Erste Schritte mit Amazon VPC mithilfe der CLI AWS

Dieses Tutorial führt Sie durch die Erstellung einer Virtual Private Cloud (VPC) mithilfe der AWS Befehlszeilenschnittstelle (AWS CLI). Sie erfahren, wie Sie eine VPC mit öffentlichen und privaten Subnetzen einrichten, Internetkonnektivität konfigurieren und EC2 Instances bereitstellen, um eine gemeinsame Webanwendungsarchitektur zu demonstrieren.

Voraussetzungen

Stellen Sie vor Beginn dieses Tutorials sicher, dass Sie über Folgendes verfügen:

1. Das AWS CLI Wenn Sie die CLI installieren müssen, folgen Sie der [AWS CLI - Installationsanleitung](#).
2. Hat Ihre AWS CLI mit den entsprechenden Anmeldeinformationen konfiguriert. Führen Sie `aws configure` aus, falls Sie Ihre Anmeldeinformationen noch nicht eingerichtet haben.
3. Grundlegendes Verständnis von Netzwerkkonzepten.
4. [Identity and Access Management für Amazon VPC](#) um VPC-Ressourcen in Ihrem AWS Konto zu erstellen und zu verwalten.

Kostenüberlegungen

In diesem Tutorial werden AWS Ressourcen erstellt, für die möglicherweise Kosten in Ihrem Konto anfallen. Die Hauptkosten entfallen auf das NAT-Gateway (0,045 USD pro Stunde zuzüglich Datenverarbeitungsgebühren) und die EC2 Instances (t2.micro, jeweils etwa 0,0116 USD pro Stunde). Wenn Sie dieses Tutorial in einer Stunde abschließen und anschließend alle Ressourcen bereinigen, belaufen sich die Gesamtkosten auf etwa 0,07 USD. Zur Kostenoptimierung in Entwicklungsumgebungen können Sie anstelle eines NAT-Gateways eine NAT-Instance nutzen, was die Kosten erheblich senken kann.

Lassen Sie uns überprüfen, ob Ihr System ordnungsgemäß konfiguriert ist, bevor Sie fortfahren AWS CLI .

```
aws configure list
```

Sie sollten Ihren AWS Zugriffsschlüssel, Ihren geheimen Schlüssel und Ihre Standardregion sehen. Außerdem sollten Sie sich vergewissern, dass Sie die erforderlichen Berechtigungen haben, um VPC-Ressourcen zu erstellen.

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

Dieser Befehl zeigt Ihre AWS Konto-ID, Benutzer-ID und ARN an und bestätigt, dass Ihre Anmeldeinformationen gültig sind.

Erstellen einer VPC

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk, das Ihrem AWS Konto gewidmet ist. In diesem Abschnitt erstellen Sie eine VPC mit dem CIDR-Block 10.0.0.0/16, der bis zu 65 536 IP-Adressen bereitstellt.

Erstellen Sie die VPC

Der folgende Befehl erstellt eine neue VPC und weist ihr ein Namens-Tag zu.

```
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications  
'ResourceType=vpc,Tags=[{Key=Name,Value=MyVPC}]'
```

Notieren Sie sich die VPC-ID in der Ausgabe. Sie benötigen sie für spätere Befehle. Für die Zwecke dieses Tutorials verwenden wir die VPC-ID „vpc-0123456789abcdef0“. Ersetzen Sie diesen Beispielwert in allen Befehlen durch Ihre tatsächliche VPC-ID.

Aktivieren von DNS-Unterstützung und Hostnamen

Standardmäßig sind DNS-Auflösung und DNS-Hostnamen in einer neuen VPC deaktiviert. Aktivieren Sie dieses Feature, damit Instances in Ihrer VPC Domainnamen auflösen können.

```
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-support  
aws ec2 modify-vpc-attribute --vpc-id vpc-0123456789abcdef0 --enable-dns-hostnames
```

Diese Befehle erzeugen bei erfolgreicher Ausführung keine Ausgabe. DNS-Unterstützung und Hostnamenauflösung sind für Ihre VPC jetzt aktiviert.

Erstellen von Subnetzen

Subnetze sind Segmente des IP-Adressbereichs einer VPC, in dem Sie Gruppen isolierter Ressourcen platzieren können. In diesem Abschnitt erstellen Sie öffentliche und private Subnetze in zwei Availability Zones, um eine hohe Verfügbarkeit zu erzielen.

Abrufen verfügbarer Availability Zones

Rufen Sie zuerst die in Ihrer Region verfügbaren Availability Zones ab.

```
aws ec2 describe-availability-zones
```

In diesem Tutorial verwenden wir die ersten beiden Availability Zones. Notieren Sie sich ihre Namen in der Ausgabe („us-east-1a“ und „us-east-1b“).

Erstellen öffentlicher Subnetze

Öffentliche Subnetze werden für Ressourcen verwendet, die über das Internet erreichbar sein müssen, z. B. Webserver.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ1}]'
```

Notieren Sie sich die Subnetz-ID in der Ausgabe. Für dieses Tutorial verwenden wir „subnet-0123456789abcdef0“ als Beispiel für das erste öffentliche Subnetz.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.1.0/24 \
  --availability-zone us-east-1b \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Public-Subnet-AZ2}]'
```

Notieren Sie sich die Subnetz-ID in der Ausgabe. Für dieses Tutorial verwenden wir „subnet-0123456789abcdef1“ als Beispiel für das zweite öffentliche Subnetz.

Erstellen privater Subnetze

Private Subnetze werden für Ressourcen verwendet, die nicht direkt über das Internet erreichbar sein sollten, z. B. Datenbanken.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
  --cidr-block 10.0.2.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ1}]'
```

Notieren Sie sich die Subnetz-ID in der Ausgabe. Für dieses Tutorial verwenden wir „subnet-0123456789abcdef2“ als Beispiel für das erste private Subnetz.

```
aws ec2 create-subnet \
  --vpc-id vpc-0123456789abcdef0 \
```

```
--cidr-block 10.0.3.0/24 \  
--availability-zone us-east-1b \  
--tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private-Subnet-AZ2}]'
```

Notieren Sie sich die Subnetz-ID in der Ausgabe. Für dieses Tutorial verwenden wir „subnet-0123456789abcdef3“ als Beispiel für das zweite private Subnetz.

Sie haben jetzt vier Subnetze: zwei öffentliche und zwei private Subnetze, verteilt auf zwei Availability Zones.

Tipp: Achten Sie bei der Planung Ihrer CIDR-Blöcke darauf, dass sie sich nicht mit Ihren bestehenden Netzwerken überschneiden. Für Produktionsumgebungen sollten Sie genügend IP-Adressen für künftiges Wachstum zuweisen und die Subnetze aus Sicherheits- und Verwaltungsgründen angemessen dimensionieren.

Konfigurieren der Internetverbindung

Damit Ressourcen in Ihrer VPC mit dem Internet kommunizieren können, müssen Sie ein Internet-Gateway erstellen und anfügen. In diesem Abschnitt richten Sie die Internetverbindung für Ihre VPC ein.

Erstellen eines Internet-Gateways

Ein Internet-Gateway ermöglicht die Kommunikation zwischen der VPC und dem Internet.

```
aws ec2 create-internet-gateway \  
--tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=MyIGW}]'
```

Notieren Sie sich die Internet-Gateway-ID in der Ausgabe. Für dieses Tutorial verwenden wir „igw-0123456789abcdef0“ als Beispiel.

Anfügen eines Internet-Gateways an Ihre VPC

Nachdem Sie ein Internet-Gateway erstellt haben, fügen Sie es an Ihre VPC an.

```
aws ec2 attach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id  
vpc-0123456789abcdef0
```

Erstellen und Konfigurieren von Routing-Tabellen

Routing-Tabellen enthalten Regeln (Routen), die bestimmen, wohin der Netzwerkverkehr geleitet wird. Erstellen Sie als Erstes eine Routing-Tabelle für Ihre öffentlichen Subnetze.


```
aws ec2 create-route-table \  
  --vpc-id vpc-0123456789abcdef0 \  
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Public-RT}]'
```

Notieren Sie sich die Routing-Tabellen-ID in der Ausgabe. Für dieses Tutorial verwenden wir „rtb-0123456789abcdef0“ als Beispiel für die erste öffentliche Routing-Tabelle.

Fügen Sie dem Internet-Gateway in der öffentlichen Routing-Tabelle eine Route hinzu.

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef0 --destination-cidr-block  
0.0.0.0/0 --gateway-id igw-0123456789abcdef0
```

Ordnen Sie die öffentlichen Subnetze der neuen Routing-Tabelle zu.

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id  
subnet-0123456789abcdef0  
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef0 --subnet-id  
subnet-0123456789abcdef1
```

Erstellen Sie jetzt eine Routing-Tabelle für Ihre privaten Subnetze.

```
aws ec2 create-route-table \  
  --vpc-id vpc-0123456789abcdef0 \  
  --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Private-RT}]'
```

Notieren Sie sich die Routing-Tabellen-ID in der Ausgabe. Für dieses Tutorial verwenden wir „rtb-0123456789abcdef1“ als Beispiel für die private Routing-Tabelle.

Ordnen Sie die privaten Subnetze der privaten Routing-Tabelle zu.

```
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id  
subnet-0123456789abcdef2  
aws ec2 associate-route-table --route-table-id rtb-0123456789abcdef1 --subnet-id  
subnet-0123456789abcdef3
```

Erstellen eines NAT-Gateways

Mit einem NAT-Gateway können Instances in privaten Subnetzen ausgehenden Datenverkehr zum Internet initiieren und eingehenden Datenverkehr aus dem Internet verhindern. Das ist wichtig für Instances, die Updates herunterladen oder auf externe Services zugreifen müssen.

Zuweisen einer Elastic-IP

Weisen Sie Ihrem NAT-Gateway zuerst eine Elastic-IP-Adresse zu.

```
aws ec2 allocate-address --domain vpc
```

Notieren Sie sich die Zuweisungs-ID in der Ausgabe. Für dieses Tutorial verwenden wir „eipalloc-0123456789abcdef0“ als Beispiel.

Erstellen des NAT-Gateways

Erstellen Sie mit der zugewiesenen Elastic-IP ein NAT-Gateway in einem Ihrer öffentlichen Subnetze.

```
aws ec2 create-nat-gateway \
  --subnet-id subnet-0123456789abcdef0 \
  --allocation-id eipalloc-0123456789abcdef0 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=MyNATGateway}]'
```

Notieren Sie sich die NAT-Gateway-ID in der Ausgabe. Für dieses Tutorial verwenden wir „nat-0123456789abcdef0“ als Beispiel.

Warten Sie, bis das NAT-Gateway verfügbar ist, bevor Sie fortfahren.

```
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-0123456789abcdef0
```

Hinzufügen einer Route zum NAT-Gateway

Fügen Sie in der private Routing-Tabelle eine Route zum NAT-Gateway hinzu, damit Instances in privaten Subnetzen auf das Internet zugreifen können.

```
aws ec2 create-route --route-table-id rtb-0123456789abcdef1 --destination-cidr-block
0.0.0.0/0 --nat-gateway-id nat-0123456789abcdef0
```

Hinweis: Für Produktionsumgebungen kann es sinnvoll sein, in jeder Availability Zone, in der Sie private Subnetze haben, ein NAT-Gateway zu erstellen, um Single Points of Failure zu vermeiden.

Konfigurieren der Subnetz-Einstellungen

Konfigurieren Sie Ihre öffentlichen Subnetze so, dass die Zuweisung von IP-Adressen für Instances, die darin gestartet werden, automatisch erfolgt.

```
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef0 --map-public-ip-on-launch
aws ec2 modify-subnet-attribute --subnet-id subnet-0123456789abcdef1 --map-public-ip-on-launch
```

Dadurch erhalten Instances, die in Ihren öffentlichen Subnetzen gestartet werden, standardmäßig eine öffentliche IP-Adresse, sodass sie über das Internet erreichbar sind.

Erstellen von Sicherheitsgruppen

Sicherheitsgruppen dienen als virtuelle Firewalls für Ihre Instances, um den ein- und ausgehenden Datenverkehr zu steuern. In diesem Abschnitt erstellen Sie Sicherheitsgruppen für Webserver und Datenbankserver.

Erstellen einer Sicherheitsgruppe für Webserver

```
aws ec2 create-security-group \
  --group-name WebServerSG \
  --description "Security group for web servers" \
  --vpc-id vpc-0123456789abcdef0
```

Notieren Sie sich die ID der Sicherheitsgruppe in der Ausgabe. In diesem Tutorial verwenden wir „sg-0123456789abcdef0“ als Beispiel für die Webserver-Sicherheitsgruppe.

Lassen Sie HTTP- und HTTPS-Datenverkehr zu Ihren Webservern zu.

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp --port 80 --cidr 0.0.0.0/0
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef0 --protocol tcp --port 443 --cidr 0.0.0.0/0
```

Hinweis: In Produktionsumgebungen sollten Sie den eingehenden Datenverkehr auf bestimmte IP-Bereiche beschränken, statt den Datenverkehr von 0.0.0.0/0 (beliebige IP-Adresse) zuzulassen.

Erstellen einer Sicherheitsgruppe für Datenbankserver

```
aws ec2 create-security-group \
  --group-name DBServerSG \
  --description "Security group for database servers" \
  --vpc-id vpc-0123456789abcdef0
```

Notieren Sie sich die ID der Sicherheitsgruppe in der Ausgabe. In diesem Tutorial verwenden wir „sg-0123456789abcdef1“ als Beispiel für die Datenbankserver-Sicherheitsgruppe.

Lassen Sie nur MySQL/Aurora Datenverkehr von Webservern zu.

```
aws ec2 authorize-security-group-ingress --group-id sg-0123456789abcdef1 --protocol tcp  
--port 3306 --source-group sg-0123456789abcdef0
```

Diese Konfiguration sorgt dafür, dass nur Instances in der Webserver-Sicherheitsgruppe eine Verbindung zu Ihren Datenbankservern über Port 3306 herstellen können. Dabei gilt das Prinzip der geringsten Berechtigung.

Ihre VPC-Konfiguration überprüfen

Nachdem Sie alle erforderlichen Komponenten erstellt haben, überprüfen Sie, ob Ihre VPC korrekt eingerichtet ist.

VPC überprüfen

```
aws ec2 describe-vpcs --vpc-id vpc-0123456789abcdef0
```

Subnetze überprüfen

```
aws ec2 describe-subnets --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Routing-Tabellen überprüfen

```
aws ec2 describe-route-tables --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Internet-Gateway überprüfen

```
aws ec2 describe-internet-gateways --filters "Name=attachment.vpc-  
id,Values=vpc-0123456789abcdef0"
```

NAT-Gateway überprüfen

```
aws ec2 describe-nat-gateways --filter "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Sicherheitsgruppenüberprüfen

```
aws ec2 describe-security-groups --filters "Name=vpc-id,Values=vpc-0123456789abcdef0"
```

Mit diesen Befehlen werden detaillierte Informationen zu jeder Komponente Ihrer VPC zurückgegeben, sodass Sie überprüfen können, ob alles richtig konfiguriert ist.

Stellen Sie EC2 Instanzen bereit

Nachdem Sie Ihre VPC-Infrastruktur erstellt haben, können Sie EC2 Instances bereitstellen, um zu demonstrieren, wie die Architektur funktioniert. Dafür starten Sie einen Webserver in einem öffentlichen Subnetz und einen Datenbankserver in einem privaten Subnetz.

Erstellen eines Schlüsselpaares für den SSH-Zugriff

Als Erstes erstellen Sie ein Schlüsselpaar für die sichere Verbindung zu Ihren Instances:

```
aws ec2 create-key-pair --key-name vpc-tutorial-key --query 'KeyMaterial' --output text  
> vpc-tutorial-key.pem  
chmod 400 vpc-tutorial-key.pem
```

Dieser Befehl erstellt ein neues Schlüsselpaar und speichert den privaten Schlüssel in einer Datei mit eingeschränkten Berechtigungen.

Suchen des neuesten Amazon-Linux-2-AMI

Suchen Sie das neueste Amazon-Linux-2-AMI zur Verwendung für Ihre Instances:

```
aws ec2 describe-images --owners amazon \  
--filters "Name=name,Values=amzn2-ami-hvm-*-x86_64-gp2" "Name=state,Values=available" \  
\   
--query "sort_by(Images, &CreationDate)[-1].ImageId" --output text
```

Notieren Sie sich die AMI-ID in der Ausgabe. Für dieses Tutorial verwenden wir „ami-0123456789abcdef0“ als Beispiel.

Starten eines Webserver im öffentlichen Subnetz

Starten Sie nun eine EC2 Instance im öffentlichen Subnetz, die als Webserver dient:

```
aws ec2 run-instances \  
--image-id ami-0123456789abcdef0 \  
--count 1 \  

```

```
--instance-type t2.micro \  
--key-name vpc-tutorial-key \  
--security-group-ids sg-0123456789abcdef0 \  
--subnet-id subnet-0123456789abcdef0 \  
--associate-public-ip-address \  
--user-data '#!/bin/bash  
            yum update -y  
            yum install -y httpd  
            systemctl start httpd  
            systemctl enable httpd  
            echo "<h1>Hello from $(hostname -f)</h1>" > /var/www/html/index.html' \  
--tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=WebServer}]'
```

Notieren Sie sich die Instance-ID in der Ausgabe. In diesem Tutorial verwenden wir „i-0123456789abcdef0“ als Beispiel für die Webserver-Instance.

Starten eines Datenbankservers im privaten Subnetz

Starten Sie als Nächstes eine EC2 Instance im privaten Subnetz, die als Datenbankserver dient:

```
aws ec2 run-instances \  
--image-id ami-0123456789abcdef0 \  
--count 1 \  
--instance-type t2.micro \  
--key-name vpc-tutorial-key \  
--security-group-ids sg-0123456789abcdef1 \  
--subnet-id subnet-0123456789abcdef2 \  
--user-data '#!/bin/bash  
            yum update -y  
            yum install -y mariadb-server  
            systemctl start mariadb  
            systemctl enable mariadb' \  
--tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=DBServer}]'
```

Notieren Sie sich die Instance-ID in der Ausgabe. Für dieses Tutorial verwenden wir „i-0123456789abcdef1“ als Beispiel für die Datenbankserver-Instance.

Aufrufen Ihres Webservers

Sobald Ihre Webserver-Instance ausgeführt wird, können Sie über ihre öffentliche IP-Adresse darauf zugreifen:

```
aws ec2 describe-instances \  

```

```
--instance-ids i-0123456789abcdef0 \  
--query 'Reservations[0].Instances[0].PublicIpAddress' \  
--output text
```

Dieser Befehl gibt die öffentliche IP-Adresse Ihres Webserver aus. Für dieses Tutorial verwenden wir „203.0.113.10“ als Beispiel.

Sie können jetzt diese URL in Ihrem Webbrowser öffnen: <http://203.0.113.10>

Herstellen einer Verbindung zu Ihren Instances mit SSH

Verbindung zu Ihrem Webserver herstellen:

```
ssh -i vpc-tutorial-key.pem ec2-user@203.0.113.10
```

Zum Verbinden mit Ihrem Datenbankserver müssen Sie zuerst eine SSH-Verbindung zu Ihrem Webserver und dann zu Ihrem Datenbankserver herstellen:

```
# Get the private IP of the database server  
aws ec2 describe-instances \  
  --instance-ids i-0123456789abcdef1 \  
  --query 'Reservations[0].Instances[0].PrivateIpAddress' \  
  --output text
```

Dieser Befehl gibt die private IP-Adresse Ihres Datenbankservers aus. Für dieses Tutorial verwenden wir „10.0.2.10“ als Beispiel.

```
# First SSH to web server, then to database server  
ssh -i vpc-tutorial-key.pem -A ec2-user@203.0.113.10  
ssh ec2-user@10.0.2.10
```

Dadurch wird die von Ihnen erstellte Netzwerkarchitektur demonstriert: Der Webserver ist öffentlich zugänglich und der Datenbankserver ist nur aus der VPC zugänglich.

Fehlerbehebung

Hier finden Sie häufig auftretende Probleme, die beim Erstellen einer VPC auftreten können, und Schritte zur Behebung:

CIDR-Block-Überschneidungen

Wenn Sie eine Fehlermeldung zu CIDR-Blocküberschneidungen erhalten, stellen Sie sicher, dass sich die CIDR-Blöcke für Ihre VPC und Subnetze nicht mit vorhandenen VPCs oder Subnetzen in Ihrem Konto überschneiden.

Berechtigungsfehler

Wenn Berechtigungsfehler auftreten, stellen Sie sicher, dass Ihr IAM-Benutzer oder Ihre IAM-Rolle die erforderlichen Berechtigungen zum Erstellen und Verwalten von VPC-Ressourcen hat. Möglicherweise müssen Sie die `AmazonVPCFullAccess`-Richtlinie anfügen oder eine benutzerdefinierte Richtlinie mit den erforderlichen Berechtigungen erstellen.

Grenzwerte für Ressourcen

AWS Konten haben Standardbeschränkungen für die Anzahl der VPCs Subnetze und anderen Ressourcen, die Sie erstellen können. Wenn Sie diese Limits erreichen, können Sie über das AWS Support Center eine Erhöhung beantragen.

Abhängigkeitsfehler bei der Bereinigung

Beim Bereinigen von Ressourcen können Abhängigkeitsfehler auftreten, wenn Sie versuchen, Ressourcen in der falschen Reihenfolge zu löschen. Achten Sie darauf, Ressourcen immer in umgekehrter Reihenfolge ihrer Erstellung zu löschen, angefangen bei den Ressourcen mit der größten Abhängigkeit.

Bereinigen von Ressourcen

Wenn Sie Ihre VPC fertiggestellt haben, können Sie die Ressourcen bereinigen, damit keine Gebühren anfallen. Löschen Sie die Ressourcen in umgekehrter Reihenfolge ihrer Erstellung, um Abhängigkeiten korrekt zu handhaben.

EC2 Instanzen beenden

```
aws ec2 terminate-instances --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
aws ec2 wait instance-terminated --instance-ids i-0123456789abcdef0 i-0123456789abcdef1
```

Schlüsselpaare löschen

```
aws ec2 delete-key-pair --key-name vpc-tutorial-key
rm vpc-tutorial-key.pem
```

NAT-Gateway löschen


```
aws ec2 delete-nat-gateway --nat-gateway-id nat-0123456789abcdef0
aws ec2 wait nat-gateway-deleted --nat-gateway-ids nat-0123456789abcdef0
```

Elastic-IP freigeben

```
aws ec2 release-address --allocation-id eipalloc-0123456789abcdef0
```

Sicherheitsgruppen löschen

```
aws ec2 delete-security-group --group-id sg-0123456789abcdef1
aws ec2 delete-security-group --group-id sg-0123456789abcdef0
```

Routing-Tabellen löschen

Suchen Sie zunächst nach der Zuordnung der Routentabelle IDs:

```
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef0
aws ec2 describe-route-tables --route-table-id rtb-0123456789abcdef1
```

Trennen Sie dann die Zuordnung der Routing-Tabellen zu den Subnetzen (ersetzen Sie die Zuordnung IDs durch die aus Ihrer Ausgabe):

```
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef0
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef1
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef2
aws ec2 disassociate-route-table --association-id rtbassoc-0123456789abcdef3
```

Löschen Sie nun die Routing-Tabellen:

```
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef1
aws ec2 delete-route-table --route-table-id rtb-0123456789abcdef0
```

Internet-Gateway trennen und löschen

```
aws ec2 detach-internet-gateway --internet-gateway-id igw-0123456789abcdef0 --vpc-id
vpc-0123456789abcdef0
aws ec2 delete-internet-gateway --internet-gateway-id igw-0123456789abcdef0
```

Subnetze löschen

```
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef0
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef1
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef2
aws ec2 delete-subnet --subnet-id subnet-0123456789abcdef3
```

Löschen Sie die VPC

```
aws ec2 delete-vpc --vpc-id vpc-0123456789abcdef0
```

In die Produktion übergehen

In diesem Tutorial erfahren Sie, wie Sie mit der AWS CLI eine VPC erstellen. Beachten Sie bei Produktionsumgebungen die folgenden bewährten Methoden für Sicherheit und Architektur:

1. Regeln für Sicherheitsgruppen: Beschränken Sie den eingehenden Datenverkehr auf bestimmte IP-Bereiche, statt den Datenverkehr von 0.0.0.0/0 zuzulassen.
2. Hohe Verfügbarkeit: Stellen Sie NAT-Gateways in jeder Availability Zone bereit, in der Sie private Subnetze haben, um Single Points of Failure zu vermeiden.
3. Netzwerk ACLs: Implementieren Sie das Netzwerk ACLs als zusätzliche Sicherheitsebene, die über Sicherheitsgruppen hinausgeht.
4. VPC Flow Logs: Aktivieren Sie VPC Flow Logs, um Netzwerkverkehrsmuster zu überwachen und zu analysieren.
5. Ressourcen-Tagging: Implementieren Sie eine umfassende Tagging-Strategie, um das Ressourcenmanagement zu verbessern.

Weitere Informationen zum Einrichten produktionsreifer Architekturen finden Sie unter [AWS Well-Architected Framework](#) and [Bewährte Methoden für die AWS -Sicherheit](#).

Nächste Schritte

Nachdem Sie eine VPC mit öffentlichen und privaten Subnetzen erstellt haben, können Sie:

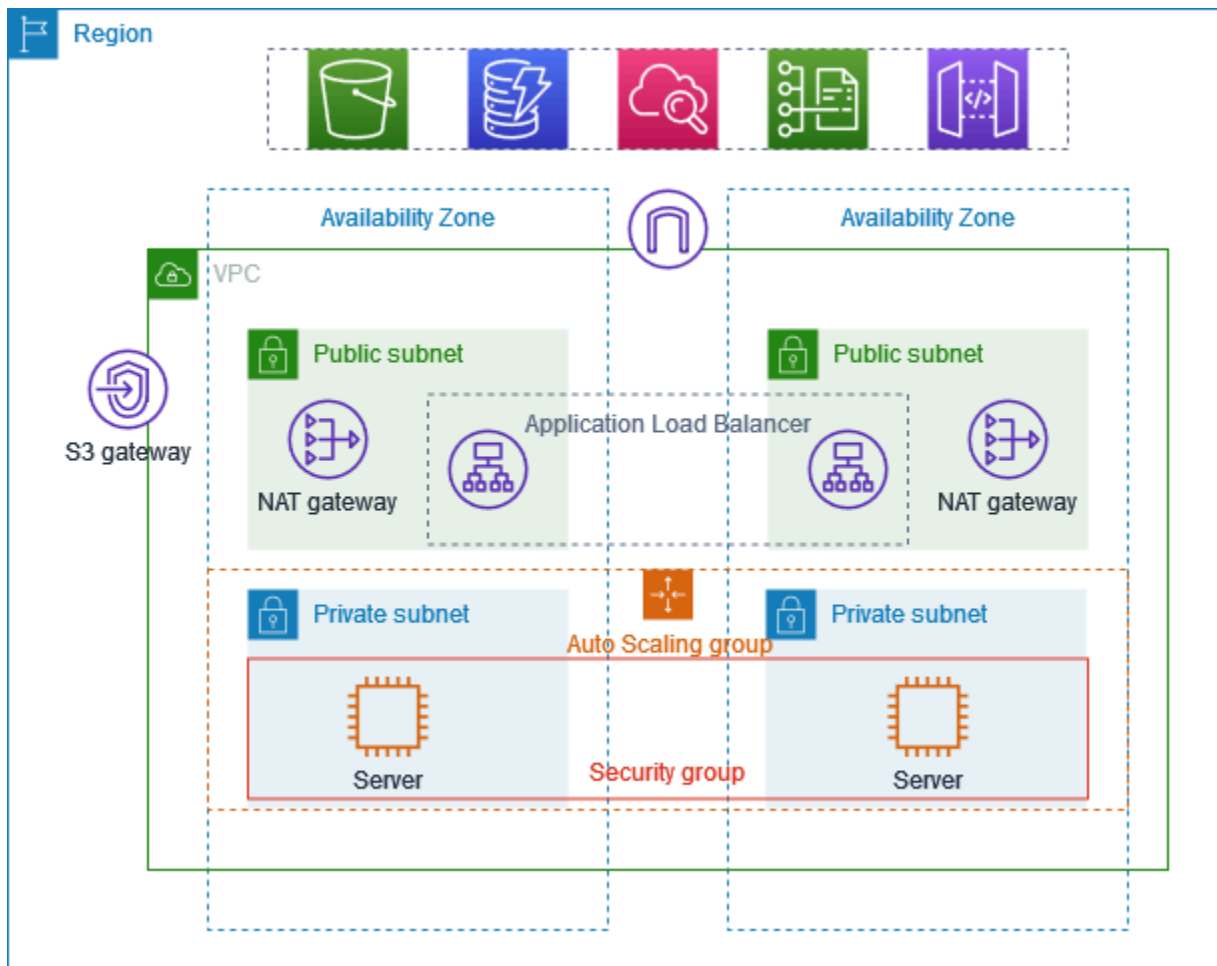
1. [Starten Sie EC2 Instances](#) in Ihren öffentlichen oder privaten Subnetzen.
2. [Load Balancer bereitstellen](#), um den Datenverkehr auf mehrere Instances zu verteilen.
3. [Auto-Scaling-Gruppen](#) für hohe Verfügbarkeit und Skalierbarkeit einrichten.
4. [RDS-Datenbanken](#) in Ihren privaten Subnetzen konfigurieren.

5. [Implementieren Sie VPC-Peering](#), um sich mit anderen zu verbinden. VPCs
6. [VPN-Verbindungen einrichten](#), um Ihre VPC mit Ihrem On-Premises-Netzwerk zu verbinden.

Erstellen einer VPC mit privaten Subnetzen und NAT-Gateways mit der AWS CLI

In diesem Tutorial wird gezeigt, wie Sie über die AWS CLI eine VPC erstellen, die Sie für Server in einer Produktionsumgebung verwenden können. Um die Resilienz zu verbessern, stellen Sie Server in zwei Availability Zones bereit und verwenden dabei eine Auto-Scaling-Gruppe und einen Application Load Balancer. Für zusätzliche Sicherheit werden Sie die Datenbankserver in privaten Subnetzen bereitstellen. Die Server empfangen Anfragen über den Load Balancer und können über NAT-Gateways eine Verbindung zum Internet herstellen. Um die Resilienz zu verbessern, stellen Sie ein NAT-Gateway in jeder Availability Zone bereit.

Das folgende Diagramm bietet einen Überblick über die genutzten Ressourcen in diesem Tutorial. 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.



Voraussetzungen

Bevor Sie mit diesem Tutorial beginnen, brauchen Sie Folgendes:

- Die AWS CLI muss installiert und mit Berechtigungen zum Erstellen von VPC-Ressourcen, EC2-Instances, Load Balancern und Auto-Scaling-Gruppen konfiguriert sein. Informationen zur Installation von AWS CLI finden Sie unter [Installieren oder Aktualisieren der neuesten Version von AWS CLI](#).
- Grundkenntnisse der VPC-Konzepte, einschließlich Subnetzen, Routing-Tabellen und Internet-Gateways.
- Der JSON-Prozessor der jq-Befehlszeile muss installiert sein. Dies wird verwendet, um die Ausgabe von AWS CLI-Befehlen zu parsen. Informationen zum Installieren von jq finden Sie unter [jq herunterladen](#).
- Ausreichende Service Quotas für die zu erstellenden Ressourcen, einschließlich:
- mindestens 2 verfügbare Elastic-IP-Adressen

- mindestens 2 NAT-Gateways
- mindestens 1 VPC
- mindestens 4 Subnetze
- mindestens 1 Application Load Balancer

Geschätzte Kosten: Für die in diesem Tutorial erstellten Ressourcen fallen Gebühren in Ihrem AWS-Konto an: NAT-Gateways: ~0,045 \$ pro Stunde, zuzüglich Datenverarbeitungsgebühren Elastic-IP-Adressen: kostenlos, wenn sie mit laufenden Instances verknüpft sind, andernfalls ~0,005 \$ pro Stunde EC2-Instances: variiert je nach Instance-Typ (in diesem Tutorial: t3.micro) Application Load Balancer: ~0,0225 \$ pro Stunde zuzüglich Datenverarbeitungsgebühren

Erstellen der VPC und der Subnetze

Als Erstes erstellen Sie eine VPC mit dem CIDR-Block 10.0.0.0/16, der bis zu 65 536 private IP-Adressen bereitstellt.

```
# Create a VPC with CIDR block 10.0.0.0/16
aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications
  'ResourceType=vpc,Tags=[{Key=Name,Value=ProductionVPC}]'
```

Daraufhin erhalten Sie ein Ergebnis, das dem hier dargestellten entspricht:

```
{
  "Vpc": {
    "CidrBlock": "10.0.0.0/16",
    "DhcpOptionsId": "dopt-abcd1234",
    "State": "pending",
    "VpcId": "vpc-abcd1234",
    "OwnerId": "123456789012",
    "InstanceTenancy": "default",
    "Ipv6CidrBlockAssociationSet": [],
    "CidrBlockAssociationSet": [
      {
        "AssociationId": "vpc-cidr-assoc-abcd1234",
        "CidrBlock": "10.0.0.0/16",
        "CidrBlockState": {
          "State": "associated"
        }
      }
    ]
  }
}
```

```
    ],
    "IsDefault": false,
    "Tags": [
      {
        "Key": "Name",
        "Value": "ProductionVPC"
      }
    ]
  }
}
```

Notieren Sie sich die VPC-ID in der Ausgabe (z. B. `vpc-abcd1234`). Diese ID verwenden Sie in nachfolgenden Befehlen.

Als Nächstes identifizieren Sie zwei Availability Zones in Ihrer Region, um eine ausfallsichere Architektur zu erstellen.

```
# Get available Availability Zones
aws ec2 describe-availability-zones --query 'AvailabilityZones[0:2].ZoneName' --output
text
```

Daraufhin erhalten Sie ein Ergebnis, das dem hier dargestellten entspricht:

```
us-east-1a us-east-1b
```

Jetzt erstellen Sie vier Subnetze: zwei öffentliche Subnetze für den Load Balancer und die NAT-Gateways sowie zwei private Subnetze für Ihre Anwendungsserver. Ersetzen Sie `vpc-abcd1234` durch Ihre tatsächliche VPC-ID und `us-east-1a` und `us-east-1b` durch Ihre tatsächlichen Availability Zones.

```
# Create public subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.0.0/24 \
  --availability-zone us-east-1a \
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet1}]'

# Create private subnet in first AZ
aws ec2 create-subnet \
  --vpc-id vpc-abcd1234 \
  --cidr-block 10.0.1.0/24 \
```

```
--availability-zone us-east-1a \  
--tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet1}]'  
  
# Create public subnet in second AZ  
aws ec2 create-subnet \  
  --vpc-id vpc-abcd1234 \  
  --cidr-block 10.0.2.0/24 \  
  --availability-zone us-east-1b \  
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PublicSubnet2}]'  
  
# Create private subnet in second AZ  
aws ec2 create-subnet \  
  --vpc-id vpc-abcd1234 \  
  --cidr-block 10.0.3.0/24 \  
  --availability-zone us-east-1b \  
  --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=PrivateSubnet2}]'
```

Jeder Befehl gibt eine Ausgabe zurück, die die Subnetz-ID enthält. Notieren Sie sich diese IDs zur Verwendung in nachfolgenden Befehlen:

- Öffentliches Subnetz 1: subnet-abcd1234
- Privates Subnetz 1: subnet-abcd5678
- Öffentliches Subnetz 2: subnet-efgh1234
- Privates Subnetz 2: subnet-efgh5678

Erstellen und konfigurieren der Internetverbindung

In diesem Abschnitt erstellen Sie ein Internet-Gateway, das die Kommunikation zwischen Ihrer VPC und dem Internet ermöglicht, und fügen es Ihrer VPC an.

```
# Create an Internet Gateway  
aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-  
gateway,Tags=[{Key=Name,Value=ProductionIGW}]'
```

Der Befehl gibt eine Ausgabe zurück, die die Internet-Gateway-ID enthält. Notieren Sie sich diese ID (zum Beispiel igw-abcd1234).

Fügen Sie den Internet-Gateway an Ihre VPC an. Ersetzen Sie igw-abcd1234 durch Ihre tatsächliche Internet-Gateway-ID und vpc-abcd1234 durch Ihre tatsächliche VPC-ID.

```
# Attach the Internet Gateway to the VPC
aws ec2 attach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-abcd1234
```

Als Nächstes erstellen Sie Routing-Tabellen für Ihre öffentlichen und privaten Subnetze. Ersetzen Sie `vpc-abcd1234` durch Ihre tatsächliche VPC-ID.

```
# Create a route table for public subnets
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
  'ResourceType=route-table,Tags=[{Key=Name,Value=PublicRouteTable}]'

# Create route table for private subnet in first AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
  'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable1}]'

# Create route table for private subnet in second AZ
aws ec2 create-route-table --vpc-id vpc-abcd1234 --tag-specifications
  'ResourceType=route-table,Tags=[{Key=Name,Value=PrivateRouteTable2}]'
```

Jeder Befehl gibt eine Ausgabe zurück, die die ID der Routing-Tabelle enthält. Notieren Sie sich diese IDs:

- Öffentliche Routing-Tabelle: `rtb-abcd1234`
- Private Routing-Tabelle 1: `rtb-efgh1234`
- Private Routing-Tabelle 2: `rtb-ijkl1234`

Fügen Sie dem Internet-Gateway in der öffentlichen Routing-Tabelle eine Route hinzu, um den Internetzugang zu aktivieren. Ersetzen Sie `rtb-abcd1234` durch Ihre tatsächliche Routing-Tabellen-ID und `igw-abcd1234` durch Ihre tatsächliche Internet-Gateway-ID.

```
# Add a route to the Internet Gateway
aws ec2 create-route --route-table-id rtb-abcd1234 --destination-cidr-block 0.0.0.0/0
  --gateway-id igw-abcd1234
```

Ordnen Sie die Subnetze ihren jeweiligen Routing-Tabellen zu. Ersetzen Sie die Routing-Tabellen-IDs und die Subnetz-IDs durch Ihre tatsächlichen IDs.

```
# Associate public subnets with the public route table
```



```
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-abcd1234
aws ec2 associate-route-table --route-table-id rtb-abcd1234 --subnet-id subnet-efgh1234

# Associate private subnets with their respective route tables
aws ec2 associate-route-table --route-table-id rtb-efgh1234 --subnet-id subnet-abcd5678
aws ec2 associate-route-table --route-table-id rtb-ijkl1234 --subnet-id subnet-efgh5678
```

Erstellen von NAT-Gateways

Über NAT-Gateways können Instances in privaten Subnetzen eine Verbindung mit dem Internet oder anderen AWS-Services herstellen. Sie verhindern aber, dass das Internet eine Verbindung mit diesen Instances initiiert. Zuerst weisen Sie Ihren NAT-Gateways Elastic-IP-Adressen zu.

```
# Allocate Elastic IP for NAT Gateway in first AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=NAT1-EIP}]'

# Allocate Elastic IP for NAT Gateway in second AZ
aws ec2 allocate-address --domain vpc --tag-specifications 'ResourceType=elastic-ip,Tags=[{Key=Name,Value=NAT2-EIP}]'
```

Jeder Befehl gibt eine Ausgabe zurück, die die Zuweisungs-ID enthält. Notieren Sie sich diese IDs:

- EIP 1 Zuweisungs-ID: eipalloc-abcd1234
- EIP 2 Zuweisungs-ID: eipalloc-efgh1234

Erstellen Sie NAT-Gateways in jedem öffentlichen Subnetz. Ersetzen Sie die Subnetz-IDs und die Zuweisungs-IDs durch Ihre tatsächlichen IDs.

```
# Create NAT Gateway in public subnet of first AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-abcd1234 \
  --allocation-id eipalloc-abcd1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway1}]'

# Create NAT Gateway in public subnet of second AZ
aws ec2 create-nat-gateway \
  --subnet-id subnet-efgh1234 \
  --allocation-id eipalloc-efgh1234 \
  --tag-specifications 'ResourceType=natgateway,Tags=[{Key=Name,Value=NAT-Gateway2}]'
```

Jeder Befehl gibt eine Ausgabe zurück, die die NAT-Gateway-ID enthält. Notieren Sie sich diese IDs:

- NAT-Gateway 1: nat-abcd1234
- NAT-Gateway 2: nat-efgh1234

Die Bereitstellung von NAT-Gateways dauert einige Minuten. Warten Sie, bis sie verfügbar sind, bevor Sie fortfahren. Ersetzen Sie die NAT-Gateway-IDs durch Ihre tatsächlichen IDs.

```
# Wait for NAT Gateways to be available
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-abcd1234
aws ec2 wait nat-gateway-available --nat-gateway-ids nat-efgh1234
```

Fügen Sie in den privaten Routing-Tabellen Routen zu den NAT-Gateways hinzu, damit Instances in privaten Subnetzen auf das Internet zugreifen können. Ersetzen Sie die Routing-Tabellen-IDs und die NAT-Gateway-IDs durch Ihre tatsächlichen IDs.

```
# Add route to NAT Gateway 1 in private route table 1
aws ec2 create-route \
  --route-table-id rtb-efgh1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-abcd1234

# Add route to NAT Gateway 2 in private route table 2
aws ec2 create-route \
  --route-table-id rtb-ijkl1234 \
  --destination-cidr-block 0.0.0.0/0 \
  --nat-gateway-id nat-efgh1234
```

Erstellen eines VPC-Endpunkts für Amazon S3

Ein VPC-Endpunkt für Amazon S3 ermöglicht Instances in Ihren privaten Subnetzen den Zugriff auf S3, ohne das NAT-Gateway zu nutzen. Dadurch werden die Datenübertragungskosten gesenkt und die Netzwerkleistung verbessert. Ersetzen Sie vpc-abcd1234 durch Ihre tatsächliche VPC-ID und die Routing-Tabellen-IDs durch Ihre tatsächlichen IDs.

```
# Get the prefix list ID for S3 in your region
S3_PREFIX_LIST_ID=$(aws ec2 describe-prefix-lists --filters "Name=prefix-
list-name,Values=com.amazonaws.${(aws configure get region)}.s3" --query
'PrefixLists[0].PrefixListId' --output text)
```

```
# Create the VPC endpoint for S3
aws ec2 create-vpc-endpoint \
  --vpc-id vpc-abcd1234 \
  --service-name com.amazonaws.${(aws configure get region)}.s3 \
  --route-table-ids rtb-efgh1234 rtb-ijkl1234 \
  --tag-specifications 'ResourceType=vpc-endpoint,Tags=[{Key=Name,Value=S3-Endpoint}]'
```

Der Befehl gibt eine Ausgabe zurück, die die VPC-Endpoint-ID enthält. Notieren Sie sich diese ID (zum Beispiel `vpce-abcd1234`).

Configure Security Groups (Sicherheitsgruppen konfigurieren)

Sicherheitsgruppen dienen als virtuelle Firewalls für Ihre Instances, um den ein- und ausgehenden Datenverkehr zu steuern. Erstellen Sie eine Sicherheitsgruppe für den Load Balancer, die eingehenden HTTP-Datenverkehr von überall zulässt. Ersetzen Sie `vpc-abcd1234` durch Ihre tatsächliche VPC-ID.

```
# Create security group for the load balancer
aws ec2 create-security-group \
  --group-name LoadBalancerSG \
  --description "Security group for the load balancer" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-group,Tags=[{Key=Name,Value=LoadBalancerSG}]'
```

Der Befehl gibt eine Ausgabe zurück, die die Sicherheitsgruppen-ID enthält. Notieren Sie sich diese ID (zum Beispiel `sg-abcd1234`).

Lassen Sie eingehenden HTTP-Datenverkehr zum Load Balancer zu. Ersetzen Sie `sg-abcd1234` durch die tatsächliche Sicherheitsgruppen-ID Ihres Load Balancers.

```
# Allow inbound HTTP traffic from anywhere
aws ec2 authorize-security-group-ingress \
  --group-id sg-abcd1234 \
  --protocol tcp \
  --port 80 \
  --cidr 0.0.0.0/0
```

Erstellen Sie eine Sicherheitsgruppe für die Anwendungsserver, die eingehenden Datenverkehr nur vom Load Balancer zulässt. Ersetzen Sie `vpc-abcd1234` durch Ihre tatsächliche VPC-ID.

```
# Create security group for the application servers
aws ec2 create-security-group \
  --group-name AppServerSG \
  --description "Security group for the application servers" \
  --vpc-id vpc-abcd1234 \
  --tag-specifications 'ResourceType=security-
group,Tags=[{Key=Name,Value=AppServerSG}]'
```

Der Befehl gibt eine Ausgabe zurück, die die Sicherheitsgruppen-ID enthält. Notieren Sie sich diese ID (zum Beispiel sg-efgh1234).

Lassen Sie eingehenden HTTP-Datenverkehr von der Sicherheitsgruppe des Load Balancers zu den Anwendungsservern zu. Ersetzen Sie sg-efgh1234 durch die tatsächliche Sicherheitsgruppen-ID Ihres Anwendungsservers und sg-abcd1234 durch die tatsächliche Sicherheitsgruppen-ID Ihres Load Balancers.

```
# Allow inbound HTTP traffic from the load balancer security group
aws ec2 authorize-security-group-ingress \
  --group-id sg-efgh1234 \
  --protocol tcp \
  --port 80 \
  --source-group sg-abcd1234
```

Erstellen einer Startvorlage für EC2-Instances

Eine Startvorlage enthält die Konfigurationsinformationen zum Starten einer Instance, z. B. die AMI-ID, den Instance-Typ und die Sicherheitsgruppen. Erstellen Sie zunächst ein Benutzerdatenskript, das beim Start der Instance ausgeführt wird.

```
cat > user-data.sh << 'EOF'
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
echo "<h1>Hello from $(hostname -f) in $(curl -s http://169.254.169.254/latest/meta-
data/placement/availability-zone)</h1>" > /var/www/html/index.html
EOF
```

Codieren Sie das Benutzerdatenskript in Base64.

```
USER_DATA=$(base64 -w 0 user-data.sh)
```

Rufen Sie die ID des neuesten Amazon-Linux-2-AMI ab.

```
# Get the latest Amazon Linux 2 AMI ID
aws ec2 describe-images --owners amazon --filters "Name=name,Values=amzn2-ami-hvm-*x86_64-gp2" "Name=state,Values=available" --query 'sort_by(Images, &CreationDate)[-1].ImageId' --output text
```

Erstellen Sie eine Startvorlage mit der AMI-ID, dem Instance-Typ, der Sicherheitsgruppe und den Benutzerdaten. Ersetzen Sie `sg-efgh1234` durch die tatsächliche Sicherheitsgruppen-ID Ihres Anwendungsservers und `$AMI_ID` und `$USER_DATA` durch die Werte, die in den vorherigen Befehlen zurückgegeben wurden.

```
# Create a launch template
aws ec2 create-launch-template \
  --launch-template-name AppServerTemplate \
  --version-description "Initial version" \
  --tag-specifications 'ResourceType=launch-template,Tags=[{Key=Name,Value=AppServerTemplate}]' \
  --launch-template-data '{
    "NetworkInterfaces": [{
      "DeviceIndex": 0,
      "Groups": ["sg-efgh1234"],
      "DeleteOnTermination": true
    }],
    "ImageId": "ami-abcd1234",
    "InstanceType": "t3.micro",
    "UserData":
      "IyEvYmluL2Jhc2gKeXVtIHVwZGF0ZSAtcQp5dW0gaW5zdGFsbCAtcSBodHRwZApzeXN0ZW1jdGwgc3RhcnQgaHR0cGQKc
      +SGVsbG8gZnJvbSAkKGhvc3RuYW1lIC1mKSBpbjAkKGN1cmwgLXMgaHR0cDovLzE2OS4yNTQuMTY5LjI1NC9sYXR1c3QvbW
      "TagSpecifications": [{
        "ResourceType": "instance",
        "Tags": [{
          "Key": "Name",
          "Value": "AppServer"
        }]
      }]
    }'
```

Erstellen eines Load Balancers und einer Zielgruppe

Eine Zielgruppe leitet Anforderungen über das Protokoll und die Port-Nummer, die Sie angeben, an registrierte Ziele wie EC2-Instances weiter. Erstellen Sie eine Zielgruppe für Ihre Anwendungsserver. Ersetzen Sie `vpc-abcd1234` durch Ihre tatsächliche VPC-ID.

```
# Create a target group
aws elbv2 create-target-group \
  --name AppTargetGroup \
  --protocol HTTP \
  --port 80 \
  --vpc-id vpc-abcd1234 \
  --target-type instance \
  --health-check-protocol HTTP \
  --health-check-path / \
  --health-check-port traffic-port
```

Der Befehl gibt eine Ausgabe zurück, die den Zielgruppen-ARN enthält. Notieren Sie sich diesen ARN (zum Beispiel `arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/AppTargetGroup/abcd1234`).

Erstellen Sie einen Application Load Balancer in den öffentlichen Subnetzen. Ersetzen Sie die Subnetz- und Sicherheitsgruppen-IDs durch Ihre tatsächlichen IDs.

```
# Create a load balancer
aws elbv2 create-load-balancer \
  --name AppLoadBalancer \
  --subnets subnet-abcd1234 subnet-efgh1234 \
  --security-groups sg-abcd1234 \
  --tags Key=Name,Value=AppLoadBalancer
```

Der Befehl gibt eine Ausgabe zurück, die den Load-Balancer-ARN enthält. Notieren Sie sich diesen ARN (zum Beispiel `arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234`).

Warten Sie, bis der Load Balancer aktiv ist, und fahren Sie dann fort. Ersetzen Sie `arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234` durch den tatsächlichen ARN Ihres Load Balancers.

```
# Wait for load balancer to be active
```

```
aws elbv2 wait load-balancer-available \  
  --load-balancer-arns arn:aws:elasticloadbalancing:us-  
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234
```

Erstellen Sie einen Listener für den Load Balancer, der HTTP-Datenverkehr an die Zielgruppe weiterleitet. Ersetzen Sie den Load-Balancer-ARN und den Zielgruppen-ARN durch Ihre tatsächlichen ARNs.

```
# Create a listener  
aws elbv2 create-listener \  
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/  
app/AppLoadBalancer/abcd1234 \  
  --protocol HTTP \  
  --port 80 \  
  --default-actions Type=forward,TargetGroupArn=arn:aws:elasticloadbalancing:us-  
east-1:123456789012:targetgroup/AppTargetGroup/abcd1234
```

Erstellen einer Auto-Scaling-Gruppe

Eine Auto-Scaling-Gruppe enthält eine Sammlung von EC2-Instances, die zur automatischen Skalierung und Verwaltung als logische Gruppierung behandelt werden. Erstellen Sie eine Auto-Scaling-Gruppe, die die Startvorlage verwendet und Instances in die privaten Subnetze platziert. Ersetzen Sie die Subnetz-IDs und den Zielgruppen-ARN durch Ihre tatsächlichen Werte.

```
# Create an Auto Scaling group  
aws autoscaling create-auto-scaling-group \  
  --auto-scaling-group-name AppAutoScalingGroup \  
  --launch-template LaunchTemplateName=AppServerTemplate,Version='$Latest' \  
  --min-size 2 \  
  --max-size 4 \  
  --desired-capacity 2 \  
  --vpc-zone-identifier "subnet-abcd5678,subnet-efgh5678" \  
  --target-group-arns arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/  
AppTargetGroup/abcd1234 \  
  --health-check-type ELB \  
  --health-check-grace-period 300 \  
  --tags Key=Name,Value=AppServer,PropagateAtLaunch=true
```

Testen Sie Ihre Konfiguration

Nachdem die Auto-Scaling-Gruppe Instances gestartet hat und diese die Zustandsprüfungen bestanden haben, können Sie Ihren Load Balancer testen. Rufen Sie den DNS-Namen des Load Balancers ab. Ersetzen Sie den Load-Balancer-ARN durch Ihren tatsächlichen ARN.

```
# Get the DNS name of the load balancer
aws elbv2 describe-load-balancers \
  --load-balancer-arns arn:aws:elasticloadbalancing:us-
east-1:123456789012:loadbalancer/app/AppLoadBalancer/abcd1234 \
  --query "LoadBalancers[0].DNSName" \
  --output text
```

Verwenden Sie curl, um die Anwendung mit dem Namen des Load Balancers zu testen.

```
curl http://LoadBalancerName
```

Wenn Sie die Seite mehrmals aktualisieren, sollten Sie Antworten von verschiedenen Instances in verschiedenen Availability Zones sehen.

Bereinigen von Ressourcen

Wenn Sie mit diesem Tutorial fertig sind, sollten Sie alle Ressourcen löschen, damit keine weiteren Gebühren anfallen. Ersetzen Sie alle IDs durch Ihre tatsächlichen Ressourcen-IDs.

```
# Delete the Auto Scaling group
aws autoscaling delete-auto-scaling-group \
  --auto-scaling-group-name AppAutoScalingGroup \
  --force-delete

# Wait for the Auto Scaling group to be deleted
sleep 60

# Delete the load balancer
aws elbv2 delete-load-balancer \
  --load-balancer-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/
app/AppLoadBalancer/abcd1234

# Wait for the load balancer to be deleted
sleep 30

# Delete the target group
```



```
aws elbv2 delete-target-group \  
  --target-group-arn arn:aws:elasticloadbalancing:us-east-1:123456789012:targetgroup/  
AppTargetGroup/abcd1234  
  
# Delete the launch template  
aws ec2 delete-launch-template \  
  --launch-template-name AppServerTemplate  
  
# Delete the NAT Gateways  
aws ec2 delete-nat-gateway --nat-gateway-id nat-abcd1234  
aws ec2 delete-nat-gateway --nat-gateway-id nat-efgh1234  
  
# Wait for the NAT Gateways to be deleted  
sleep 90  
  
# Release the Elastic IPs  
aws ec2 release-address --allocation-id eipalloc-abcd1234  
aws ec2 release-address --allocation-id eipalloc-efgh1234  
  
# Delete the VPC endpoint  
aws ec2 delete-vpc-endpoints --vpc-endpoint-ids vpce-abcd1234  
  
# Wait for security group dependencies to clear  
sleep 30  
  
# Delete the security groups  
aws ec2 delete-security-group --group-id sg-efgh1234  
aws ec2 delete-security-group --group-id sg-abcd1234  
  
# Detach the Internet Gateway  
aws ec2 detach-internet-gateway --internet-gateway-id igw-abcd1234 --vpc-id vpc-  
abcd1234  
  
# Delete the Internet Gateway  
aws ec2 delete-internet-gateway --internet-gateway-id igw-abcd1234  
  
# Delete the route tables  
aws ec2 delete-route-table --route-table-id rtb-efgh1234  
aws ec2 delete-route-table --route-table-id rtb-ijkl1234  
aws ec2 delete-route-table --route-table-id rtb-abcd1234  
  
# Delete the subnets  
aws ec2 delete-subnet --subnet-id subnet-abcd1234  
aws ec2 delete-subnet --subnet-id subnet-efgh1234
```

```
aws ec2 delete-subnet --subnet-id subnet-abcd5678
aws ec2 delete-subnet --subnet-id subnet-efgh5678

# Delete the VPC
aws ec2 delete-vpc --vpc-id vpc-abcd1234
```

Nächste Schritte

Nachdem Sie eine VPC mit privaten Subnetzen und NAT-Gateways erstellt haben, können Sie sich die folgenden Themen ansehen:

- [Security best practices for your VPC](#)
- [Protokollieren von IP-Datenverkehr mit VPC Flow Logs](#)
- [Skalierungsrichtlinien für Auto-Scaling-Gruppen](#)
- [Zustandsprüfungen für Load-Balancer-Zielgruppen](#)

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 dieses Limit erhöhen, sodass Sie Hunderte VPCs pro Region haben 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 von, die CIDRs Sie einer einzelnen VPC zuweisen können.
VPC-Block-Ausschlüsse vom öffentlichen Zugriff pro Konto und Region	50	Ja. Informationen zur Erhöhung finden Sie unter	Die Anzahl der VPC BPA-Ausschlüsse , die Sie in einem Konto erstellen können.

Name	Standard	Anpassbar	Kommentare
		Anfordern einer Service-Quota-Erhöhung im AWS -Support-Benutzerhandbuch.	

DNS

Jede EC2 Instanz kann 1024 Pakete pro Sekunde pro Netzwerkschnittstelle an den Route 53-Resolver senden (insbesondere an 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 AWS-Konto VPCs VPCs Kontingent gilt sowohl für Einzelpersonen als auch für gemeinsam genutzte Benutzer.
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 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 VPCs pro Region. 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	Ja	
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 Support-Fall öffnen. Siehe [Anfordern einer Service-Quota-Erhöhung](#) im AWS -Support-Benutzerhandbuch.

Name	Standard	Anpassbar	Kommentare
Präfixlisten pro Region	100	Ja	

Name	Standard	Anpassbar	Kommentare
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 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	10.000	Ja	Dieses Kontingent gilt pro Ressourcentyp, der auf eine Präfixliste verweisen kann. Beispielsweise können Sie 10 000 Verweise auf eine Präfixliste für alle Sicherheitsgruppen sowie 10 000 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 Ihr 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, 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 Einzelpersonen AWS-Konto VPCs und gemeinsam genutzte VPCs Personen. Dieses Limit wird pro Availability Zone (AZ) durchgesetzt. Wenn es sich beispielsweise um drei Netzwerkschnittstellen handelt AZs, 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-Tabellen können zwar mit mehreren Subnetzen geteilt werden, ein Subnetz kann aber jeweils nur mit einer Routing-Tabelle verknüpft sein.
Routen pro Routing-Tabelle (nicht verteilte Routen)	500	Ja	Sie können dieses Kontingent auf maximal 1.000 erhöhen; dies beeinträchtigt jedoch möglicherweise die Netzwerkleistung. Dieses Kontingent wird getrennt für IPv4 Routen und IPv6 Routen 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.

Route Server

Name	Standard	Anpassbar	Kommentare
Route Server pro VPC	5	Ja. Informationen zur Erhöhung finden Sie unter Anfordern einer Service-Quota-Erhöhung im AWS - Support-Benutzerhandbuch.	
Routenserver-Endpunkte pro Route Server	10	Ja. Informationen zur Erhöhung finden Sie unter Anfordern einer Service-Quota-Erhöhung im AWS - Support-	

Name	Standard	Anpassbar	Kommentare
		Benutzerhandbuch.	
Peering-Sitzungen pro Netzwerkschnittstelle	20	Ja. Informationen zur Erhöhung finden Sie unter Anfordern einer Service-Quota-Erhöhung im AWS - Support-Benutzerhandbuch.	
Routenserver-Endpunkte pro Route Server und Subnetz	2	Nein	Aus Redundanzgründen können Sie nur zwei Endpunkte im selben Subnetz für denselben Route Server haben.
Routen pro Routenserver-Peer	100	Nein	Das ist die Anzahl der Routen, die dynamisch über einen Routenserver-Peer angekündigt werden können
Routen pro Route Server	100	Nein	Das ist die Anzahl der Routen, die in der Forwarding Information Base (FIB) eines Route Servers installiert werden können.

Sicherheitsgruppen

Name	Standard	Anpassbar	Kommentare
VPC-Sicherheitsgruppen pro Region	2.500	Ja	Dieses Kontingent gilt für Einzelpersonen AWS-Konto VPCs und gemeinsam genutzte VPCs Personen. 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.
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 Sicherheitsgruppe 60 Regeln für eingehenden Datenverkehr und 60 Regeln für ausgehenden Datenverkehr haben. Darüber hinaus wird dieses Kontingent für IPv4 Regeln und IPv6 Regeln separat durchgesetzt. Für ein Konto mit dem Standardkontingent von 60 Regeln kann eine Sicherheitsgruppe 60 Regeln für eingehenden IPv4 Datenverkehr und 60 Regeln für eingehenden Datenverkehr haben. IPv6 Weitere Informationen 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.

Name	Standard	Anpassbar	Kommentare
			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 Sicherheitsgruppe darf 1.000 nicht überschreiten. Informationen zur Reduzierung des Kontingents für Sicherheitsgruppen pro Netzwerkschnittstelle unter den Standardwert von 5 finden Sie unter Service-Quota-Erhöhung anfordern im AWS -Support-Benutzerhandbuch. Sie nutzen das gleiche Verfahren zum Beantragen einer Verringerung wie bei einer Erhöhung.

VPC-Subnetz-Freigabe

Für freigegebene VPC-Subnetze gelten alle VPC-Standardkontingente.

Name	Standard	Anpassbar	Kommentare
Teilnehmerkonten pro VPC	100	Ja	Dies ist die maximale Anzahl unterschiedlicher Teilnehmerkonten, mit denen Subnetze in einer VPC freigegeben werden können. Dies ist ein Pro-VPC-Kontingent, und es gilt für alle in einer VPC freigegebenen Subnetze. VPC-Besitzer können die Netzwerkschnittstellen und Sicherheitsgruppen

Name	Standard	Anpassbar	Kommentare
			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) besteht aus IP-Adressen, Netzwerkschnittstellen und CIDRs verwalteten Präfixlisten. 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 Servicekontingente. Selbst wenn für eine VPC NAU-Kapazität verfügbar ist, können Sie keine Ressourcen in die VPC bringen, wenn die Ressourcen ihre Servicekontingente 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 interregionalen Peering-Verbindungen. VPCs VPCs die über verschiedene Regionen miteinander verbunden sind, tragen nicht zu dieser Zahl bei.

Drosselung der EC2 Amazon-API

Informationen zur EC2 Drosselung durch Amazon finden Sie unter [Drosselung von Anfragen](#) im Amazon Developer Guide. EC2

Zusätzliche Kontingentressourcen

Weitere Informationen finden Sie hier:

- [AWS Client VPN Kontingente](#) im Administratorhandbuch AWS Client VPN
- [Direct Connect -Kontingente](#) im AWS 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 Transit Gateways Guide.

Dokumentverlauf

In der folgenden Tabelle sind die wichtigen Änderungen in jeder Version des Benutzerhandbuchs zu Amazon VPC beschrieben.

Änderung	Beschreibung	Datum
VPC-Verschlüsselungskontrollen	Sie können jetzt mithilfe von VPC-Verschlüsselungskontrollen die Verschlüsselung während der Übertragung für den Netzwerkverkehr innerhalb Ihrer VPC erzwingen. Diese Funktion bietet zentrale Funktionen zur Durchsetzung und Überwachung von Verschlüsselungssichtlinien.	21. November 2025
Regionale NAT-Gateways für die automatische Multi-AZ-Erweiterung	Sie können jetzt regionale NAT-Gateways verwenden, die sich je nach Workload-Footprint automatisch über Availability Zones erstrecken. Regionale NAT-Gateways bieten eine vereinfachte Einrichtung, verbesserte Sicherheit und automatische Hochverfügbarkeit ohne manuelles Eingreifen.	19. November 2025
Weiterleiten von eingehenden VPC-Datenverkehr an öffentliche IP-Adressen	Sie können jetzt erweiterte Routing-Regeln konfigurieren, um eingehenden Datenverkehr aus dem Internet an bestimmte öffentliche IP-Adressen innerhalb Ihrer VPC	13. August 2025

weiterzuleiten, sodass Sie den Datenverkehrsfluss und die Routing-Entscheidungen für eingehende Szenarien detaillierter steuern können.

[Dynamisches Routing in Ihrer VPC mit Amazon VPC Route Server](#)

Amazon VPC Route Server vereinfacht das Routing des Datenverkehrs zwischen Workloads, die innerhalb einer VPC bereitgestellt werden, und ihren Internet-Gateways. Mit dieser Funktion aktualisiert der VPC-Routenserver die VPC- und Gateway-Route-Tabellen dynamisch mit Ihren bevorzugten IPv4 IPv6-Route-Tabellen, um die Routing-Fehlertoleranz für diese Workloads zu erreichen. Auf diese Weise können Sie den Datenverkehr innerhalb einer VPC automatisch umleiten, was die Verwaltbarkeit des VPC-Routings und die Interoperabilität mit Workloads von Drittanbietern verbessert.

31. März 2025

[AWS verwaltetes Richtlinien-Update](#)

Für Amazon VPC wurden die verwalteten Richtlinien `AmazonVPCFullAccess` und `AmazonVPCReadOnlyAccess` aktualisiert.

9. Dezember 2024

[Unterstützung deklarativer Richtlinien für VPC BPA](#)

Wenn Sie AWS Organizations verwenden, um Konten in Ihrer Organisation zu verwalten, können Sie eine deklarative Richtlinie verwenden, um VPC BPA für die Konten in der Organisation durchzusetzen.

01. Dezember 2024

[VPC Block Public Access \(BPA\)](#)

Mit VPC Block Public Access (BPA) können Sie verhindern, dass Ressourcen in VPCs und Subnetzen, die Sie in einer Region besitzen, über Internet Gateways und Internet Gateways nur für ausgehenden Datenverkehr über das Internet erreichen oder von dort aus erreicht werden.

19. November 2024

[Freigegebene Sicherheitstgruppen](#)

Mit dieser Funktion können Sie eine Sicherheitsgruppe mit Konten anderer AWS Organizations teilen.

30. Oktober 2024

[Sicherheitsgruppen-VPC-Zuordnungen](#)

Mit dieser Funktion können Sie eine Sicherheitsgruppe mehreren VPCs in derselben Region zuordnen.

30. Oktober 2024

[NAT-Gateway-MTU-Unterstützung](#)

NAT-Gateways unterstützen Datenverkehr mit einer maximalen Übertragungseinheit (Maximum Transmission Unit, MTU) von 8 500.

10. September 2024

Private IPv6 Adressierung	Informationen zur privaten IPv6 Adressierung wurden hinzugefügt. Private IPv6 Adressen sind nur in Amazon VPC IP Address Manager verfügbar.	8. August 2024
IPv6 bevorzugte Leasingzeit	Sie können jetzt wählen, wie oft eine laufende Instance, IPv6 der eine zugewiesene Instanz zugewiesen ist, die DHCPv6 Leasingverlängerung durchläuft.	20. Februar 2024
Überprüfung und Verbesserung der Struktur des Leitfadens	Die Struktur des Leitfadens wurde überprüft und es wurden Verbesserungen vorgenommen, um das Kundenerlebnis bei der Suche nach Informationen für bestimmte Szenarien zu verbessern.	20. Februar 2024
AWS verwaltetes Policy-Update	Für Amazon VPC wurden die verwalteten Richtlinien AmazonVPCFullAccess und AmazonVPCReadOnlyAccess aktualisiert.	8. Februar 2024
AWS verwaltetes Richtlini enupdate	Für Amazon VPC wurden die verwalteten Richtlinien AmazonVPCCrossAccountNetworkInterfaceOperations aktualisiert.	25. September 2023

[EC2-Classic ist veraltet](#)

Bei EC2 -Classic wurden EC2 Instanzen 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

[Fügen Sie sekundäre IPv4 Adressen zu NAT-Gateways hinzu](#)

Sie können öffentliche und private NAT-Gateways sekundäre private IPv4 Adressen hinzufügen. Sekundäre IPv4 Adressen erhöhen die Anzahl der verfügbaren Ports und erhöhen daher 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 Bereitstellungstream von Amazon Data Firehose als Ziel für Flow-Protokolldaten angeben.

8. September 2022

<u>NAT-Gateway-Bandbreite</u>	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
<u>Mehrere IPv6 CIDR-Blöcke</u>	Sie können einer VPC bis zu fünf IPv6 CIDR-Blöcke zuordnen.	12. Mai 2022
<u>Reorganisation</u>	Allgemeine Reorganisation des Benutzerhandbuchs von Amazon Virtual Private Cloud.	2. Januar 2022
<u>NAT-Gateway zu IPv6 IPv4</u>	Das NAT-Gateway unterstützt die Netzwerkadressübersetzung von IPv6 nach IPv4, im Volksmund auch bekannt als NAT64.	24. November 2021
<u>IPv6-nur Subnetze in VPCs</u>	Sie können Subnetze erstellen , in denen Sie IPv6 nur - Instances starten können. IPv6 EC2	23. November 2021
<u>Lieferoptionen von VPC-Flow-Protokollen an Amazon S3</u>	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 Subnetze VPCs, 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 das Ziel einer Route so festlegen, dass es einem gesamten IPv4 oder einem IPv6 CIDR-Block eines Subnetzes in Ihrer VPC entspricht.

30. August 2021

[Ressourcen IDs - und Tagging-Unterstützung für 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 ausschließlich ausgehende private Kommunikation zwischen VPCs oder zwischen einer VPC und Ihrem lokalen 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-Log-Felder sind verfügbar, und Sie können ein benutzerdefiniertes Format für Flow-Logs angeben, die in Logs veröffentlicht werden. CloudWatch	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 Netzwerkrenzgruppen	Sie können Netzwerkrenzgruppen für Sie VPCs von der Amazon VPC-Konsole aus konfigurieren.	22. 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-Protokolldatenständen ausgegeben werden sollen.	11. September 2019
VPC Sharing	Sie können Subnetze, die sich in derselben VPC befinden, mit mehreren Konten in derselben AWS Organisation gemeinsam nutzen.	27. November 2018
Ein Standard-Subnetz erstellen	Sie können ein Standard-Subnetz 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
CloudWatch Amazon-Metriken für NAT-Gateways	Sie können CloudWatch Metriken für Ihr NAT-Gateway einsehen.	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 Unterstützung	Sie können Ihrer VPC einen IPv6 CIDR-Block zuordnen und Ressourcen in Ihrer 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 ClassicLink Ihre EC2 -Classic-Instance mit einer VPC in Ihrem Konto verknüpfen. Sie können VPC-Sicherheitsgruppen mit der EC2 -Classic-Instance verknüpfen und so die Kommunikation zwischen Ihrer EC2 -Classic-Instance und Instances in Ihrer VPC über private IP-Adressen 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, mehreren VPCs pro AWS Konto und mehreren VPN-Verbindungen pro VPC hinzugefügt.

3. August 2011

[Dedicated Instances](#)

Dedicated Instances sind EC2 Amazon-Instances, die innerhalb Ihrer VPC gestartet werden und Hardware ausführen, die für einen einzelnen Kunden reserviert ist.

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.