Amazon Virtual Private Cloud

Handbuch "Erste Schritte"

API Version 2012-12-01

Amazon Web Services

Amazon Virtual Private Cloud: Handbuch "Erste Schritte"

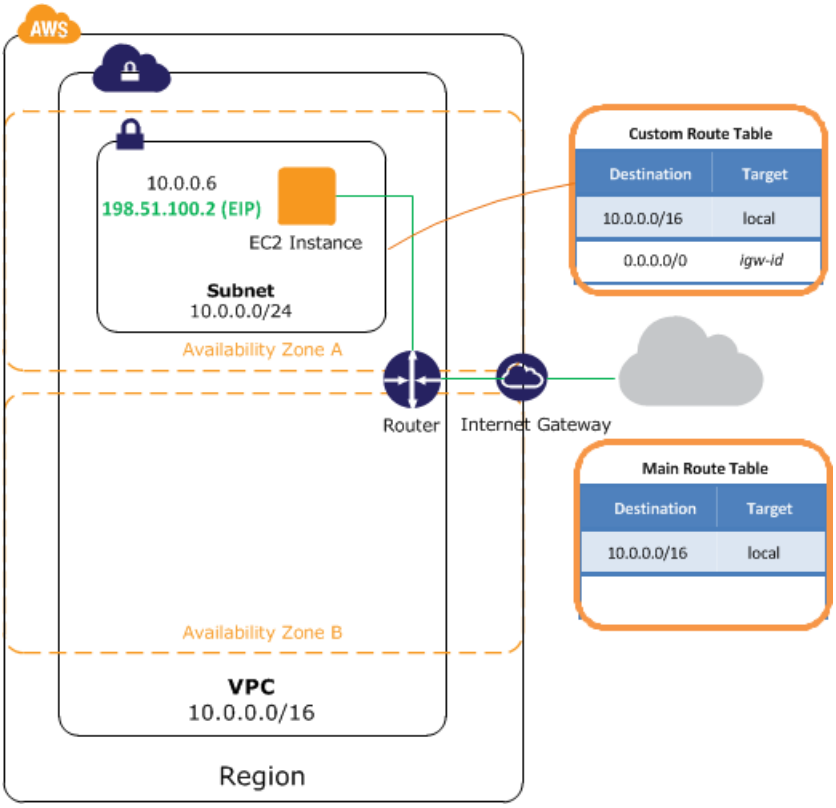
Amazon Web Services

Übersicht über die Übung

Eine Virtual Private Cloud (VPC) ist ein virtuelles Netzwerk, das weitgehend einem herkömmlichen Netzwerk entspricht, wie Sie es in Ihrem Rechenzentrum betreiben, jedoch die Vorzüge der skalierbaren Infrastruktur von Amazon Web Services (AWS) nutzen kann. Nachdem Sie die Aufgaben in dieser Übung ausgeführt haben, verfügen Sie über eine in einer nondefault VPC ausgeführte Amazon EC2-Instance, auf die Sie über SSH (bei Linux-Instances) oder Remotedesktop (bei Windows-Instances) über das Internet zugreifen können.

Eine Übersicht über Amazon VPC finden Sie unter What is Amazon VPC? im *Amazon Virtual Private Cloud User Guide*.

Das folgende Diagramm zeigt die Architektur, die Sie im Verlauf der Übung in diesem Handbuch erstellen. Die Sicherheitsgruppe, die Sie eingerichtet und der Sie die Instance zugeordnet haben, lässt Datenverkehr nur an bestimmten Ports zu und blockiert Kommunikation mit der Instance gemäß den von Ihnen festgelegten Regeln. Das Verwenden einer Elastic-IP-Adresse (EIP) ermöglicht, dass eine Instance in einer VPC, die ansonsten privat ist, aus dem Internet über ein Internet-Gateway erreicht werden kann (und beispielsweise als Webserver fungieren kann).



Das folgende Tabelle enthält eine Übersicht der Aufgaben, die Sie im Verlauf der Übung in diesem Handbuch ausführen.

Schritt 1: Registrieren für Amazon VPC (p. 4)	Registrieren Sie sich für Amazon VPC, falls noch nicht erfolgt.
Schritt 2: Erstellen der VPC und des Subnetzes (p. 5)	Lassen Sie den VPC-Assistenten die folgenden Aufgaben für Sie erledigen: 1. Erstellen einer VPC, d. h., eines isolierten Teils der AWS-Cloud. 2. Erstellen eines Internet-Gateways, das Ihre VPC direkt mit dem Internet verbindet und Zugriff auf andere AWS-Ressourcen wie Amazon Simple Storage Service (Amazon S3) bietet und Herstellen einer Verbindung damit. 3. Erstellen eines Amazon VPC-Subnetzes, d. h., eines Segments des VPC-IP-Adressbereichs, in dem Sie Amazon EC2-Instances starten können. Mithilfe von Subnetzen können Sie Instances basierend auf Ihren Sicherheitsanforderungen und betrieblichen Erfordernissen gruppieren. 4. Einichten des Routings in der VPC, um Datenverkehr zwischen Subnetz und Internet zu ermöglichen. Ihre VPC hat einen eingebauten Router, wie Sie im Diagramm erkennen können.

Schritt 3: Erstellen einer Sicherheitsgruppe in Ihrer VPC (p. 8)	Richten Sie in der Amazon VPC-Konsole eine Sicherheitsgruppe zum Steuern des eingehenden und ausgehenden Datenverkehrs für die Instance ein.
Schritt 4: So starten Sie eine Instance in Ihrer VPC (p. 9)	Starten Sie über die Amazon EC2-Konsole eine Instance im Subnetz. Die Instance erhält eine private IP-Adresse aus dem Adressbereich des Subnetzes.
Schritt 5: Weisen Sie der Instance eine Elastic IP-Adresse zu (p. 14)	Wählen Sie über die Amazon VPC-Konsole eine Elastic IP-Adresse aus und weisen Sie sie der Instance zu. Eine Elastic IP-Adresse stellt der Instance zusätzlich zu ihrer privaten Adresse eine öffentliche IP-Adresse zur Verfügung, sodass auf die Instance über das Internet zugegriffen werden kann.
Optionaler Schritt: Löschen der VPC (p. 16)	Beenden Sie Ihre Instance über die Amazon EC2-Konsole und löschen Sie sie Ihre VPC über die Amazon VPC-Konsole.

Erste Schritte mit Amazon VPC

Dieses Handbuch bietet eine praxisorientierte Einführung in die Verwendung von Amazon VPC über die AWS Management Console. Die Übung im vorliegenden Handbuch leitet Sie durch ein einfaches Szenario. Sie richten eine VPC mit einem einzigen öffentlichen Subnetz ein, in dem eine EC2-Instance mit einer Elastic IP-Adresse ausgeführt wird.

Topics

Eine Übersicht über die Übung finden Sie unter Übersicht über die Übung (p. 1). Eine einführende Übersicht über Amazon VPC finden Sie unter What is Amazon VPC? im *Amazon Virtual Private Cloud User Guide*.

Schritt 1: Registrieren für Amazon VPC

Wenn Sie ein AWS-Konto anlegen, registriert AWS das Konto automatisch bei allen AWS-Services einschließlich Amazon EC2 und Amazon VPC. Berechnet werden Ihnen nur die Services, die Sie nutzen. Bei diesem Beispiel sind die Gebühren minimal.

Wenn Sie bereits ein AWS-Konto haben, wechseln Sie zum nächsten Schritt. Wenn Sie kein AWS-Konto haben, befolgen Sie diese Schritte zum Erstellen eines Kontos.

So erstellen Sie ein Amazon-Konto

1. Wechseln Sie zu http://aws.amazon.com, und klicken Sie auf Jetzt anmelden.
2. Folgen Sie den Anweisungen auf dem Bildschirm.
   Der Anmeldeprozess umfasst einen Telefonanruf und die Eingabe einer PIN über die Telefontastatur.

Sie werden per E-Mail von uns benachrichtigt, sobald Ihr Konto aktiv ist und verwendet werden kann.

Schritt 2: Einrichten der VPC und des Internet-Gateways

In diesem Schritt erstellen Sie mithilfe des VPC-Assistenten eine VPC. Der Assistent führt die folgenden Schritte für Sie aus:

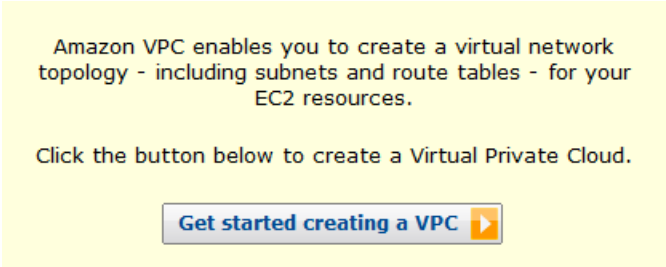
Tip

Nach Wunsch können Sie diese Schritte manuell über die AWS Management Console ausführen.

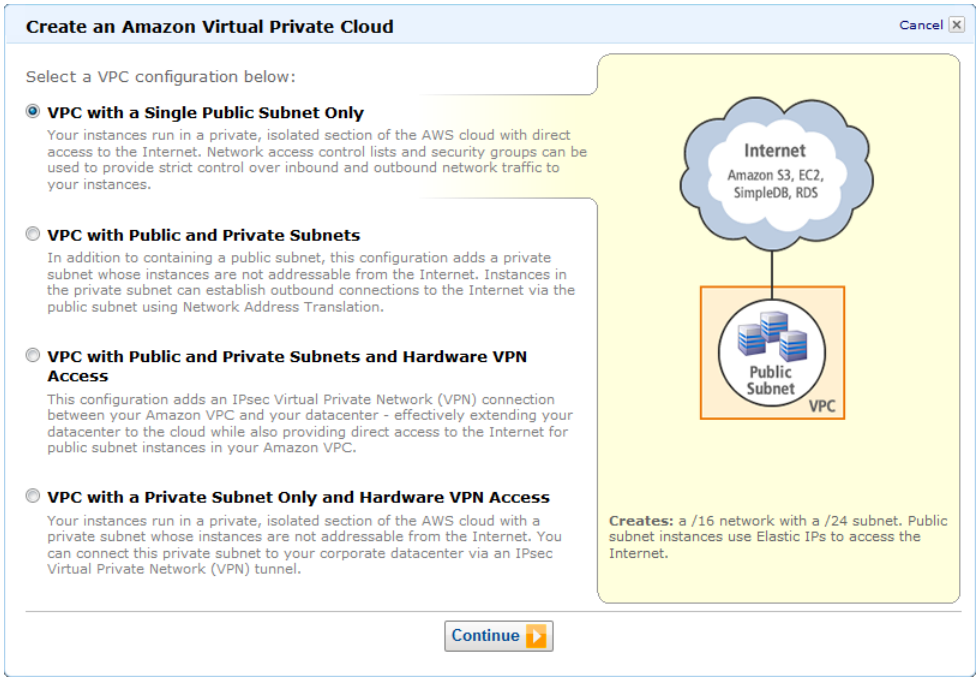
- Erstellen einer VPC der Größe "/16" (ein Netzwerk mit 65 536 privaten IP-Adressen).
- Verbinden eines Internet-Gateways mit der VPC.
- Hinzufügen eines Subnetzes der Größe "/24" (Bereich von 256 privaten IP-Adressen).
- Einrichten des Routings für Ihre VPC, und zwar so, dass Datenverkehr zwischen dem Subnetz und dem Internet-Gateway fließen kann.

So erstellen Sie eine VPC mithilfe des VPC-Assistenten in der AWS Management Console

1. Melden Sie sich bei der AWS Management Console an, und öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/vpc/.
2. Klicken Sie im VPC-Dashboard auf Get started creating a VPC.



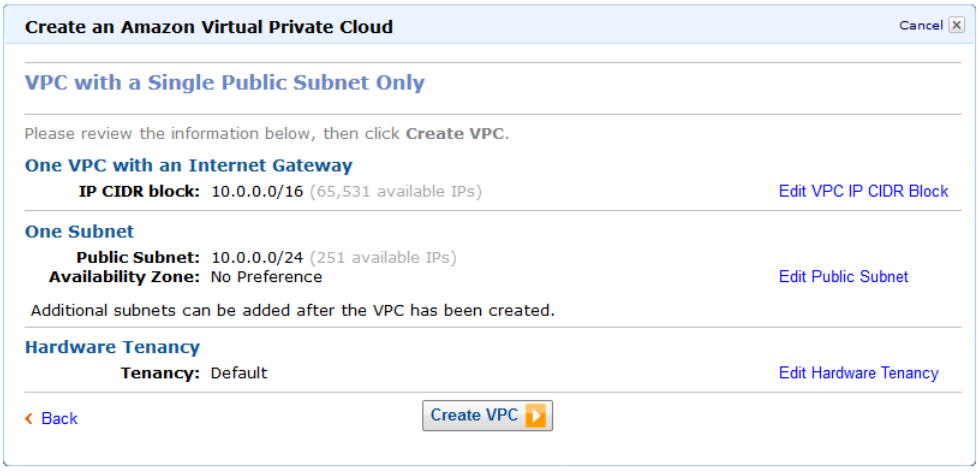
3. Wählen Sie die erste Option, VPC with a Single Public Subnet Only, und klicken Sie auf Continue.



4. Auf der Bestätigungsseite werden die CIDR-Bereiche, die für Ihre VPC und das Subnetz verwendet werden (10.0.0.0/16 bzw. 10.0.0.0/24) und die Mandanteneinstellung für Hardware angezeigt. Nehmen Sie die gewünschten Änderungen an diesen Einstellungen vor und klicken Sie auf Create VPC, um VPC, Internet-Gateway, Subnetz und Routing-Tabelle zu erstellen.

Note

Informationen zur CIDR-Notation finden Sie im Wikipedia-Artikel zu CIDR (Classless Internet-Domain Routing). Weitere Informationen zum Hardware-Mandantenmodell finden Sie im unter Using EC2 Dedicated Instances im *Amazon Virtual Private Cloud User Guide*.



5. Ein Statusfenster zeigt den Fortschritt an. Nach Abschluss des Prozesses wird in einem Statusfenster bestätigt, dass Ihre VPC erfolgreich erstellt wurde. Klicken Sie auf Close, um das Statusfenster zu schließen und zum VPC-Dashboard zurückzukehren.

Überprüfen der Komponenten Ihrer VPC

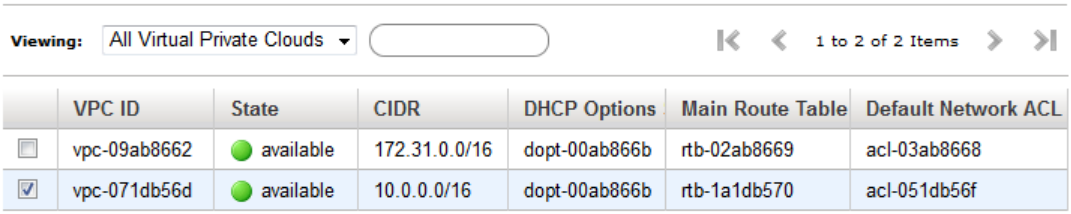
Beim Durcharbeiten der Übung in diesem Handbuch können Sie die Standardeinstellungen für die Komponenten verwenden, die der VPC-Assistent für Sie erstellt hat. In diesem Abschnitt wird beschrieben, wie Sie diese Komponenten und ihre Einstellungen in der VPC-Konsole anzeigen können.

Klicken Sie im Navigationsbereich auf Your VPCs und wählen Sie dann die zuvor erstellte VPC aus.

Tip

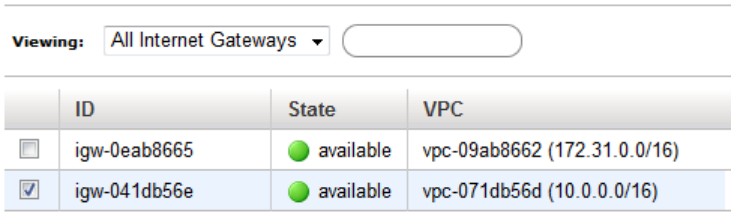
Sie müssen die Seite möglicherweise aktualisieren, damit die VPC angezeigt wird.

In der Konsole werden die zuvor erstellte VPC angezeigt. Jede VPC weist eine Gruppe von DHCP-Optionen, eine Haupt-Routing-Tabelle und standardmäßige Netzwerk-ACL auf. Weitere Informationen finden Sie unter DHCP Options Sets, Route Tables und Network ACLs im *Amazon Virtual Private Cloud User Guide*.



	VPC ID	State	CIDR	DHCP Options	Main Route Table	Default Network ACL
☐	vpc-09ab8662	available	172.31.0.0/16	dopt-00ab866b	rtb-02ab8669	acl-03ab8668
☑	vpc-071db56d	available	10.0.0.0/16	dopt-00ab866b	rtb-1a1db570	acl-051db56f

Um Informationen zu Ihren Internet-Gateways anzuzeigen, klicken Sie im Navigationsbereich auf Internet Gateways.

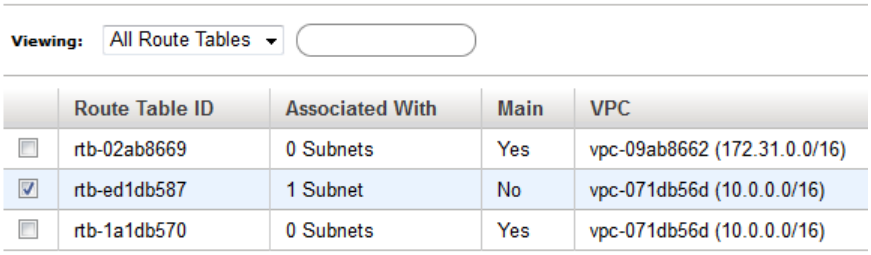


	ID	State	VPC
☐	igw-0eab8665	available	vpc-09ab8662 (172.31.0.0/16)
☑	igw-041db56e	available	vpc-071db56d (10.0.0.0/16)

Die zuvor erstellte VPC hat zwei Routing-Tabellen. Die VPC verfügt standardmäßig über die Haupt-Routing-Tabelle und der VPC-Assistent hat eine benutzerdefinierte Routing-Tabelle erstellt. Ihr Subnetz wird der benutzerdefinierten Routing-Tabelle zugeordnet, d. h., der Fluss des Datenverkehrs im Subnetz wird anhand der Routen in dieser Tabelle gesteuert. Wenn Sie Ihrer VPC ein neues Subnetz hinzufügen, verwendet es standardmäßig die Haupt-Routing-Tabelle.

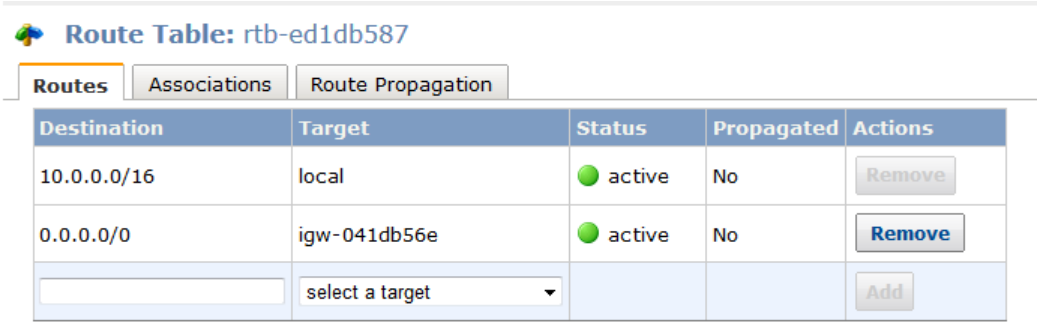
So zeigen Sie Ihre Routing-Tabellen an

1. Klicken Sie im Navigationsbereich auf Route Tables.
2. Wählen Sie die benutzerdefinierte Routing-Tabelle aus (die Spalte Main enthält No), um im Detailbereich die Routing-Informationen anzuzeigen.

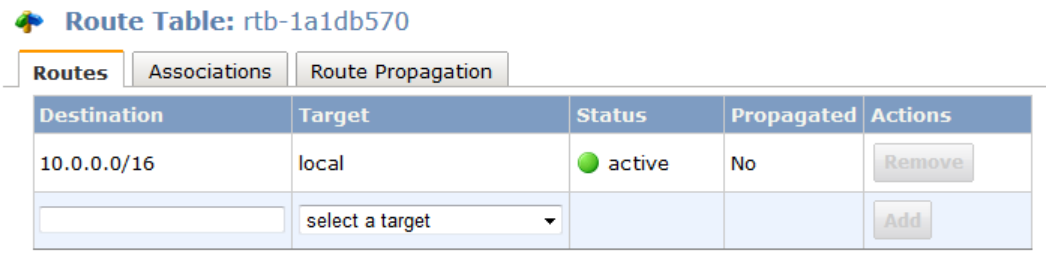


3. Die erste Zeile der Tabelle enthält die lokale Route, die Instances in der VPC die Kommunikation ermöglicht. Diese Route ist standardmäßig in jeder Routing-Tabelle vorhanden und kann nicht entfernt werden.

   Die zweite Zeile enthält die Route, die der VPC-Assistent hinzugefügt hat. Diese ermöglicht, dass der an IP-Adressen außerhalb der VPC (0.0.0.0/0) gerichtete Datenverkehr aus dem Subnetz zum Internet-Gateway fließen kann. Dieses Subnetz wird als *öffentliches Subnetz* bezeichnet, weil sämtlicher Datenverkehr aus dem Subnetz zum Internet-Gateway gesendet wird.



4. Wählen Sie die Haupt-Routing-Tabelle aus. Die Haupt-Routing-Tabelle verfügt nur über eine lokale und keine anderen Routen. Daher sind alle neuen Subnetze, die Sie erstellen, zunächst nicht über das Internet verfügbar (d. h., sie sind *private Subnetze*. Wenn Sie ein neues Subnetz als öffentliches Subnetz zugänglich machen möchten, können Sie entweder das Routing in der Haupt-Routing-Tabelle ändern oder dem Subnetz eine benutzerdefinierte Routing-Tabelle zuordnen.



Schritt 3: Einrichten einer Sicherheitsgruppe in Ihrer VPC

Eine *Sicherheitsgruppe* fungiert als virtuelle Firewall zum Steuern des Datenverkehrs, der in die dazugehörigen Instances geleitet werden darf. Wenn Sie Sicherheitsgruppen verwenden möchten,

erstellen Sie eine Gruppe und fügen die gewünschten Regeln für eingehenden und ausgehenden Datenverkehr hinzu. Weisen Sie anschließend Ihre Instances der Sicherheitsgruppe zu, wenn Sie sie starten. Wenn Sie Regeln zur Sicherheitsgruppe hinzufügen oder daraus entfernen, gelten diese Änderungen automatisch für die Instances, die der Gruppe zugewiesen sind.

Ihre VPC verfügt über eine *Standardsicherheitsgruppe*. Instances, die keiner anderen Sicherheitsgruppe zugewiesen sind, werden der Standardsicherheitsgruppe zugewiesen. Wir könnten zwar die Standardsicherheitsgruppe für diese Übung verwenden, erstellen aber stattdessen die Gruppe `WebServerSG`. Sie geben diese Sicherheitsgruppe an, wenn Sie eine Instance in Ihrer VPC starten.

Topics

Regeln für die Sicherheitsgruppe "WebServerSG"

Die Regeln für eingehenden Datenverkehr steuern, welcher Datenverkehr die der Sicherheitsgruppe zugewiesenen Instances erreicht (d. h. Quelle des Datenverkehrs und Listening-Port für die Instance). Sämtlicher Rückdatenverkehr darf die Instances automatisch erreichen. Wenn ein Client im Internet beispielsweise eine Anforderung an einen Webserver in Ihrer VPC in der Sicherheitsgruppe `WebServerSG` sendet, kann die Instance unabhängig von möglichen für die Gruppe geltenden Regeln für ausgehenden Datenverkehr antworten. Auf diese Weise sind Sicherheitsgruppen zustandsbehaftet.

Die Regeln für ausgehenden Datenverkehr steuern, an welche Ziele die der Sicherheitsgruppe zugewiesenen Instances Datenverkehr senden können (Ziel des Datenverkehrs und Ziel-Port). Sämtlicher Rückdatenverkehr (z. B. eine Antwort vom Host, der den Datenverkehr empfängt) darf automatisch die Instances unabhängig von den für die Sicherheitsgruppe geltenden Regeln für eingehenden Datenverkehr erreichen.

In der folgenden Tabelle sind die Regeln für ein- und ausgehenden Datenverkehr für die Sicherheitsgruppe `WebServerSG` und deren Zweck beschrieben.

Note

Wenn in Ihrem Unternehmen nur Linux oder nur Windows genutzt wird, müssen Sie nicht den Zugriff für sowohl SSH als auch RDP hinzufügen.

Eingehend			
Quell-IP	Protokoll	Port-Bereich	Kommentare
0.0.0.0/0	TCP	80	Eingehenden HTTP-Zugriff von beliebigen Quellen zulassen
0.0.0.0/0	TCP	443	Eingehenden HTTPS-Zugriff von beliebigen Quellen zulassen
Öffentlicher IP-Adressbereich Ihres Heimnetzwerks	TCP	22	Eingehenden SSH-Zugriff aus Ihrem Heimnetzwerk zulassen (nur Linux/UNIX)

Öffentlicher IP-Adressbereich Ihres Heimnetzwerks	TCP	3389	Eingehenden RDP-Zugriff aus Ihrem Heimnetzwerk zulassen (nur Windows)
Ausgehend			
Ziel-IP	Protokoll	Port-Bereich	Kommentare
0.0.0.0/0	TCP	80	Ausgehenden HTTP-Zugriff auf Server im Internet zulassen (z. B. für Software-Updates)
0.0.0.0/0	TCP	443	Ausgehenden HTTPS-Zugriff auf Server im Internet zulassen (z. B. für Software-Updates)

In dieser Übung fügen Sie keine Regel hinzu, die ermöglicht, dass der Sicherheitsgruppe zugewiesene Instances miteinander kommunizieren. Wenn Sie diese Art der Kommunikation wünschen, müssen Sie der Sicherheitsgruppe eine entsprechende Regel hinzufügen. Weitere Informationen finden Sie unter Security Groups im *Amazon Virtual Private Cloud User Guide*.

Erstellen der Sicherheitsgruppe "WebserverSG"

So erstellen Sie die Sicherheitsgruppe "WebServerSG"

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/.
2. Klicken Sie im Navigationsbereich auf Security Groups.
3. Klicken Sie auf die Schaltfläche Create Security Group.
4. Geben Sie als Namen der Sicherheitsgruppe `WebServerSG` und eine Beschreibung ein. Wählen Sie im Menü VPC die ID Ihrer VPC aus und klicken Sie auf Yes, Create.

Standardmäßig enthält jede Sicherheitsgruppe am Anfang nur eine Regel für ausgehenden Datenverkehr, die sämtlichen von der Instance ausgehenden Datenverkehr zulässt. Sie müssen Regeln hinzufügen, um eingehenden Datenverkehr zuzulassen oder den ausgehenden Datenverkehr einzuschränken.

Hinzufügen von Regeln zur Sicherheitsgruppe "WebserverSG"

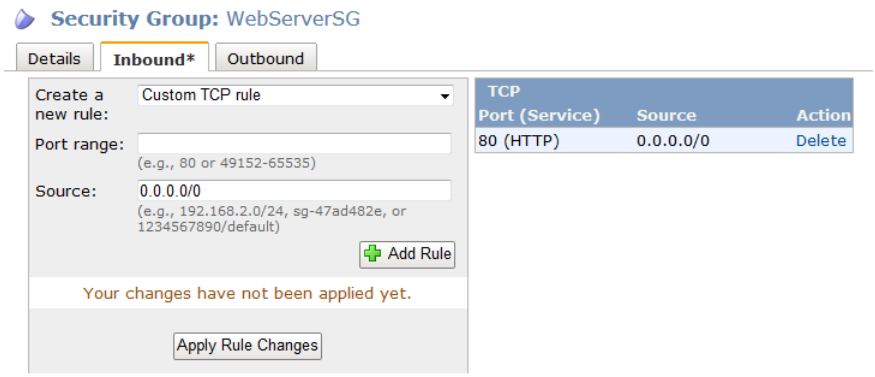
So fügen Sie Regeln zur Sicherheitsgruppe "WebserverSG" hinzu

1. Klicken Sie im Navigationsbereich auf Security Groups, um Ihre Sicherheitsgruppen anzuzeigen.
2. Wählen Sie die zuvor erstellte Sicherheitsgruppe `WebServerSG` aus. Der Detailbereich enthält eine Registerkarte für Informationen zur Sicherheitsgruppe sowie Registerkarten für das Arbeiten mit ihren Regeln für ein- und ausgehenden Datenverkehr.
3. Sie können Regeln hinzufügen, um eingehenden HTTP- und HTTPS-Zugriff von überall aus zuzulassen:

    a. Wählen Sie auf der Registerkarte Inbound den Eintrag `HTTP` in der Dropdown-Liste Create a new rule aus und vergewissern Sie sich, dass Source auf `0.0.0.0/0` festgelegt ist.

    b. Klicken Sie auf Add Rule. Dadurch wird eine Regel zum Zulassen von HTTP-Zugriff von überall aus hinzugefügt. Beachten Sie, dass die Schaltfläche Apply Rule Changes aktiviert ist und der

Text "Your changes have not been applied yet" über der Schaltfläche angezeigt wird. Zum Übernehmen von Regeländerungen klicken Sie auf diese Schaltfläche, nachdem Sie alle Regeln für eingehenden Datenverkehr hinzugefügt haben.



c. Wählen Sie `HTTPS` in der Dropdown-Liste Create a new rule aus und vergewissern Sie sich, dass Source auf `0.0.0.0/0` festgelegt ist.

d. Klicken Sie auf Add Rule. Dadurch wird eine Regel zum Zulassen von HTTPS-Zugriff von überall aus hinzugefügt.

4. Fügen Sie Regeln für eingehenden SSH- und Remotedesktop (RDP)-Zugriff aus dem öffentlichen IP-Adressbereich Ihres Netzwerks zur Gruppe hinzu:

Caution

Wenn Sie `0.0.0.0/0` verwenden, lassen Sie für alle IP-Adressen den Zugriff auf Ihre Instance über SSH oder RDP zu. Für eine kurze Übung ist dies akzeptabel, für Produktionsumgebungen aber unsicher. Für die Produktion wird nur eine bestimmte IP-Adresse bzw. ein bestimmter Adressbereich für den Zugriff auf Ihre Instance autorisiert.

Tip

Sie können auch mithilfe eines Service die öffentlichen IP-Adresse Ihres Computers abrufen. Geben Sie zum Auffinden eines Service, der Ihnen Ihre IP-Adresse nennt, den Suchausdruck "wie ist meine IP-Adresse" ein. Wenn Sie eine Verbindung über einen Internetdienstanbieter oder hinter einer Firewall ohne statische IP-Adresse herstellen, müssen Sie den von Client-Computern verwendeten IP-Adressbereich herausfinden.

a. Wählen Sie auf der Registerkarte Inbound in der Dropdown-Liste `SSH`Create a new rule die Option aus.

b. Geben Sie in das Feld Source den öffentlichen IP-Adressbereich Ihres Netzwerks ein (z. B. 192.0.2.0/24). Wenn Sie den Adressbereich nicht kennen, können Sie für diese Übung `0.0.0.0/0` verwenden (siehe die Angaben unter "Achtung" und "Tipp" für diesen Schritt).

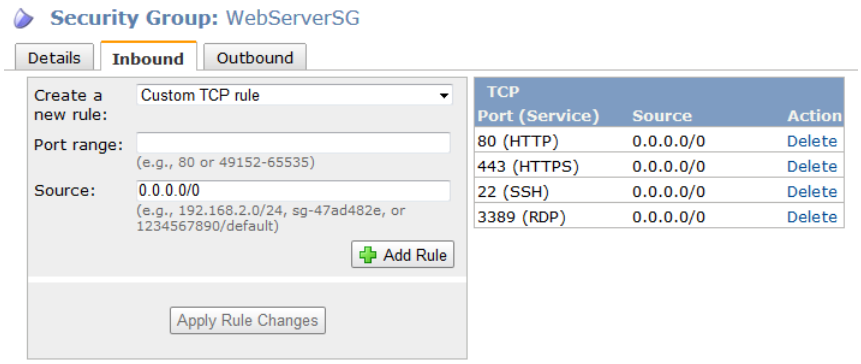
c. Klicken Sie auf Add Rule.

d. Wählen Sie `RDP` in der Dropdown-Liste Create a new rule aus.

e. Geben Sie in das Feld Source den öffentlichen IP-Adressbereich Ihres Heimnetzwerks ein. Wenn Sie den Adressbereich nicht kennen, können Sie für diese Übung `0.0.0.0/0` verwenden (siehe die Angaben unter "Achtung" und "Tipp" für diesen Schritt).

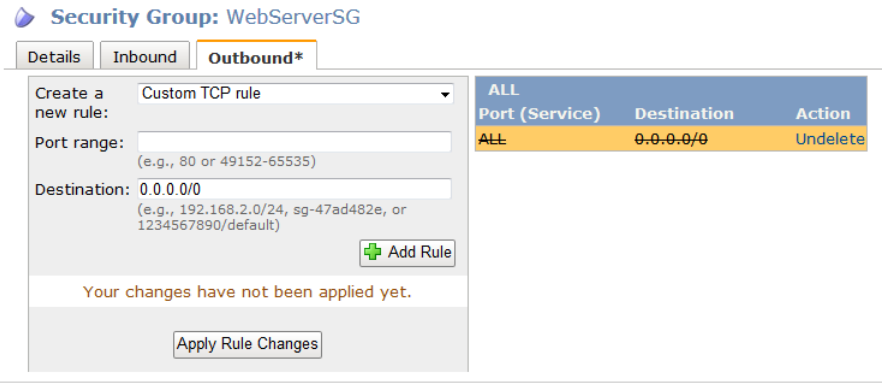
f. Klicken Sie auf Add Rule.

5. Klicken Sie auf Apply Rule Changes, um diese Regeln für eingehenden Datenverkehr zu übernehmen.



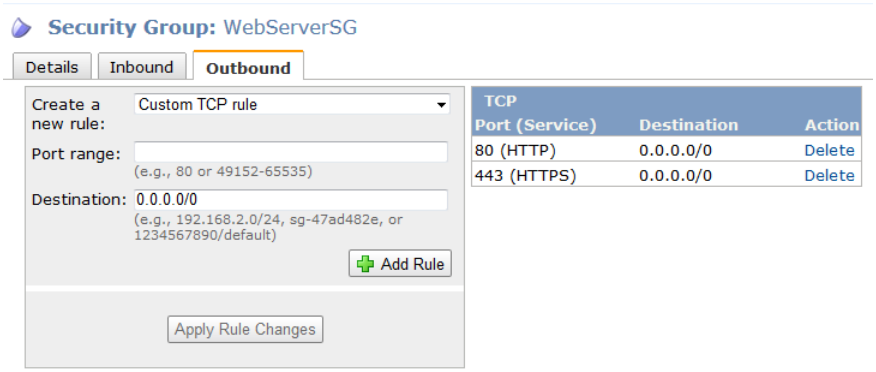
6. Beschränken Sie den ausgehenden Zugriff aus der Gruppe an beliebige Ziele auf HTTP und HTTPS:

   a. Suchen Sie auf der Registerkarte Outbound die Standardregel, die sämtlichen ausgehenden Datenverkehr zulässt, und klicken Sie auf Delete. Die Regel ist zum Löschen markiert. Die Regel wird jedoch erst angewendet, wenn Sie auf Apply Rule Changes klicken, was erfolgt, nachdem Sie alle Regeln für ausgehenden Datenverkehr für HTTP und HTTPS hinzugefügt haben.



   b. Wählen Sie HTTP in der Dropdown-Liste Create a new rule aus und klicken Sie auf Add Rule. Dadurch wird eine Regel zum Zulassen von ausgehendem HTTP-Zugriff von überall aus hinzugefügt.
   c. Wählen Sie HTTPS in der Dropdown-Liste Create a new rule aus und klicken Sie auf Add Rule. Dadurch wird eine Regel zum Zulassen von ausgehendem HTTPS-Zugriff von überall aus hinzugefügt.

7. Klicken Sie auf Apply Rule Changes, um diese Regeln für ausgehenden Datenverkehr zu übernehmen.

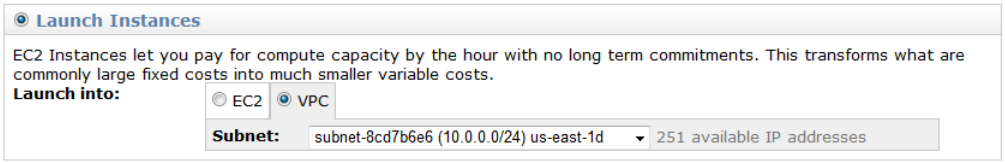


Schritt 4: So starten Sie eine Instance in Ihrer VPC

Wenn Sie eine Amazon EC2-Instance in einer VPC starten, müssen Sie die IP-Adresse eines Subnetzes in der VPC angeben.

So starten Sie eine EC2-Instance in einer VPC

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Wählen Sie auf der Navigationsleiste die Region für die Instance aus. In dieser Übung können Sie die Standardregion verwenden. Weitere Informationen zu Regionen und Availability Zones finden Sie unter Regions and Availability Zones im *Amazon Elastic Compute Cloud User Guide*.
3. Klicken Sie im Dashboard auf die Schaltfläche Launch Instance.
4. Wählen Sie auf der Seite Create a New Instance die Option Classic Wizard aus und klicken Sie auf Continue.
5. Auf der Seite CHOOSE AN AMI wird auf der Registerkarte Quick Start eine Liste mit Basiskonfigurationen angezeigt, die Amazon Machine Images (AMI) genannt werden. Wählen Sie das gewünschte AMI aus und klicken Sie auf die Schaltfläche Select.
6. Übernehmen Sie auf der Seite INSTANCE DETAILS im Menü Instance Type die Standardeinstellung Micro (t1.micro), um eine einzelne Micro-Instance zu starten.
7. Vergewissern Sie unter Launch Instances, dass Ihr Subnetz im Dropdown-Listenfeld Subnet ausgewählt ist, und klicken Sie dann auf Continue.



8. Unter Advanced Instance Options können Sie die für die Instance zu verwendende IP-Adresse angeben. In dieser Übung lassen Sie das Feld IP Address allerdings leer und klicken auf Continue, um die Standardeinstellungen zu übernehmen.
9. Klicken Sie auf Continue, um das Standardspeichergerät zu verwenden.
10. Geben Sie die für Ihre Instance gewünschten Tags an, und klicken Sie auf Continue.
11. Auf der Seite Create Key Pair können Sie ein vorhandenes Schlüsselpaar auswählen oder ein neues erstellen. In dieser Übung erstellen Sie ein Schlüsselpaar.

    a. Klicken Sie auf Create new Key Pair.

b. Geben Sie einen Namen für Ihr Schlüsselpaar ein (z. B. `VPC_Keypair`) und klicken Sie dann auf Create & Download your Key Pair. Sie benötigen den Inhalt des persönlichen Schlüssels, um nach dem Starten Ihrer Instance eine Verbindung zu ihr herzustellen. Amazon Web Services speichert den privaten Teil von Schlüsselpaaren nicht.

c. Speichern Sie, wenn Sie dazu aufgefordert werden, den privaten Schlüssel an einem sicheren Ort in Ihrem System, und klicken Sie auf Continue.

12. Wählen Sie auf der Seite CONFIGURE FIREWALL die Option Choose one or more of your existing Security Groups aus. Wählen Sie die zuvor erstellte Gruppe `WebServerSG` aus und klicken Sie dann auf Continue.
13. Überprüfen Sie auf der Seite REVIEW Ihre Einstellungen. Wenn Sie mit den gewählten Optionen zufrieden sind, klicken Sie auf Launch, um Ihre Instance zu starten.

Schritt 5: Weisen Sie der Instance eine Elastic IP-Adresse zu

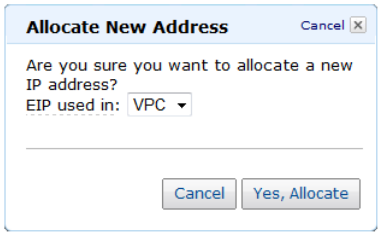
Standardmäßig ist eine Instance in einer VPC privat. Sie können eine Instance in einer VPC öffentlich machen, indem Sie ihr ein Internet-Gateway zuordnen und die Instance mit einer öffentlichen IP-Adresse versehen. In dieser Übung haben Sie mit dem VPC-Assistenten ein Internet-Gateway für Ihre VPC erstellt. Nun erstellen Sie eine Elastic IP-Adresse, bei der es sich um eine öffentliche IP-Adresse handelt, die zu Ihrem AWS-Konto gehört. Sie verknüpfen diese mit Ihrer Instance, damit der Zugriff aus dem Internet darauf möglich ist.

Weitere Informationen zu Elastic IP-Adressen finden Sie im Amazon Virtual Private Cloud User Guide unter *Elastic IP Addresses;*.

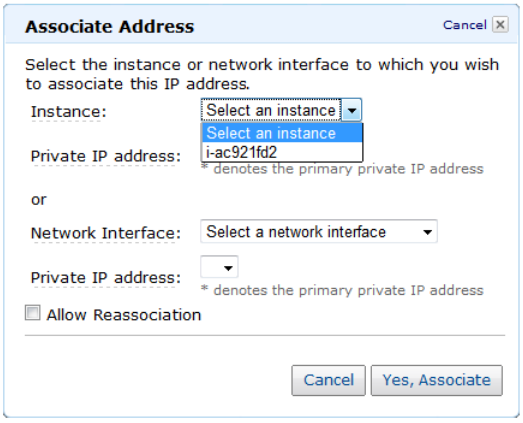
So wird eine Elastic IP-Adresse zugeordnet

1. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/.
2. Klicken Sie im Navigationsbereich auf Elastic IPs.
3. Klicken Sie auf die Schaltfläche Allocate New Address.

4. Wählen Sie in Liste EIP used in: die Option VPC aus und klicken Sie auf Yes, Allocate.



5. Wählen Sie die Elastic IP-Adresse in der Liste aus und klicken Sie auf die Schaltfläche Associate Address.
6. Wählen Sie im Dialogfeld Associate Address die Instance aus, der die Adresse zugeordnet werden soll, und klicken Sie auf Yes, Associate.



Auf Ihre Instance kann jetzt über das Internet zugegriffen werden. Sie können auch in Ihrem Heimnetzwerk auf die Instance über SSH oder Remotedesktop (RDP) zugreifen, indem Sie die Elastic IP-Adresse der Instance als Adresse angeben, mit der die Verbindung hergestellt werden soll. Anweisungen zum Herstellen einer Verbindung mit einer Linux-Instance finden Sie unter Connect to Your Linux Instance im *Amazon Elastic Compute Cloud User Guide*. Anweisungen zum Herstellen einer Verbindung mit einer Windows-Instance finden Sie unter Connect to Your Windows Instance im *Amazon Elastic Compute Cloud Microsoft Windows Guide*.

Damit ist die Übung abgeschlossen. Sie haben Ihre VPC eingerichtet, eine Instance wird in Ihrer VPC ausgeführt und Sie können sich über das Internet mit Ihrer Instance verbinden. Sie können Ihre Instance und VPC weiter nutzen oder die Instance beenden und die VPC löschen. Informationen zum Bereinigen und weitere VPC-Dokumentation finden Sie in Wie geht es weiter? (p. 16).

Wie geht es weiter?

Topics

Wenn Sie das vorherige Beispiel in diesem Handbuch durchgearbeitet haben, haben Sie eine VPC eingerichtet und darin eine Instance gestartet. Nach Wunsch können Sie Ihre VPC weiter nutzen. Andernfalls können Sie sie löschen. Unabhängig davon, ob Sie Ihre VPC löschen oder nicht, können Sie auch weitere VPCs erstellen.

Optionaler Schritt: Löschen der VPC

Ehe Sie eine VPC löschen können, müssen Sie alle Instances beenden, die in der VPC ausgeführt werden. Beim Löschen einer VPC werden auch die ihr zugeordneten Ressourcen gelöscht, z. B. Subnetze, Sicherheitsgruppen, Netzwerk-ACLs, DHCP-Optionsgruppen, Routing-Tabellen und Internet-Gateways.

So löschen Sie die VPC

1. Öffnen Sie die Amazon EC2-Konsole unter https://console.aws.amazon.com/ec2/.
2. Klicken Sie im Navigationsbereich auf Instances.
3. Klicken Sie mit der rechten Maustaste auf die in der VPC ausgeführte Instance und wählen Sie Terminate aus.
4. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf Yes, Terminate.
5. Öffnen Sie die Amazon VPC-Konsole unter https://console.aws.amazon.com/.
6. Klicken Sie im Navigationsbereich auf Your VPCs.
7. Wählen Sie die VPC aus und klicken Sie auf die Schaltfläche Delete.
8. Wenn Sie zur Bestätigung aufgefordert werden, klicken Sie auf Yes, Delete.

AWS-Konto und Anmeldeinformationen

Im vorliegenden Handbuch wurde erläutert, wie Sie sich für den Service registrieren und ein AWS-Konto erstellen. Darüber hinaus haben Sie eine kurze Übung ausgeführt. Nach Beendigung der Übung empfehlen wir Ihnen, zusammen mit einem Administrator oder Kollegen in Ihrer Organisation zu prüfen, ob bereits ein AWS-Konto und Anmeldeinformationen für künftige Interaktionen mit AWS zur Verfügung stehen.

Wenn Sie Eigentümer oder Administrator eines Kontos sind und mehr über AWS Identity and Access Management wissen möchten, navigieren Sie zu http://aws.amazon.com/iam und Using AWS Identity and Access Management.

Mehr Sicherheit für Ihre VPC

Wenn Sie zusätzlich zu Ihrer Sicherheitsgruppe eine weitere Sicherheitsebene einrichten möchten, können Sie Netzwerk-ACLs (Access Control Lists, Zugriffskontrolllisten) verwenden. Netzwerk-ACLs steuern den Datenverkehr auf Subnetzebene. In dieser Übung werden nur Sicherheitsgruppen verwendet. Diese steuern den Datenverkehr auf Instance-Ebene. Weitere Informationen zu Netzwerk-ACLs finden Sie unter Network ACLs im *Amazon Virtual Private Cloud User Guide*.

Weitere Szenarien für Amazon VPC

In dieser Anleitung wird ein einfaches Szenario für Amazon VPC vorgestellt. Der VPC-Assistent unterstützt weitere Szenarien. Eine detaillierte Erläuterung dieser Szenarien finden Sie unter Scenarios for Amazon VPC im *Amazon Virtual Private Cloud User Guide*.

Möglichkeiten des Zugriffs auf Amazon VPC

In dieser Anleitung wird die Verwendung von Amazon VPC über die AWS Management Console beschrieben. Sie können den Service weiter über die Konsole nutzen oder eine der anderen Möglichen ausprobieren.

Weitere Verwendung der Konsole

Im Amazon Virtual Private Cloud User Guide finden Sie weitere Informationen, wie Sie Amazon VPC über die Konsole verwenden.

Verwenden der Befehlszeilen-Schnittstelle

Amazon EC2 und Amazon VPC verfügen über eine Java-basierte Befehlszeilen-Schnittstelle. Diese Befehlszeilen-Tools bieten eine schnelle Möglichkeit, Amazon EC2 und Amazon VPC ohne Codierung für die API oder Verwendung einer Bibliothek auszuführen. Weitere Informationen zu den ersten Schritten mit den Befehlszeilen-Tools finden Sie unter Getting Started with the Command Line Tools im *Amazon Elastic Compute Cloud User Guide*. Eine umfassende Beschreibung der Befehle finden Sie in der Amazon Elastic Compute Cloud Command Line Reference.

Verwenden einer vorhandenen Bibliothek

Amazon EC2 und Amazon VPC nutzen dieselbe Programmierschnittstelle. Wenn Sie Amazon VPC lieber über eine API verwenden möchten, stehen Bibliotheken und Ressourcen für die folgenden Sprachen zur Verfügung:

- Java
- PHP
- Python
- Ruby
- Windows und .NET

Bibliotheken und Beispiel-Code finden Sie unter Amazon EC2 Sample Code & Libraries.

Direkte Codierung für die Web-Service-API

Wenn Sie Code direkt für die API für Amazon EC2 und Amazon VPC schreiben möchten, lesen Sie Making Requests im *Amazon Elastic Compute Cloud User Guide*. In diesem Handbuch wird beschrieben, wie Sie API-Anforderungen erstellen und authentifizieren sowie Amazon EC2 und Amazon VPC mithilfe von APIs nutzen können. Eine umfassende Beschreibung der API-Funktionen finden Sie in der Amazon Elastic Compute Cloud API Reference.

Weiterführende Dokumentation

In diesem Handbuch "Erste Schritte" für Amazon VPC werden die Grundlagen der Verwendung von Amazon VPC behandelt. Die folgende Tabelle enthält weitere Dokumentation zu Amazon VPC.

Beschreibung	Dokumentation
Informationen zur Verwendung von Amazon VPC	Amazon Virtual Private Cloud User Guide
Informationen zum Konfigurieren Ihres Kunden-Gateways (wenn Sie eine VPN-Verbindung mit Ihrer VPC verwenden möchten)	Amazon Virtual Private Cloud Network Administrator Guide
Praktische Einführung in Amazon EC2	Erste Schritte mit Amazon EC2
Informationen zur Verwendung von Amazon EC2	Amazon Elastic Compute Cloud User Guide
Beschreibungen der Befehle für Amazon EC2 und Amazon VPC	Amazon Elastic Compute Cloud Command Line Reference
Beschreibungen der API-Funktionen, Datentypen und Fehlermeldungen für Amazon EC2 und &VPC ;.	Amazon Elastic Compute Cloud API Reference
Schnellreferenz häufig verwendeter Befehle für Amazon VPC	Amazon Virtual Private Cloud Quick Reference Card

Weitere Hilferessourcen

Wir empfehlen Ihnen, sich an den AWS-Diskussionsforen zu beteiligen. Dies sind Community-Foren, in denen Benutzer über technische Fragen zu AWS-Services diskutieren. Das Amazon VPC-Forum finden Sie unter https://forums.aws.amazon.com/forum.jspa?forumID=58.

Außerdem können Sie AWS Premium Support abonnieren, einen schnellen und individuellen Supportkanal, um Hilfe zu erhalten. Weitere Informationen finden Sie unter http://aws.amazon.com/premiumsupport.

Ihr Feedback ist uns wichtig

Ihre Anregungen helfen uns, unsere Dokumentation so hilfreich und verständlich wie möglich zu gestalten. Teilen Sie uns Ihre ersten Erfahrungen mit Amazon VPC in unserer Umfrage für Einsteiger mit.

Vielen Dank.